Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Forschungsinstitut für öffentliche und private Sicherheit

Steven Kleemann & Clemens Arzt

Vertrauenswürdige IT für autonomes Fahren

IT-Sicherheit, Datensicherheit, Datenschutz und Produkthaftung in automatisierten Kraftfahrzeugen aus Sicht des deutschen, europäischen und internationalen Rechts

Berlin · Mai 2023

FORSCHUNGSINSTITUT FÜR ÖFFENTLICHE UND PRIVATE SICHERHEIT
(FÖPS BERLIN)

Steven Kleemann / Clemens Arzt

Vertrauenswürdige IT für autonomes Fahren

IT-Sicherheit, Datensicherheit, Datenschutz und Produkthaftung in automatisierten Kraftfahrzeugen aus Sicht des deutschen, europäischen und internationalen Rechts

Berlin ■ Mai 2023

FÖPS Digital #11 ■

Steven Kleemann & Clemens Arzt:
Vertrauenswürdige IT für autonomes Fahren. IT-Sicherheit, Datensicherheit, Datenschutz und Produkthaftung in automatisierten Kraftfahrzeugen aus Sicht des deutschen, europäischen und internationalen Rechts

FÖPS Digital Nr. 11
Herausgegeben vom Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin) der Hochschule für Wirtschaft und Recht Berlin
www.foeps-berlin.org

DOI: https://doi.org/10.4393/opushwr-4216
HWR Berlin
Berlin, Mai 2023

Inhaltsverzeichnis

Einführung

Automatisiertes und vernetztes Fahren spielt eine gewichtige Rolle in der Debatte um zukünftige Mobilität. In diesem Zusammenhang entstehen neben gesellschaftlichen Fragen über Akzeptanz und Sinnhaftigkeit auch zahlreiche neue rechtliche Fragestellungen und Herausforderungen. Dabei steht zunächst das deutsche Straßenverkehrsrecht im Zentrum. Aber auch internationale und europäische rechtliche Rahmenbedingungen müssen berücksichtigt werden. Mit Blick auf die zunehmende Verarbeitung von (personenbezogenen) Daten in automatisierten und vernetzten Kraftfahrzeugen werden dabei offenkundig auch Fragen des Datenschutzrechts aufgeworfen. Daneben haben Haftungs- und Produktsicherheitsfragen eine gewichtige Relevanz. Vergleichsweise neu im Kontext des Kraftfahrzeugverkehrs sind hingegen die Auswirkungen des IT-Sicherheitsrechts, das angesichts der Bedrohungen für die Cybersicherheit von Kraftfahrzeugen zunehmend in den Fokus rückt.

Die vorliegende Veröffentlichung basiert im Wesentlichen auf Ergebnissen des BMBF-Forschungsprojekts „Vertrauenswürdige IT für autonomes Fahren (VITAF)".[1] Nach eher einführenden Aspekten in Kapitel 1 werden wir in Kapitel 2 vertieft Fragen des aktuellen Rechtsrahmens für automatisierte und vernetzte Kraftfahrzeuge diskutieren. Im Vordergrund stehen dabei Fragen der IT-Sicherheit, der Datensicherheit und des Datenschutzes in vernetzten automatisierten und autonomen Kraftfahrzeugen. Einen Schwerpunkt bildet dabei eine Analyse aus Sicht der Anforderungen aus der Datenschutzgrundverordnung. Dies wird in Kapitel 3 ergänzt durch eine Analyse der datenschutzrechtlichen Anforderungen im Straßenverkehrsgesetz. Kapitel 4 widmet sich einerseits Fragen der IT- und Cybersicherheit und andererseits haftungsrechtlichen Aspekten. Dabei werden die aktuellen Entwicklungen im Straßenverkehrsgesetz, der zugehörigen Autonome-Fahrzeuge-Genehmigungs- und Betriebs-Verordnung (AFGBV) und internationale Entwicklungen auf UNECE-Ebene in den Fokus genommen. Abschließend werden unsere Forschungsergebnisse in Kapitel 5 kurz zusammengefasst und in Kapitel 6 der weitere Forschungsbedarf dargelegt.

1 Der Beitrag geht auf Ausarbeitungen im Teilvorhaben „Rechtsfragen der IT-Sicherheit bei autonomen Fahrzeugen" des vom BMBF zwischen Januar 2019 und März 2022 geförderten Forschungsprojekts VITAF (Förderkennzeichen 16KIS0839) zurück (https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/vitaf).

Ergänzend soll in diesem Zusammenhang auf eine weitere Veröffentlichung[2] aus dem Projekt VITAF verwiesen werden, in der vertieft konkrete technische Anforderungen beschrieben und technische Maßnahmen abgeleitet werden, die eine enge „Verflechtung" von Recht und Technik vornehmen und konkrete Lösungen für die IT-Sicherheit in automatisierten und vernetzten Kraftfahrzeugen vorschlagen. Hiermit können für die berechtigten Forderungen nach Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen konkrete Maßnahmen vorgestellt werden.

[2] Arzt/Kleemann/Plappert/Rieke/Zelle, Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung – Rechtliche und technische Anforderungen im Verbund, MMR 2022, 593-614, Download unter: https://www.hwr-berlin.de/fileadmin/portal/Dokumente/Prof-Seiten/Arzt/MMR_07-2022_-_Beilage_Fahrzeugautomatisierung_und_DV-Recht.pdf (letzter Abruf aller Quellen im Internet am 20.11.22).

1. Fahrzeugdaten, Privacy und Datenschutz

Einleitend werden wir uns in diesem Kapitel zunächst mit grundlegenden Fragestellungen aus Sicht der Technik und des Schutzes personenbezogener Daten befassen.

1.1 Abgrenzung des Konzepts „Privacy" und Datenschutz

Der Begriff „*privacy*" stammt eher aus dem angloamerikanischen Rechtsraum, wobei das ‚Recht auf *privacy*' von dem ‚*right to be let alone*' abgeleitet wird.[3] Im deutschen und europäischen Raum ist der Begriff Privatheit ein unbestimmter Rechtsbegriff.[4] Weder auf nationaler noch auf internationaler Ebene hat sich bisher eine einheitliche Definition durchsetzen können.[5] Das deutsche Verfassungsrecht und auch die Europäische Menschenrechtskonvention und die Grundrechtecharta beschränken sich in Art. 8 EMRK beziehungsweise Art. 7 und 8 EuGRCh lediglich darauf, Teilbereiche von Privatheit zu konkretisieren, wobei eine Definition von Privatheit als Rechtsgut ausbleibt. Gleiches gilt für das Grundgesetz, welches kein ausdrückliches Grundrecht auf Privatheit vorsieht. Der Schutz gründet daher auf einem Konstrukt unterschiedlicher Grundrechte. Dazu zählen der Schutz des privaten Raums gemäß Art. 13 GG, der Schutz der Vertraulichkeit individueller Kommunikation nach Art. 10 GG, der Schutz der Familie gemäß Art. 6 GG und das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 GG. Letzteres ist Ausgangspunkt für das Grundrecht auf informationelle Selbstbestimmung, welches als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG angesehen wird.[6] Das Grundrecht auf informationelle Selbstbestimmung ist sodann die Grundlage für das nationale Datenschutzrecht. Der europarechtliche Schutz leitet sich aus den beschriebenen Art. 7 und 8 EuGRCh beziehungsweise Art. 8 EMRK ab.

Privacy und Datenschutz sind demnach nicht gleichzusetzen.[7] Die Begriffe werden oftmals vermischt, sollten allerdings dahingehend richtig verwandt werden, dass ein Teilbereich *privacy* (oder Privatheit) aus Art. 7 GRCh abgeleitet wird und damit das Recht auf

[3] Siehe dazu schon: *Warren/Brandeis*, The Right to Privacy. Harvard Law Review, vol. 4, no. 5, 1890, 193-220, S. 193 f.

[4] *Schiedermair,* Der Schutz des Privaten als internationales Grundrecht, Jus Publicum 216, Mohr Siebeck, 2012, S. 59.

[5] Vgl. *Sandfuchs*, Privatheit wider Willen? – Verhinderung informationeller Preisgabe im Internet nach deutschem und US-amerikanischem Verfassungsrecht, Internet und Gesellschaft 2, Mohr Siebeck, 2015, S. 7; *Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, Jus Publicum 216, Mohr Siebeck, 2012, S. 18 ff./S. 59.

[6] Volkszählungsurteil, BVerfGE 65, 1.

[7] *Hansen*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 25 Rn. 23.

Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation normiert, also das Grundrecht auf Privatsphäre adressiert. Hingegen ist der Schutz personenbezogener Daten, also das Grundrecht auf Datenschutz, in Art. 8 GRCh normiert.[8] Darüber hinaus verzichtet beispielsweise die Datenschutzgrundverordnung (DSGVO) explizit auf Begriffe wie *privacy* oder *Privatsphäre*, und benutzt stattdessen (in der deutschen, wie der amtlichen englischen Version) den Begriff des Datenschutzes, wie beispielsweise in Art. 25 DSGVO (*Datenschutz* durch Technikgestaltung / *Data Protection* by Design). Privatheit oder *privacy* sind allerdings aufgrund der häufigen Verweise der DSGVO auf die Rechte und Freiheiten natürlicher Personen und das Recht auf Privatsphäre nach Art. 7 GRCh implizit von der DSGVO umfasst.[9]

Für ein umfassendes Verständnis von *privacy* abseits der DSGVO muss im Einzelfall erläutert werden, welches Konzept dem entsprechenden Fall zugrunde liegt. Die Anforderungen aus einem ISO-Standard oder IEC-Normen geben dafür Anknüpfungspunkte, sind allerdings nicht deckungsgleich mit den Bestimmungen der DSGVO. Weiterhin ist zu bedenken, dass ISO-, IEC- oder DIN-Standards private Normungsvorschriften von Organisationen ohne Gesetzgebungskompetenz sind und, wenngleich sie zur Begründung von Gerichtsurteilen herangezogen werden, keine rechtliche Bindungswirkung besitzen.[10] Technische Regeln und Normen gehören indes zu wichtigen Instrumenten des Technikrechts und können als Ausprägung eines außerrechtlichen Prozesses in Wirtschaft, Industrie und Handwerk auf die Rechtsordnung abzielen oder in dieser durch Verweisung auf solche Normen eine indirekte Bindungswirkung entfalten.[11] Allerdings wird auch vertreten, dass das spezielle Konzept *Privacy by Design* umfassender ist als der sich hauptsächlich auf die rechtliche Gestaltung von Technologie beziehende Ansatz von *Data Protection by Design*.[12] Demnach soll *Privacy by Design* neben den datenschutzrechtlichen Aspekten auch ethische Kriterien umfassen.[13]

Für den hier bearbeiteten Kontext des automatisierten und autonomen Fahrens mit speziellem Fokus auf die rechtliche Technikgestaltung, den Anknüpfungspunkten im Straßenverkehrsgesetz (StVG) sowie der rechtlichen Beurteilung aus europäischer Sicht, erscheint jedoch die Terminologie „*Data Protection (by Design and Default)*“ vorzugswürdig.

[8] *Hansen*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 25 Rn. 23.

[9] Ebd.

[10] *Kloepfer*, Instrumente des Technikrechts, in: *Honsel/Lerche* (Hrsg.), Handbuch des Technikrechts, S. 180 ff.

[11] A.a.O., S. 178 f.

[12] *Vásquez*, Privacy by Design und das autonome Fahrzeug, DuD 2022, 98 (S. 99).

[13] Ebd.

Die Gewährleistung von Datenschutz (und auch *privacy*) im Rahmen einer vertrauenswürdigen IT für automatisiertes Fahren erfordert eine Vermeidung oder zumindest weitestgehende Minimierung der Verarbeitung personenbezogener Daten durch Datenschutz durch Technikgestaltung (*Data Protection by design*) und Datenschutz durch datenschutzfreundliche Voreinstellungen (*Data Protection by default*), mit dem Ziel, nur die zur Nutzung und Bedienung unbedingt erforderlichen personenbezogenen Daten zu verarbeiten und insbesondere im Rahmen der Vernetzung nach außen preiszugeben.

1.2 Kategorisierung von Kraftfahrzeugdaten

Wurden Kraftfahrzeuge in der Vergangenheit nicht notwendigerweise als erstes mit Fragen der Datenverarbeitung in Verbindung gebracht, jedenfalls nicht mit personenbezogenen, hat sich in jüngster Vergangenheit ein regelrechter „Kampf um die Kfz-Daten“[14] automatisierter und vernetzter Kraftfahrzeuge entwickelt. Dabei geht es nicht ausschließlich um die Digitalisierung des Kraftfahrzeugs im Sinne elektronischer Services zur Komfortsteigerung, sondern auch um die Kommunikation der Fahrzeuge untereinander (*Vehicle-to-Vehicle*, V2V), mit der umgebenden Infrastruktur (*Vehicle-to-Infrastructure*, V2I), dem Backend (*Vehicle-to-Backend*, V2B) oder auch mit anderen Entitäten (*Vehicle-to-Everything*, V2X). Dabei ist das vorrangige Ziel nicht mehr die Steigerung des Komforts oder der Bequemlichkeit, sondern die grundlegende Steuerung der Kraftfahrzeuge und damit einhergehend die zunehmende Übernahme sicherheitsrelevanter Tätigkeiten wie Bremsen oder Längs- und Querführung vom Menschen durch Technik. Vormals als rein technisch und für die Fahrzeugführer*innen als Information angesehenen Daten wie solche zur Motorelektronik, zur Batterie, Geschwindigkeit, Software oder Ähnliches werden zunehmend in Echtzeit verarbeitet, um den sicheren Betrieb des Kraftfahrzeugs gewährleisten zu können. Nur durch den weiteren Einbau von immer mehr informationstechnischen Elementen können moderne Assistenz- und Automatisierungssysteme überhaupt realisiert werden. Die Erfassung, Verarbeitung, Weiterleitung und Speicherung unterschiedlichster Datenarten ermöglicht es erst, neue Anwendungen und Geschäftsmodelle zu entwickeln.[15]

Die zunehmende Datenverarbeitung im Kraftfahrzeug birgt neben den technischen Schwierigkeiten insbesondere auch datenschutzrechtliche Probleme. Um diesen zu begegnen, ist es erforderlich, die Kraftfahrzeugdaten einzuordnen und speziell nach perso-

[14] *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507 (S. 507).

[15] *Krauß/Waidner*, IT-Sicherheit und Datenschutz im vernetzten Fahrzeug, DuD 6/2015, 383 ff. (384).

nenbezogenen und nicht-personenbezogenen zu kategorisieren sowie die datenschutzrechtlich Betroffenen und Verantwortlichen zu ermitteln. Darüber hinaus muss die Kommunikation von Fahrzeugen, das Auslesen und die Speicherung von Kraftfahrzeugdaten sowie die IT Sicherheit während dieser Vorgänge in datenschutzkonformer Weise geregelt sein. Es muss demnach bei der Digitalisierung von Kraftfahrzeugen und speziell bei deren Kommunikation mit anderen Fahrzeugen und Entitäten im Rahmen der Vernetzung darum gehen, die Technik wie auch den rechtlichen Rahmen dahingehend auszugestalten, dass die positiven Effekte der Fahrzeugautomatisierung[16] eintreten und gleichzeitig Gefahren die sich durch den Betrieb automatisierter Kraftfahrzeuge wie auch aufgrund der Verarbeitung von personenbezogenen Daten ergeben, in bestmöglicher Art und Weise minimiert werden.

Damit Kraftfahrzeuge in automatisierten Modi fahren können, benötigen diese eine gewisse Grundausstattung an Kraftfahrzeugzustands-, Umfeld- und Innenraumerfassungssensoren. Um dabei Fahrzeugdaten generell zu kategorisieren, gibt es unterschiedliche Ansätze. Der Verband der Automobilindustrie (VDA) hat dazu beispielsweise eine Übersicht erstellt, bei welcher sowohl die Daten-Kategorien (siehe nachfolgende Abbildung), wie auch deren Datenschutzrelevanz gruppiert werden.[17]

Abbildung 1: Landkarte der Daten-Kategorien beim vernetzten Fahrzeug (aus: Verband der Automobilindustrie, Datenschutz-Prinzipien für vernetzte Fahrzeuge. Berlin 2014).

[16] Vgl. *Schulz*, Sicherheit im Straßenverkehr und autonomes Fahren, NZV 2017, 548.

[17] Abrufbar unter: https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html.

Bei der Kategorisierung des VDA sowie auch in den weiteren Ausführungen der Übersicht wird den im Fahrzeug selbst erzeugten technischen Daten eine geringe Datenschutzrelevanz zugeschrieben und angegeben, dass solche Daten soweit wie möglich „rein technische" Daten bleiben sollen.[18] Da solche Daten, die hauptsächlich die Fahrzeugfunktion und damit die Betriebssicherheit (*safety*) gewährleisten sollen, im hier interessierenden Kontext einen höheren Relevanzwert haben als kundeneingebrachte Daten bezüglich Komfort- oder Infotainment Funktionen (trotz derer hoher datenschutzrechtlicher Relevanz), werden diese (technischen) Daten im weiteren Projektverlauf vorrangig im Fokus stehen und auf ihre datenschutzrechtliche Relevanz hin untersucht.

Die Kategorisierung des VDA eignet sich zwar für einen ersten Überblick, jedoch können damit nicht sämtliche im Kraftfahrzeug anfallende Daten datenschutzrechtlich in angemessener Weise eingeordnet werden. Es gibt beispielsweise in der Kategorie der durch Gesetz zweckgebundenen Daten die VO (EG) Nr. 715/2017,[19] die den Zugang und den Zweck der Erhebung von Diagnosedaten regelt,[20] jedoch keine Rechtsgrundlage für die Erhebung und Verwendung dieser Daten darstellt.[21] In diesem Fall sind die datenschutzrechtlichen Vorschriften einschlägig, welche für personenbezogene Daten gelten. Weiterhin lassen sich nicht alle Kraftfahrzeugdaten starr in eine dieser Kategorien einordnen. Möglicherweise entsteht auch erst durch Kumulation verschiedener, vom VDA als datenschutzrechtlich nicht relevant eingestufter Daten, die datenschutzrechtliche Bedeutung.[22]

Um die datenschutzrechtliche Bedeutung zu prüfen, erscheint es ratsam, die Daten weitergehend zu kategorisieren. Vorab ist festzustellen, dass der vorherrschend verwandte Terminus „Fahrzeugdaten"[23] dahingehend ungenau ist, als in § 33 Abs. 1 Nr. 1 StVG Fahrzeugdaten als „*Daten über Beschaffenheit, Ausrüstung, Identifizierungsmerkmale, Prüfung, Kennzeichnung und Papiere des Fahrzeugs sowie über tatsächliche und rechtliche Verhältnisse in Bezug auf das Fahrzeug, insbesondere auch über die Haftpflichtversicherung, die Kraftfahrzeugbesteuerung des Fahrzeugs und die Verwertung oder Nichtentsorgung des Fahrzeugs als Abfall im Inland*" legaldefiniert sind. Daher sollte im hier interessierenden Bereich, dem sicheren funktionieren automatisierter Kraftfahrzeuge, eher von

[18] S. Abbildung 1.

[19] Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typgenehmigung von Kraftfahrzeugen hinsichtlich der Emissionen von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und Euro 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge.

[20] S. Artikel 6 der Verordnung (EG) Nr. 715/2007.

[21] *Raith*, Das vernetzte Automobil – Im Konflikt zwischen Datenschutz und Beweisführung, DuD-Fachbeiträge, Springer Vieweg, 2019, S. 21.

[22] Ebd.

[23] *Karikari*, Big Data in der Automobilindustrie – Die Erhebung von Fahrzeugfunktionsdaten als Rechtsproblem, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2018, S. 28.

Kraftfahrzeugfunktionsdaten gesprochen werden, soweit diese Daten keinen Personenbezug beinhalten und auch nicht erlauben, diesen herzustellen.

Zur weiteren Kategorisierung von Daten, die durch die Sensortechnik und Vernetzung der Kraftfahrzeuge generiert und verarbeitet werden, wird vorgeschlagen, diese in *Identifikationsdaten* und *Merkmalsdaten* einzuteilen.[24] Bei Identifikationsdaten handelt es sich um solche, die den/die Fahrer*in, Eigentümer*in oder Halter*in identifizieren.[25] Dazu zählen in erster Linie das Kfz-Kennzeichen und die 17-stellige Fahrzeug-Identifizierungsnummer (FIN) oder auch *Vehicle Identification Number* (VIN). Diese muss gemäß § 59 Abs. 1 Nr. 4 StVZO seitens des Herstellers am Kraftfahrzeug angebracht werden und zählt zu den in § 33 Abs. 1 Nr. 1 StVG genannten Fahrzeugdaten, welche im Fahrzeugregister gespeichert werden müssen. Damit ist über die FIN nicht nur das Kraftfahrzeug identifizierbar, sondern auch dessen Halter*in. Fallen bei der Nutzung des Kraftfahrzeugs Daten an, welche mit diesen Identifikationsdaten (Kfz-Kennzeichen oder FIN) in irgendeiner Art und Weise verknüpft werden können, handelt es sich um personenbezogene Daten und damit unterliegen diese dem geltenden Datenschutzrecht.[26] Laut Herstellerangaben ist eine Erhebung von Daten im Kraftfahrzeug ohne Verknüpfung mit der FIN nach derzeitigem technischen Stand nicht möglich und eine mögliche Anonymisierung damit erst nach Übermittlung aus dem Kraftfahrzeug heraus realisierbar.[27]

Merkmalsdaten können in Zustands- und Verhaltensdaten unterteilt werden. Dabei sind Zustandsdaten technische Daten zur (technischen) „Konstitution", in der sich das Kraftfahrzeug befindet. Verhaltensdaten beziehen sich auf das Verhalten der Fahrer*innen und deren Art und Weise der Kraftfahrzeugsteuerung.[28] Bei Zustandsdaten handelt es sich um Angaben, die grundsätzlich nur das Kraftfahrzeug, also eine Sache, betreffen. Es sind technische Kraftfahrzeugdaten, welche indes unter Umständen auch Rückschlüsse auf das Fahrverhalten zulassen. Dazu gehören Angaben zu Motorsteuergeräten, und -elektronik,

[24] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 158; *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507 (S. 509 f.).

[25] *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507 (S. 509).

[26] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge, S. 1 (Nr. 1).

[27] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 159.

[28] *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507 (S. 510).

zur Batterie, aber auch zu Software sowie zum Fehlerspeicher oder der Multimedia-Einheit.[29] Verhaltensdaten hingegen können beispielsweise Fahr- und Rastzeiten oder das Lenk-, Brems- und Beschleunigungsverhalten sein.[30] Diese haben offenkundig Personenbezug, weil hierüber auch das Verhalten von Fahrzeuglenker*innen erfasst werden können, wobei mit zunehmender Automatisierung der Anteil personenbezogener Daten hier zurückgehen dürfte.

Demnach wird es im Rahmen von Kraftfahrzeugdaten kaum Daten geben, die rein technisch sind und keinen Personenbezug aufweisen. Diese Feststellung ist dahingehend unproblematisch, da dies nicht bedeutet, dass eine Verarbeitung dieser Daten per se unzulässig wäre, sondern lediglich, dass das Datenschutzrecht Anwendung findet.

Der immense Zuwachs an Datenaustausch, -verarbeitung und -erhebung sowie Big-Data-Analytics macht es möglich und immer wahrscheinlicher, dass einem Datum irgendwann auch eine Person zugeordnet werden kann. Dies gilt natürlich auch im Rahmen der Fahrzeugautomatisierung. Die DSGVO begegnet diesen Problemen dadurch, dass sie einen sehr weiten Schutzbereich aufweist, der bereits greift, wenn eine etwaige Identifizierung erst in der Zukunft möglich ist. Ein derart weites Verständnis ist mit Art. 4 Abs. 1 Nr. 1 DSGVO insoweit vereinbar, als dieser keine Voraussetzungen für die Identifizierbarkeit einer betroffenen Person normiert. Das bedeutet nicht, dass das Kriterium „Personenbezug“ obsolet ist. Reine Sachdaten sind weiterhin vom Anwendungsbereich ausgeschlossen. Gemäß Art. 6 DSGVO gilt im Datenschutzrecht das Verbot mit Erlaubnisvorbehalt. Aus diesem Grund ist es nötig, für die weitere Ausarbeitung die möglichen Gründe für eine Datenverarbeitung (z.B. Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO, zur Erfüllung einer rechtlichen Verpflichtung nach lit. c oder aufgrund eines berechtigten Interesses lit. f) darzulegen.

[29] *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507 (S. 510).

[30] Ebd.

1.3 Datenhoheit

In der Diskussion bezüglich den Rechten an Daten stehen sich viele Ansichten gegenüber.[31] Es ist die Rede von Datenhoheit, Dateneigentum oder Datenbesitz. Wurde die Diskussion anfangs noch intensiv um ein „Dateneigentum" geführt,[32] fand in letzter Zeit ein Paradigmenwechsel hin zu einem Konzept des „Datenbesitzes" statt.[33] Grund ist, dass bisher keine Rechtsposition an digitalen Daten beziehungsweise maschinenlesbar codierten Informationen, welche mit dem Sacheigentum oder geistigem Eigentum vergleichbar wären, in irgend einer Art und Weise begründet werden konnte. Ausgangspunkt der Diskussion um ein „Dateneigentum" gründete maßgeblich auf der Frage, wie mit den Daten vernetzter Kraftfahrzeuge umzugehen sei.[34]

Hinsichtlich automatisierter und vernetzter Fahrzeuge gab es immer wieder Kritik in Richtung der Kraftfahrzeughersteller, da sie die Hoheit über die Gestaltung von Schnittstellen innehaben und dadurch letztlich auch ohne zugewiesenem Recht jedenfalls die faktische Hoheit über Kraftfahrzeugdaten besitzen.[35] Das unterstreicht die These, dass es weniger um exklusives Eigentum, den Besitz oder ein sonstiges „Recht an Daten" geht, sondern vielmehr um den Zugang zu diesen Daten und die weitere Nutzung derselben. Durch eine Regelung bezüglich des Datenzugangs könnten bestehende Probleme im Zusammenhang mit der monopolisierten Hoheit an Daten adressiert werden.[36]

Jedenfalls wenn es sich um personenbezogene Daten handelt, sollte die von der Datenverarbeitung betroffene Person selbst entscheiden können, wer diese Daten verarbeiten darf. Insbesondere wenn sich die Datenverarbeitung lediglich auf eine Einwilligung (Art. 6 Abs. 1 lit. a DSGVO) stützt. Das bedeutet nicht, dass beispielsweise eine Person,

[31] Vgl. zur Diskussion u.a.: *Hornung/Spiecker gen. Döhmann*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Einleitung Rn. 310; *Martini/Kolain/Neumann/Rehorst/Wagner*, Datenhoheit MMR-Beil. 2021, 3; *Schweitzer*, Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, 569; *Hoeren*, Datenbesitz statt Dateneigentum MMR 2019, 5; *Stender-Vorwachs/Steege*, Wem gehören unsere Daten?, NJOZ 2018, 1361; 25; *Kühling/Sackmann*, Irrweg „Dateneigentum", ZD 2020, 24; *Michl*, „Datenbesitz" – ein grundrechtliches Schutzgut?, NJW 2019, 2729; *Wischmeyer/Herzog*, Daten für alle? – Grundrechtliche Rahmenbedingungen für Datenzugangsrechte, NJW 2020, 288; im speziellen Kontext der Fahrzeugautomatisierung beispielhaft: *Bundesministerium für Verkehr und digitale Infrastruktur* (Hrsg.), „Eigentumsordnung" für Mobilitätsdaten?, August 2017; *Hoeren*, Ein Treuhandmodell für Autodaten? – § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion, NZV 2018, 153; *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507; *Wendt*, Autonomes Fahren und Datenschutz – eine Bestandsaufnahme, ZD-Aktuell 2018, 06034.

[32] *Michl*, „Datenbesitz" – ein grundrechtliches Schutzgut?, NJW 2019, 2729.

[33] Ebd.

[34] *Kühling/Sackmann*, Irrweg „Dateneigentum", ZD 2020, 24, S. 25.

[35] A.a.O., S. 26.

[36] Ebd.

welche ein Kraftfahrzeug mit automatisierter Fahrzeugsteuerung benutzt selbst entscheiden kann, ob dem Hersteller des Kraftfahrzeugs der Zugriff auf die zur Steuerung notwendigen Daten erteilt werden soll oder nicht, sondern, dass die von der Datenverarbeitung betroffene Person technisch und organisatorisch in die Lage versetzt wird, über die Verarbeitung zu entscheiden. Hier hat der Gesetzgeber erstmals mit dem neuen § 1g Abs. 3 StVG Vorgaben geschaffen, die dieses Problem adressieren.[37] Demzufolge sollen die Kraftfahrzeughersteller, den Halter*innen die Datenhoheit über die beim Betrieb des Kraftfahrzeugs mit sogenannter autonomer Fahrfunktion anfallenden Daten ermöglichen.[38] Darüber hinaus wäre allerdings die Ausarbeitung eines verkehrsmittelübergreifenden Mobilitätsdatengesetz[39] eine geeignetere Maßnahme um dieser Problematik adäquat zu begegnen, anstelle der zersplitterten Regelungen wie sie jetzt in § 63a und § 1g im StVG zu finden sind.

[37] BR-Drs. 155/21, S. 38.

[38] S. dazu Abschnitt 3.3.

[39] Vgl. Ausführungen in: *vzbv – Verbraucherzentrale Bundesverband*, Positionspapier Fahrerlos alle Mitnehmen – Automatisierte und vernetzte Mobilität aus Verbrauchersicht, Positionspapier vom 6.3.2021, S. 8 ff.

2. IT-Sicherheit, Datensicherheit und Datenschutz im automatisierten und autonomen Fahrzeug aus rechtlicher Sicht

Im Zusammenhang mit dem automatisierten und vernetzten Fahren stellt sich die Frage, welches Recht hinsichtlich der IT-Sicherheit, der Datensicherheit und des Datenschutzes überhaupt Anwendung findet. Entsprechende Regelungen finden sich sowohl im nationalen Recht wie dem Bundesdatenschutzgesetz (BDSG), dem Telekommunikationsgesetz (TKG) und auch im Telemediengesetz (TMG). Hier ist jedoch anzumerken, dass der Gesetzgeber zum 1. Dezember 2021 das TKG und TMG novelliert hat und das neue Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) eingeführt hat.[40]

Auf europäischer Ebene ist vornehmlich die Datenschutzgrundverordnung (DSGVO) einschlägig, die unmittelbar geltendes Recht in allen EU-Mitgliedsstaaten darstellt. Eine eindeutige Abgrenzung oder abstrakte Beantwortung der Frage, welches Recht Anwendung findet, ist im Bereich der Fahrzeugautomatisierung nicht ohne weiteres möglich.[41] Ist ein Kraftfahrzeug mit einem freien Internetzugang ausgestattet, kann dies als Signalübertragungsleistung gesehen werden und damit liegt ein Telekommunikationsdienst vor, welcher den Vorgaben der §§ 91 ff. TKG-a.F. zu Bestands-, Standort-, und Verkehrsdaten unterliegt.[42] Handelt es sich bei dem Internetzugang allerdings um einen solchen, bei dem seitens der Hersteller weitere Leistungen angeboten werden, kann von einem Telemediendienst ausgegangen werden und die Regelungen der §§ 11 ff. TMG-a.F. kommen in Betracht.[43] Letzten Endes bedarf es immer einer Einzelfallbetrachtung jedes einzelnen Dienstes in der konkreten Situation, um festzustellen, welches Recht Anwendung findet. Über alle dem schwebt sogleich die Frage, inwiefern die nationalen Regelungen seit Inkrafttreten der DSGVO überhaupt noch Anwendung finden oder von dieser überlagert beziehungsweise verdrängt werden.

2.1 Nationales Recht

Die einschlägigen nationalen Regelwerke wurden bereits vorab kurz beschrieben. Welche konkreten datenschutzrechtlichen Vorgaben im BDSG, dem TKG und TMG und dem

[40] Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz, TTDSG), BGBl. 2021 I S. 1982, in Kraft seit 1. Dezember 2021.

[41] *Eul*, Teil 10.2 Connected Cars, in: *Leupold/Wiebe/Glossner* (Hrsg.) Münchener Anwaltshandbuch IT-Recht, 4. Auflage 2021, Rn. 28.

[42] Ebd.

[43] Ebd.

neuen TTDSG für den hier interessierenden Kontext relevant sind, soll im Folgenden erörtert werden. Vorab ist es allerdings ratsam, die Besonderheit des Datenschutzrechts im europäischen Mehrebenensystem kurz zu erläutern, um zu verdeutlichen, weshalb eine Auseinandersetzung mit der unterschiedlichen Anwendbarkeit des mitgliedsstaatlichen Datenschutzrechts und der DSGVO erforderlich ist. Hier ist insbesondere auf die sogenannten Öffnungsklauseln der DSGVO hinzuweisen, welche die Regelungshoheit bezüglich einer zu regelnden Rechtsmaterie an die jeweiligen Nationalstaaten übertragen.[44] Hinzu kommt, dass das Datenschutzrecht im Gegensatz zur sonstigen kontinentaleuropäischen Sichtweise nicht trennscharf zwischen Privatrecht und öffentlichem Recht unterscheidet.[45] Deutlich wird dies beispielsweise durch die Unterscheidung zwischen Anspruchsebene und Durchsetzungsebene eines datenschutzrechtlichen Anspruchs. Gegner eines solchen Anspruchs sind stets „Verantwortliche" und „Auftragsverarbeiter" (Art. 82 DSGVO), die allerdings sowohl natürliche Personen sein können, wie auch juristische Personen des öffentlichen oder privaten Rechts.[46] Für den hier interessierenden Kontext sind allerdings insbesondere die Öffnungsklauseln relevant, um festzustellen, inwiefern die nationalen Regelungen anstelle der DSGVO Anwendung finden.

2.1.1 Datenschutz im Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) war bis Inkrafttreten der DSGVO die primäre Rechtsquelle für die Datenverarbeitung in Deutschland. Im BDSG fanden sich vor Einführung der DSGVO die grundlegenden Regelungen bezüglich der Verarbeitung von personenbezogenen Daten. Hierbei ist zu beachten, dass trotz Namensgleichheit des Bundesdatenschutzgesetzes mit dem vorherigen Gesetz (BDSG a.F.), die Vorgängerregelung in nahezu allen Regelungen von der neuen abweicht, weshalb eine eindeutige Zuordnung stets notwendig ist.[47] Obwohl die DSGVO die Datenverarbeitung weitreichend regelt und Vorrang vor den nationalen Regelungen hat, gilt daneben weiterhin das BDSG mit Regelungen zur Verarbeitung personenbezogener Daten. Dies gilt indes nur, soweit entweder Öffnungsklauseln vorgesehen sind oder für Gebiete, die vom Anwendungsbereich der DSGVO ausgenommen sind. Beispiele dafür sind gemäß Art. 2 Abs. 2 lit. d DSGVO Datenverarbeitung zum Zweck der Strafverfolgung und Strafvollstreckung oder nach lit. b die gemeinsame Außen- und Sicherheitspolitik der EU betreffend.

[44] *Oster*, Internationale Zuständigkeit und anwendbares Recht im Datenschutz, ZEuP 2021, 275, S. 278.

[45] Ebd.

[46] Ebd.

[47] *Bretthauer/Müllmann/Spiecker gen. Döhmann*, Datenschutzrechtliche Aspekte neuer Mobilitätskonzepte im Öffentlichen Nahverkehr, 2021, S. 24.

Obwohl es also im hier untersuchten Kontext punktuelle Anknüpfungspunkte im BDSG geben kann, wird in der weiteren Betrachtung vorrangig die DSGVO als weit ausgreifende rechtliche Grundlage untersucht.

2.1.2 Telekommunikationsgesetz, Telemediengesetz & Telekommunikation-Telemedien-Datenschutz-Gesetz

Alle nach dem 31.03.2018 zugelassenen Kraftfahrzeuge und leichte Nutzfahrzeuge müssen nach der eCall-VO[48] das sogenannte eCall-System verbaut haben, bei welchem in einer Unfallsituation automatisch ein Notruf an die zuständige Notrufzentrale (112 Nummer) abgesetzt und einen Mindestdatensatz (Unfallzeitpunkt, Fahrtrichtung, Koordinaten, FIN und Serviceprovider ID) übermittelt wird.[49] Damit ist im Kraftfahrzeugsektor flächendeckend Mobilfunktechnik zu verwenden. Neben dieser verpflichtenden Vorgabe wird die Mobilfunktechnik auch seitens der Hersteller für software- und mobilfunkbasierte Dienstleistungen eingesetzt.[50] Hier stellt sich die Frage, ob aufgrund dieser Dienste wie etwa Live-Navigation, die Kraftfahrzeughersteller als Telekommunikationsanbieter i.S.d. § 3 Nr. 6 TKG-a.F.[51] respektive dem neuen TTDSG (hierzu sogleich) einzustufen sind und ob bezüglich etwaiger Internetverbindungen die oben unter 2. erwähnten §§ 91 ff. TKG-a.F. aufgrund der Signalübertragungsleistung greifen. Die Diskussion dazu ist insofern relevant, als das Kraftfahrzeughersteller, wenn Sie nach § 3 Nr. 24 TKG-a.F. als Telekommunikationsanbieter eingestuft werden, ein „strengeres regulatorisches Regime" gilt, als wenn diese lediglich nach Nr. 25 TKG-a.F. als telekommunikationsgestützter Dienst gelten oder nach § 1 Abs. 1 TMG-a.F., als Telemediendienst angesehen werden. Allerdings ist wie oben beschrieben das TKG und TMG novelliert sowie das TTDSG eingeführt worden.

Mit dem TTDSG wurden jedoch lediglich die europäischen Vorgaben aus der ePrivacy-Richtlinie[52] (ePrivacy-RL) in nationales Recht umgesetzt. Wenn es zur Einführung der ePrivacy-Verordnung (ePrivacy-VO) kommt, wird diese unmittelbar in den europäischen Mitgliedsstaaten gelten und das TTDSG eventuell an einigen Stellen verdrängen. Das TTDSG hat einen weiten Anwendungsbereich und könnte auch Auswirkungen auf

[48] VO (EU) 2015/758 des Europäischen Parlaments und des Rates v. 29.4.2015.

[49] *Wendt*, Autonomes Fahren und Datenschutz – eine Bestandsaufnahme, ZD Aktuell 2018, 06034.

[50] *Brockmeyer*, Teil 15.5 Big Data im vernetzten Verkehr, in: *Hoeren/Sieber/Holznagel* (Hrsg.) Handbuch Multimedia-Recht, Werkstand: 57. EL September 2021, Rn. 3.

[51] Außer Kraft getreten am 01.12.2021 aufgrund Gesetzes vom 23.06.2021 (BGBl. I S. 1858).

[52] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

automatisierte und vernetzte Kraftfahrzeuge haben.[53] Relevant ist in diesem Zusammenhang § 25 TTDSG. Dieser ist praktisch wortgleich mit Art. 5 Abs. 3 ePrivacy-RL, der die Integrität von sogenannten Endeinrichtungen gegen unbefugtes Auslesen und Speichern von Informationen schützt.[54] Eine Endeinrichtung ist in § 2 Abs. 2 Nr. TTDSG als „jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten […]" definiert. Unter diese Definition können auch Kraftfahrzeuge fallen.[55] Vernetzte Kraftfahrzeuge verfügen beispielsweise über eine SIM-Karte, die wiederum mit dem Internet verbunden ist und über das Kraftfahrzeug-Backend, welches als Einrichtung im Sinne des § 2 Abs. 2 Nr. 6 TTDSG anzusehen ist, wird eine Schnittstelle zum Telekommunikationsnetz geschaffen.

Da § 25 TTDSG den Art. 5 Abs. 3 ePrivacy-RL umsetzt, geht dieser gemäß Art. 95 DSGVO den Regelungen der DSGVO vor. Inwiefern weitere Regelungen des TTDSG die der DSGVO verdrängen, wird hier nicht weiter untersucht. Eine vertiefte Analyse dieser Fragen konnte aufgrund der kurz vor Projektende erfolgten Rechtsänderungen nicht mehr geleistet werden. Folglich findet auch keine weitere Auseinandersetzung mit den Regelungen des alten Telekommunikations- und Telemediengesetz statt. Festzuhalten ist allerdings noch, dass es Ziel der E-Privacy-VO ist, die Vorgaben bezüglich elektronischer Kommunikation an die DSGVO anzunähern, ohne dabei über die Maßgaben der DSGVO hinauszugehen.[56] Aus diesem Grund war es angebracht, in der weiteren datenschutzrechtlichen Untersuchung auf die DSGVO zu fokussieren.

2.2 Europäisches Recht

Die Datenschutzgrundverordnung als europäische Verordnung gilt direkt in den Mitgliedsstaaten der EU, und es bedarf hierzu keines Umsetzungsaktes in das nationale Recht. Im Gegenteil, solche Akte wären sogar unzulässig, wenn die unmittelbare Geltung

[53] *Wasilewski*, Datenschutz bei Connected Cars – Das passt wie die Faust aufs Auge!?, CTRL 1/22, S. 49; *Grages*, Rechtfertigung und Zweckänderung im Spannungsverhältnis von DSGVO und TTDSG, CR 2021, 834 (S. 836); *Hanloser*, Schutz der Geräteintegrität durch § 25 TTDSG, ZD 2021, 399 (S. 400).

[54] *Hanloser*, Schutz der Geräteintegrität durch § 25 TTDSG, ZD 2021, 399 (S. 399).

[55] *Grages*, Rechtfertigung und Zweckänderung im Spannungsverhältnis von DSGVO und TTDSG, CR 2021, 834 (S. 836); *Hanloser*, Schutz der Geräteintegrität durch § 25 TTDSG, ZD 2021, 399 (S.400); *Piltz*, Das neue TTDSG aus Sicht der Telemedien, CR 2021, 555 (S. 559); *Wasilewski*, Datenschutz bei Connected Cars – Das passt wie die Faust aufs Auge!?, CTRL 1/22, S. 49.

[56] *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*, E-Privacy-Verordnung, https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Telefon-Internet/Positionen/ePrivacy_Verordnung.html.

der Verordnung dadurch fraglich erscheinen könnte.[57] Die DSGVO geht somit, wie bereits unter 2.1 und 2.1.1. beschrieben, den nationalen Regelungen vor. In der Literatur wie auch in der Praxis wird das Themenfeld Fahrzeugautomatisierung im Grunde ausschließlich anhand der DSGVO diskutiert, weshalb eine dezidierte Auseinandersetzung mit dieser Verordnung und ihrer auf den europäischen Grundrechtsschutz abstellenden Schutzrichtung notwendig ist.

Der zentrale Begriff des Datenschutzrechts ist das Tatbestandsmerkmal des personenbezogenen Datums. Das Vorhandensein des Personenbezugs stellt die Verknüpfung zwischen technischer Datenverarbeitung und der rechtlichen Betroffenheit einer natürlichen Person her und löst die Anwendung des Datenschutzrechts aus.[58] Weiterhin wird mit Vorhandensein personenbezogener Daten, der Anwendungsbereich des primär- und verfassungsrechtlichen Schutzes dieser Daten und das Recht auf informationelle Selbstbestimmung im Sinne von Art. 7 und 8 GRCh sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG eröffnet.[59]

Für den Bereich des automatisierten und vernetzten Fahrens hat sich (wie den Ausführungen in Abschnitt 2.1.1 zu entnehmen ist) ergeben, dass hier insbesondere die DSGVO als anwendbares Recht einschlägig ist. Die speziellen Normen des TKG, TMG oder BDSG sind hier in den meisten Fällen nicht in gleichem Maße von Interesse, beziehungsweise verweisen ihrerseits im Wesentlichen lediglich auf die DSGVO oder wurden jüngst im Rahmen der Novelle des Telekommunikationsgesetzes (siehe auch das TTDSG) überarbeitet und konnten daher hier nicht mehr berücksichtigt werden. Die für den hier interessierenden Kontext einschlägige DSGVO wird daher im Folgenden im Detail betrachtet.

2.3 Personenbezug Art. 4 Nr. 1 DSGVO

Die zentrale Frage, ob die DSGVO anwendbar ist oder nicht, richtet sich nach dem Vorhandensein eines Personenbezuges. Dieser ist in Art. 4 Nr. 1 DSGVO definiert und umfasst

> *„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*

[57] *Bretthauer/Müllmann/Spiecker gen. Döhmann*, Datenschutzrechtliche Aspekte neuer Mobilitätskonzepte im Öffentlichen Nahverkehr, 2021, S. 24.

[58] *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 1.

[59] Ebd.

> *Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind".*

Diese Definition in Art. 4 Nr. 1 DSGVO ersetzt sowohl die ehemalige Definition des § 3 Abs. 1 BDSG a.F., als auch (soweit die DSGVO anwendbar ist) alle anderen vorausgehenden nationalen Definitionen.[60] Mit Verabschiedung des BDSG n.F. hat der Gesetzgeber darüber hinaus auf eine eigenständige Definition des Begriffs im neuen BDSG verzichtet, weshalb auf nationaler Ebene die Vorgaben der DSGVO, soweit diese anwendbar ist, unmittelbar gelten.[61]

Die Auslegung des Begriffs muss autonom und vor dem Hintergrund der europäischen Methodenlehre und des europäischen Rechts erfolgen, wobei die bestehende nationale Rechtsprechung dahingehend weiter Bedeutung hat, dass nationale Gerichte wie auch internationale Rechtsanwender europäisches Recht eigenständig auslegen.[62] Die „letztinstanzliche Auslegungskontrolle" liegt dabei beim Europäischen Gerichtshof (EuGH).[63] Der Begriff des personenbezogenen Datums muss, um einen tatsächlich effektiven Schutz bieten zu können, sehr weit ausgelegt werden.[64] Dabei ist vornehmlich auf den Sinn und Zweck der DSGVO einzugehen. Dieser stellt den Schutz der personenbezogenen Daten und der Grundrechte und Grundfreiheiten natürlicher Personen dar (vgl. Art. 1 Abs. 2 DSGVO). Das bedeutet, dass nicht der technische Schutz der personenbezogenen Daten vorrangiges Ziel der Verordnung ist, sondern die Achtung und Wahrung der Grundrechte und Grundfreiheiten der von der Verarbeitung betroffenen Person.[65] Zur Auslegung von Art. 4 Nr. 1 DSGVO können darüber hinaus maßgeblich die Erwägungsgründe 26 bis 30 DSGVO herangezogen werden.

Das Konzept der personenbezogenen Daten im Datenschutzrecht ist überdies binär.[66] Das bedeutet, dass die Verarbeitung der in Frage stehenden Daten entweder vollständig oder

[60] *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 7.

[61] A.a.O., Rn. 9.

[62] A.a.O., Rn. 2.

[63] *Pechstein/Drechsler*, in *Riesenhuber* (Hrsg.), Europäische Methodenlehre, 4. Auflage 2021, § 7 Rn. 14.

[64] EuGH C-465/00, C-138/01, C-139/01, EUR 2004, 276 Rn. 43.

[65] *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 3.

[66] A.a.O., Rn. 14.

gar nicht unter den Anwendungsbereich der DSGVO fällt. Wenn keine personenbezogenen Daten vorliegen, ist das gesamte Rechtsgebiet nicht anwendbar, weshalb eine klare Regelung der Grenzen des Anwendungsbereichs der DSGVO erforderlich ist.[67]

Bei automatisierten und vernetzten Kraftfahrzeugen spielen aber insbesondere technische Daten eine große Rolle, welche zunächst schwerlich einen Personenbezug aufweisen. Bei näherer Betrachtung kann allerdings häufig auch ein Personenbezug festgestellt werden. Die durch die Sensortechnik produzierten Identifikations- und Merkmalsdaten erlangen demnach dann datenschutzrechtliche Relevanz, wenn sie einen solchen Personenbezug aufweisen. Hiermit sind im Rahmen dieses Beitrags indes nicht mittels Sensor erfasste Umgebungsdaten wie etwa Bilder von Fußgänger*innen gemeint, die unstreitig Personenbezug aufweisen, aber hier nicht Untersuchungsgegenstand sind. Dennoch kann eine Vielzahl auf den ersten Blick rein technischer beziehungsweise fahrzeugbezogener Daten oftmals bei näherer Betrachtung durchaus auch einen Personenbezug aufweisen. Das ist jedenfalls dann der Fall, wenn diese Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person enthalten, welche im Regelfall solche sind, die die jeweiligen Nutzer*innen des Fahrzeugs und beispielsweise deren Bremsverhalten oder auch das Verhalten im Rahmen der automatisierten Steuerung, beinhalten.[68]

Es kommt bei der Frage, ob es sich bei Kraftfahrzeugfunktionsdaten (auch) um personenbezogene Daten handelt lediglich darauf an, ob eine Identifizierung durch die kumulative Kombinierung von Informationen erreicht werden kann.[69] Dabei muss allerdings einbezogen werden, mit welchen Mitteln und Zusatzwissen die verantwortliche Stelle einen Personenbezug herstellen kann. Unter dem BDSG a.F. und der Datenschutzrichtlinie (DSRL) war dies umstritten.[70] Auf der einen Seite wurde in Teilen der Literatur und bei den Aufsichtsbehörden die sogenannte objektive oder absolute Theorie vertreten, auf der anderen, die als herrschend zu bezeichnende subjektive oder relative Theorie.[71] Nach objektiver Sichtweise reicht es aus, dass die verantwortliche Stelle oder ein beliebiger Dritter in der Lage ist, die Information auf eine Person zu beziehen, ganz gleich ob tatsächlich von der Möglichkeit Gebrauch gemacht wird oder nicht.[72] Die Individuellen Fähigkeiten

[67] *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 14.

[68] *Forgó*, Datenschutzrechtliche Fragestellungen des autonomen Fahrens, in: *Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.5 Rn. 16 f.

[69] *Steege*, Ist die DS-GVO zeitgemäß für das autonome Fahren?, MMR 2019, 509 (S. 510).

[70] *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 58.

[71] Vgl. Ausführungen in: *Klar/Kühling,* in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, Art. 4 Nr. 1 Rn. 26; *Gola*, in: *Gola* (Hrsg.) DS-GVO, 2. Auflage 2018, Art. 4 Rn. 17 ff.; *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 58 ff.

[72] *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 58.

und Mittel der verantwortlichen Stelle bleiben dabei ohne Bedeutung.[73] Demgegenüber sollen nach subjektiver Theorie lediglich die Mittel berücksichtigt werden, die der verantwortlichen Stelle tatsächlich und im konkreten Einzelfall zur Verfügung stehen.[74] Dadurch sollen nicht nur die faktischen Mittel ausschlaggebend sein, sondern auch der Aufwand zur Identifizierung, die Kosten, Zeit und Arbeitskraft miteinbezogen werden.

In der Rechtsprechung[75] und mit Einführung der DSGVO wurde dieser Streit mittlerweile überwiegend zugunsten der subjektiven Theorie entschieden, wobei starke Beschränkungen und die Übernahme einiger objektiver Elemente eingeflossen sind.[76] Der EuGH stellt dabei fest, dass es indes „nicht erforderlich ist, dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden“[77] und damit abstraktes Drittwissen von der verantwortlichen Stelle mitberücksichtigt werden muss. Dies gilt allerdings nur, wenn und soweit dieses Wissen und die Mittel vernünftigerweise eingesetzt werden können.[78]

Für die Anwendung auf automatisierte Kraftfahrzeuge bedeutet das, dass auch dort im Einzelfall festgestellt werden muss, welche Mittel die verantwortliche Stelle selbst oder eine andere Person nach allgemeinem Ermessen wahrscheinlich und vernünftigerweise nutzen wird, um einen Personenbezug herzustellen. Die genannte Kategorie der Merkmalsdaten ist beispielsweise dann bezüglich einer bestimmten Person relevant, wenn Informationen über Schaltvorgänge oder häufiges Beschleunigen und Bremsen dazu genutzt werden, um etwas über das Fahrverhalten der Kraftfahrzeugführenden auszusagen. Ebenfalls könnte eine häufige Warnung eines Parksensors darauf schließen lassen, dass der/die Fahrer*in Schwierigkeiten hat, Abstände einzuschätzen.[79] Die möglichen Beispielsfälle lassen sich dabei um unzählige erweitern. Ausschlaggebend ist, wie dargestellt, ob die verantwortliche Stelle wahrscheinlich und vernünftigerweise Mittel nutzten wird, um einen Personenbezug solcher Daten herzustellen.

[73] *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 58.

[74] *Klar/Kühling,* in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, Art. 4 Nr. 1 Rn. 26 ff.

[75] EuGH C-582/14, NVwZ 2017, 213.

[76] *Moos/Rothkegel*, EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite, MMR 2016, 842 (S. 846); *Richter*, EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite, EuZW 2016, 909 (S. 913); *Karg*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 1 Rn. 60.

[77] EuGH C-582/14, NVwZ 2017, 213 Rn. 43.

[78] *Richter*, EuGH: Speicherung von IP-Adressen beim Besuch einer Internetseite, EuZW 2016, 909 (S. 913).

[79] *Schwichtenberg*, Datenschutz in drei Stufen – Ein Auslegungsmodell am Beispiel des vernetzten Automobils, DuD-Fachbeiträge, Springer Vieweg, 2018, S. 118.

2.4 Vorliegen einer Verarbeitung Art. 4 Nr. 2 DSGVO

Weiter ist zu prüfen, ob eine Verarbeitung im Sinne des Datenschutzrechts vorliegt. Gemäß Art. 4 Nr. 2 DSGVO ist eine Verarbeitung jeder „mit oder ohne Hilfe automatisierter Verfahren ausgeführte […] Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten […]". Daran anschließend folgt eine beispielhafte, nicht abschließende Aufzählung solcher Verarbeitungsvorgänge, wie etwa das Erheben, Speichern, Verändern oder Löschen personenbezogener Daten.

Das BDSG a.F. definierte in § 3 Abs. 3-5 noch einzelne Phasen der Verarbeitung, wohingegen die DSGVO auf eine solche Differenzierung verzichtet. Einzelnen Phasen im BDSG a.F. waren beispielsweise Erheben, Verarbeiten und Nutzen. Da aufgrund der Einführung der DSGVO jede Phase gleichermaßen unter einem Erlaubnisvorbehalt steht und einer Legitimation im Sinne von Art. 6 Abs. 1 DSGVO bedarf, ist eine solche Unterteilung nicht mehr nötig.[80] Die in Art. 4 Nr. 2 DSGVO beispielhaft genannten Verarbeitungsvorgänge sind zwar in Teilen identisch mit den Phasen des BDSG a.F., stellen aber keine Definitionen mehr dar, was dem Verständnis der DSGVO hingegen nicht zuträglich ist.[81]

Der Begriff der Verarbeitung wird nun durch eine Kombination höchst abstrakter Begriffsbestimmungen und der zahlreichen, diese illustrierenden Beispiele des Art. 4 Nr. 2 DSGVO definiert. Gemäß der Formulierung des Art. 4 Nr. 2 DSGVO ist Datenverarbeitung jeder Vorgang, der in irgendeiner Art und Weise im Zusammenhang mit personenbezogenen Daten steht. Damit ist der Anwendungsbereich denkbar weit. Es spielt keine Rolle, ob die Verarbeitung in einem Vorgang oder mehreren geschieht, auch nicht, ob diese am selben Ort oder zeitlich oder räumlich getrennt stattfindet.[82] Ebenfalls unerheblich ist die Intensität oder Dauer des Umgangs mit den Daten. Das führt dazu, dass etwa im Cache eines Browsers temporär zwischengespeicherte Daten oder die kurzzeitig erfolgte Extraktion eines Kraftfahrzeugkennzeichens aus einer Bilddatei, welches nach Abgleich (inklusive der Kennzeichendaten) gelöscht wird, Datenverarbeitungsvorgänge darstellen.[83]

Einzig tatsächlich abgrenzendes Kriterium ist damit die Vorgabe, dass der Vorgang im Zusammenhang mit personenbezogenen Daten stehen muss. Ist dies erfüllt, ist jeder

[80] *Gola*, in: *Gola* (Hrsg.) DS-GVO, 2. Auflage 2018, Art. 4 Rn. 30.

[81] *Roßnagel*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 2 Rn. 7.

[82] A.a.O., Rn. 11.

[83] BVerfGE 150, 244; *Roßnagel,* Verfassungsrechtliche Grenzen polizeilicher Kfz-Kennzeichenerfassung, NJW 2008, 2547 (S. 2548 mwN); *Roßnagel*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 2 Rn. 11.

denkbare Vorgang mit diesen Daten, bis hin zur Pseudonymisierung, Anonymisierung oder Löschung der Daten ein Verarbeitungsvorgang im Sinne des Art. 4 Nr. 2 DSGVO.[84]

Das BDSG in seiner neuen Fassung enthält keine Konkretisierung des Verarbeitungsbegriffs, was insofern bedauerlich ist, als eine Definition und Präzisierung des abstrakten Verarbeitungsbegriffs der DSGVO, wie vormals durch § 3 Abs. 3-5 BDSG a.F. vorgenommen, nicht mehr erfolgt. Eine solche Klarstellung wäre jedoch in hohem Maße hilfreich gewesen und stellt für eine rechtssichere Anwendung der DSGVO ein Manko dar. Für das BDSG n.F. ist folglich die Definition des Art. 4 Nr. 2 DSGVO mit all ihren Schwächen maßgeblich.[85]

Für automatisiertes Fahren bedeutet das folglich, dass auch Daten in einem flüchtigen Speicher, welche nach Auswertung durch das technische System sofort wieder überschrieben werden, unter den Verarbeitungsbegriff der DSGVO fallen.[86] Die Dauer des Vorgangs spielt, wie dargestellt, gerade keine Rolle. Fraglich erscheint allerdings, ob es einer Differenzierung bedürfe, ob die Daten durch einen Menschen wahrgenommen werden könnten – unabhängig von tatsächlicher Kenntnisnahme – oder ausschließlich durch das System zum Zweck der Fahrzeugsteuerung verarbeitet und laufend überschrieben werden.[87] Handelt es sich bei einer solchen Verarbeitung um personenbezogene Daten, wie Positionsdaten (Insbesondere bei Verknüpfung mit der FIN), müsste auch diese konsequenter Weise als Datenverarbeitung im Sinne des Art. 4 Nr. 2 DSGVO angesehen werden. Darüber hinaus erscheint es in der tatsächlichen Praxis auch fraglich, ob die Daten unmittelbar überschrieben werden oder allein zur Gewährleistung von IT-Sicherheit oder zur Produktbeobachtung oder dergleichen, Mechanismen zur Speicherung oder Übertragung vorgesehen sind.[88] Damit wäre die Streitfrage, ob es sich um eine Verarbeitung handelt oder nicht sogleich obsolet. Aus dem bisher Gesagten folgt, dass die Bewertung, ob eine Datenverarbeitung vorliegt, dahingehend unproblematisch ist, dass im Sinne der DSGVO jeglicher Umgang mit Daten – sofern Personenbezug besteht – als Verarbeitung im Sinne des Art. 4 Nr. 2 DSGVO bewertet werden muss.

[84] *Roßnagel*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 4 Nr. 2 Rn. 12.

[85] A.a.O., Rn. 34.

[86] Siehe dazu auch BVerfG „Kfz-Kennzeichenkontrollen 2“, BVerfGE 150, 244 – 309.

[87] Vgl. dazu ähnlich *Klink-Straub/Straub*, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3202).

[88] Ebd.

2.5 Datenschutzrechtlich Betroffene Person Art. 4 Nr. 1 DSGVO

Datenschutzrechtlich Betroffener ist im Sinne des Art. 4 Nr. 1 DSGVO jede „identifizierte oder identifizierbare natürliche Person". Betroffener ist die Person, die bei Verarbeitung ihrer personenbezogenen Daten geschützt werden soll. Deutlich wird dabei, dass Betroffener nur eine natürliche Person sein kann und keine juristische, womit der Anwendungsbereich auf letztere entfällt. Enthalten die Daten über juristische Personen allerdings Angaben, die auf einzelne natürliche Personen schließen lassen, unterliegen sie dem Anwendungsbereich der DSGVO.[89] Zu den weiteren Anforderungen an die Identifizierbarkeit kann auf die Ausführungen unter 2.3 verwiesen werden.

Bei der Nutzung automatisierter und vernetzter Kraftfahrzeuge kann es durchaus Unterschiede bei der Feststellung geben, wer Betroffener im Sinne des Art. 4 Nr. 1 DSGVO ist. Potenziell Betroffene können die Halter*innen, Eigentümer*innen, Fahrer*innen oder Dritte, wie beispielsweise Mitfahrer*innen oder Passanten, sein.[90] Halter*in und Eigentümer*in fallen oft, aber nicht ausschließlich zusammen. Ist darüber hinaus der/die Kraftfahrzeughalter*in nicht identisch mit dem/der Fahrer*in (wie zum Beispiel im Leasing), ist nicht ohne weiteres festzustellen, wer Betroffener ist. Lediglich wenn eine hinreichend enge Verknüpfung zwischen Fahrer*in und Halter*in besteht, die zur Identifizierbarkeit führen kann, ist die Betroffenheit in einem solchen Fall feststellbar. Demnach bedarf es zur Feststellung der Betroffenheit eine konkrete Einzelfallbetrachtung.[91] Ändert sich darüber hinaus der/die Halter*in des Kraftfahrzeugs, hat dies ebenfalls Auswirkungen auf die Bestimmung, wer betroffen ist.

Bei einem Auseinanderfallen der Rollen Eigentümer-Halter-Fahrer*in bestehen allerdings häufig weitere Rechtsbeziehungen, wie ein Arbeits- oder Mietvertrag, woraufhin dennoch eine gegenseitige Beziehbarkeit bestehen kann und unter Umständen alle drei Betroffene im Sinne des Datenschutzrechts sein können.[92] Zudem wird es in Zukunft wahrscheinlich vermehrt auch andere Fälle geben, etwa wenn die Nutzung des Kraftfahrzeugs mittels Anmeldung mit einem persönlichen Profil, wie es beispielsweise bei Carsharing-Anbietern üblich ist, erfolgt. Selbst bei privater Nutzung wird es mit zunehmen-

[89] *Gola*, in: *Gola* (Hrsg.) DS-GVO, 2. Auflage 2018, Art. 4 Rn. 25.

[90] *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507 (S. 509).

[91] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 145.

[92] *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507 (S. 509).

der Automatisierung und Vernetzung immer wahrscheinlicher, dass sich die Fahrer*innen mit weiteren Geräten wie Smartphones oder sonstigen Geräten und dem Kraftfahrzeug verbinden, so dass diese auch als Fahrer*in identifiziert werden können.

2.6 Datenschutzrechtlich Verantwortlicher Art. 4 Nr. 7 DSGVO

Der datenschutzrechtlich Verantwortliche ist gemäß Art. 4 Abs. 1 Nr. 7 DSGVO eine „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". Aus dieser Verantwortung resultieren vielerlei Pflichten aus dem Datenschutzrecht.

Bei der Datenverarbeitung in automatisierten und vernetzten Kraftfahrzeugen besteht ein Problem in der Vielzahl an denkbaren verantwortlichen Stellen. Verantwortlicher ist nach Art. 4 Nr. 7 DSGVO derjenige, der über das Ob, Warum und Wie der Datenverarbeitung entscheidet, also eine gewisse „Datenherrschaft" ausübt.[93] Dabei muss sowohl nach Speicherort als auch nach Zugriffsmöglichkeiten unterschieden werden. Einerseits kommen Hersteller, Händler*innen, Reparaturwerkstätten, die Halter*innen oder Fahrer*innen in Betracht.[94] Andererseits kommen angesichts der weiteren vielfältigen wirtschaftlichen Interessenlagen an den Kraftfahrzeugdaten noch eine Reihe weiter möglicher Verantwortlicher wie Versicherungen, Leasinggeber oder Carsharing-Anbieter und dergleichen in Betracht. Daher kann hier auch von mehrpolaren Verhältnissen gesprochen werden, weshalb die Frage nach dem Verantwortlichen und damit dem Adressaten der umfänglichen Pflichten aus der DSGVO nicht mehr a priori beantwortet werden kann, sondern im konkreten Einzelfall erörtert werden muss.[95]

Einige, nicht abschließende Beispielsfälle für die genannten möglichen Verantwortlichen können sein: Die Hersteller, welche die Kraftfahrzeuge mit Sensoren und Software zum

[93] *Klink-Straub/Straub,* Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3203); *Forgó*, Datenschutzrechtliche Fragestellungen des autonomen Fahrens, in: *Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.5 Rn. 23.

[94] *Forgó*, Datenschutzrechtliche Fragestellungen des autonomen Fahrens, in: *Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.5 Rn. 23.

[95] *Klink-Straub/Straub,* Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3203).

Verarbeiten der Daten ausstatten und somit die technischen Voraussetzungen für die Erhebung, Speicherung und Übermittlung überhaupt erst schaffen.[96] Problematisch in diesem Fall ist, dass solange der Hersteller zwar über die Zwecke und Mittel der Datenverarbeitung entscheidet, aber lediglich datenverarbeitende Produkte herstellt, ist der sachliche Anwendungsbereich des Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 2 DSGVO nicht eröffnet, da hierzu ein automatisierter Verarbeitungsvorgang personenbezogener Daten vorliegen muss.[97] Besteht allerdings eine permanente Datenübertragung („online Auto") zu einem vom Hersteller oder ihm beauftragen Auftragsverarbeiter betriebenen Server, ist der Hersteller als Verantwortlicher anzusehen.[98]

Werden Daten nicht automatisch übertragen, sondern lediglich im Kraftfahrzeug gespeichert („offline Auto"), sind die Datenschutzbehörden in ihrer gemeinsamen Erklärung mit dem VDA[99] auf Grundlage des alten BDSG davon ausgegangen, dass der Hersteller zum Zeitpunkt der Datenspeicherung noch nicht verantwortliche Stelle gemäß § 3 Abs. 7 BDSG a.F. ist, sondern erst im Rahmen einer Erhebung nach § 3 Abs. 3 BDSG a.F., also erst dann, wenn die Daten tatsächlich ausgelesen werden.[100] Allerdings muss hier beachtet werden, dass der Hersteller in der Regel die technische Gestaltung, Schnittstellen und Auslesemöglichkeiten bestimmt und somit zumindest indirekt (beispielsweise über Vertragswerkstätten) an die Daten gelangt und damit auch als von Anfang an Verantwortlicher angesehen werden kann.[101]

Weiterhin ist im Rahmen eines *pay as you drive* (PAYD) -Tarifs die Versicherung als Verantwortliche Stelle zu betrachten, wenn diese die durch den Betroffenen zur Verfügung gestellten Daten zum Fahrverhalten speichert oder anderweitig Zugriff darauf hat.[102]

[96] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 141.

[97] Ebd.

[98] *Klink-Straub/Straub*, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3202).

[99] S. http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/01/Gemeinsame_Erklaerung_VDA_Datenschutzbehoerden.pdf.

[100] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA), Nr. 3.

[101] *Weichert*, Der Personenbezug von Kfz-Daten, NZV 2017, 507, S. 512.

[102] *Klink-Straub/Straub*, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3202).

Vertragshändler*innen haben in der Regel nach Abschluss des Kaufs keinen Zugriff mehr auf die Kraftfahrzeugdaten und kommen daher lediglich für die im Rahmen des Kaufvertrags anfallenden Daten als Verantwortliche in Betracht.[103]

Eigentümer*innen und Halter*innen sind insofern als Verantwortliche anzusehen, wenn sie Zugriff auf die Daten der Fahrerenden oder der Insassen haben, wobei in diesem Zusammenhang auf die Beschränkungen des Art. 2 Abs. 2 lit. c DSGVO zu verweisen ist, wonach bei ausschließlich persönlicher oder familiärer Tätigkeit die DSGVO keine Anwendung findet.[104]

Nach der eCall-VO[105] müssen alle nach dem 31.3.2018 zugelassenen Kraftfahrzeuge und leichte Nutzfahrzeuge das sogenannte eCall-System verbaut haben, bei welchem in einer Unfallsituation automatisch ein Notruf an die zuständige Notrufzentrale (112 Nummer) abgesetzt und einen Mindestdatensatz (Unfallzeitpunkt, Fahrtrichtung, Koordinaten, FIN und Serviceprovider ID) übermittelt wird.[106] Damit kann auch die Notrufleitstelle als verantwortliche Stelle gelten. Weiterhin können sich Halter*innen auch für einen zusätzlichen TPS-eCall („*third party service*“) entscheiden und den Notruf damit zunächst von einem, seitens des Herstellers betriebenen, Call Center aufnehmen lassen, wodurch dieses dann verantwortliche Stelle ist.[107]

Infrastruktur, Teledienste- oder Telekommunikationsanbieter können ebenfalls Verantwortliche im Sinne der DSGVO sein, denn diese koordinieren und überwachen die Kommunikation.[108] Ob es sich bei Infrastrukturanbietern um öffentliche oder private Stellen handelt ist bei der Frage nach dem Verantwortlichen unerheblich, denn sobald eine Verarbeitung von personenbezogenen Daten stattfindet und eine Stelle über die Mittel und den Zweck dieser entscheidet, gelten sie unabhängig ihrer Ausgestaltung als Verantwortliche im Sinne der DSGVO.[109]

Weitere Konstellationen sind darüber hinaus denkbar und bedürfen im konkreten Fall einer gesonderten Betrachtung.

[103] *Klink-Straub/Straub*, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3202).

[104] Ebd.

[105] VO (EU) 2015/758 des Europäischen Parlaments und des Rates v. 29.4.2015.

[106] *Wendt*, Autonomes Fahren und Datenschutz – eine Bestandsaufnahme, ZD Aktuell 2018, 06034.

[107] *Klink-Straub/Straub*, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3202).

[108] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 143.

[109] Ebd.

2.7 Zulässigkeit der Datenverarbeitung Art. 6 DSGVO

Wenn es sich bei der Verarbeitung von Daten um personenbezogene handelt, ist nach der Systematik des Art. 6 Abs. 1 DSGVO für jedwede Verarbeitung derselben, grundsätzlich eine Ermächtigungsgrundlage erforderlich (Verbot mit Erlaubnisvorbehalt). Ausgehend von Art. 7 und 8 GRCh und dem Grundsatz der Rechtmäßigkeit (Art. 5 Abs. 1 lit. a DSGVO) ist Art. 6 DSGVO eine der zentralen materiellen Normen im Datenschutzrecht und die Grundlage für die Zulässigkeit der Verarbeitung personenbezogener Daten.[110] Aus der Entstehungsgeschichte und insbesondere aus der Systematik des Art. 6 DSGVO ergibt sich, dass jede Verarbeitung personenbezogener Daten von einem der Erlaubnistatbestände des Art. 6 Abs. 1. lit. a-f gedeckt sein muss.[111] Die Auflistung der Erlaubnistatbestände ist zudem abschließend. Damit ist sichergestellt, dass den Anforderungen des Art. 8 Abs. 2 S. 1 GRCh vollständig gerecht wird und es keinerlei Verarbeitungsvorgang ohne konkrete Rechtsgrundlage geben kann.[112]

Für das automatisierte und vernetzte Fahren sind vor allen Dingen die Erlaubnistatbestände gemäß Art. 6 Abs. 1 lit. a, b, c und f DSGVO (Einwilligung, Vertragsverhältnis, aufgrund einer rechtlichen Verpflichtung oder des berechtigten Interesses des Verantwortlichen) von Interesse. Diese werden im Folgenden daher näher in die Diskussion eingeführt.

2.7.1 Einwilligung Art. 6 Abs. 1 lit. a DSGVO

Nach Art. 6 Abs. 1 lit. a DSGVO bedarf es einer Einwilligung der betroffenen Person zur Verarbeitung der sie betreffenden personenbezogenen Daten. In Art. 4 Nr. 11 DSGVO ist die Einwilligung als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“, legaldefiniert. Das Erfordernis der eindeutig bestätigenden Handlung ist darüber hinaus in Erwägungsgrund 32 S. 3 DSGVO konkretisiert und legt fest, dass Stillschweigen oder vorangekreuzte Kästchen nicht genügen. Daraus folgt, dass sogenannte „Opt Out“-Verfahren zur Einholung der Einwilligung nicht mehr zulässig sind.[113] Die weiteren Bedingungen bezüglich der Einwilligung sind in Art. 7 DSGVO geregelt.

[110] *Albrecht*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 6 Rn. 1.

[111] Ebd.

[112] Ebd.

[113] *Albers/Veit* in *Wolff/Brink* (Hrsg.) BeckOK, 40. Ed. 1.11.2021, DS-GVO Art. 6 Rn. 24.

Betrachtet man den Stellenwert der Einwilligung im Datenschutzrecht und insbesondere in der DSGVO, könnte unter Umständen verfrüht auf eine Datenschutzlösung, bei welcher der Nutzer selbstbestimmt und frei über seine Daten entscheiden kann, geschlossen werden. Die informierte Einwilligung wird oftmals als „Eckpfeiler des Datenschutzrechts“[114] oder „genuiner Ausdruck des Rechts auf informationelle Selbstbestimmung“[115] erachtet. Es ist allerdings fraglich, inwiefern Menschen abseits theoretischer Konzepte wirklich und effektiv Kontrolle über ihre Daten, deren Verarbeitung oder einen damit selbstbestimmten Umgang haben. Ferner ist zu beobachten, dass zum Beispiel ein Großteil der Internetnutzer*innen sich offenbar keine Gedanken um Privatheit im Netz und dem Schutz informationeller Selbstbestimmung macht.[116] Hinzu kommt, dass in der Theorie durch das Erfordernis der Einwilligung ein hohes Maß an Selbstbestimmung suggeriert wird, jedoch ist die Praxis oftmals divergent gelagert.

Vor dem Hintergrund automatisierter und vernetzter Kraftfahrzeuge stellen sich verschiedene Fragen bezüglich der Einwilligung. Dazu zählen beispielsweise die Fragen, gegenüber wem eine solche Einwilligung abgegeben wird, da die Kraftfahrzeuge in der Regel nicht direkt beim Hersteller, sondern einem (Gebrauchtwagen)Händler oder von einem Privaten gekauft werden. Müsste nach einem Update erneut in die Datenverarbeitung eingewilligt werden oder sogar vor jedem Fahrtantritt? Was geschieht bei einem Widerruf der Einwilligung und ist dieser dann bezüglich der notwendigen Datenverarbeitung zur Kraftfahrzeugsteuerung überhaupt ohne weiteres möglich? Art. 7 Abs. 3 DSGVO sieht explizit vor, dass eine Einwilligung jederzeit widerrufen werden kann. Sogenannte „Take it or leave it“-Situationen, bei denen es keine Möglichkeit zur Nutzung ohne Einwilligung gibt, sollten durch die DSGVO gerade vermieden werden (Vgl. Art. 7 Abs. 4 DSGVO). Teilweise wird die Einwilligung auch kritisiert, indem beispielsweise gefordert wird „sich der Erkenntnis nicht mehr zu verschließen, dass die Einwilligung das schlechteste Rechtsinstrument zur Sicherstellung informationeller Selbstbestimmung ist.“[117]

Im Rahmen der Einwilligung ist daher noch wesentlicher Konkretisierungsbedarf zu erkennen, um die Diskrepanz zwischen theoretischer Schutzidee und tatsächlich wirksamer Schutzmechanismen aufzulösen. Dies gilt umso mehr in den vorab beschriebenen Szenarien bezüglich automatisierter Kraftfahrzeuge.

[114] *Albrecht*, #DSGVO, Teil 2: Klare Einwilligung als Eckpfeiler, https://goo.gl/F6Eksz.

[115] *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts 2001, S. 72.

[116] *Moll*, Die Zukunft des Rechts auf informationelle Selbstbestimmung aus medienpsychologischer Sicht, in: *Friedewald/Lamla/Roßnagel* (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, S. 53 ff.

[117] *Veil*, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686 (S. 688).

2.7.2 Vertragsverhältnis Art. 6 Abs. 1 lit. b DSGVO

Art. 6 Abs. 1 lit. b DSGVO erlaubt die Datenverarbeitung einer betroffenen Person in zwei Varianten, entweder, wenn diese zur Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Damit ist die Vorschrift fast textgleich mit der vorherigen Regelung der Art. 7 lit. b EG-DSRL und entspricht inhaltlich teilweise dem § 28 Abs. 1 Satz 1 Nr. 1 BDSG a.F.[118]

Im Kontext automatisierter Kraftfahrzeuge befinden sich allerdings Eigentümer*in, Halter*in, Fahrer*in oder Mitfahrer*in in keinem solchen Vertragsverhältnis mit dem Hersteller, weshalb sich in diesem Fall der Hersteller bei der Datenverarbeitung nicht auf Art. 6 Abs. 1 lit. b DSGVO berufen kann. Andere Konstellationen, die eine Datenverarbeitung aufgrund eines Vertrags ermöglichen könnten, wären Verträge mit einer Versicherung im Rahmen von Telematik-Tarifen (PAYD-Tarife), bei einem Mietwagenunternehmen und den Mieter*innen oder zwischen den Eigentümer*innen, Halter*innen oder Fahrer*innen und beispielsweise einem Pannendienst oder einer Werkstatt.[119]

Auch hier gilt, wie die obigen Ausführungen verdeutlichen, dass es häufig auf den konkreten Einzelfall ankommt und keine pauschale Aussage für alle Fälle getroffen werden kann.

2.7.3 Gesetzliche Grundlage Art. 6 Abs. 1 lit. c DSGVO

Art. 6 Abs. 1 lit. c DSGVO ermöglicht die Datenverarbeitung auch dann, wenn sie zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen notwendig ist. Dabei stellt die Regelung selbst keinen eigenen Erlaubnistatbestand für die Datenverarbeitung dar.[120] Die eigentliche Legimitationsgrundlage muss sich im Unionsrecht oder im mitgliedsstaatlichen nationalen Recht finden. Eine Verpflichtung durch privatautonome Vereinbarung kann demzufolge nicht ausreichen, um sich auf Art. 6 Abs. 1 lit. c DSGVO zu berufen. Die Verpflichtung kann sich ausschließlich aus einer Rechtsgrundlage im Sinne des Art. 6 Abs. 3 S. 1 DSGVO ergeben.[121] Eine auf Art. 6 Abs. 1 lit. c DSGVO gestützte Erlaubnis zur Datenverarbeitung ist lediglich auf die Erfüllung der jeweiligen gesetzlichen Pflicht beschränkt, kann jedoch nicht darüber hinaus gehen.[122] Das bedeutet, dass nur solche Daten, Verarbeitungsschritte und Speicherzeiträume legitim sind, die zur

[118] *Wedde*, in: *Däubler/Wedde/Weichert/Sommer* (Hrsg.) EU-DSGVO und BDSG, 1. Auflage 2018, Art. 6 lit. b Rn. 25.

[119] *Klink-Straub/Straub*, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3204).

[120] *Buchner/Petri* in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, Art. 6 Rn. 73.

[121] *Roßnagel*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 6 Abs. 1 Rn. 51.

[122] A.a.O., Rn. 57.

Erfüllung einer gesetzlichen Pflicht erforderlich sind. Nach Erfüllung sind diese, sofern keine Aufbewahrungspflicht besteht, zu löschen.[123]

Existiert eine Norm, die als rechtliche Verpflichtung dienen soll, muss sich diese unmittelbar auf die Datenverarbeitung beziehen. Einzig der Umstand, dass die für die Datenverarbeitung verantwortliche Person personenbezogene Daten verarbeiten muss, um irgendeine rechtliche Verpflichtung erfüllen zu können, reicht nicht aus.[124] Eine eindeutige Vorgabe, welchen Konkretions- und Präzisionsgrad die rechtliche Verpflichtung aufweisen muss, ergibt sich jedoch nicht aus Art. 6 Abs. 1 lit. c DSGVO.[125] Aufgrund des Abstraktions- und Typisierungsgrades von Gesetzen können jedoch die Regelungselemente „zur Erfüllung" der Verpflichtung „erforderlich" noch limitierende Maßgaben setzen.[126] Je genauer und detaillierter die Rechtsvorschriften ausgestaltet sind und konkrete Pflichten zur Verarbeitung bestimmter Daten für im Gesetz festgelegte sachlich bestimmte Pflichten oder Aufgaben enthalten, desto umfangreicher kann auch die Erforderlichkeit anerkannt werden.[127]

Im Rahmen des automatisierten Fahrens finden sich auf nationaler Ebene solche gesetzlichen Grundlagen z.B. im StVG. Hier wäre an § 63a StVG und den neuen § 1g StVG zu denken. Ob diese den Anforderungen an Art. 6 Abs. 1 lit. c DSGVO genügen, wird durchaus kontrovers diskutiert und erscheint fraglich.[128] In Kapitel 3 unter Abschnitt 3.1 und 3.3 wird dies auch im hiesigen Kontext deutlich.

2.7.4 Berechtigtes Interesse des Verantwortlichen Art. 6 Abs. 1 lit. f DSGVO

Art. 6 Abs. 1 lit. f erlaubt die Verarbeitung personenbezogener Daten, soweit diese „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich [ist], sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen." Wann es sich um berechtigte Interessen handelt, konkretisiert Erwägungsgrund 47 DSGVO. Bei diesem Zulässigkeitstatbestand handelt es sich um eine zentrale Interessenabwägungsklausel, die neben der Einwilligung in der Praxis als relevanteste Rechtsgrundlage für die

[123] *Roßnagel*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 6 Abs. 1 Rn. 57.

[124] *Albers/Veit* in *Wolff/Brink* (Hrsg.) BeckOK, 40. Ed. 1.11.2021, DS-GVO Art. 6 Rn. 48.

[125] A.a.O., Rn. 50.

[126] A.a.O., Rn. 48.

[127] A.a.O., Rn. 50.

[128] Vgl. *Steege,* Gesetzentwurf zum autonomen Fahren (Level 4), SVR 2021, 128, S. 135; *Steinrötter*: Datenschutz als Gretchenfrage für autonome Mobilität, ZD 2021, 513, S. 514.

private Datenverarbeitung angesehen wird.[129] Aufgrund der Flexibilität soll ein notwendiger Ausgleich zwischen den Rechten der betroffenen Personen (Art. 7 und 8 GRCh) und den Interessen und Grundrechten Dritter in allen Konstellationen ermöglicht werden.[130] Durch diese Regelung soll das rigorose Verbotsprinzip ein gewisses Korrektiv erfahren,[131] wobei damit allerdings auch eine mangelnde Voraussehbarkeit seitens der betroffenen Person einerseits und Rechtsunsicherheit für den Verantwortlichen andererseits einhergeht.[132] Beruft sich der Verantwortliche auf seine berechtigten Interessen, steht dies dennoch unter dem grundsätzlichen Vorbehalt, dass keine überwiegenden Interessen, Grundfreiheiten oder Grundrechte der von der Datenverarbeitung betroffenen Person dieser Verarbeitung entgegenstehen und somit den Schutz der personenbezogenen Daten erfordern.[133]

Die Verarbeitung von personenbezogenen Daten aufgrund von Art. 6 Abs. 1 lit. f DSGVO erfordert drei Prüfschritte, welche vor der Verarbeitung durchgeführt werden müssen.[134] Als erstes muss der Verantwortliche untersuchen, ob ein berechtigtes Interesse der betroffenen Person gegen die Verarbeitung besteht und falls dies bereits bejaht wird, hat die Verarbeitung zu unterbleiben.[135] Ist das berechtigte Interesse hingegen gegeben, muss in einem zweiten Schritt geprüft werden, ob Grundrechte, Grundfreiheiten oder Interessen der betroffenen Person entgegenstehen, wobei dies hinsichtlich des Rechts auf informationelle Selbstbestimmung praktisch immer gegeben sein wird.[136] Daher muss im dritten Schritt eine Interessenabwägung zwischen den beiden Positionen erfolgen. Aus Sicht des Verantwortlichen sind häufig rechtliche, ideelle, aber vor allem wirtschaftliche Interessen von Belang.

Im Zusammenhang mit vernetzten und automatisierten Kraftfahrzeugen, wird insbesondere für den Hersteller aufgrund fehlender direkter Vertragsbeziehungen mit dem Betroffenen der Auffangtatbestand des Art. 6 Abs. 1 lit. f DSGVO von Interesse sein. Die Hersteller, aber wahrscheinlich auch alle anderen Beteiligten, werden ein Interesse daran haben, dass während der automatisierten Fahrt das Kraftfahrzeug bestimmungsgemäß

[129] *Schantz*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 6 Rn. 86.

[130] Ebd.

[131] *Schulz*, in: *Gola* (Hrsg.) DS-GVO, 2. Auflage 2018, Art. 6 Rn. 4.

[132] *Schantz*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 6 Rn. 86.

[133] *Wedde*, in: *Däubler/Wedde/Weichert/Sommer* (Hrsg.) EU-DSGVO und BDSG, 1. Auflage 2018, Art. 6 Rn. 101.

[134] A.a.O., Rn. 102.

[135] Ebd.

[136] Ebd.

und sicher funktioniert.[137] Hierbei ist zu unterscheiden, dass die Eingriffsintensität bei einer Verarbeitung vergleichsweise gering ausfällt und ein berechtigtes Interesse bejaht werden kann, wenn die personenbezogenen Daten nach Erhebung sofort wieder gelöscht oder überschrieben werden und ausschließlich vom automatisierten System, (vgl. oben unter 2.4), ohne dass eine andere Person auf diese Zugriff hat, erhoben wird. Der Grundsatz der Zweckbindung muss dabei gewahrt werden. Allerdings werden in vielen Fallkonstellationen die Daten wohl länger als lediglich zur Auswertung durch das automatisierte System erforderliche Zeit verarbeitet werden. Insbesondere wenn diese an den Hersteller übertragen werden, damit dieser auswerten kann, ob das Fahrzeug bestimmungsgemäß genutzt und regelmäßig gewartet wurde. Wobei hier fraglich ist, ob das berechtigte Interesse primär darin liegen kann, dass sich der Hersteller in einem möglichen Rechtsstreit oder Garantiefall einen Wissensvorsprung verschaffen kann, um reine wirtschaftliche Ansprüche abzuwehren.[138] Bei Daten, die zur Produktbeobachtung oder -verbesserung anonymisiert oder pseudonymisiert übertragen werden, wird ein berechtigtes Interesse schon eher zu bejahen sein. In die gleiche Richtung der Datenverarbeitung zielt darüber hinaus auch § 63a StVG ab, welcher beispielsweise die Datenverarbeitung zum Zwecke der Unfallforschung ermöglicht.[139]

2.8 Data Protection by Design & Data Protection by Default

Die Vorgaben des Datenschutzes durch Technikgestaltung (*data protection by design*) und datenschutzfreundliche Voreinstellung (*data protection by default*), welche sich aus Art. 25 DSGVO ergeben, werden im Zusammenhang mit der Automatisierung und Vernetzung von Kraftfahrzeugen häufig und prominent erwähnt. Was hingegen oftmals ausbleibt, ist eine Konkretisierung oder Beschreibung, was damit eigentlich gemeint ist und inwiefern dies die Entwicklung von Kraftfahrzeugen tatsächlich beeinflusst.

Art. 25 DSGVO beschreibt in seinem ersten Absatz die Grundsätze von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen und beschränkt sich auf verschiedene Kriterien, anhand derer sich die getroffenen Maßnahmen messen lassen müssen und ebenfalls, wann, also zu welchem Zeitpunkt diese Maßgaben berücksichtigt werden müssen.[140] Mit Ausnahme der Pseudonymisierung werden jedoch keiner-

[137] *Klink-Straub/Straub*, Nächste Ausfahrt DS-GVO – Datenschutzrechtliche Herausforderungen beim automatisierten Fahren, NJW 2018, 3201 (S. 3204).

[138] Ebd.

[139] Ebd.

[140] *Hartung*, in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, Art. 25 Rn. 1.

lei konkret zu treffende Maßnahmen benannt. Auf die in Art. 25 Abs. 1 genannten Anforderungen setzt der zweite Absatz auf und beschreibt die Grundsätze datenschutzfreundlicher Voreinstellungen. Konstituiert wird eine Pflicht die Datenverarbeitung so auszugestalten, dass nur die für den konkreten Zweck notwendigen und erforderlichen Daten verarbeitet werden. Das konkrete Zusammenspiel der beiden Absätze scheint indes nicht vollständig klar.[141] Genannt werden jedoch Beispiele dafür, worauf der Grundsatz (*Data Protection by Default*) anzuwenden ist und spezielle Vorgaben für die Veröffentlichung personenbezogener Daten. Absatz 3 verweist schließlich auf die Vorteile, die mit einer Zertifizierung einhergehen. Hier wird deutlich, dass es einer konkretisierenden Auslegung der Norm im speziellen Einzelfall bedarf. Sinn und Zweck der Regelung ist, bereits zu einem frühen Zeitpunkt Datenschutz bei der Auswahl, Festlegung und Einrichtung von datenverarbeitenden Systemen zu berücksichtigen.

Adressat der Verpflichtung aus Art. 25 DSGVO ist ausschließlich der für die Datenverarbeitung Verantwortliche. Hersteller oder Produzenten sollen hingegen keine unmittelbaren Normadressaten sein.[142] Hier ist jedoch hervorzuheben, dass die in Art. 25 Abs. 1 DSGVO beschriebene Pflicht bereits bei der Festlegung der Mittel für die Verarbeitung zu beachten ist und dadurch Hersteller und Entwickler*innen mittelbar, beziehungsweise de facto über ihre Marktmacht, eine datenschutzrechtliche „Vorfeldwirkung" trifft.[143] Im Zusammenhang mit automatisierten und vernetzten Kraftfahrzeugen kann hier festgehalten werden, dass die Hersteller maßgeblich über die Mittel und die Ausgestaltung der Schnittstellen bestimmen und sie damit die Pflicht des Art. 25 DSGVO trifft.

Die Pflicht des Verantwortlichen ist es sodann, angemessene technisch-organisatorische Maßnahmen zu treffen. Solche Maßnahme sind beispielsweise die in Art. 24 und Art. 32 DSGVO genannten. Hier ist lediglich die Zielrichtung beziehungsweise die Eigenschaften insofern erweitert, dass nicht nur reine Sicherheit gewährleistet werden soll, sondern auch Grundsätze wie Datenvermeidung implementiert werden müssen. Konkrete Beispiele für technisch-organisatorische Maßnahmen finden sich in Art. 25 Abs. 1 DSGVO bis auf die in Art. 4 Nr. 5 DSGVO definierte Pseudonymisierung (als Mittel zur Datenminimierung nach Art. 5 Abs. 1 lit. c) nicht. Allerdings sind zweifelsfrei auch die weiteren Grundsätze des Art. 5 Abs. 1 DSGVO umzusetzen.[144] Neben der genannten Pseudonymisierung kommt demzufolge auch der in Art. 5 Abs. 1 lit. a genannte Grundsatz der Transparenz

[141] *Hartung*, in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, Art. 25 Rn. 1.

[142] *Baumgartner*, in *Ehmann/Selmayr* (Hrsg.), Datenschutz-Grundverordnung 2. Auflage 2018, Art. 25 Rn. 5; *Hartung*, in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, Art. 25 Rn. 13.

[143] *Hansen*, in: *Simitis / Hornung / Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 25 Rn. 20 f.; *Hartung*, in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, Art. 25 Rn. 13.

[144] *Nolte/Werkmeister*, in *Gola* (Hrsg.) DS-GVO, 2. Auflage 2018, Art. 25 Rn. 14 f.; *Hartung*, in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, Art. 25 Rn. 16.

in Betracht, welcher durch die technische Einbindung von Datenschutzhinweisen (bspw. im Multimediasystem oder Head-up-Display eines Kraftfahrzeugs) realisiert werden könnte.

Weiterhin kann Datenminimierung beispielsweise durch Aggregieren von personenbezogenen Daten oder der Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten erreicht werden.[145] Die in Art. 5 Abs. 1 lit. f DSGVO genannten Integrität und Vertraulichkeit kann durch die Maßnahmen nach Art. 32 DSGVO gewährleistet werden. Dazu zählen Verschlüsselungs-, Zugangs- und Zutrittskontrollen. Konkrete technische Maßnahmen können in diesem Kontext etwa der Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptokonzepts sein, das Härten von IT-Systemen, so dass diese keine oder möglichst wenige Nebenfunktionalitäten aufweisen oder auch die Implementierung eines sicheren Authentifizierungsverfahrens.[146]

Die konkrete im Projekt VITAF erarbeitete Maßnahme, die die Anforderungen von Datenschutz durch Technikgestaltung umsetzt, ist ein Verfahren, welches auf den C-ITS Empfehlungen[147] basiert und ein auf Threshold RSA-Verschlüsselung basiertes Konzept zur Härtung des Ableitungsprozesses pseudonymer Identitäten beschreibt. Hier kann auf die im Forschungsprojekt VITAF erfolgten Ausarbeitungen verwiesen werden. Demzufolge kann das im C-ITS beschriebene Verfahren für die Pseudonymisierung von V2X-Kommunikation genutzt werden. Dieses beruht darauf, dass aus der Langzeit-Identität eines Kraftfahrzeugs viele pseudonyme Identitäten abgeleitet werden, die dann kurzfristig für die V2X Kommunikation genutzt werden. Damit kann ein Kraftfahrzeug höchstens so lange getrackt werden, wie das Kurzzeitzertifikat gültig ist. Eine Verknüpfung der zufällig erzeugten Zertifikate miteinander ist dabei nicht möglich. Dies ist allerdings nur möglich, wenn ein potenzieller Angreifer nicht den Ableitungsprozess kennt beziehungsweise dieser nicht angegriffen werden kann.

Weitere Maßnahmen und Anforderungen aus dem Bereich Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung werden nachfolgend in Kapitel 3

[145] Weitere Beispiele dafür finden sich im Standard-Datenschutzmodell, Version 2.0b, S. 36 f., abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf.

[146] Weitere Beispiele dafür finden sich im Standard-Datenschutzmodell, a.a.O., S. 32 f.

[147] Richtlinie 2010/40/EU Des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern; vgl. auch https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Automotive/Kooperative_Intelligente_Verkehrssysteme/Kooperative_Intelligente_Verkehrssysteme.html.

anhand der Neuregelungen im StVG untersucht und finden sich darüber hinaus an anderer Stelle beschrieben.[148]

[148] Vgl. *Arzt/Kleemann/Plappert/Rieke/Zelle*, Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung – Rechtliche und technische Anforderungen im Verbund, MMR 2022, 593-614.

3. Datenschutzrechtliche Anforderungen an automatisiertes und autonomes Fahren im Straßenverkehrsgesetz

Im Straßenverkehrsgesetz (StVG) finden sich seit der Novelle 2017 konkrete Anknüpfungspunkte bezüglich der Datenverarbeitung im Zusammenhang mit hoch- und vollautomatisiertem Fahren (§ 63a StVG) sowie seit 2021 für Kraftfahrzeuge mit sogenannten autonomen Fahrfunktionen (§ 1g StVG). Im Folgenden wird zunächst § 63a StVG analysiert und sodann § 1g StVG. Darüber hinaus wird der sogenannte Fahrmodusspeicher (*Data Storage Systems for Automated Driving*, DSSAD) und Unfalldatenspeicher (*Event Data Recorder*, EDR) betrachtet.

3.1 § 63a StVG

Mit der Änderung des Straßenverkehrsgesetzes im Juni 2017 wurde § 63a StVG neu eingefügt. In fünf Absätzen werden dort Regelungen bezüglich der Datenverarbeitung von Kraftfahrzeugen mit hoch- oder vollautomatisierten Fahrfunktionen beschrieben. Diese Regelung findet keine Anwendung auf autonome Kraftfahrzeuge[149] beziehungsweise solche mit autonomen Fahrfunktionen.[150]

In § 63a Abs. 1 StVG wird die ereignisbasierte Datenspeicherung bei Wechsel der Fahrzeugsteuerung zwischen dem System (gemäß § 1a StVG) und der kraftfahrzeugführenden Person geregelt. Dabei werden die Positions- und Zeitangaben mittels Satellitennavigationssystem (GPS) gespeichert. Ebenfalls sollen diese Daten gespeichert werden, wenn es eine Aufforderung an die kraftfahrzeugführende Person seitens des Systems gibt, die Steuerung zu übernehmen oder wenn eine technische Störung auftritt. Diese Regelung impliziert, dass Kraftfahrzeuge mit hoch- oder vollautomatisierten Fahrfunktionen herstellerseitig so ausgestattet sein müssen, dass eine derartige Datenverarbeitung überhaupt möglich ist.[151] Nicht in § 63a StVG geregelt ist der Speicherort für die erhobenen Daten.

Für die technische Ausgestaltung, die Art und Weise und den Ort der Speicherung sollte auf Grundlage des § 63b Nr. 1 StVG eine Rechtsverordnung erlassen werden. Dies blieb

[149] *Stender-Vorwachs/Steege*, Kleine SIM-Karte – große Konsequenz: Automobilhersteller als TK-Anbieter?, MMR 2018, 212, (S. 216).

[150] Siehe dazu auch Abschnitt 3.3 zu § 1g StVG.

[151] *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 199 ff.

allerdings bisher aus. Als Grund wurde angeführt, dass es erst einer internationalen Einigung bedürfe, bevor hier Vorgaben geschaffen werden.[152] Bei Schaffung eigener nationaler Standards wurde seitens der Bundesregierung erachtet, dass dies zu Handelshemmnissen im Bereich von Kraftfahrzeugen führen könnte.[153] Da die Adressat*innen der Speicherverpflichtung gemäß § 63b Nr. 2 auch erst per noch zu erlassender Verordnung bestimmt werden soll, besteht auch hier Unklarheit.[154] Das Fehlen einer solchen Verordnung hat zur Folge, dass alternative Möglichkeiten in der Literatur diskutiert wurden und werden. Dazu zählen die Speicherung im Kraftfahrzeug selbst,[155] die Speicherung auf den Servern der Hersteller,[156] bei einem sog. Datentreuhänder[157] oder auch die Kombination der Speicherung im Kraftfahrzeug und einem Datentreuhänder.[158]

Für die Speicherung im Kraftfahrzeug spricht, dass die von der Datenverarbeitung betroffene Person damit die Datenhoheit innehat.[159] Dagegen spricht, dass diese Handhabung möglicherweise Missbrauchspotenziale bezüglich der Löschung oder Verfälschung der Daten durch die Halter*innen birgt und der Herausgabeanspruch von Daten erschwert sein könnte.[160] Andererseits trifft die kraftfahrzeughaltende Person gemäß § 63a Abs. 3 StVG auch die Übermittlungspflicht der Daten, was wiederum für eine Speicherung im Kraftfahrzeug selbst spricht.[161]

Bei einer Speicherung auf Servern der Hersteller wären diese vor Manipulation durch die Halter*innen geschützt, was für eine Speicherung dort spricht. Sollen die Daten allerdings für eine Geltendmachung von Ansprüchen gegen den Hersteller genutzt werden, könnte dieser unter Umständen die Herausgabe erschweren.[162] Die aus datenschutzrechtlicher

[152] *Brockmeyer*, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge?, ZD 2018, 258, (S. 259); *Reibach*, Black Box und Datenschutz beim automatisierten Fahren, DSRITB 2017, 161 (S. 165).

[153] BT-Drs. 18/11300, S. 15.

[154] *Stender-Vorwachs/Steege*, Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 218.

[155] *Wagner/Goeble*, Freie Fahrt für das Auto der Zukunft?, ZD 2017, 263 (S. 267); *Jungbluth*, 56. Deutscher Verkehrsgerichtstag, 2018, S. 41.

[156] *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 209.

[157] *Brockmeyer*, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge?, ZD 2018, 258 (S. 258 ff.).

[158] 56. Deutscher Verkehrsgerichtstag, AK II, Empfehlung Nr. 5.

[159] *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 207.

[160] Ebd.

[161] *Jungbluth*, 56. Deutscher Verkehrsgerichtstag, 2018, S. 41.

[162] *Wagner/Goeble*, Freie Fahrt für das Auto der Zukunft?, ZD 2017, 263 (S. 267).

Sicht erheblichere Gefahr besteht indes darin, dass durch die zu speichernden Daten unter Umständen Bewegungsprofile erstellt werden könnten. Eine weitere technisch zu klärende Frage besteht darin, wie die Daten übertragen werden sollen. Die bestehende Netzabdeckung wird kaum ausreichen, um zu jedem Zeitpunkt und in jeder Situation eine Übermittlung zu gewährleisten. Daraus folgt, dass es doch auch wieder einer zumindest irgendwie gearteter Zwischenspeicherung im Kraftfahrzeug bedarf.

Die Variante der Speicherung bei einem Datentreuhänder wird vornehmlich von Versicherungen als optimale Lösung dargestellt.[163] Hier stellt sich natürlich auch zu aller erst die Frage der technischen Ausgestaltung, auf die § 63a beziehungsweise § 63b aufgrund fehlender Verordnung keine Antwort gibt. Weiterhin ist völlig unklar, wer dieser Datentreuhänder sein soll, also für diese Funktion berechtigt ist. Zur Debatte stehen einerseits große Digitalkonzerne wie Google oder auch Versicherungen. Ob diese allerdings Interesse an einer sparsamen und datenminimierenden Verarbeitung haben, erscheint äußerst fraglich. Dazu müssten auch Sicherheitsanforderungen an Server gesetzlich festgeschrieben werden. Ebenfalls ungeklärt ist, ob ein solcher Treuhänder beispielsweise für die gesamte EU zuständig wäre oder jeder Mitgliedsstaat einen oder sogar mehrere Datentreuhänder haben sollte. Hier stellen sich gewichtige kartellrechtliche Fragen, aber auch datenschutzrechtliche. Die gesamte Strukturierung und Implementierung ist demnach nicht geklärt.[164]

Bezüglich datenschutzrechtlicher Vorgaben ist beispielsweise auf die Datenportabilität gemäß Art. 20 DSGVO zu verweisen, welche bei einem solchen Modell ungeklärt ist. Zudem ist ein solches Modell hinsichtlich des Kopplungsverbots aus Art. 7 Abs. 4 DSGVO problematisch. Beispielsweise könnte ein Versicherungsunternehmen den Abschluss des Versicherungsvertrags davon abhängig machen, dass die Datenspeicherung ausschließlich bei einem bestimmten, möglicherweise eigenen, Treuhänder zu erfolgen hat.[165] Bei dem Modell der Speicherung im Kraftfahrzeug und bei einem Datentreuhänder stellen sich indes die gleichen Fragen wie vorab beschrieben. Hier bestehen viele Unklarheiten, welche auch in den letzten Jahren seit Einführung des § 63a StVG nicht beseitigt wurden.

In § 63a Abs. 2 StVG wird die Datenübermittlung an Behörden, welche nach jeweiliger landesrechtlicher Zuständigkeit Verkehrsverstöße ahnden, geregelt. Diesen Behörden sind auf Verlangen lediglich die Daten zu übermitteln, die für den Zweck nach Absatz 1

[163] *Brockmeyer*, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge?, ZD 2018, 258.

[164] Vgl. dazu ausführlich: ebd.

[165] A.a.O., S. 262.

im Zusammenhang mit den in diesem Zusammenhang geführten Verfahren der eingeleiteten Kontrolle notwendig sind.[166] Unklar ist in diesem Zusammenhang einerseits, wer Adressat der Norm sein soll, ob die Daten tatsächlich übermittelt werden sollen oder lediglich, wie in der Gesetzesbegründung beschrieben, ein „Auslesen der Daten",[167] also eine stationäre Bereithaltung derselben erfolgen soll. Die zuständige Behörde wird ebenfalls nicht konkretisiert. Aufgrund des Wortlauts, dass die nach Landesrecht für die Ahndung von Verkehrsverstößen zuständigen Behörden gemeint sind, wären diese wohl die jeweiligen Landespolizeibehörden, örtlichen Strafverfolgungsbehörden und die gemäß § 44 Abs. 1 S. 1 StVO zuständigen Straßenverkehrsbehörden.[168]

Der Umfang der Daten ist nach § 63a Abs. 2 S. 3 StVG auf das Maß zu beschränken, das für den Zweck der Feststellung des Absatzes 1 im Zusammenhang mit dem durch diese Behörden geführten Verfahren der eingeleiteten Kontrolle notwendig ist. Hier müsste seitens der Kraftfahrzeughersteller sichergestellt werden, dass die Kraftfahrzeughalter*innen und Führer*innen den Umfang der Daten technisch überhaupt darauf reduzieren können, wenn diese zur Übermittlung verpflichtet würden.

Absatz 3 regelt sodann die Übermittlung an Dritte und führt solche Fälle abschließend enumerativ in Nr. 1 und Nr. 2 auf. Gemäß Nr. 1 müssen Kraftfahrzeughalter*innen Daten, die zur Geltendmachung, Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit einem in § 7 Abs. 1 StVG geregelten Ereignis erforderlich sind, übermitteln. Nach Nr. 2 muss eine Übermittlung auch dann stattfinden, wenn das entsprechende Kraftfahrzeug mit automatisierter Fahrfunktion an diesem Ereignis beteiligt war. Normadressaten sind hier eindeutig die Kraftfahrzeughalter*innen. In diesem Fall kann das in der Praxis allerdings dahingehend zu Problemen führen, wenn aufgrund von Leasing oder Vermietung die Halter*innen gar nicht die tatsächliche Sachherrschaft über das Kraftfahrzeug haben.[169] Der Gesetzgeber hätte zur Umgehung dieses Problem einfach auf den Besitzer anstelle des Eigentümers abstellen können.

Die maximale Speicherfrist für die nach § 63a Abs. 1 StVG erhobenen Daten beträgt gemäß Absatz 4 sechs Monate. Danach sind diese zu löschen. Anders, wenn das Kraftfahrzeug an einem in § 7 Abs. 1 StVG geregelten Ereignis beteiligt gewesen ist. Dann sind die erhobenen Daten erst nach drei Jahren zu löschen. Die maximale Speicherfrist ist zugleich

[166] *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 219.

[167] BT-Drs. 18/11300, S. 16 f.

[168] *Schmidt/Wessels*, Event Data Recording für das hoch- und vollautomatisierte Kfz – eine kritische Betrachtung der neuen Regelungen im StVG, NZV 2017, 357 (S. 360).

[169] *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 229.

als Minimalspeicherfrist anzusehen.[170] Diese lange Speicherdauer wird datenschutzrechtlich kritisch gesehen und als nicht notwendig erachtet.[171]

Letztlich regelt § 63a Abs. 5 StVG die anonymisierte Datenübermittlung im Zusammenhang mit der Unfallforschung. Kommt es zu einem Ereignis nach § 7 Abs. 1 StVG können gemäß § 63a Abs. 5 die nach Absatz 1 erhobenen Daten in anonymisierter Form zum Zweck der Unfallforschung an Dritte übermittelt werden. Hierbei handelt es sich um eine freiwillige Datenweitergabe und die Regelung kann nicht als datenschutzrechtlicher Erlaubnistatbestand angesehen werden, da bei anonymisierten Daten der Anwendungsbereich des Datenschutzrechts gar nicht eröffnet ist. Demnach bedarf es weder eines Erlaubnistatbestands zur Datenübermittlung, noch einer Einwilligung. Da kein weitergehender Regelungssinn erkennbar ist, handelt es sich bei Absatz 5 um eine inhaltsleere Norm.[172] Ob die Daten überhaupt tauglich sind, zur Unfallforschung beizutragen, erscheint ebenfalls zweifelhaft. Es werden keinerlei Logfiles, Systemprotokolle, Umgebungsdaten, Sensordaten oder sonstige für Fehlerursachen oder Kausalzusammenhänge relevante Daten erhoben.[173] Hinzu kommt, dass völlig unklar ist, wie die Kraftfahrzeughalter*innen die jeweiligen Daten auslesen und diese anschließend anonymisieren und in anonymisierter Form übertragen sollen. Der praktische und faktische Nutzen dieser Regelung kann stark bezweifelt werden.

Zudem wird die Verfassungsmäßigkeit des § 63a StVG im Hinblick auf datenschutzrechtliche Erwägungen als fraglich erachtet.[174] Die Verfassungsmäßigkeit einer Norm richtet sich danach, ob diese hinreichend bestimmt, konkret und verhältnismäßig ist. Wie oben ausgeführt, ist bereits die technische Ausgestaltung, der Speicherort und dergleichen nicht bestimmt und die Regelung dazu in Absatz 1 unbestimmt. § 63a Abs. 2 StVG ist hinsichtlich des Normadressaten der Herausgabepflicht und bezüglich des zwingend zu übermittelnden Datenumfangs ebenfalls unbestimmt.[175] Unverhältnismäßig ist weiterhin

[170] *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 235.

[171] *Wagner/Goeble*, Freie Fahrt für das Auto der Zukunft?, ZD 2017, 263 (S. 268).

[172] *Schmidt/Wessels*, Event Data Recording für das hoch- und vollautomatisierte Kfz – eine kritische Betrachtung der neuen Regelungen im StVG, NZV 2017, 357 (S. 363).

[173] *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 236.

[174] Vgl. dazu die Ausführungen in: a.a.O., Rn. 240 ff.

[175] *Brockmeyer*, Treuhänder für Mobilitätsdaten – Zukunftsmodell für hoch- und vollautomatisierte Fahrzeuge?, ZD 2018, 258 (S. 261); *Spiegel*, DSRITB 2017, 691, S. 700; *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 242.

eine fehlende, gesetzlich verankerte Erheblichkeitsschwelle für den Zugriff auf relevante Daten.[176] Ebenso ist die in Absatz 4 festgelegte Speicherdauer unverhältnismäßig.

Zwar kann der vom Gesetzgeber verfolgte Zweck der Beweisbarkeit und Sicherung von Pflichten nach § 1b StVG, die Ahndung von Verkehrsverstößen (§ 63a Abs. 2) und die Beweisbarkeit des Kausalverlaufs als legitim erachtet werden. Die Regelung müsste indes auch inhaltlich geeignet sein, diesen verfolgten Zweck zu erreichen. Ob dies hier der Fall ist, kann bezweifelt werden. Nicht geeignet ist die Regelung jedenfalls für eine mögliche Entlastung der kraftfahrzeughaltenden Person. Die zu speichernden Daten enthalten zwar Positions- und Zeitangaben sowie Informationen über den Wechsel zwischen Fahrzeugführer*in und automatisiertem System, die für einen Regressanspruch jedoch wichtigen Daten wie Systemdaten, Daten aus dem Fehlerspeicher, den Steuergeräten oder Sensordaten, allerdings nicht.[177] § 63a Abs. 2 StVG wird zudem als unverhältnismäßig angesehen. Grund ist der schwammige Wortlaut der Norm, welcher auch verdachtsfreie Kontrollen ermöglicht, ohne dass dabei eine Güterabwägung zwischen Sach- und Personenschaden erforderlich wäre. Eine solch undifferenzierte Handhabung genügt nicht, um einen solch intensiven Eingriff in das Recht auf informationelle Selbstbestimmung zu rechtfertigen.[178]

Da es hier, wie beschrieben, keine abschließende Lösung bezüglich der Datenverarbeitung und -speicherung gibt und erhebliche Zweifel an der Verfassungsmäßigkeit des § 63a StVG bestehen, soll dieser hier nicht weiter im Detail erörtert werden. Beachtlich ist, dass entgegen der vorherigen Argumente (zu § 63a StVG) bezüglich internationaler Harmonisierungsbestrebungen und etwaiger Handelshemmnisse bei nationalen „Alleingängen" im Zusammenhang mit der StVG-Novelle 2021 eine entsprechende Verordnung (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung – AFGBV)[179] zur Ausgestaltung technischer Details inklusive der Datenverarbeitung von Kraftfahrzeugen mit autonomer Fahrfunktion erlassen wurde. Daher sind für den hier interessierenden Kontext die Neuregelungen im Straßenverkehrsgesetz einschließlich des § 1g StVG und der AFGBV von gewichtigerem praktischen Interesse als § 63a StVG und der in diesem Zusammenhang seit 2017 nicht weiter verfolgten Verordnungsermächtigung in § 63b StVG. Einzig der sogenannte Fahrmodusspeicher (*Data Storage Systems for Automated Driving*, DSSAD) und Unfalldatenspeicher (*Event Data Recorder*, EDR), welche ihre Grundlage in § 63a StVG haben, werden folglich kurz erläutert. Anschließend sollen § 1g

[176] *Stender-Vorwachs/Steege,* Grundrechtliche Implikationen autonomen Fahrens, in: *Oppermann/Stender-Vorwachs* (Hrsg.), Autonomes Fahren, 2. Auflage, Kapitel 3.6.1. Rn. 242.

[177] A.a.O., Rn. 244.

[178] A.a.O., Rn. 248.

[179] BR-Drs. 86/22 vom 24.02.2022.

StVG, welcher die Datenverarbeitung für Kraftfahrzeuge mit autonomen Fahrfunktionen regelt und die dazugehörigen technischen Konkretisierungen in der AFGBV ausführlich betrachtet werden.

3.2 Fahrmodusspeicher (DSSAD) & Unfalldatenspeicher (EDR)

Fahrmodusspeicher (DSSAD) und Unfalldatenspeicher (EDR) sind in erster Linie Geräte, die für die Speicherung von Daten aufgrund signifikanter sicherheitstechnisch relevanter Vorfälle vorgesehen sind.

Während der EDR zur erleichterten Beweisbarkeit eines tatsächlichen Unfallgeschehens, also zur nachträglichen Plausibilität des Kausalverlaufs und auch für die Unfallforschung und Produktverbesserung vorgesehen ist,[180] soll das DSSAD System vornehmlich die Interaktionen zwischen den Fahrer*innen und dem automatisierten System speichern.[181] Der Fahrmodusspeicher soll dabei festhalten, wer aufgefordert ist das Kraftfahrzeug zu steuern und wer es tatsächlich steuert. Rechtliche Grundlage für den Einbau des DSSAD Gerätes in Kraftfahrzeuge ist § 63a StVG. Insbesondere der Fahrmodusspeicher, welcher den Wechsel beziehungsweise die Aufforderung zur Übernahme der Kraftfahrzeugsteuerung vom automatisierten System aufzeichnen soll, ist bei hoch- und vollautomatisierten Kraftfahrzeugen (bis SAE-Level 3) nötig. Bei autonomen Kraftfahrzeugen, welche ohne fahrzeugführende Person agieren sollen, ist dieser hingegen obsolet. Damit ist § 63a StVG hier als Grundlage für den DSSAD anzusehen und der Anwendungsbereich dieser Geräte ist auf hoch- und vollautomatisierte Kraftfahrzeuge beschränkt.

Sinn und Zweck des DSSAD ist – wie beschrieben – die Beweissicherung zur nachträglichen Feststellung, wer das Kraftfahrzeug gesteuert hat und wer es eventuell hätte steuern müssen.[182] Die im DSSAD gespeicherten Daten sollen über die standardisierte On-Board-Diagnose-Schnittstelle (OBD-Schnittstelle) ausgelesen werden können und angemessen gegen Manipulationen geschützt sein.[183] Da verhältnismäßig wenige Datenpunkte gespeichert werden sollen (GPS-Position und Zeit bei Wechsel des Fahrmodus, Übergabeaufforderung oder technische Störung), ist der Fahrmodusspeicher als eher datensparsam

[180] *Schmid/Wessels*, Event Data Recording für das hoch- und vollautomatisierte Kfz – eine kritische Betrachtung der neuen Regelungen im StVG, NZV 2017, 357 (S. 357).

[181] *Raith*, Das vernetzte Automobil – Im Konflikt zwischen Datenschutz und Beweisführung, DuD-Fachbeiträge, Springer Vieweg, 2019, S. 354 f.

[182] *Wagner*, Das neue Mobilitätsrecht – Der Rechtsrahmen zum automatisierten und vernetzten Fahren, Nomos, 2021, S. 170.

[183] A.a.O., S. 136.

anzusehen.[184] Fahrer*innenprofile oder Streckenprotokolle dürfen nicht erstellt werden. Jedoch gilt auch hier, dass es für die konkrete datenschutzrechtliche Bewertung des DSSAD erforderlich wäre nicht nur zu wissen, was dieser Speicher aufzeichnen soll (§ 63a Abs. 1 StVG), sondern auch wie dies technisch umgesetzt werden soll, wo der DSSAD verbaut sein soll und auf welche Art und Weise die Speicherung erfolgen soll. Auch hier stellt sich das Problem wie sonst im Kontext des §63a StVG, nämlich die fehlende Konkretisierung und technische Ausgestaltung durch eine niemals erlassene Verordnung. Schwierigkeiten im Zusammenhang mit dem Datenschutzrecht und der generellen Verfassungsmäßigkeit des § 63a StVG wurden bereits im vorherigen Abschnitt beschrieben.

Der *Event Data Recorder* soll es ermöglichen, aus einzelnen Steuergeräten, detaillierte Aussagen über deren Funktionsweise zu geben. Der EDR selbst hat keine eigenen Sensoren und befindet sich in der Regel in Airbag-Steuergeräten.[185] Entgegen der Bezeichnung „Event…" soll der EDR nicht bei jeglichem „Ereignis" (Event) die entsprechenden Daten speichern, sondern lediglich im Fall eines Unfalls oder unfallartigem Ereignis.[186] Zur Definition solcher Ereignisse bedarf es der Konkretisierung beziehungsweise Festlegung eines Schwellenwertes unterhalb der Kollision. Generell soll der EDR 30 Sekunden vor und 15 Sekunden nach einem solchen Ereignis die entsprechenden Daten aufzeichnen.[187] Technisch ist ein EDR daher so auszustatten, dass dieser einerseits über einen Ringspeicher verfügt welcher ständig überschrieben wird und daneben über einen Festspeicher für die Aufzeichnung der Daten im Fall eines Unfalls.[188] Die genaue Ausgestaltung sollte indes ebenfalls vom Gesetzgeber festgelegt werden.

Ereignisse, die zur Aufzeichnung führen, sind beispielsweise erhebliche Negativbeschleunigungen, die ein Rückhaltesystems (Airbag oder Gurtstraffer) auslösen, oder auch besondere Fahrmanöver wie ein seitlicher Anstoß an einen Bordstein mit erhöhter Geschwindigkeit (beispielsweise bei einem Fahrzeugdrift). Ein solches Fahrmanöver könnte vom System als mit hoher Wahrscheinlichkeit unfallartiges Ereignis eingestuft werden

[184] *Raith*, Das vernetzte Automobil – Im Konflikt zwischen Datenschutz und Beweisführung, DuD-Fachbeiträge, Springer Vieweg, 2019, S. 355.

[185] *Nugel*, Auslesen von Fahrzeugdaten auf Grundlage der DS-GVO, ZD 2019, 341 (S. 342).

[186] *Raith*, Das vernetzte Automobil – Im Konflikt zwischen Datenschutz und Beweisführung, DuD-Fachbeiträge, Springer Vieweg, 2019, S. 362.

[187] So jedenfalls bereits die Empfehlung des Arbeitskreises V des 41. Deutschen Verkehrsgerichtstages 2003, abrufbar unter https://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/empfehlungen_41_vgt.pdf.

[188] *Fothen/Böhm/Paula*, Kann die Verwendung digitaler Fahrzeugdaten zur Rekonstruktion von Verkehrsunfällen unterhalb der Schwelle schwerster Unfallereignisse verhältnismäßig sein?, NZV 2020, 284 (S. 284).

und die Auslösung der Speicherung begründen.[189] Welche Daten genau gespeichert werden, müsste ebenfalls gesetzlich festgelegt werden. Datenschutzrechtlich relevant ist die Speicherung, wenn die gespeicherten technischen Daten sowohl mit einem Zeitstempel, als auch mit Positionsdaten abgelegt werden.[190] Daraus könnten sich problemlos Bewegungsprofile erstellen lassen und damit ein tiefer Eingriff in das Recht auf informationelle Selbstbestimmung einhergehen.[191] Der Eingriff wird jedoch dahingehend gemindert, dass die Daten fortlaufend überschrieben werden und die Speicherdauer, wie beschrieben, auf einen kurzen Zeitraum begrenzt definiert ist. Es muss also technisch sichergestellt werden, dass ein ständiges Überschreiben erfolgt und die Events, die zum Auslösen der Speicherung führen, so definiert werden, dass diese nur Unfälle und unfallartige Ereignisse umfassen. Damit kann eine etwaige Erstellung von Bewegungsprofilen verhindert werden.

Weitere Regelungen zur Datenspeicherung im Kraftfahrzeug finden sich in den Neuerungen im Straßenverkehrsgesetz. Eine Regelung zur Datenspeicherung für den Wechsel zwischen automatisierter Steuerung und menschlichen Kraftfahrzeugführer*innen ist im neuen § 1g StVG nicht enthalten, weshalb jedenfalls der Fahrmodusspeicher in diesem Zusammenhang nicht von Interesse ist. Die in § 1g StVG eingefügten Neuerungen bezüglich Konfliktsituationen (wie beispielsweise Unfälle) sowie die weiteren datenschutzrelevanten Anforderungen für Kraftfahrzeuge mit autonomen Fahrfunktionen werden nachfolgend im Detail erörtert und bewertet.

3.3 § 1g StVG

Die oben beschriebenen Schwierigkeiten und offenen Fragen, die sich im Zusammenhang mit der Datenverarbeitung im Rahmen von Fahrzeugautomatisierung stellen, kann auch die Neuregelung in § 1g StVG nicht ausreichend beantworten.[192] Das zeigt sich bereits darin, dass das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) deutliche Bedenken im Vorfeld der Neuregelung geäußert hat und es womöglich mit der neuen

[189] *Fothen/Böhm/Paula*, Kann die Verwendung digitaler Fahrzeugdaten zur Rekonstruktion von Verkehrsunfällen unterhalb der Schwelle schwerster Unfallereignisse verhältnismäßig sein?, NZV 2020, 284 (S. 284).

[190] *Raith*, Das vernetzte Automobil – Im Konflikt zwischen Datenschutz und Beweisführung, DuD-Fachbeiträge, Springer Vieweg, 2019, S. 361 f.

[191] A.a.O., S. 362.

[192] Die nachfolgenden Ausführungen finden sich so bereits in: *Arzt/Kleemann/Plappert/Rieke/Zelle*, Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung – Rechtliche und technische Anforderungen im Verbund, MMR 2022, 594 ff.

Regierung Nachbesserungen geben oder die Ausarbeitung eines übergreifenden Mobilitätsdatengesetz erfolgen könnte.[193]

Nach § 1g Abs. 1 S. 1 StVG sind Kraftfahrzeughalter*innen verpflichtet, 13 verschiedene Kategorien von Daten beim Betrieb des Kraftfahrzeugs zu speichern. Fraglich ist indes, wie diese eine solche Speicherung vornehmen sollen, legen doch die Hersteller fest, wie und wo Daten im Kraftfahrzeug automatisch gespeichert werden und welche Schnittstellen es für den Datenaustausch dort geben soll. Zweifelhaft erscheint auch, ob die Norm in der jetzigen Fassung als rechtliche Verpflichtung im Sinne des Art. 6 Abs. 1 lit. c Datenschutzgrundverordnung (DSGVO) genügt.[194] Die rechtliche Verpflichtung aus Art. 6 Abs. 1 lit. c DSGVO ist keine, die vertraglich begründet wird, sondern diese besteht Kraft objektiven Rechts der Europäischen Union oder eines Mitgliedstaats.[195] Grundlegende Voraussetzung der Datenverarbeitung aufgrund einer rechtlichen Verpflichtung ist dabei die klare und präzise Festlegung zumindest des Verarbeitungszwecks.[196]

Ungeklärt ist auch, in welchem Format solche Daten dem Kraftfahrt-Bundesamt (KBA) und der in § 1g StVG genannten Stellen[197] zur Verfügung gestellt werden sollen. Wenn die in § 1g Abs. 1 S. 1 Nr. 1-13 StVG genannten Daten gespeichert und gegebenenfalls übermittelt werden sollen, müssten hier die Kraftfahrzeughersteller selbst adressiert und festgelegt werden, dass diese die genannten Daten in einem für die empfangenden Stellen lesbaren Format zur Verfügung stellen oder dies den Kraftfahrzeughalter*innen oder über das Fahrzeug verfügenden Personen technisch und organisatorisch ermöglichen müssen. Die in § 1g Abs. 1 StVG gelisteten Daten enthalten sowohl solche, bei denen ein Personenbezug angenommen werden kann (z.B. Nr. 1 Fahrzeugidentifikationsnummer und Nr. 2 Positionsdaten), wie auch solche, die rein technische Daten darstellen. Die Norm beschränkt sich demnach nicht auf rein technische Daten, sondern beinhaltet auch die Verarbeitung von personenbezogenen Daten. Inwiefern damit ein Personenbezug und die Anwendbarkeit des Datenschutzrechts gegeben sind, gilt es im Einzelnen festzustellen.

[193] www.handelsblatt.com/politik/deutschland/plaene-des-verkehrsministers-mangelnder-datenschutz-justizministerin-lehnt-scheuers-gesetz-zum-autonomen-fahren-ab/26830532.html; Verbraucherzentrale Bundesverband e. V., Stellungnahme zum Entwurf eines Gesetzes zum Autonomen Fahren sowie der Autonome Fahrzeug-Genehmigungs- und Betriebsverordnung vom 1.2.2021, S. 10 f.

[194] *Steege*, Gesetzentwurf zum autonomen Fahren (Level 4), SVR 2021, 128 (135).

[195] *Frenzel* in: *Paal/Pauly* (Hrsg.), DS-GVO – BDSG 2. Auflage 2018, Art. 6 Rn. 16; *Albers/Veit* in *Wolff/Brink* (Hrsg.) BeckOK, 40. Ed. 1.11.2021, DS-GVO Art. 6 Rn. 48.

[196] *Buchner/Petri* in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, DS-GVO Art. 6 Rn. 82.

[197] Nachfolgend als „zuständige Behörden" im Zusammenhang mit den Neuregelungen im StVG und der AFGBV genannt, siehe auch § 1 Abs. 3 AFGBV.

Die in § 1g Abs. 1 aufgeführten Daten wurden im Gesetzgebungsvorgang teilweise angepasst und konkretisiert. Auffällig ist, dass ein früherer Referentenentwurf noch vorsah, diese Daten nur „beim Betrieb eines Kraftfahrzeugs mit autonomer Fahrfunktion zu speichern", während das Gesetz dies nun für den gesamten „Betrieb des Kraftfahrzeugs" fordert. Unklar bleibt auch, in welchem Verhältnis § 1g Abs. 1 gegenüber den Absätzen 2, 4 und 5 steht. Scheint die Pflicht zur Speicherung der Daten gemäß dem Wortlaut in § 1g Abs. 1 während des gesamten Betriebs zu bestehen, sollen die genannten Daten gemäß § 1g Abs. 2 jedoch lediglich anlassbezogen in den in Absatz 2 Nr. 1-4 genannten Fällen gespeichert werden.

Fraglich ist auch, ob § 1g Abs. 2 StVG eine hinreichend präzise Abgrenzung zu den Regelungen zur Datenspeicherung nach § 63a StVG[198] beinhaltet. Zwar gilt § 63a StVG nur für die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion im Sinne des § 1a, während § 1g StVG die Datenverarbeitung von Kraftfahrzeugen mit autonomen Fahrfunktionen regelt. Die Regelungsorte scheinen indes keiner konsistenten Systematik zu folgen.

Beachtlich ist die im Laufe des Gesetzgebungsprozesses erweiterte Begründung zu § 1g Abs. 3 StVG. Hier wird nunmehr gesetzlich verankert, dass die Kraftfahrzeughersteller technisch und organisatorisch den Kraftfahrzeughalten*innen die „Datenhoheit"[199] über die beim Betrieb der autonomen Fahrfunktion anfallenden Daten ermöglichen müssen.[200] Der Grund dafür – und das ist bedeutsam – ist die Annahme, dass Kraftfahrzeughalter*innen die Berechtigten hinsichtlich der Daten beim autonomen Fahren sind.[201] Hiermit bezieht die Bundesregierung Stellung zu einem in der Literatur höchst umstrittenen Thema.[202] Allerdings sind auch hier, wie bei den meisten Neuregelungen, lediglich die Kraftfahrzeughalter*innen vom Gesetz erfasst. Nicht geregelt wurde, inwiefern beispielsweise die betroffenen Fahrzeugführer*innen oder auch Passagiere und deren personenbezogenen Daten (z.B. zu Ort und Zeit der Kraftfahrzeugnutzung) vom Gesetz abgedeckt

[198] Zur Kritik siehe nur: *Hoeren,* Ein Treuhandmodell für Autodaten? – § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion, NZV 2018, 153; *Lutz,* Fahrzeugdaten und staatlicher Datenzugriff, DAR 2019, 125; *Schirmer*, Augen auf beim automatisierten Fahren! Die StVG-Novelle ist ein Montagsstück, NZV 2017, 253; *Steege*, Autonomes Fahren und die staatliche Durchsetzung des Verbots der Rechtswidrigkeit, NZV 2019, 459; *Steinrötter*, Datenschutz als Gretchenfrage für autonome Mobilität, ZD 2021, 513, 513 ff.

[199] Vgl. zur Diskussion die Ausführungen unter 1.3.

[200] BR-Drs. 155/21 (S. 38).

[201] BR-Drs. 155/21 (S. 38).

[202] Vgl. dazu beispielsweise die Positionen in: *Weichert*, Datenschutz im Auto – Teil 1, SVR 2014, 201; *Weichert*, Datenschutz im Auto – Teil 2, SVR 2014, 241; *Stender-Vorwachs/Steege*, Wem gehören unsere Daten?, NJOZ 2018, 1361; *Hoeren*, Ein Treuhandmodell für Autodaten? – § 63 a StVG und die Datenverarbeitung bei Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion, NZV 2018, 153; *Kühling/Sackmann*, Irrweg „Dateneigentum", ZD 2020, 24; *Steege*, Gesetzentwurf zum autonomen Fahren (Level 4), SVR 2021, 1.

werden und welche Regelungen hinsichtlich ihrer personenbezogenen Daten gelten sollen. Hinzu kommen Daten aus der sensorischen Umfelderfassung. Auch hier sprechen gute Gründe dafür, diese offenen Punkte in einem verkehrsmittelübergreifenden Mobilitätsdatengesetz zu regeln.[203] In einem solchen Gesetz könnte eine Klassifikation von Daten und der Verteilung der Rollen von Betroffenen und Verantwortlichen geregelt werden, ebenso wie Anonymisierungspflichten oder die konkrete Ausgestaltung von *data protection by design* und *data protection by default* (Art. 25 DSGVO, Erwägungsgrund 78). Die Umsetzung einer solchen Regelung sollte indes auf EU-Ebene geschehen, um nicht in Widerspruch mit der DSGVO zu geraten.[204]

Darüber hinaus werden die Hersteller in § 1g Abs. 3 verpflichtet, den Kraftfahrzeughalter*innen bestimmte Einstellungsmöglichkeiten zur Privatsphäre zu eröffnen und über die Datenverarbeitung in der autonomen Fahrfunktion zu informieren. Fraglich ist, ob § 1g Abs. 3 die Diskussion bezüglich *data protection by design* und *data protection by default* ausreichend abbildet. Dass die Regierung in der Begründung von „*privacy by design*" spricht (ein Terminus, welcher sich weder in der deutschen, noch in der englischen Version der DSGVO findet) unterstreicht, dass hier offenbar noch kein abschließend durchdachtes Konzept zur Anwendung kommt. Nach Art. 25 Abs. 2 DSGVO muss der für die Datenverarbeitung Verantwortliche, welcher nach § 1g Abs. 3 S. 1 zumindest hinsichtlich der Schaffung der Voraussetzungen der Hersteller wäre, geeignete technische und organisatorische Maßnahmen treffen, die sicherstellen, dass durch Voreinstellung ausschließlich personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere im Zusammenhang mit der Verarbeitung durch Dritte (beispielsweise Verkehrsplattformen, Road-Side-Units oder generell V2X-Kommunikation) sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der betroffenen Person einem unbestimmten Kreis von Personen zugänglich gemacht werden. Dass § 1g Abs. 3 dies hinreichend umsetzt, muss bezweifelt werden.

Nach § 1g Abs. 6 StVG dürfen Behörden, die für die Genehmigung, Prüfung und Überwachung des Betriebsbereichs zuständig sind, Daten nach Absatz 1 und die Namen sowie Qualifikation der Technischen Aufsicht erheben, speichern und verwenden. Diese Daten sind gemäß § 1g Abs. 6 S. 2 StVG, sobald sie für die Zwecke nach Satz 1 nicht mehr erfor-

[203] Vgl. Ausführungen in: vzbv – Verbraucherzentrale Bundesverband, Positionspapier Fahrerlos alle Mitnehmen – Automatisierte und vernetzte Mobilität aus Verbrauchersicht, Positionspapier vom 6.3.2021, S. 8 ff.

[204] *Wagner*, Gesetz zum autonomen Fahren – Streitpunkte im Gesetzgebungsverfahren, SVR 2021, 287 (S. 291).

derlich sind, unverzüglich zu löschen, spätestens aber drei Jahre nach Einstellung des Betriebs des entsprechenden Kraftfahrzeugs. Damit ist nur hinsichtlich nicht mehr in Betrieb befindlicher Kraftfahrzeuge eine konkrete Speicherdauer angegeben, wohingegen die Zulässigkeit sonst am eher vagen Maßstab der Erforderlichkeit zu messen ist. Die genannte Speicherdauer und unverzügliche Löschung nach Wegfall der Erforderlichkeit gilt auch für Daten, die nach § 1g Abs. 4 beim KBA gespeichert werden. Hinsichtlich der unverzüglichen Löschung nach Wegfall der Erforderlichkeit für Daten nach § 1g Abs. 4 und 6 ist daher unklar, was die erforderliche „Überwachung des sicheren Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion" konkret umfasst und wann und unter welchen Voraussetzungen diese entfällt. Hier ist eine Konkretisierung nötig, um auch die Löschfrist in datenschutzkonformer Art und Weise umzusetzen.

Problematisch ist zudem, dass die gesamte Neuregelung in § 1g StVG ausschließlich die Datenverarbeitung im Kraftfahrzeug selbst und deren Übermittlung an das KBA und zuständige Behörden regelt (§ 1g Abs. 1 S. 2), soweit dies für deren Aufgabenerfüllung (Überwachung des sicheren Betriebs und Betriebsbereichs, § 1g Abs. 4 und 6) erforderlich ist. Was hingegen nicht geregelt scheint, ist die Datenverarbeitung für und aus der Vernetzung von Kraftfahrzeugen untereinander (Vehicle-to-Vehicle, V2V) wie auch solchen aus der Kommunikation mit der Infrastruktur oder anderen Entitäten (Vehicle-to-Everything, V2X). Auch Daten aus Kraftfahrzeugen, die bei den Herstellern selbst verarbeitet werden und zur Steuerung des Kraftfahrzeugs notwendig sind, werden von den Regelungen zur Datenverarbeitung nicht erfasst. Ferner finden sich keinerlei Regelungen bezüglich unterschiedlicher Kommunikationsstandards (WLAN oder Mobilfunk), was im Sinne der Technologieneutralität zu erklären wäre. Diese Art der (externen) Datenverarbeitung ist lediglich in der Verordnung (AFGBV) spezifiziert (dazu unter 3.1 im Detail). Hier hätten einerseits bereits Anknüpfungspunkte im StVG geschaffen werden können.

Andererseits verfolgt der Gesetzgeber mit der gesamten Ausgestaltung der Neuregelungen im Gesetz einen dynamischen Ansatz. Grundsätzliche Anforderungen und Definitionen werden im Gesetz normiert, wohingegen die konkreten technischen Spezifika sodann in einer Rechtsverordnung geregelt werden.[205] Damit soll frühzeitig und flexibel auf künftige technische Weiterentwicklungen reagiert werden können, indem nicht ggf. das Gesetz geändert, sondern lediglich die Verordnung an technische Neuerungen angepasst werden muss.[206] Eine ähnliche Handhabung ist auch auf EU-Ebene zu erkennen. Bei der

[205] *Wolfers/Schlenkhoff*, Autonomes Fahren ist möglich: Deutschland als regulatorischer Tempomacher, RAW 1/2022, 24 (S. 29).

[206] Ebd.

Ausgestaltung der am 6. Juli 2022 in Kraft tretenden Verordnung EU 2019/2144,[207] welche erstmalig auch unionsrechtliche Definitionen der Begriffe „automatisiertes“[208] und „vollautomatisiertes Fahrzeug“[209] enthält, werden grundsätzliche Definitionen und technische Vorgaben innerhalb der Verordnung geregelt und für die technischen Detailfragen ist eine noch zu erarbeitenden Durchführungsverordnung mit umfangreichen und detaillierten Anhängen vorgesehen.[210]

[207] Verordnung (EU) 2019/2144 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Typgenehmigung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge im Hinblick auf ihre allgemeine Sicherheit und den Schutz der Fahrzeuginsassen und von ungeschützten Verkehrsteilnehmern, zur Änderung der Verordnung (EU) 2018/858 [...].

[208] Art. 3 Abs. 2 Nr. 21 Verordnung (EU) 2019/2144.

[209] Art. 3 Abs. 2 Nr. 22 Verordnung (EU) 2019/2144.

[210] *Wolfers/Schlenkhoff*, Autonomes Fahren ist möglich: Deutschland als regulatorischer Tempomacher, RAW 1/2022 (S. 31).

4. IT-Sicherheit, Produktsicherheit und Produkthaftungsrecht

IT-Sicherheit, Produktsicherheit und auch haftungsrechtliche Fragen spielen im Zusammenhang mit vernetzten und automatisierten Kraftfahrzeugen eine zunehmend wichtige Rolle. Dies spiegelt sich maßgeblich in der Entwicklung des IT-Sicherheitsrechts wieder, wobei besonderer Wert auf die Funktionsfähigkeit, Verfügbarkeit und Integrität dieser Systeme gelegt werden muss. Die hieran anknüpfenden Fragen finden sich in den jüngst verabschiedeten nationalen wie internationalen Regelungen zur Fahrzeugautomatisierung wieder. Die DSGVO, das IT-Sicherheitsgesetz, aber auch die speziellen Regelungen wie das Gesetz zum autonomen Fahren, die dazugehörige Verordnung (AFGBV), Regelungen auf UNECE-Ebene, aber auch das novellierte Produkthaftungsrecht oder branchenspezifische IT-Sicherheitsstandards adressieren die Thematik der Rechts- und Betriebssicherheit solcher Systeme.

Im Folgenden werden daher die für den hier interessierenden Kontext einschlägigen Themenkomplexe aus dem Bereich der IT-Sicherheit, Produktsicherheit und -haftung dargestellt und insbesondere die Anknüpfungspunkte, welche sich aus der neuen Rechtslage im Zusammenhang mit dem StVG sowie den UNECE-Regelungen ergeben im Detail analysiert.

4.1 IT-Sicherheit

Wie bereits unter Kapitel 2 beschrieben, sind Datensicherheit und IT-Sicherheit nicht per se gleichzusetzen. IT-Sicherheit im Rahmen des IT-Sicherheitsgesetz soll die Sicherheit informationstechnischer Systeme verbessern, wobei insbesondere die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität dieser Systeme geschützt werden soll.[211] Das IT-SicherheitsG, welches als Artikelgesetz Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), des Atomgesetzes (AtG), des Energiewirtschaftsgesetzes (EnWG), Telemedien- und Telekommunikationsgesetzes (TMG, TKG) und des Bundeskriminalamtsgesetzes (BKAG) enthielt, betrifft insbesondere die sogenannten kritischen Infrastrukturen.[212]

[211] *Conrad*, in: *Auer-Reinsdorff/Conrad* (Hrsg.) Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Rn. 9.

[212] *Conrad/Eckhardt*, in: *Auer-Reinsdorff/Conrad* (Hrsg.) Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Rn. 248 ff.

Entscheidend ist hierbei, wer als Betreiber kritischer Infrastrukturen anzusehen ist und inwiefern die Automobilindustrie davon betroffen sein könnte.[213] Nach aktuellem Stand sind die Regelungen des BSIG nicht ohne weiteres auf das automatisierte Fahren anwendbar, wobei andere Akteure aus dem Sektor Informationstechnik und Telekommunikation, welche für das automatisierte Fahren signifikant sind, durchaus davon umfasst sind (BSI-KritisV § 5).[214] Es ist anzunehmen, dass bei der künftigen Entwicklung auch eine geeignete IT-Infrastruktur im Bereich automatisierter Kraftfahrzeuge benötigt wird und diese sodann unter die erhöhten Anforderungen des IT-SicherheitsG fallen kann.[215] Ähnlich hat sich auch die Bundesregierung auf die Frage geäußert, inwieweit „es sich beim automatisierten und autonomen Fahren um einen Bestandteil einer kritischen Infrastruktur, die dann durch das IT-Sicherheitsgesetz adressiert würde", handelt.[216] Die Bundesregierung ist dabei der Ansicht, dass die für automatisiertes und vernetztes Fahren „relevante IT-Infrastruktur […] eine kritische Infrastruktur im Sinne des IT-Sicherheitsgesetzes [ist], wenn sie unter Anhang 7, Ziffer 1, Buchstaben d oder e der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) fällt und die jeweiligen Schwellenwerte erreicht. Denkbar ist, dass Anbieter von Systemen für automatisiertes und autonomes Fahren auf Dienstleistungen kritischer Infrastrukturen zurückgreifen, z.B. im Sektor Informationstechnik und Telekommunikation."[217] Hier kommt es also maßgeblich auf die künftige Ausgestaltung der IT-Infrastruktur und den Rückgriff auf diese seitens der Kraftfahrzeughersteller an.

Werden unter IT-Sicherheit auch die in den Datenschutzgesetzen vorgegebenen Schutzziele bezüglich Datensicherheit verstanden, fallen weitere Aspekte darunter. Insbesondere der bereits erwähnte Art. 32 DSGVO ist hier einschlägig, da dort geregelt wird, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen muss, um dem Risiko, welches durch die Verarbeitung einhergeht, ein entsprechend angemessenes Schutzniveau gegenüberzustellen. Dieser risikobasierte Ansatz der DSGVO steht in einem engen Zusammenhang zur IT-Sicherheit.[218]

[213] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 154 f.

[214] Vereinigung der Bayerischen Wirtschaft e. V., Positionspapier: Zukunft automatisiertes Fahren – Datenschutz und Datensicherheit, S. 29.

[215] Ebd.

[216] BT-Drs. 19/16420, S. 7 Nr. 62.

[217] BT-Drs. 19/17204 S. 15.

[218] *Conrad*, in: *Auer-Reinsdorff/Conrad* (Hrsg.) Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Rn. 180.

Darüber hinaus finden sich in der DSGVO verschiedene Gewährleistungsziele wieder, welche sich auf die Schutzziele der Informationssicherheit beziehen.[219] Informationssicherheit umfasst dabei sowohl technische wie auch nicht-technische Systeme und orientiert sich in der Praxis im Rahmen des IT-Sicherheitsmanagements an ISO/IEC Normen und dem IT-Grundschutz, wodurch die Überschneidung bezüglich der Gewährleistungsziele der DSGVO und der Schutzziele der Informationssicherheit kenntlich wird. Zu diesen Zielen zählen die Datenminimierung, Verfügbarkeit, Integrität Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit.[220] Zu finden sind diese in zentralen Normen der DSGVO, wie Art. 5, welcher beispielsweise die Transparenz für Betroffene von Verarbeitungen personenbezogener Daten (Art. 5 Abs. 1 lit. a DSGVO), Zweckbindung einer Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. b DSGVO), Datenminimierung einer Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. c DSGVO), Richtigkeit personenbezogener Daten (Art. 5 Abs. 1 lit. d DSGVO), Speicherbegrenzung personenbezogener Daten (Art. 5 Abs. 1 lit. e DSGVO), Integrität personenbezogener Daten (Art. 5 Abs. 1 lit. f DSGVO, Art. 32 Abs. 1 lit. b DSGVO), und die Vertraulichkeit personenbezogener Daten (Art. 5 Abs. 1 lit. f DSGVO, Art. 32 Abs. 1 lit. b DSGVO), regelt. Weiterhin bestimmen die bereits erwähnten Artikel 25 und 32 DSGVO zentrale Aspekte mit Bezug zur Datensicherheit. Dazu zählen Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DSGVO), Verfügbarkeit der Systeme, Dienste und Daten (Art. 32 Abs. 1 lit. b und lit. c DSGVO), Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO), Wiederherstellbarkeit der Daten und des Datenzugriffs (Art. 32 Abs. 1 lit. c DSGVO) und die Evaluierbarkeit (Art. 32 Abs. 1 lit. d DSGVO).[221]

Bezüglich der hier beschriebenen Anforderungen, gab es durch die jüngst eingeführten Normen und Vorgaben im StVG (§ 1g und AFGBV) und auf UNECE-Ebene (Regelung 155 und 156) Entwicklungen im Bereich IT-Sicherheit, respektive speziell zu Cybersicherheit. Diese werden nachfolgend detailliert analysiert und eingeordnet.

4.1.1 Neuregelungen im StVG

Im Straßenverkehrsgesetz sind mit der letzten Novelle 2021 auch Neuerungen bezüglich der IT-Sicherheit mitaufgenommen worden. Insbesondere die Autonome-Fahrzeuge-

[219] Standard-Datenschutzmodell, Version 2.0b, S. 9 ff., abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf.

[220] A.a.O., S. 10.

[221] A.a.O., S. 12 ff.

Genehmigungs-und-Betriebs-Verordnung (AFGBV) enthält hier Anknüpfungspunkte.[222] Cybersicherheit und Software-Updates spielen im Automobilbereich eine immer wichtigere Rolle. Speziell mit Blick auf die zunehmende Vernetzung von Kraftfahrzeugen untereinander wie auch mit der Infrastruktur und anderen Entitäten, steigt die Gefahr von potenziellen Cyberbedrohungen und -angriffen. Relevant ist daher vornehmlich die im Zusammenhang mit der aktuellen StVG-Novelle vorgelegte AFGBV, welche konkret Cybersicherheitsmaßnahmen für Kraftfahrzeuge adressiert und dabei auf die UNECE-Regelung 155 (Uniform provisions concerning the approval of vehicles with regard to cyber security and of cybersecurity management systems)[223] verweist. Zu beachten ist zudem die UNECE-Regelung 156 (Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system),[224] die Vorgaben für Software-Updates enthält. Mit steigender Fahrzeugautomatisierung werden die Nutzung von Software und relevante Security-Updates, welche auch sogenannte „Software-over-the-air-Updates" beinhalten können, für die Kraftfahrzeugsteuerung immer relevanter. Daher ist es notwendig, diese auch gegen potenziell sicherheitsrelevante Cyberangriffe über eine Schnittstelle für over-the-air-Updates abzusichern.

4.1.2 Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV)

Ergänzung sollen die neuen Normen des StVG in der AFGBV finden. Hiermit sollen die in §§ 1d bis 1l StVG neu geregelten Anforderungen konkretisiert und die für die Genehmigung autonomer Fahrfunktionen zu erfüllenden Vorgaben bestimmt werden. Regelungen zur Datenverarbeitung sind in § 15 AFGBV vorgesehen, wonach nähere Anforderungen zu den genauen Zeitpunkten der Datenspeicherung, den Parametern der Datenkategorien und den Datenformaten in Anlage 2 der AFGBV geregelt werden sollen. Dort werden die in § 1g Abs. 1 Nr. 1-13 StVG genannten Daten teilweise hinsichtlich des Zeitpunkts der Datenspeicherung, Parametern der Datenkategorien und Datenformaten spezifiziert. Dabei werden in der Anlage lediglich beispielhaft Datenformate genannt. Welche Daten im konkreten Einzelfall bei welchem Kraftfahrzeug von spezifischen Herstellern anfallen und in welchem Datenformat, kann daher nicht aus der Norm selbst abgeleitet werden, sondern bedarf einer Einzelfallbetrachtung.

[222] Die nachfolgenden Ausführungen finden sich so bereits in: *Arzt/Kleemann/Plappert/Rieke/Zelle*, Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung – Rechtliche und technische Anforderungen im Verbund, MMR 2022, 596 ff.

[223] ECE/TRANS/WP.29/2020/79 REVISED abrufbar unter: http://www.unece.org/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

[224] ECE/TRANS/WP.29/2020/80, abrufbar unter https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29/ECE-TRANS-WP29-2020-080e.pdf.

Unstreitig ist dabei, dass es sich bei einer Datenverarbeitung in Verbindung mit der Fahrzeugidentifikationsnummer (FIN) und bei Positionsdaten um personenbezogene Daten im Sinne von Art. 4 Nr. 1 DSGVO handelt. Während ein früherer Entwurf der AFGBV[225] noch Beispiele enthielt, welche Daten etwa als Vernetzungsparameter nach § 1g Abs. 1 Nr. 7 StVG angesehen werden können (IMSI, IMEI oder einer Rufnummer[226]), fehlt hierzu in der verabschiedeten Version jegliche Konkretisierung. In Bezug auf die weiteren genannten Daten stellt sich in allen Fällen die Frage, inwiefern es technisch möglich oder auch sinnvoll ist, einzelne Daten, welche in den Steuergeräten der Kraftfahrzeuge generiert werden, von der FIN zu trennen und wie in der Praxis tatsächlich dabei verfahren wird. Sollen Daten prinzipiell von der FIN getrennt werden, müsste sichergestellt werden, dass diese auch weiterhin für den eigentlichen Zweck (etwa der sicheren Erfüllung der Fahraufgabe oder der Datenspeicherung bei Konfliktszenarien) brauchbar sind. Problematisch wäre indes, wenn dies dazu führte, dass eine Identifikation später dennoch durch die Zusammenführung mit weiteren Daten möglich ist. Demzufolge stellen sich hier Fragen bezüglich der Zweckbindung gemäß Art. 5 Abs. 1 lit. b DSGVO, aber hinsichtlich der wirksamen und sinnvollen Pseudonymisierung (Art. 4 Nr. 5 DSGVO) oder Anonymisierung. Bei einer Anonymisierung ist die DSGVO nicht anwendbar (vgl. auch Erwägungsgrund 26 DSGVO). Scheidet eine Trennung aus Gründen der zweckgemäßen Nutzbarkeit aus, können alle damit verbundenen Daten personenbezogene Daten darstellen. Hier gilt es, die Vorgaben der DSGVO wie auch aus dem Recht auf informationelle Selbstbestimmung im Einzelfall einzuhalten.

Zu beachten sind darüber hinaus auch die Anforderungen an Kraftfahrzeuge mit autonomer Fahrfunktion, die in der Anlage 1 zur Verordnung beschrieben sind. Hier soll lediglich auf zwei Bereiche Bezug genommen werden: den digitalen Datenspeicher gemäß Anlage 1 Teil 3 und die dort in Teil 5 beschriebenen Anforderungen an die Sicherheit im Bereich der Informationstechnologie.

4.1.2.1 Digitaler Datenspeicher

Im digitalen Datenspeicher von Kraftfahrzeugen mit autonomen Fahrfunktionen sollen (sobald dafür entsprechende datenschutzrechtliche Regelungen in Kraft getreten sind)

[225] Entwurf einer Verordnung zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen (Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung - AFGBV), Referentenentwurf des Bundesministeriums für Verkehr und digitale Infrastruktur, Bearbeitungsstand 27.01.2021, Anlage III.

[226] IMSI, IMEI oder Rufnummer stellen regelmäßig personenbezogene Daten dar, vgl. dazu: Beschluss des Düsseldorfer Kreises vom 16.06.2014, Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter, S. 5, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/Archiv/DuesseldorferKreis/OHApps.pdf;jsessionid=31DF534E3CE16B7ABA6D9BE81835E33C.intranet222?__blob=publicationFile&v=2; *Graulich* in: *Schenke/Graulich/Ruthig* (Hrsg.), Sicherheitsrecht des Bundes, § 18 BKAG Rn. 23.

die Daten ereignisbasiert ausschließlich für die in § 1g StVG genannten Zwecke gespeichert werden. Dazu zählen die Durchführung von Verkehrssicherheitsanalysen und die Bewertung der Wirksamkeit spezifischer Maßnahmen wie etwa das Verhalten des Kraftfahrzeugs in Konfliktszenarien, die für die Zuordnung von Haftung und rechtlicher Verantwortung und für Forschung zum Zweck der Verbesserung der Verkehrssicherheit und der Gewährleistung datenschutzrechtlicher Vorgaben gespeichert werden.[227] Diese Daten sollen gemäß § 15 Abs. 2 AFGBV nur für das KBA und die in § 1g StVG genannten zuständigen Behörden zum Zwecke einer Nachprüfung der Erfüllung der Voraussetzungen der Genehmigung und der mit der Genehmigung verbundenen Überwachungspflichten zur Verfügung stehen. Konkret heißt es dazu in Anlage 1 Teil 3 der AFGBV, dass der integrierte Datenspeicher den Vorgaben der Art. 24, 25 und 32 DSGVO entsprechen muss und „ereignisbasiert und während des Betriebes nach § 9 Absatz 5 und § 15 Daten des Kraftfahrzeugs mit autonomer Fahrfunktion ausschließlich zu dem Zweck der Verbesserung der Verkehrssicherheit erfasst, speichert und verwendet". Dabei sind „die zu erfassenden Daten […] in § 1g Absatz 1 des Straßenverkehrsgesetzes in Verbindung mit Anlage 2 zu dieser Verordnung abschließend geregelt."[228]

Diese ausschließliche Beschränkung der Nutzung und abschließende Aufzählung der zu verarbeitenden Daten ist auf den ersten Blick aus datenschutzrechtlicher Perspektive zu begrüßen. Allerdings fällt auf, dass bei den genannten Verkehrssicherheitsanalysen unklar ist, ob und ggf. welche weiteren Daten verarbeitet werden, die über die § 1g Abs. 1 StVG genannten hinausgehen. Darüber hinaus werden bereits in § 1g Abs. 2 Nr. 1-4 StVG nicht nur das Unfallszenario genannt, sondern explizit auch weitere Anlässe zur Datenspeicherung. Weiter berechtigt § 1g Abs. 4 StVG das KBA alle in Absatz 1 genannten Daten und gemäß Nr. 2 Vor- und Nachname der als Technische Aufsicht eingesetzten Person sowie Nachweise über ihre fachliche Qualifikation zu „speichern und zu verwenden, soweit dies für die Überwachung des sicheren Betriebs des Kraftfahrzeugs mit autonomer Fahrfunktion erforderlich ist".

Unklar bleibt indes der Maßstab der Erforderlichkeit.[229] In § 1g Abs. 5 StVG wird als Zweck der Datenverarbeitung die Forschung genannt. Hier ist jedoch zu beachten, dass § 1g Abs. 5 S. 1 Hs. 3 StVG die Datenverarbeitung für Forschungszwecke auf nicht personenbezogene Daten beschränkt. § 1g Abs. 6 StVG erlaubt den für die Überprüfung des Betriebsbereichs zuständigen Behörden die Daten gemäß Absatz 6 Nr. 1 und 2 zu erheben, speichern und zu verwenden, sofern es für die Überprüfung und Überwachung des

[227] Vgl. Ausführungen in AFGBV Anlage 1 Teil 3, und § 1g StVG.

[228] AFGBV Anlage 1 Teil 3.

[229] *Haupt*, Auf dem Weg zum autonomen Fahren, NZV 2021, 172, (S. 175).

Betriebsbereichs notwendig ist. Letztlich können auch Dritte die Herausgabe von Daten für die Geltendmachung von Haftungsansprüchen gemäß § 1g Abs. 7 StVG verlangen. Die in der AFGBV beschriebene ausschließliche Beschränkung der Nutzung der Daten zum Zweck der Erhöhung der Verkehrssicherheit stimmt demzufolge nicht überein mit den anderen in § 1g StVG genannten Zwecken der Datenverarbeitung.

Das Datenschutzniveau des Datenspeichers soll von den Herstellern entsprechend dem Stand der Technik bezüglich Datenschutz- und Sicherheitsvorgaben sichergestellt werden. Es muss ein System zur Zugangskontrolle sowie kryptographische Schutzverfahren entsprechend den technischen Richtlinien des Bundesamtes für die Sicherheit in der Informationstechnik (BSI-TR) geben, wobei das BSI bereits in die Ausgestaltung einzubeziehen ist. Der Datenspeicher darf nicht flüchtig sein und die Daten müssen auch im stromlosen Zustand erhalten bleiben. Laut AFGBV soll der Datenspeicher ab Beginn der Kraftfahrzeugzulassung die Daten ausschließlich im Kraftfahrzeug speichern.[230]

Der Zugang zu den gespeicherten Daten soll über die normierte 16-polige On-Board-Diagnose-Schnittstelle (OBD-Schnittstelle) über ein Kommunikationsmodul nach ISO 22900-1:2008-03 (Straßenfahrzeuge - Modulare Kommunikationsschnittstelle im Kraftfahrzeug (MVCI) - Teil 1: Hardwaredesign Anforderungen) unter Verwendung der proprietären Software des Herstellers oder über die proprietäre Schnittstelle erfolgen. In bestimmten Situationen oder Ereignissen sollen die Daten auch über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung) an die zuständige Stelle übermittelt werden können.[231] Hier stellt sich die Frage, wie realisiert werden soll, dass alle notwendigen Daten an das KBA über die OBD-Schnittstelle übertragen und abgesichert werden können, wenn nur in nicht näher definierten Ausnahmefällen oder nach ebenfalls nicht näher bestimmten Ereignissen diese über eine WAN-Verbindung an die zuständige staatliche Stelle gesendet werden.[232] Während in der Entwurfsfassung der AFGBV, welche der Europäischen Kommission zur Notifizierung vorlag,[233] noch ein etwaiger Hinweis auf eine solche Situation in der damaligen Anlage I Teil 5 Nr. 14 zu finden war, in der es hieß: „[e]rkennt der Hersteller Manipulationen am Kraftfahrzeug mit autonomer Fahrfunktion, so sind diese unverzüglich dem Kraftfahrt-Bundesamt und der […] zuständigen Behörde […] mitzuteilen und entsprechende Maßnahmen einzuleiten“, findet sich dieser in der verabschiedeten Fassung nicht mehr. Ob dieser (versteckte) Hinweis eine solche

[230] Vgl. dazu AFGBV Anlage 1 Teil 3 Nr. 13.2, und Anlage 2.

[231] Vgl. Ausführungen in AFGBV Anlage 1 Teil 3 Nr. 13.2.

[232] Vgl. Ausführungen in ebd.

[233] Entwurf einer Verordnung zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, Notifizierungsnummer: 2021/344/D, Bearbeitungsstand 10.6.2021, https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2021&num=344.

Situation gemeint haben könnte oder ob die in § 1g Abs. 2 StVG genannten Anlässe die „bestimmten Ereignisse" darstellen, die eine Übertragung[234] per WAN-Verbindung ermöglichen, bleibt indes völlig unklar. Hier bedarf es einer weiteren Konkretisierung durch den Verordnungsgeber. Darüber hinaus ist auch unklar, ob Kraftfahrzeughalter*innen über die Datenübertragung per WAN benachrichtigt werden müssen und wie die Nachvollziehbarkeit des Inhalts der Datenübertragung gewährleistet ist.

Zugang und Abruf der gespeicherten Daten soll nur für das KBA und die zuständige Stelle möglich sein.[235] Gleiches gilt für die Datenspeicherung und Datenübermittlung.[236] Die Datenübertragung und Speicherung soll laut AFGBV den Anforderungen an die Sicherheit der Informationstechnologie, wie in Teil 5 der Anlage 1 zur AFGBV beschrieben, genügen. Insbesondere sollen die Daten gemäß dem Stand der Technik und unter Beachtung der Vorgaben aus Art. 24, 25 und 32 DSGVO vor missbräuchlicher Verwendung und Manipulation geschützt werden.

Die notwendige Schnittstelle birgt die Gefahr, dass Daten während der Übermittlung an die zum Empfang berechtigten Stellen abgefangen werden. Die nach § 1g StVG zu speichernden Daten können durchaus personenbezogene sein. Hier könnte im Zusammenhang mit der in der AFGBV getroffenen Regelung zur Übermittlung von Daten über eine Weitverkehrsnetz-Anbindung (WAN-Verbindung), eine potenzielle datenschutzrechtliche Schwachstelle geschaffen worden sein.

Die vorab beschriebenen Regelungen beziehen sich vorrangig auf die Datenverarbeitung im Kraftfahrzeug, auf den Zugriff auf diese Daten sowie teilweise die Übertragung an das Kraftfahrzeug. Für die Übertragung muss laut AFGBV eine sichere elektronische Steuereinheit (SECU) als Informationsgateway genutzt werden, welche den Schutz von Daten, die extern an das Kraftfahrzeug gesendet[237] werden, sicherstellen soll.[238] Für die Frage, ob es auch einer vertraulichen Datenübertragung aus dem Kraftfahrzeug bedarf, findet sich lediglich ein Hinweis in Anlage 1 Teil 1 Nr. 6 und insbesondere in Teil 3 Nr. 13.2 lit. d der AFGBV, wonach die Datenspeicherung und die Datenübermittlung an das KBA und die in der AFGBV genannten zuständigen Behörden, den Anforderungen an die Sicherheit

[234] Handelt es sich bei dem in der AFGBV genutzten Begriff „Übertragung" oder „Datenübertragung" um personenbezogene Daten, ist damit im hier behandelten Kontext eine Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO gemeint. Eine Übertragung kann in beide Richtungen erfolgen. Sowohl das Empfangen, als auch das Senden von personenbezogenen Daten an und in das Kraftfahrzeug sind davon umfasst.

[235] AFGBV Anlage 1 Teil 3 Nr. 13.2 lit. b.

[236] AFGBV Anlage 1 Teil 3 Nr. 13.2 lit. d.

[237] Das Senden von Kraftfahrzeugdaten mit Personenbezug stellt eine Datenübertragung i.S.d. Art 4 Nr. 2 DSGVO dar, wobei die Verantwortlichkeit im hier vorliegenden Kontext gemäß Art. 4 Nr. 7 DSGVO i.d.R. beim Hersteller liegen wird.

[238] AFGBV Anlage 1 Teil 1 Nr. 6.

im Bereich der Informationstechnologie genügen sollen. Die Daten müssen dem Stand der Technik gemäß und unter Beachtung der Vorgaben der Artikel 24, 25 und 32 der DSGVO vor Manipulation und missbräuchlicher Verwendung geschützt werden. Hier bedarf es der Klärung, wie die durch die AFGBV geforderte Schnittstelle und der Zugang zu dieser autorisiert werden und die Authentizität des Auslesenden[239] geprüft werden kann.

Offen ist demnach, wie eine Ende-zu-Ende-Vertraulichkeit auf beiden Seiten tatsächlich sichergestellt werden kann. Weiterhin scheint noch nicht abschließend geklärt zu sein, ob eine vertrauliche Übermittlung der Daten innerhalb des Kraftfahrzeugs von der Speicherstelle zur WAN-Verbindung sichergestellt werden muss. Es ist hier also notwendig, zwischen verschiedenen Formen der Datenverarbeitung (Verarbeitung im Kraftfahrzeug, Übermitteln von Daten an das Kraftfahrzeug und Empfangen von Daten) zu differenzieren und das jeweilige Level an Schutz im Detail zu beschreiben. Bezüglich der Sicherheit der Funkverbindungen ist festzuhalten, dass diese gemäß der AFGBV gegen unerlaubte Zugriffe in der Art geschützt werden müssen, wie es die Artikel 24, 25 und 32 der DSGVO vorgeben und darüber hinaus der Aufbau der Verbindung und die Datenübertragung nach dem Stand der Technik mit offenen und etablierten Standards gesichert und verschlüsselt werden muss.[240] Dazu wird beispielhaft auf Transport Layer Security (TLS) Version 1.3 verwiesen, bei der wie in der technischen Richtlinie TR-02102-2[241] kryptografische Verfahren Empfehlungen und Schlüssellängen beschrieben sind.

Die Integrität der Datenverarbeitung in Kraftfahrzeugen kann auch durch die Wartung und Instandhaltung berührt werden, insbesondere mit Blick auf Kraftfahrzeuge mit autonomen Fahrfunktionen aufgrund der hohen Abhängigkeit dieser Kraftfahrzeuge von einer Vielzahl von Datenerhebungen und -verarbeitungen. Die Wartbarkeit von Kraftfahrzeugen mit autonomen Fahrfunktionen muss daher seitens der Hersteller sichergestellt werden. Deshalb haben diese Hersteller gemäß § 12 Abs. 1 Nr. 1-7 AFGBV umfangreiche Dokumentationspflichten zu erfüllen. Dazu zählen unter anderem nach Nr. 3 „ein Konzept zur Sicherheit im Bereich der Informationstechnologie nach Anlage 1 Nummer 15 zu erstellen und nach Anlage 3 Nummer 4 zu dokumentieren." Nach Nr. 4 ist „die Durchführbarkeit einer wiederkehrenden technischen Fahrzeugüberwachung nach Anlage 1 Nummer 7.3 zu dieser Verordnung sicherzustellen". Gemäß Nr. 7 hat der Hersteller

[239] Das Auslesen von Kraftfahrzeugdaten mit Personenbezug stellt eine Datenübertragung i.S.d. Art 4 Nr. 2 DSGVO dar, wobei der/die Auslesende als Verantwortliche/r gemäß Art. 4 Nr. 7 DSGVO gilt.

[240] AFGBV Anlage 1 Teil 5, Nr. 16.

[241] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf;jsessionid=9BC508348FB80D4169577C6B7A95BC97.internet461?__blob=publicationFile&v=4.

– wie bereits beschrieben – „nach den Anforderungen an den digitalen Datenspeicher nach Anlage 1 Nummer 13 ein Sicherheitskonzept zu erstellen, das den Vorgaben der Artikel 24, 25 und 32 der [DSGVO] entspricht und eine Datenschutzfolgeabschätzung nach Artikel 35 der [DSGVO] beinhaltet."

Die Halter*innen sind wiederum gemäß § 13 Abs. 1 Nr. 1 und 3. AFGBV dazu verpflichtet sicherzustellen, dass, „unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen die Fahrzeugsysteme für die aktive und passive Sicherheit des Kraftfahrzeuges mit autonomer Fahrfunktion regelmäßig überprüft werden, [und] 3. unter Zugrundelegung der vom Hersteller zur Verfügung gestellten Reparatur- und Wartungsinformationen ab dem Tag der Zulassung zum Straßenverkehr alle 90 Tage eine Gesamtprüfung nach den Vorgaben des Betriebshandbuches für das Kraftfahrzeugs mit autonomer Fahrfunktion" durchzuführen. Weiterhin muss nach § 13 Abs. 1 Nr. 2 AFGBV täglich vor Betriebsbeginn eine erweiterte Abfahrkontrolle gemäß den Anforderungen nach Absatz 7 durchgeführt werden. Das bedeutet, dass vor jedem Betriebsbeginn eine Probefahrt mit aktiviertem autonomem System durchgeführt werden muss, bei welcher neben der Bremsanlage (§ 13 Abs. 7 Nr. 1 AFGBV), Lenkanlage (Nr. 2) und weiteren (Nr. 3-7) auch gemäß Nr. 6 „Sicherheitsrelevante elektronisch geregelte Fahrzeugsysteme sowie die Sensorik zur Erfassung externer und interner Parameter" überprüft werden müssen. Neben der Frage, wie eine solche Anforderung in der Praxis umgesetzt werden soll, ist auch nicht ersichtlich, was bei möglichen Fehlermeldungen geschehen soll. Eine Pflicht, die alle 90 Tage anstehende Gesamtprüfung nach § 13 Abs. 1 Nr. 3 an das KBA und die für ihre Aufgabenerfüllung weiteren zuständigen Behörden zu übermitteln, ist gemäß Nr. 4 auch nur auf diese Prüfung beschränkt und nicht auch auf die erweiterte Abfahrkontrolle nach Nr. 2.

In Anlage 3 Nr. 2 der AFGBV werden die Anforderungen an das Betriebshandbuch spezifiziert. Ziel ist es „den sicheren Betrieb des Kraftfahrzeugs mit autonomer Fahrfunktion zu gewährleisten". Dafür „soll das Betriebshandbuch die Bedienung, Wartung, Gesamtprüfung, Diagnose des Kraftfahrzeuges und die dem Datenschutz und der Datensicherheit dienenden Parameter detailliert darstellen." Das Betriebshandbuch muss dabei mindestens die folgenden Punkte enthalten: ein Rollen-Rechte-Pflichten-Konzept für die zum Betrieb nötigen Tätigkeiten; Definition der erforderlichen Kompetenzen zur Ausübung der zum Betrieb nötigen Tätigkeiten; Umfang, Ablauf, Zeitpunkte und Intervalle von Wartungsmaßnahmen; Sicherheitshinweise im Sinne der Beachtung von Grenzwerten für die technischen Funktionen; Entstörungs- oder Sicherheitsmaßnahmen, die im

Falle einer Störung des Betriebes zu ergreifen sind; Dokumente für Wartungs- und Reparaturmaßnahmen inklusive der nötigen Vorlagen und eine Darstellung der dem Datenschutz und der Datensicherheit dienenden Funktionalitäten.[242]

4.1.2.2 Anforderungen an die Sicherheit im Bereich der Informationstechnologie

Die Datenspeicherung und die Datenübermittlung sollen den Anforderungen an die Sicherheit im Bereich der Informationstechnologie genügen. Insbesondere müssen die Daten gemäß dem Stand der Technik vor Manipulation und missbräuchlicher Verwendung geschützt werden. Die dafür notwendigen Anforderungen an die Sicherheit der Informationstechnologie sind sodann in Anlage 1 Teil 5 der AFGBV beschrieben. Im Vergleich zum ersten Entwurf der AFGBV[243] ist in der verabschiedeten Version dieser Teil erheblich gekürzt worden. In AFGBV Anlage 1 Teil 5 ist vorgesehen, dass die vom Hersteller zu erfüllenden Anforderungen im Bereich der Informationstechnologie den Anforderungen der jeweils geltenden Fassung von UNECE-Regelung 155 zu entnehmen sind. Die Anforderungen der Ziffern 1., 3., 4. und 5.3.1. bis 5.3.5. der UNECE-Regelung 155 sollen dabei indes entfallen. Das zu erstellende Sicherheitskonzept muss den Vorgaben der Art. 24, 25 und 32 DSGVO entsprechen und eine Datenschutzfolgeabschätzung nach Art. 35 DSGVO enthalten. Sämtliche weitere Anforderungen, die in der vorherigen Version enthalten waren und als Konkretisierung zu § 1f Abs. 3 Nr. 1-6 StVG gesehen werden konnten, sind in der beschlossenen Fassung nicht mehr enthalten.

Anforderungen, die die Hersteller in diesem Zusammenhang erfüllen müssen, sind jedoch weiterhin in § 1f Abs. 3 zu finden und besagen, dass über den gesamten Entwicklungs- und Betriebszeitraum das Kraftfahrzeug mit autonomer Fahrfunktion vor Angriffen auf die elektronische und elektrische (E/E) Architektur des Kraftfahrzeuges sowie auf die mit dem Kraftfahrzeug in Verbindung stehende E/E Architektur abgesichert werden muss und dies auch gegenüber dem KBA und weiteren zuständigen Behörden nachzuweisen ist. Dass die mit dem Kraftfahrzeug in Verbindung stehende (E/E) Architektur mit abgesichert sein muss, kann eigentlich nur bedeuten, dass die Hersteller externe Cyberangriffe auf ihre Kraftfahrzeuge, welche über andere, mit dem Kraftfahrzeug in Verbindung stehende Entitäten durchgeführt werden, erkennen müssen bzw. unverzüglich nach Bekanntwerden einen solchen Angriff gemäß § 1f Abs. 3 Nr. 6 StVG dem KBA und

[242] Vgl. AFGBV Anlage 3 Nr. 2.

[243] Entwurf einer Verordnung zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, Notifizierungsnummer: 2021/344/D, Bearbeitungsstand 10.6.2021, https://ec.europa.eu/growth/tools-databases/tris/de/search/?trisaction=search.detail&year=2021&num=344.

den dort genannten zuständigen Behörden melden und notwendige Maßnahmen einleiten.

In der früheren Version der AFGBV war hier zudem konkret die Absicherung vor Angriffen in Verbindung mit Software-Updates mit eingeschlossen,[244] wodurch auch indirekt die UNECE-Regelung 156 im Kontext der Neuregelungen relevant geworden wäre. Die verabschiedete Verordnung enthält diesen wichtigen Zusatz nicht mehr. Dennoch wird es schwerlich möglich sein, die Vorgaben der UNECE-Regelung 156 bezüglich Software-Updates im Kontext von Kraftfahrzeugen mit autonomen Fahrfunktionen und deren Cybersicherheit auszuklammern. Die maßgeblichen Anforderungen an die Hersteller im Bereich der Cybersicherheit werden unter anderem in der UNECE-Regelung 155 und der UNECE-Regelung 156 festgelegt und sind daher beide hier Untersuchungsgegenstand.

Um diesen Anforderungen zu entsprechen, ist seitens der Hersteller dem KBA und den zuständigen Behörden die Existenz und Nutzung eines Cyber Security Management Systems (CSMS) nachzuweisen. Das CSMS soll Cybersicherheitsrisiken identifizieren, evaluieren und entschärfen. Die dort identifizierten Risiken und das entsprechende CSMS dürfen nicht die Sicherheit der Kraftfahrzeuginsassen oder anderer am Verkehr beteiligter Personen und insbesondere deren Leib oder Leben beeinträchtigen. Mit Bezug auf vom Kraftfahrzeug übermittelte oder empfangene Daten sollen die Schutzziele laut AFGBV mindestens die Vertraulichkeit, Integrität, Verfügbarkeit, Nachweisbarkeit, Authentizität und Verantwortlichkeit umfassen.[245]

Unter IT-Sicherheit können auch die im Datenschutzrecht vorgegebenen Schutzziele zu Datensicherheit verstanden werden, weil Datensicherheit ein Mittel der Gewährleistung von Datenschutz ist. Speziell Art. 32 DSGVO ist hier einschlägig. Danach müssen die Verantwortlichen (hier: die Hersteller) geeignete technische und organisatorische Maßnahmen treffen, um Risiken im Kontext der Datenverarbeitung ein angemessenes Schutzniveau gegenüberzustellen. Dieser risikobasierte Ansatz der DSGVO steht in einem engen Zusammenhang zur IT-Sicherheit.[246]

[244] Entwurf einer Verordnung zur Durchführung des Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes, Notifizierungsnummer: 2021/344/D, Bearbeitungsstand 10.6.2021, Anlage I Teil 5 Nr. 14.

[245] Siehe hinsichtlich Integrität, Authentizität und Verfügbarkeit AFGBV Anlage 1 Teil 1 Nr. 6 und bezüglich Vertraulichkeit, Nachweisbarkeit und Verantwortlichkeit verweist die AFGBV auf die entsprechenden Artikel 24, 25, 32 der DSGVO sowie auf die Vorgaben aus der UNECE-Regelung 155.

[246] *Conrad*, in: *Auer-Reinsdorff/Conrad* (Hrsg.) Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Rn. 180.

Darüber hinaus etabliert die DSGVO verschiedene Gewährleistungsziele, welche sich auf die Schutzziele der Informationssicherheit beziehen.[247] Informationssicherheit umfasst dabei technische wie auch nicht-technische Systeme und orientiert sich in der Praxis im Rahmen des IT-Sicherheitsmanagements an ISO/IEC Normen und dem IT-Grundschutz, wodurch die Überschneidung hinsichtlich der Gewährleistungsziele der DSGVO und der Schutzziele der Informationssicherheit kenntlich wird.

Zu diesen Zielen zählen die Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit.[248] Diese Schutzziele finden sich direkt[249] oder indirekt[250] auch in der AFGBV und müssen demzufolge bei allen Kraftfahrzeugen mit autonomen Fahrfunktionen und deren elektronischer und elektrischer Architektur beachtet werden. Im Zusammenhang mit dem Datenschutzrecht sind diese Schutzziele in zentralen Normen der DSGVO, zum Beispiel in Art. 5, zu finden. Dieser regelt beispielsweise die Transparenz für Betroffene von Verarbeitungen personenbezogener Daten (Art. 5 Abs. 1 lit. a DSGVO), Zweckbindung einer Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. b DSGVO), Datenminimierung einer Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 lit. c DSGVO), Richtigkeit personenbezogener Daten (Art. 5 Abs. 1 lit. d DSGVO), Speicherbegrenzung personenbezogener Daten (Art. 5 Abs. 1 lit. e DSGVO), Integrität personenbezogener Daten (Art. 5 Abs. 1 lit. f DSGVO, Art. 32 Abs. 1 lit. b DSGVO) und die Vertraulichkeit personenbezogener Daten (Art. 5 Abs. 1 lit. f DSGVO, Art. 32 Abs. 1 lit. b DSGVO). Auch Art. 25 und 32 DSGVO regeln zentrale Aspekte mit Bezug zur Datensicherheit. Dazu zählen Datenschutz durch Voreinstellungen (Art. 25 Abs. 2 DSGVO), Verfügbarkeit der Systeme, Dienste und Daten (Art. 32 Abs. 1 lit. b und lit. c DSGVO), Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO), Wiederherstellbarkeit der Daten und des Datenzugriffs (Art. 32 Abs. 1 lit. c DSGVO) und die Evaluierbarkeit (Art. 32 Abs. 1 lit. d DSGVO).[251]

Für die Datenspeicherung, insbesondere aber die Anforderungen an die Sicherheit im Bereich der Informationstechnologie, spielt die Integrität aus technischer und rechtlicher Sicht eine wesentliche Rolle. Integrität eines Systems bedeutet in diesem Zusammenhang, dass Daten und Informationen sicher und nachweislich nicht verändert worden sind. In-

[247] Standard-Datenschutzmodell, Version 2.0b, S. 9 ff., abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf.

[248] Ebd.

[249] AFGBV Anlage 1 Teil 1 Nr. 6 listet Integrität, Authentizität und Verfügbarkeit auf.

[250] AFGBV Anlage 1 Teil 5 Nr. 15.

[251] Standard-Datenschutzmodell, Version 2.0b, S. 12 ff., abrufbar unter: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methode_V2.0b.pdf.

tegrität stellt demnach die nachvollziehbare Unversehrtheit und Korrektheit von elektronischen Daten dar.[252] Da Integrität eines der drei Hauptziele von Datensicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) darstellt, sind im Bereich von Kraftfahrzeugen mit autonomen Fahrfunktionen die Datensicherheitsmaßnahmen nach der DSGVO von Bedeutung.

Im Gegensatz zu den Neuregelungen im StVG, welche sich hauptsächlich auf die Datenverarbeitung im Kraftfahrzeug beschränken, ist in Teil 1 Nr. 6 der Anlage 1 der AFGBV für Kraftfahrzeuge mit autonomer Fahrfunktion auch die Übertragung von Daten an das Kraftfahrzeug erwähnt. Eine Kommunikation des Kraftfahrzeugs mit autonomer Fahrfunktion mit anderen Kraftfahrzeugen oder mit Infrastruktureinrichtungen soll zulässig sein[253] und ist für deren Funktion essentiell. Demnach sollen die zur selbstständigen Bewältigung der Fahraufgabe im autonomen Betrieb notwendigen Daten und Informationen von externen technischen Einheiten (beispielsweise Backends oder Servern eines Anbieters, externe Sensoren, Smartphone oder zukünftig auch Anordnungen nach Straßenverkehrsrecht (wie etwa ein Stopp-Schild oder Anordnungen einer Lichtzeichenanlage) vom Kraftfahrzeug sicher empfangen und verwendet werden können.[254] Eine solche Übertragung soll dem aktuellen Stand der Technik entsprechen und die Vorgaben der DSGVO (insbesondere den Art. 24, 25, 32 und 35 DSGVO) erfüllen. Es sollen über eine Bedrohungsanalyse Risiken identifiziert werden und ein Absicherungskonzept mit wirksamen Maßnahmen eingeführt werden.[255] Weiter soll für die Datenübertragung eine zentrale SECU genutzt werden. Diese dient als Informationsgateway im Kraftfahrzeug. Die SECU kommuniziert intern an die Kommunikationsbusse des Kraftfahrzeugs und an den physischen On-Board-Diagnose II-Anschluss (OBD II) oder an eine proprietäre Schnittstelle des Herstellers. Die Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung sind dabei ebenfalls in dem bereits oben beschriebenen Teil 5 der AFGBV zu finden. Hierzu zählt die Sicherstellung u.a. der Integrität, Authentizität und Verfügbarkeit der Datenübertragung.

Maßnahmen zur Gewährleistung der Datensicherheit werden in den Artikeln 24, 25 und 32 DSGVO normiert. In Art. 24 DSGVO wird neben der generellen Verpflichtung zum Schutz personenbezogener Daten auch die Gewährleistung der Datensicherheit, also die

[252] *Conrad*, in: *Auer-Reinsdorff/Conrad* (Hrsg.) Handbuch IT- und Datenschutzrecht, 3. Auflage 2019, § 33 Rn. 9.

[253] AFGBV Anlage 1 Teil 1 Nr. 6.

[254] Ebd.

[255] Ebd.

Durchführung technisch-organisatorische Maßnahmen zum Schutz verarbeiteter personenbezogener Daten, festgeschrieben.[256] Art. 24 DSGVO bezüglich der Verantwortung des für die Verarbeitung Verantwortlichen wird durch Art. 25 zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen und Art. 32 DSGVO zur Sicherheit der Verarbeitung personenbezogener Daten konkretisiert, indem Art. 25 DSGVO dem Verantwortlichen spezifische Pflichten bezüglich des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen vorgibt. Überdies regelt Art. 32 DSGVO als nähere Konkretisierung des allgemeinen Grundsatzes der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO) die Pflicht, ein angemessenes Schutzniveau für die Sicherheit personenbezogener Daten zu gewährleisten.[257] Als notwendige Maßnahmen werden in Art. 32 DSGVO unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 lit. a DSGVO) benannt. Hinzu kommt die Notwendigkeit, die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherzustellen (Art. 32 Abs. 1 lit. b) sowie die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c DSGVO). Gefordert ist zudem ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 Abs. 1 lit. d DSGVO).

Die von den Herstellern entwickelten Systeme müssen demzufolge insbesondere die genannten Vorgaben erfüllen und dies muss nachweislich und dauerhaft bescheinigt werden, um eine Genehmigung für ihr Kraftfahrzeug mit autonomen Fahrfunktionen zu erhalten. Kraftfahrzeuge müssen zwingend vor Hackerangriffen geschützt werden. Dabei ist ein Zusammenspiel von technischen Standards und rechtlichen Vorgaben notwendig. Nur eine holistische Kraftfahrzeugarchitektur kann Betriebssicherheit (*safety*) und Informationssicherheit (*security*) bei gleichzeitiger Berücksichtigung der datenschutzrechtlichen Vorgaben gewährleisten. Dazu gehört auch eine Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO vor der kommerziellen Einführung hiervon erfasster Datenverarbeitungen.

Da in der AFGBV unter anderem direkt Bezug auf die UNECE-Regelung 155 genommen wird,[258] werden im vorliegenden Kontext einschlägige UNECE-Regelungen im Folgenden näher betrachtet.

[256] *Hartung*, in: *Kühling/Buchner* (Hrsg.), DS-GVO – BDSG, 2. Auflage 2018, Art. 24 Rn. 11.

[257] *Martini,* in: *Paal/Pauly* (Hrsg.), DS-GVO BDSG, 3. Aufl. 2021, DS-GVO Art. 32 Rn. 2.

[258] AFGBV Anlage 1, Teil 5, Nr. 15.

4.1.3 UNECE-Regelungen

Auf der internationalen Ebene werden wichtige Rechtsinstrumente im Bereich des Kraftfahrzeugverkehrs durch die Wirtschaftskommission der Vereinten Nationen für Europa (United Nations Economic Commission for Europe - UNECE) und dort die Working Party on Road Traffic Safety, welche 2017 in Global Forum for Road Traffic Safety - WP.1[259] (nachfolgend WP.1) umbenannt wurde, weiterentwickelt und interpretiert. Diese Arbeitsgruppen sind zwar nicht direkt zuständig auch datenschutzrechtliche Vorgaben zu definieren, allerdings werden dort Regelungen erarbeitet, welche Auswirkungen darauf haben, dass Daten im Kraftfahrzeug verarbeitet werden.[260] In den Arbeitsgruppen werden technische Regeln (nachfolgend UNECE-Regeln) erarbeitet, welche sich am Stand der Technik orientieren und genaue Maßgaben zu Bauteilen oder Kraftfahrzeugfunktionen enthalten.[261] Dazu zählen etwa Regelungen zur Lenkung (UNECE-Regelung 79) und die Überarbeitung von UNECE-Regelung 79,[262] die UNECE-Regelung 157 (Automated Lane Keeping Systems – ALKS) oder die UNECE-Regelung 13-H zu automatisierten Bremsen.

Neben der bereits genannten WP.1 ist für die Entwicklung im Bereich automatisierter Kraftfahrzeuge auch das World Forum for Harmonization of Vehicle Regulations - WP.29 (nachfolgend WP.29) zu nennen, wo seit 2018 die Unterarbeitsgruppe für Automated and Connected Driving (GRVA – Group Responsive Voiture Automatique) für automatisiertes und vernetztes Fahren verantwortlich ist.[263] Hier werden einerseits im Kontext des automatisierten Fahrens datenschutzrechtlich relevante Vorgaben erarbeitet, wie solche zum sogenannten Fahrmodusspeicher (DSSAD) und zum Unfalldatenspeicher (EDR).[264] Andererseits zählen zu den Schwerpunkten der GRVA im Rahmen von safety und security auch funktionale Anforderungen an Cybersecurity, Software-Updates oder

[259] Vgl. www.unece.org/trans/main/welcwp1.html.

[260] *Wagner*, Das neue Mobilitätsrecht – Der Rechtsrahmen zum automatisierten und vernetzten Fahren, Nomos, 2021, S. 136.

[261] A.a.O., S. 35.

[262] *Lutz*, Neue Vorschriften für das automatisierte und autonome Fahren – ein Überblick, DAR 2021, 182 (S. 182 f.); *Will*, Die innovative völkerrechtliche UNECE-Regelung für Automatisierte Spurhaltesysteme (ALKS), NZV 2020, 163 (S. 166 f.).

[263] https://unece.org/transport/vehicle-regulations/working-party-automatedautonomous-and-connected-vehicles-introduction.

[264] *Wagner*, Das neue Mobilitätsrecht – Der Rechtsrahmen zum automatisierten und vernetzten Fahren, Nomos, 2021, S. 130 ff.

auch Validierungsmethoden.[265] Zu Cybersecurity und Software-Updates wurden die UN-ECE-Regelungen 155[266] (Cybersicherheit) und 156[267] (Software-Updates) veröffentlicht. Die AFGBV schreibt in diesem Zusammenhang vor, dass „[d]ie vom Hersteller zu erfüllenden Anforderungen bezüglich der Sicherheit im Bereich der Informationstechnologie […] den Anforderungen der […] UN-Regelung Nr. 155" zu entnehmen sind.[268] Das Sicherheitskonzept muss den Vorgaben der Artikel 24, 25 und 32 der DSGVO entsprechen.[269] Hier wird durch die Verordnung explizit die UNECE-Regelung 155 zur Voraussetzung erklärt. Neben der völkerrechtlichen Bindung an die UNECE-Regelungen durch das Genfer Fahrzeugteileübereinkommen,[270] dessen Vertragsstaat Deutschland ist, hat zudem die Europäische Union als supranationales Mitglied die UNECE-Regelungen für die Mitgliedsstaaten mit Verpflichtungswirkung ratifiziert. Aus Sicht der Kraftfahrzeughersteller ist weiterhin insbesondere von Bedeutung, dass die Anforderungen der relevanten UNECE-Regelungen im EU-Typengenehmigungsverfahren als Voraussetzung gelten.[271]

Untergesetzliche und gesetzliche Regelungen zur Cybersicherheit werden in Zukunft eine wichtige Rolle in der Fahrzeugautomatisierung spielen. Durch die feste Einbettung der UNECE- Regelungen in die AFGBV und über den Verweis auf diese Regelungen in der EG-Typenzulassung werden Kraftfahrzeughersteller die dort geforderten Anforderungen an die Cybersicherheit im Rahmen des Genehmigungsverfahrens vorweisen müssen.[272] Daher sollen auch im Folgenden insbesondere die UNECE-Regelung 155 und 156 thematisiert werden. Die Maßnahmen der UNECE-Regelung 155 werden hier nur beispielhaft aufgeführt. Daher werden nur Anforderungen aus den allgemeinen Gewährleistungszielen abgeleitet.

[265] Die Arbeiten und aktuellen Arbeitsstände der Informal Working Groups unter GRVA können online eingesehen werden: https://wiki.unece.org/pages/viewpage.action?pageId=63310525; zum Verfahren: *Will*, Die innovative völkerrechtliche UNECE-Regelung für Automatisierte Spurhaltesysteme (ALKS), NZV 2020, 163 (S. 166).

[266] Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system E/ECE/TRANS/505/Rev.3/Add.154.

[267] Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system ECE/TRANS/WP.29/2020/80.

[268] AFGBV Anlage 1 Teil 5 Nr. 15.

[269] Ebd.

[270] Genfer Übereinkommen der Wirtschaftskommission für Europa der Vereinten Nationen vom 20.3.1958 über die Annahme harmonisierter technischer Regelungen der Vereinten Nationen 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 Regelungen der Vereinten Nationen erteilt wurden – Revision 3, ABl. EU L 274/4 vom 11.10.16.

[271] *Will*, Die innovative völkerrechtliche UNECE-Regelung für Automatisierte Spurhaltesysteme (ALKS), NZV 2020, 163 (S. 165 f.).

[272] *Wagner*, Das neue Mobilitätsrecht – Der Rechtsrahmen zum automatisierten und vernetzten Fahren, Nomos, 2021, S. 186.

4.1.3.1 UNECE-Regelung 155

Nachdem die von der WP.29 erarbeiteten Regelungen 2021 im Amtsblatt der Europäischen Union veröffentlicht wurden,[273] bestehen erstmalig auf europäischer Ebene einheitliche und verbindliche Regelungen bezüglich Cybersecurity und Software-Updates für den Automobilsektor. Der Kern der UNECE-Regelung 155 besteht in der Verpflichtung zur Einführung eines Cybersicherheitsmanagementsystems (CSMS). Nach Ziffer 2.3. der Regelung bezeichnet ein CSMS einen „systematischen, risikobasierten Ansatz zur Festlegung von organisatorischen Abläufen, Zuständigkeiten und Governance beim Umgang mit Risiken im Zusammenhang mit Cyberbedrohungen für Fahrzeuge und beim Schutz von Fahrzeugen vor Cyberangriffen."[274] Gemäß Ziffer 5. ist ein solches CSMS fortan als Voraussetzung für die Genehmigung eines Kraftfahrzeugtyps anzusehen. Kraftfahrzeughersteller haben daher gemäß Ziffer 5.1.1. relevante Maßnahmen zu treffen, welche folgendes gewährleisten sollen:

a) Erfassung und Überprüfung der gemäß dieser Regelung erforderlichen Informationen über die gesamte Lieferkette hinweg, um nachzuweisen, dass lieferantenbezogene Risiken ermittelt und bewältigt werden;

b) Dokumentation der Risikobewertung (während der Entwicklungsphase oder nachträglich), der Testergebnisse und der Minderungsmaßnahmen bezogen auf den Fahrzeugtyp, einschließlich konstruktionsbezogener Informationen zur Untermauerung der Risikobewertung;

c) Implementierung geeigneter Cybersicherheitsmaßnahmen bei der Konzeption des Fahrzeugtyps;

d) Erkennung von und Reaktion auf mögliche Cyberangriffe und

e) Protokollierung von Daten zur Unterstützung der Erkennung von Cyberangriffen und Bereitstellung von Datenforensik, um eine Analyse versuchter oder erfolgreicher Cyberangriffe zu ermöglichen

Durch die Pflicht, auch die gesamte Lieferkette nachweislich zu kontrollieren, sind Zuliefererfirmen, die Teile mit cybersicherheitsrelevanten Komponenten produzieren, mittelbar ebenfalls dieser Regelung unterworfen. Das bedeutet konsequenterweise auch, dass das Gesamtsystem des Kraftfahrzeugs zur Einhaltung aller Schutzziele ebenfalls Cloud-Services mitberücksichtigen muss.

[273] Amtsblatt der Europäischen Union, L 082, 9.3.2021, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L:2021:082:FULL&from=DE.

[274] UNECE-Regelung 155, Ziffer 2.3.

Die Anforderungen an das Cybersicherheitsmanagementsystem sind in Ziffer 7.2. beschrieben. Dazu zählen unter anderem der kraftfahrzeugherstellerseitige Nachweis gegenüber den Genehmigungsbehörden, dass das CSMS in der Entwicklungs-, Produktions- und Postproduktionsphase anwendbar ist.[275] Nachzuweisen sind nach den Ziffern 7.2.2.2. ff. insbesondere die Verfahren, welche für eine angemessene Sicherheit sorgen sollen. Dazu zählen beispielsweise „Verfahren, die innerhalb der Organisation des Herstellers für das Cybersicherheitsmanagement eingesetzt werden", „Verfahren zum Testen der Cybersicherheit eines Fahrzeugtyps", „Verfahren zur Überwachung und Erkennung von Cyberangriffen, Cyberbedrohungen und Schwachstellen von Fahrzeugtypen sowie zur Reaktion darauf, und die Verfahren, mit denen bewertet wird, ob die implementierten Cybersicherheitsmaßnahmen angesichts neu ermittelter Cyberbedrohungen und Schwachstellen noch wirksam sind".[276] Für den hier behandelten Kontext ist darüber hinaus Ziffer 7.2.2.4. nennenswert, nach welcher der Kraftfahrzeughersteller nachweisen muss, dass die in 7.2.2.2. lit. g) vorgesehene Überwachung ununterbrochen erfolgt, wobei gemäß 7.2.2.4. lit. a) Kraftfahrzeuge auch nach der Erstzulassung in die Überwachung einbezogen werden müssen und nach lit. b) „die Fähigkeit, Cyberbedrohungen, Schwachstellen und Cyberangriffe anhand von Kraftfahrzeugdaten und Fahrzeugprotokollen zu analysieren und zu erkennen" gegeben sein muss. Hieraus ergeben sich Anforderungen an den Schutz personenbezogener Daten im Sinne des Datenschutzrechts.

Mit Blick auf Ziffer 1.3. ist hervorzuheben, dass die gesamte Regelung „auch unbeschadet der Anwendung nationaler und regionaler Rechtsvorschriften zum Schutz der Privatsphäre und zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten" gilt. Das CSMS müssen sich die Kraftfahrzeughersteller zertifizieren lassen. Dieses Zertifikat soll maximal drei Jahre gültig sein und einmal im Jahr müssen die Hersteller den Genehmigungsbehörden über ihr Monitoring und über detektierte Cyberangriffe Auskunft geben.[277] Sollen Modifikationen vorgenommen werden, welche auch Sicherheitsmechanismen betreffen, ist dies ebenfalls zu melden. Bei Nonkonformität mit den Vorgaben aus der UNECE-Regelung soll als Sanktionsmittel die Konformitätsbescheinigung für das CSMS zurückgenommen werden (Ziffer 6.8.), was zur Rücknahme der Typengenehmigung hinsichtlich der Cybersicherheit führt.[278] Anstelle detaillierter technischer Vorschriften an das Endprodukt soll so der Entwicklungsprozess der Hersteller sowie die Produktbeobachtung über den gesamten Produktionszyklus geregelt

[275] UNECE-Regelung 155, Ziffer 7.2.2.1.

[276] Vgl. a.a.O., Ziffern 7.2.2.2. bis 7.2.2.5.

[277] Vgl. a.a.O., Ziffern 6.7. und 7.4.1.

[278] Vgl. a.a.O., Ziffern 6.11. und 10.1.

werden.[279] Ziel ist einerseits ein hohes Sicherheitsniveau und andererseits die nötige Flexibilität in einem sich schnell weiterentwickelnden Feld zu wahren, um nicht langfristig an bereits überholte Sicherheitsstandards gebunden zu sein.[280]

Bezüglich Datenschutz und Cybersicherheit kann auch hier ein gewisses Spannungsverhältnis erkannt werden. Während das Datenschutzrecht sehr detailliert normativ geregelt ist, existieren hinsichtlich Cybersicherheit kaum gesetzliche Vorgaben, dafür aber diverse Industriestandards. Ähnlich verhält es sich hier mit der UNECE-Regelung 155, welche Cyberangriffe zwar als Bedrohung für personenbezogene Daten erkennt, allerdings keine konkret einzuhaltenden Anforderungen bezüglich des Datenschutzes benennt. Lediglich in Ziffer 1.3. heißt es, dass die Privatsphäre und der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten gewahrt werden muss. Eine positive Entwicklung ist dabei jedoch der erkennbare Versuch einer Synthese von Datenschutz und Cybersicherheit, welcher dem Anhang zu der UNECE-Regelung entnommen werden kann. Dort werden Schwachstellen oder Angriffsmethoden, bezogen auf verschiedene Bedrohungen, identifiziert und Minderungsmaßnahmen für dieselben erörtert. Zudem werden speziell Bedrohungen für personenbezogene Daten miterfasst. So werden beispielsweise in Anhang 5, Tabelle 1A, Ziffer 4.3.6. Bedrohungen für Fahrzeugdaten/-code genannt und als Schwachstelle im Zusammenhang mit unbefugtem Zugriff auf personenbezogene Daten des Eigentümers genannt. Unter Ziffer 7.2. in Tabelle B1 zu Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Fahrzeugkommunikationskanälen wird etwa mit Blick auf das Erlangen von unbefugtem Zugriff auf Dateien oder Daten vorgegeben, dass das Systemdesign und die Zugangskontrolle so ausgelegt sein müssen, dass Unbefugte nicht auf personenbezogene oder systemkritische Daten zugreifen können.

Beispiele für Sicherheitsmaßnahmen für Backend-Systeme bietet das *Open Web Application Security Project*[281] (OWASP). Die Regelung in Tabelle B5, Ziffer 19.2. oder auch in Tabelle B7, Ziffer 31.1. sind dahingehend vergleichbar, dass nach der bei der Speicherung personenbezogener Daten bewährte Verfahren zum Schutz der Datenintegrität und -vertraulichkeit zu befolgen sind. In Tabelle C3, Ziffer 30.1. wird die Aussage aus Tabelle B7, Ziffer 31.1., auch noch um den Zusatz ergänzt, dass Beispiele für Sicherheitsmaßnahmen in ISO/SC27/WG5 zu finden sind. Fraglich ist jedoch die Verbindlichkeit dieser „Minderungsmaßnahmen", insbesondere wenn es heißt, dass lediglich Beispiele dafür in ISO-

[279] *Wagner*, Das neue Mobilitätsrecht – Der Rechtsrahmen zum automatisierten und vernetzten Fahren, Nomos, 2021, S. 187 f.

[280] A.a.O., S. 188; Zur Kritik am aktuellen Entwurf: NPM – Nationale Plattform Zukunft der Mobilität, Handlungsempfehlungen zur Typengenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, Whitepaper 2020, S. 21 ff.

[281] https://wiki.owasp.org/?title=Special:Redirect/file/OWASP_Top_10-2017_de_V1.0.pdf.

Normen zu finden sind, welche ebenfalls keine rechtliche Bindungswirkung besitzen. Die Tabellen in den Anhängen können auch nicht als abschließend angesehen werden, was der sonstigen flexiblen Ausgestaltung der Regelung auch zuwiderlaufen würde.

Zusammenfassend kann festgehalten werden, dass heute UNECE-Regelungen die entscheidenden materiellen Vorgaben für die Erteilung einer EG-Typengenehmigung enthalten.[282] Art. 57 Abs. 1 VO (EU) 2018/858[283] gibt vor, dass UN-Regelungen oder deren Änderungen, denen die Union zugestimmt hat oder die sie anwendet und die in Anhang II VO (EU) 2018/858 aufgeführt sind, Bestandteil der Anforderungen für die EU-Typgenehmigung für Kraftfahrzeuge, Systeme, Bauteile und selbstständige technische Einheiten sind. Damit werden auch künftig die Vorgaben zu Cybersicherheit aus der UNECE-Regelung 155 zumindest insofern zu beachten sein, wenn eine EU-Typengenehmigung angestrebt wird.

4.1.3.2 UNECE-Regelung 156

Die UNECE-Regelung 156 soll im Kern die Vorgaben an ein Softwareaktualisierungsmanagementsystem (Software Update Management System – SUMS) festlegen. Damit soll die Software im Kraftfahrzeug vor Manipulationen geschützt und zudem die Cybersicherheit gewährleistet werden. Die beiden UNECE-Regelungen (155 und 156) können daher als eng miteinander verknüpft angesehen werden. Das SUMS ist in UNECE-Regelung 156 unter Ziffer 2.5. definiert als „systematische[r] Ansatz zur Festlegung organisatorischer Verfahren und Vorgänge, um den Anforderungen an die Bereitstellung von Softwareaktualisierungen gemäß dieser Regelung zu entsprechen." Die Hersteller sollen somit in die Lage versetzt werden, Sicherheitslücken oder Schwachstellen zu erkennen und diese auch aus der Ferne wirksam beheben zu können.[284] Weiterhin soll damit auch für Fahrer*innen, Halter*innen und zuständige Behörden deutlich werden, welche Auswirkungen Software-Updates auf die Typengenehmigungsparameter haben, um die Genehmigung und die Einhaltung von Governance-Richtlinien nachvollziehbar zu gewährleisten.[285]

[282] *Will*, Die innovative völkerrechtliche UNECE-Regelung für Automatisierte Spurhaltesysteme (ALKS), NZV 2020, 163 (S. 166).

[283] Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30.5.18 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG.

[284] Vgl. *Wuhrmann/Deeg/Hessel*, Neue Cybersicherheits-und Softwareupdatestandards in der Automobilbranche, https://www.reuschlaw.de/fileadmin/user_upload/202103_Neue-Cybersicherheits-und-Softwareupdatestandards-in-der-Automobilbranche_DW-TD-StH.pdf.

[285] Vector Consulting Services, UNECE CSMS und SUMS, https://consulting.vector.com/de/de/solutions/cybersecurity/unece-csms-and-sums/.

Die allgemeinen Anforderungen an das SUMS, welche durch die Hersteller erfüllt werden müssen, sind unter den Ziffern 7.1. bis 7.1.4.2. der UNECE-Regelung 156 zu finden. Die Vorschriften für den Kraftfahrzeugtyp und die Softwareaktualisierungen sind in den Ziffern 7.2. bis 7.2.2.5. festgelegt. Zu den Anforderungen an das SUMS gehört beispielsweise, gemäß Ziffer 7.1.1.1. Verfahren zu entwickeln, bei denen die für diese Regelung relevanten Informationen dokumentiert und beim Kraftfahrzeughersteller geschützt aufbewahrt werden und einer Genehmigungsbehörde oder einem technischen Dienst auf Anfrage zur Verfügung gestellt werden können. Nach Ziffer 7.1.1.2. muss ein Verfahren eingeführt werden, bei dem Informationen hinsichtlich aller ursprünglichen und aktualisierten Softwareversionen, einschließlich Validierungsdaten für die Integrität und einschlägige Hardwarekomponenten eines typgenehmigten Systems, eindeutig identifiziert werden können. Ziffer 7.1.1.6. regelt zudem, dass ein Verfahren zu etablieren ist, welches dem Kraftfahrzeughersteller ermöglicht, Zielfahrzeuge für eine Softwareaktualisierung zu identifizieren.

Gemäß Ziffer 7.2.1.1. ist die Authentizität und Integrität von Softwareaktualisierungen so zu schützen, dass sowohl ihre Beeinträchtigung als auch eine ungültige Aktualisierung nach vernünftigem Ermessen ausgeschlossen sind, die Updates also nur erfolgen, wenn sie die Fahrt nicht beeinträchtigen und sicher abgeschlossen werden können. Hinsichtlich sogenannter *Software-over-the-air-Updates* (SOTA) muss der Kraftfahrzeughersteller nach Ziffer 7.2.2.1.1. sicherstellen, dass das Kraftfahrzeug im Falle einer fehlgeschlagenen oder abgebrochenen Aktualisierung in der Lage ist, die Vorversion des Systems wiederherzustellen bzw. das Kraftfahrzeug in einen sicheren Zustand zu versetzen. Dieser „sichere Zustand" ist nicht gleichzusetzen mit dem im deutschen Recht (§ 1d Abs. 4 StVG) beschriebenen „risikominimalen Zustand".[286]

Eine Aktualisierung darf gemäß Ziffer 7.2.2.1.2. nur erfolgen, wenn das Kraftfahrzeug über genügend Energie (im Sinne von Batteriekapazität) für sowohl das Software-Update als auch das etwaige Zurücksetzen auf den vorherigen Softwarestand und das Versetzen in den sicheren Zustand verfügt. Die Vorgaben an die Sicherheit von SOTA-Updates, welche herstellerseitig erfüllt werden müssen, sind insbesondere in den Ziffern 7.2.2.1.3.

[286] UNECE-Regelung 156 spricht in Ziffer 7.2.2.1.1. und 7.2.2.1.2. von „sicheren Zustand", wobei nach Ziffer 2.7. ein „Sicherer Zustand" einen Betriebsmodus ohne unverhältnismäßiges Risiko bei Ausfall eines Merkmals bezeichnet. Näher zum „risikominimalen Zustand": *Arzt/Ruth-Schumacher*, Risikobewertung unterschiedlicher Umsetzungsszenarien des Überführens eines automatisch gesteuerten Fahrzeugs in den so genannten ‚sicheren Zustand', abrufbar unter: www.hwr-berlin.de/fileadmin/portal/Dokumente/Prof-Seiten/Arzt/ARZT_Ruth-Schumacher_-_Rechtsfragen_%C3%9Cberf%C3%BChrung_in_risikominimalen_Zustand_2016.pdf; Arzt/Ruth-Schumacher, RAW 2/2017, 89.

bis 7.2.2.5. zu finden. Dort werden vorwiegend Organisationsprozesse, Dokumentationspflichten sowie Zertifizierungsprozesse festgelegt und Anforderungen an einen sicheren Softwareupdateprozess (inklusive SOTA-Updates) definiert.

Diese Anforderungen werden die Hersteller vor deutliche Herausforderungen stellen.[287] Es müssen Systeme entwickelt werden, die sowohl die Kraftfahrzeugarchitektur, als auch mit dieser in Verbindung stehende Cloud-Dienste mitberücksichtigen, da Änderungen in der Cloudstruktur auch zunächst eingehaltene Schutzziele konterkarieren können. Ferner wird durch die Vorgabe des Zurücksetzens auf einen vorherigen Softwarestand ein technischer Pfad vorgegeben, in einer ansonsten eher dynamisch gestalteten Regelung. Technische Dienste und auch die Genehmigungsbehörden sollten bei Softwareänderungen und -updates miteinbezogen werden. Prüforganisationen sollte ein entsprechender Zugang über standardisierte Kommunikationsschnittstellen gewährleistet werden, damit diese im Rahmen ihres gesetzlichen Prüfauftrags regelmäßige Inspektionen durchführen können.[288]

Im Rahmen von Updates ist stets zu prüfen, ob diese relevant für die Typengenehmigung sein könnten. Bezüglich Software-Updates ist selbst bei Einhaltung aller Vorgaben in der UNECE-Regelung 156 damit zu klären, ob diese auch materiell-rechtlich zulässig sind und die Kraftfahrzeuge nach einem solchen Update weiterhin im öffentlichen Straßenverkehr bewegt werden dürfen.[289] Neben den eingangs skizzierten Vorgaben, die ein Kraftfahrzeughersteller mit Blick auf sein SUMS einhalten und implementieren muss,[290] benötigen diese auch eine Typengenehmigung für Softwareupdateprozesse der jeweiligen Kraftfahrzeugtypen (vgl. Ziffer 5.1.).

Die UNECE-Regelung 156 definiert in Ziffer 2.1. den Begriff des „Fahrzeugtyps" vom Gegenstand der Regelung her. Der Kraftfahrzeugtyp beschreibt nach dieser Regelung Kraftfahrzeuge als solche, die sich hinsichtlich der vom Hersteller angegebenen Bezeichnung des Kraftfahrzeugtyps und nicht in wesentlichen Merkmalen der Konzeption des Kraftfahrzeugtyps in Bezug auf die Verfahren zu Softwareaktualisierung unterscheiden. Eine solche auf den Gegenstand der Regelung bezogene Definition ist auch bereits aus

[287] So auch *Haupt*, Die Verordnung zum Gesetz zum autonomen Fahren, NZV 2022, 166 (S. 168), der die Auswirkungen der Verordnung für alle, an Kraftfahrzeugen mit autonomen Fahrfunktionen, beteiligten Akteure als erheblich einstuft.

[288] NPM – Nationale Plattform Zukunft der Mobilität, Handlungsempfehlungen zur Typengenehmigung und Zertifizierung für eine vernetzte und automatisierte Mobilität, Whitepaper 2020, S. 19.

[289] *Geber*, Rechtliche Anforderungen an Software-Updates von vernetzten und automatisierten Pkw, NZV 2021, 14 (S. 14).

[290] Vgl. auch gesamte Ziffer 7. UNECE-Regelung 156.

anderen UNECE-Regelungen wie etwa in Nr. 79 (Lenksysteme) oder Nr. 83 (Schadstoffemissionen) bekannt. Diese Definition hat einen anderen Bezugspunkt für den Begriff des Kraftfahrzeugtyps als die allgemeinen Regelungen zur Typengenehmigung gemäß Art. 3 Nr. 32 VO (EU) 2018/858.[291] Nach der VO (EU) 2018/858 setzt sich ein „Fahrzeugtyp" aus den Kraftfahrzeugen zusammen, die zumindest einen gemeinsamen Firmennamen eines Herstellers haben und in Konstruktion und Montage der wesentlichen Teile der Aufbaustruktur gleich sind. Der in UNECE-Regelung 156 gewählte Definitionsansatz lässt den Schluss zu, dass „ein Fahrzeughersteller die typgenehmigten Software-Update-Prozesse in mehreren Fahrzeugtypen im Sinne der VO (EU) 2018/858 einsetzen können soll, ohne die Prozesse jeweils neu genehmigen zu lassen."[292]

Neben den oben beschriebenen technischen Anforderungen müssen Software-Updates, welche Änderungen des Kraftfahrzeugs bedingen, auch korrekt durch den Kraftfahrzeughersteller in den Genehmigungsunterlagen dargestellt werden.[293] Änderungen am Kraftfahrzeug (auch durch Software-Updates) können entweder für den betroffenen Kraftfahrzeugtyp oder für einzelne Kraftfahrzeuge vorgenommen werden. Soll der gesamte Kraftfahrzeugtyp durch Software-Updates geändert werden, richten sich die rechtlichen Anforderungen nach Art. 33 f. VO (EU) 2018/858. Danach müssen der Typengenehmigungsbehörde Änderung mit Emissions- oder Sicherheitsbezug angezeigt werden und diese Behörde entscheidet, ob dadurch eine Erweiterung oder Änderung (Revision) der Typengenehmigung erforderlich ist (Art. 33 Abs. 1 VO (EU) 2018/858) oder ob eine neue Typengenehmigung aufgrund weitreichender Änderungen beantragt werden muss (Art. 34 Abs. 1, Art. 33 Abs. 5 VO (EU) 2018/858).

Handelt es sich nur um geringfügige Datensatzanpassungen oder sogenannte Bugfixes mit lediglich beschränktem Sicherheits- oder Emissionsbezug, enthält jedenfalls der Wortlaut der VO (EU) 2018/858 trotzdem keine Ausnahme für solche Updates. Demgegenüber könnte aus teleologischer Sicht allerdings argumentiert werden, dass reine Funktionsverbesserungen nicht einen Genehmigungsprozess durchlaufen müssen und somit von der Notifizierungspflicht ausgenommen sind, da mit solchen Verbesserungen oder Fehlerbehebungen kein Risiko einhergeht.[294] Hier ist jedoch zu beachten, dass der Kraftfahrzeughersteller für diese Einschätzung der Geringfügigkeit beziehungsweise lediglich Funktionsverbesserung das Prognoserisiko trägt.

[291] *Geber*, Rechtliche Anforderungen an Software-Updates von vernetzten und automatisierten Pkw, NZV 2021, 14 (S. 16).

[292] Ebd.

[293] A.a.O., S. 17.

[294] Ebd.

Ausnahmen von der Notifizierungspflicht bestehen für Funktionen, die zwar bereits im Code vorhanden, aber noch deaktiviert sind. Hierzu finden sich auch Maßgaben in § 1h StVG, wonach Funktionen, welche in internationalen Standards noch nicht beschrieben sind, verbaut werden können, wenn diese deaktiviert sind und eine Einflussnahme dieser Fahrfunktionen auf die genehmigten Systeme ausgeschlossen ist. Wenn solche Funktionen später Gegenstand einer Typengenehmigung werden, sollen diese durch Software-Updates aktivierbar sein.[295] Eine für Kraftfahrzeughersteller weitere Möglichkeit zur Ausnahme von der Notifizierungspflicht besteht darin, die gegebenenfalls notifizierungspflichtigen Änderungen durch Software-Updates nicht im Rahmen von Anpassungen in der Typengenehmigung zu reflektieren. Damit würden allerdings alle Rechtsfragen auf Ebene der Einzelfahrzeuge und somit auf die nicht harmonisierten Rechtsordnungen der EU-Mitgliedsstaaten verlagert.[296]

4.2 Produktsicherheit

Eine Anwendung des Produktsicherheitsgesetzes (ProdSG) setzt in sachlicher Hinsicht zwingend das Vorhandensein eines „Produkts“ voraus. Die Anwendbarkeit des Gesetzes steht und fällt demnach mit der Existenz eines Produkts wie es in § 2 ProdSG definiert ist. Nach § 2 Nr. 22 ProdSG sind Produkte Waren, Stoffe oder Zubereitungen, die durch einen Fertigungsprozess hergestellt worden sind.

Im Produktsicherheitsrecht kommt dem ProdSG eine Auffang- wie auch Dachfunktion zu. § 1 Abs. 3 ProdSG besagt, dass die Vorschriften des ProdSG keine Anwendung finden, sofern in anderen Rechtsnormen entsprechende oder weitergehende Vorschriften vorgesehen sind. In diesem Zusammenhang muss für jede Bestimmung gesondert geprüft werden, ob einzelne Rechtsakte weitergehende oder entsprechende Vorschriften enthalten.[297] Im Rahmen der Fahrzeugautomatisierung können beispielsweise Hersteller Adressaten der Regelungen des ProdSG sein (vgl. § 2 Nr. 29 ProdSG), wobei im jeweiligen Kontext die Anwendbarkeit des Gesetzes geprüft werden muss. Eine pauschale Festlegung ist daher nicht möglich.

[295] BT-Drs. 19/27439, (S. 29).

[296] Siehe dazu im Detail: *Geber*, Rechtliche Anforderungen an Software-Updates von vernetzten und automatisierten Pkw, NZV 2021, 14; *Solmecke/Jockisch*, Das Auto bekommt ein Update! – Rechtsfragen zu Software in Pkws - Zulassungs- und Haftungsfragen zu softwarebasierten Fahrzeugsystemen, MMR 2016, 359.

[297] *Schucht,* in: *Klindt* (Hrsg.) Produktsicherheitsgesetz 3. Auflage 2021, § 1 ProdSG Rn. 41 ff.

Für einen Vergleich von Regelungsansätzen aus dem Datenschutzrecht (insbesondere den Regelungsansätzen zu *data protection by design* und *default*[298]) und dem Produktsicherheitsrecht erscheint das ProdSG geeignet, weshalb dieser Vergleich nachfolgend exemplarisch vollzogen wird. Die DSGVO dient dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und gemäß Art. 25 Abs. 1 DSGVO sollen mit den dort genannten Maßnahmen die Einhaltung der Verordnung und der Schutz der Rechte betroffener Personen gewährleistet werden. Das europäische Produktsicherheitsrecht soll beispielsweise gemäß Erwägungsgrund 4 der RL 2001/95/EG[299] (welche durch das ProdSG in Deutschland umgesetzt wurde) „einen Beitrag zum Schutz der Gesundheit und der Sicherheit der Verbraucher" über die allgemeine Produktsicherheit leisten und nach Art. 1 RL dieser Richtlinie sicherstellen, dass in Verkehr gebrachte Produkte sicher sind. Beide Regelungsgebiete, also sowohl das Datenschutzrecht, als auch das Produktsicherheitsrecht dienen dem grundrechtlichen Schutz und sollen die Grundfreiheiten der EU gewährleisten, regeln meist technische Sachverhalte bei denen lange Lieferketten existieren und eine Vielzahl an Akteuren existieren, die rechtlich verpflichtet oder berechtigt sein könnten.[300] Der Unterschied von Datenschutzrecht und Produktsicherheitsrecht besteht darin, dass letzteres vor allem an das Vorhandensein eines Produkts anknüpft sowie dessen Marktzugang und Inverkehrbringen, und nicht nur an dessen Betrieb. Gemäß § 1 Abs. 1 ProdSG gilt das Gesetz, wenn „im Rahmen einer Geschäftstätigkeit Produkte auf dem Markt bereitgestellt, ausgestellt oder erstmals verwendet werden". Adressaten können dabei grundsätzlich alle Wirtschaftsakteure sein, also alle in § 2 Nr. 29 ProdSG genannten Akteure und damit Hersteller, Bevollmächtigte, Einführer und Händler. Damit kann das ProdSG im Gegensatz zu Art. 25 DSGVO die Akteure entlang der gesamten Lieferkette unmittelbar in die Pflicht nehmen.[301] Damit existiert im Produktsicherheitsrecht ein Mechanismus zur Sicherstellung der Konformität entlang der Lieferkette, um Endkunden sichere Produkte anzubieten.

Im vorliegenden Kontext lohnt es sich, neben den gerade beschriebenen Gemeinsamkeiten und Unterschieden von Datenschutzrecht und Produktsicherheitsrecht, die Produktsicherheit im Rahmen von IT-Sicherheit zu erörtern und das Haftungsregime grundsätz-

[298] Vgl. dazu Ausführungen unter Kapitel 2 Abschnitt 2.8.

[299] Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit, *Amtsblatt Nr. L 011 vom 15/01/2002 S. 0004 – 0017.*

[300] *Vásquez/Kroschwald*, Produktdatenschutz: Verantwortung zwischen Herstellern und Anbietern, MMR 2020, 217, S. 220.

[301] Ebd.

lich zu beschreiben. Aus diesem Grund werden im Folgenden die einschlägigen produkthaftungsrechtlichen Normen analysiert. Bezüglich der IT-Sicherheit ist auf Abschnitt 4.1 und den dortigen Unterabschnitten zu verweisen.

4.3 Produkthaftung

Das Produkthaftungsrecht regelt auf zivilrechtlicher Ebene die Haftung des Herstellers für Schäden, die durch den Fehler eines Produkts entstanden sind und aufgrund dessen jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt wird (§ 1 ProdHaftG). Die Produkthaftung greift dann, wenn zum Beispiel der Unfall eines automatisierten Kraftfahrzeugs auf einen Konstruktions-, Fabrikations- oder Instruktionsfehler zurückzuführen ist.[302] Hersteller ist gemäß § 4 ProdHaftG sowohl der Produzent oder Importeur, als auch der Lieferant des fehlerhaften Bauteils. Die Produkthaftung greift verschuldensunabhängig, wobei der Geschädigte jedoch die Beweislast für den Fehler, den Schaden und der Kausalität zwischen diesen trägt (vgl. § 1 Abs. 4 S. 1 ProdHaftG).

Kommt es durch eine automatisierte Fahrfunktion zu einer Rechtsgutschädigung aufgrund fehlerhafter Fabrikation, Konstruktion oder Instruktion, kommt sowohl die verschuldensunabhängige Produkthaftung als auch die Produzentenhaftung nach § 823 Abs. 1 BGB in Betracht. Die Produkthaftung beruht auf den objektiven Sicherheitserwartungen der Allgemeinheit, der Schadensersatzanspruch auf Vorliegen eines für die Rechtsgutverletzung kausalen sicherheitsrelevanten Produktmangels zum Zeitpunkt des Inverkehrbringens.[303] Dagegen stellt die Haftung nach § 823 Abs. 1 BGB auf eine schuldhafte Verletzung von Sorgfalts- oder Verkehrssicherungspflichten seitens des Herstellers ab.[304] Trotz des divergierenden rechtlichen Ansatzes, liegt in der Rechtspraxis ein weitreichender Gleichlauf der Haftungssysteme vor.[305] Lediglich der dogmatische Anknüpfungspunkt unterscheidet sich demnach.[306] Während im ProdHaftG an das fehlerhafte Produkt angeknüpft wird, stellt § 823 Abs. 1 BGB auf die Verkehrspflichten des Herstellers ab.[307]

[302] *Greger*, Haftungsfragen beim automatisierten Fahren, NZV 2018, 1 (S. 4).

[303] BeckOK BGB/*Förster*, 62. Ed. 1.5.2022, ProdHaftG § 1 Rn. 16; MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG Einleitung Rn. 17.; BeckOK BGB/*Förster*, 62. Ed. 1.5.2022, ProdHaftG § 3 Rn. 8 f.

[304] BeckOK BGB/*Förster*, 62. Ed. 1.5.2022, BGB § 823 Rn. 677 f.; MüKoBGB/*Wagner*, 8. Aufl. 2020 BGB § 823 Rn. 949.

[305] *von Bodungen/Hoffmann*, Hoch- und vollautomatisiertes Fahren *ante portas* – Auswirkungen des 8. StVG-Änderungsgesetzes auf die Herstellerhaftung, NZV 2018, 97 (S. 98).

[306] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 3 Rn. 3.

[307] *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Straßenverkehr, Springer Gabler, 2019, S. 122.

Der anzulegende Sorgfaltsmaßstab ist indes ganz überwiegend der gleiche.[308] Haftungsszenarien im Bereich automatisierter und vernetzter Kraftfahrzeuge können beispielsweise vom Hersteller zu verantwortende mangelhafte In-Car-Technologien (gestörte Signalübertragung, defekte Sensoren, aber auch Softwarefehler) darstellen. Dies ist der Fall, wenn Daten dabei fehlerhaft erhoben, aggregiert, ausgewertet oder im Rahmen der V2V-Kommunikation falsch übermittelt werden und dies zu einem Unfall führt.[309] Zu klären gilt in diesem Zusammenhang jedoch grundlegend, ob eine Produkthaftung für fehlerhafte Daten überhaupt existiert und Softwarehersteller ebenfalls haften könnten. Dazu werden im Folgenden die Produkteigenschaft sowie die maßgeblichen Produktfehler dargestellt.

4.3.1 Produkt

Damit das Produkthaftungsrecht greift, muss das automatisierte Fahrzeug ein Produkt im Sinne des § 2 ProdHaftG sein. Produkte in diesem Sinne sind bewegliche Sachen, auch wenn sie Teil einer anderen beweglichen oder unbeweglichen Sache sind. Damit kann auch an Teilprodukte angeknüpft werden. Im Zusammenhang mit automatisierten Kraftfahrzeugen ist dies insofern von Interesse, da das Haftungsrisiko somit nicht allein bei dem Endhersteller liegt, sondern als Haftungsadressaten auch die jeweiligen Teilhersteller in Frage kommen.[310] Wobei Teil- und Endhersteller gemäß § 5 ProdHaftG gesamtschuldnerisch haften.[311]

Das automatisierte Kraftfahrzeug als Ganzes und auch gegenständliche Fahrzeugteile wie beispielsweise Reifen, Sensoren oder andere Teile stellen somit ein Produkt im Sinne des § 2 ProdHaftG dar.[312] Weiterhin sind solche Fälle wenig problematisch, bei denen fehlerhafte Daten bereits bei Inverkehrbringen des Produkts auf einem körperlichen Gegenstand (Datenträger) gespeichert und verbaut sind (Kombinationsprodukte oder sog. „*embedded systems*“). Das Produkthaftungsrecht soll in diesen Fällen unzweifelhaft gelten.[313] Demgegenüber ist die pauschale Qualifizierung von Software oder Daten als Produkt nicht ohne weiteres anzunehmen (siehe dazu Abschnitt 4.3.3).

[308] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 3 Rn. 6 f.

[309] *Ebers*, Haftung für fehlerhafte Daten beim autonomen Fahren, in: *Specht-Riemenschneider/Werry/Werry* (Hrsg.), Datenrecht in der Digitalisierung § 9.2 Rn. 30.

[310] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 2 Rn. 10.

[311] Ebd.

[312] *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Straßenverkehr, Springer Gabler, 2019, S. 118.

[313] *Ebers*, Haftung für fehlerhafte Daten beim autonomen Fahren, in: *Specht-Riemenschneider/Werry/Werry* (Hrsg.), Datenrecht in der Digitalisierung § 9.2 Rn. 36.

4.3.2 Produktfehler

Ein Fehler des Produkts liegt gemäß § 3 ProdHaftG dann vor, wenn das Produkt nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände berechtigterweise erwartet werden kann. Dazu zählen insbesondere die Darbietung, der Gebrauch mit dem billigerweise gerechnet werden kann und der Zeitpunkt, in dem dieses in den Verkehr gebracht wurde (§ 3 ProdHaftG). Der allgemeine Sorgfaltsmaßstab, den das Gesetz damit als Kriterium benennt, ist daher wie oben erwähnt derselbe, der im Rahmen der Produzentenhaftung relevant ist. Darüber hinaus ist es der Wille des Gesetzgebers die gleichen Kriterien anzuwenden.[314] Die Fehlerbegriffe sind demnach inhaltlich kongruent.[315] In Rechtsprechung und Literatur haben sich drei unterschiedliche, die Produkthaftung auslösende, Fehlerarten etabliert. Der Fabrikationsfehler, der Konstruktionsfehler sowie der Instruktions- bzw. Informationsfehler.[316]

Bezüglich automatisierter und vernetzter Kraftfahrzeuge stellen beispielsweise Fabrikationsfehler solche dar, welche sich auf die Datenerhebung und -verarbeitung auswirken könnten. Konstruktionsfehler könnten sich beispielsweise in bereits verbauter kraftfahrzeugeigener fehlerhafter Software niederschlagen und Instruktionsfehler könnten dann vorliegen, wenn der Hersteller es unterlässt, in geeigneter Weise über den konkreten Einsatzzweck einer automatisierten oder autonomen Steuerung zu informieren.

4.3.2.1 Fabrikationsfehler

Ein Fabrikationsfehler liegt vor, wenn der Hersteller den sich selbst auferlegten Standard für ein einzelnes Produkt nicht einhält, also wenn er „den für die Produktserie definierten Sicherheitsstandard verfehlt."[317] Dabei geht hier das Produkthaftungsrecht weiter als die Verkehrspflichten des § 823 BGB, da es gleichgültig ist, ob der Fehler für den Hersteller erkennbar oder vermeidbar (Ausreißerrisiko) gewesen ist oder nicht.[318]

Kommt es aufgrund einer Datenverarbeitung durch defekte Sensoren zu einer fehlerhaften Erhebung oder Aggregation, die zu einer Störung und einem Verkehrsunfall führt, kommt eine Haftung in Betracht. Ein Fabrikationsfehler kann sich auch dadurch realisieren, dass Daten aufgrund des Fabrikationsfehlers falsch übertragen werden und dieser

[314] BT-Drs. 11/2447, S. 17 f.

[315] *BGH*, Urt. v. 16.06.2009 – VI ZR 107/08, Rn. 12 (BGHZ 181, 253); Urt. v. 17.03.2009 – VI ZR 176/08, Rn. 6 (NJW 2009, 1669); MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 3 Rn. 3.

[316] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 3 Rn. 41.

[317] A.a.O., Rn. 42.

[318] BGH VersR 2007, 72 (73) – Limonadenflasche; OLG München BeckRS 2011, 10312 (MDR 2011, 540) – Piccolo-Flasche; MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 3 Rn. 42.

Übertragungsfehler ursächlich für die Rechtsgutsverletzung ist.[319] Da bei einem Fabrikationsfehler das einzelne Produkt hinter den sonst eingehaltenen Sicherheits- und Qualitätsstandards der anderen Produkte einer Serie zurückbleibt, handelt es sich nicht um einen Konstruktionsfehler, der die ganze Serie betrifft, sondern lediglich um das einzelne Produkt (hier das konkrete einzelne Kraftfahrzeug). Die Anwendung der Haftungsregelungen ist in einem solchen Fall unproblematisch und unterscheidet sich nicht von Fabrikationsfehlern herkömmlicher Kraftfahrzeuge ohne automatisierte Systeme.[320]

4.3.2.2 Instruktionsfehler

Instruktionsfehler sind solche, bei denen der Benutzer nicht oder nur unzureichend über die Art und Weise der Verwendung und deren inhärente Gefahren aufgeklärt wird.[321] Pflicht des Herstellers ist allerdings, zunächst die technischen Maßnahmen zur Gefahrenvermeidung auszuschöpfen und nicht lediglich auf (vermeidbare) Gefahren zu verweisen. Erst wenn diese Möglichkeiten enden, kann der Hersteller auf die darüberhinausgehenden nicht vollständig vermeidbaren Gefahren sowie auch über den vorhersehbaren Fehlgebrauch, umfassend und in angemessener Weise informieren.[322]

Im Zusammenhang der Fahrzeugautomatisierung beinhaltet eine ordnungsgemäße Instruktion, dass der Produktabnehmer weiß, für welchen konkreten Einsatzzweck das automatisierte System geeignet ist; wie es konfiguriert und bedient werden muss; in welchem Umfang es während des bestimmungsgemäßen Einsatzes gegebenenfalls überwacht werden muss; wie auf einen Systemausfall zu reagieren ist und wie das System zu warten ist.[323]

4.3.2.3 Konstruktionsfehler

Ein Konstruktionsfehler ist gegeben, wenn die technische Konzeption oder Planung insofern fehlerhaft war, dass bei Inverkehrbringen des Produkts eine gefahrlose Benutzung nicht möglich ist.[324] Dabei muss der Hersteller bei der Konstruktion die Maßnahmen ergreifen, die bei bestimmungsgemäßer Verwendung des Produkts zur Vermeidung einer konkreten Gefahr erforderlich, jedoch auch dem Hersteller zumutbar sind.[325] Darüber

[319] *Ebers*, Haftung für fehlerhafte Daten beim autonomen Fahren, in: *Specht-Riemenschneider/Werry/Werry* (Hrsg.), Datenrecht in der Digitalisierung § 9.2 Rn. 42 f.

[320] A.a.O., Rn. 43.

[321] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 3 Rn. 46.

[322] A.a.O., Rn. 47.

[323] *Ebers*, Haftung für fehlerhafte Daten beim autonomen Fahren, in: *Specht-Riemenschneider/Werry/Werry* (Hrsg.), Datenrecht in der Digitalisierung § 9.2 Rn. 57.

[324] BeckOK BGB/*Förster*, 62. Ed. 1.5.2022, ProdHaftG § 3 Rn. 30 f.

[325] BeckOK BGB/*Förster*, 62. Ed. 1.5.2022, BGB § 823 Rn. 705 ff.

hinaus muss die Konstruktion auch bei einem naheliegenden Fehlgebrauch, also über die bestimmungsgemäße Verwendung hinaus, gefahrlos nutzbar sein.[326] Das Produkt muss also seiner Konzeption nach den berechtigten Sicherheitserwartungen eines durchschnittlichen Benutzers genügen.

Der Konkretisierung der berechtigten Sicherheitserwartungen kommt daher eine entscheidende Rolle bei der Feststellung eines Produktfehlers zu. Die dabei einzuhaltenden Mindeststandards können in erster Linie den technischen Normen und gesetzlichen Sicherheitsbestimmungen entnommen werden. Mit Blick auf automatisierte Kraftfahrzeuge ist dabei insbesondere auf § 1 a Abs. 3 StVG zu verweisen, in dem die technischen Anforderungen der einzelnen Fahrfunktionen dahingehend bestimmt werden, dass sie den nationalen sowie internationalen Anforderungen entsprechen müssen (beispielsweise der RL 2007/46/EG respektive der VO (EU) 2018/858 oder den UNECE Regelungen). Diese technischen Anforderungen müssen sich wiederum an den Vorgaben des § 1a Abs. 2 StVG messen lassen. Damit liegt die Verantwortung für den Sicherheitsstandard grundsätzlich beim Normgeber, welcher dem Geschädigten jedoch nicht haftet.[327] Nicht staatliche Normungsvorschriften wie IEC 61508 und DIN ISO 26262 sind zwar auch von Belang,[328] allerdings zielen diese auf Fälle, in denen die Fahrzeugführung seitens eines menschlichen Fahrenden und nicht durch eine automatisierte Fahrfunktionen kontrolliert wird.[329]

Weiterhin gehört es auch zur Pflicht der Hersteller, dass die Software von Kraftfahrzeugen gegen externe Angriffe (Hackerangriffe) geschützt ist. Ein lückenloser Schutz kann dabei nicht gewährleistet werden. Das Kraftfahrzeug muss jedoch zum Zeitpunkt des Inverkehrbringens so konstruiert sein, dass der neueste Stand von Wissenschaft und Technik ausreichend und geeignet berücksichtigt respektive implementiert wurde, um Schäden zu verhindern.[330] Über das verbleibende Restrisiko muss der Hersteller sodann ausreichend warnen. Diesbezüglich finden sich in der StVG Novelle von 2021 und deren Konkretisierung in der AFGBV Neurungen. Die sich daraus ergebenden, von den Kraftfahrzeugherstellern einzuhaltenden, Anforderungen an die Sicherheit im Bereich der Informationstechnik der Datenübertragung wurden bereits oben unter 4.1.2 beschrieben.

[326] BeckOK BGB/*Förster*, 62. Ed. 1.5.2022, BGB § 823 Rn. 705.

[327] *Greger*, Haftungsfragen beim automatisierten Fahren, NZV 2018, 1 (S. 4).

[328] Vgl. *Jänich/Schrader/Reck,* Rechtsprobleme des autonomen Fahrens, NZV 2015, 313 (S. 317); *Lutz/Tang/Lienkamp*, Die rechtliche Situation von teleoperierten und autonomen Fahrzeugen, NZV 2013, 57 (S. 61).

[329] *von Bodungen/Hoffmann*, Autonomes Fahren – Haftungsverschiebung entlang der Supply Chain?, NZV 2016, 503 (S. 506).

[330] *Ebers*, Haftung für fehlerhafte Daten beim autonomen Fahren, in: *Specht-Riemenschneider/Werry/Werry* (Hrsg.), Datenrecht in der Digitalisierung § 9.2 Rn. 50.

Nachfolgend wird auf die Vorgaben aus § 1a Abs. 2 und § 1d Abs. 3 StVG näher Bezug genommen.

4.3.2.4 Vorgaben aus § 1a Abs. 2 StVG

Die Vorgaben, die § 1a Abs. 2 StVG enthält, betreffen die technische Ausrüstung, über die hoch- und vollautomatisierte Kraftfahrzeuge verfügen müssen. Dazu zählt, dass die Fahrfunktion gemäß § 1a Abs. 2 Nr. 2 StVG sämtliche – während der bestimmungsgemäßen automatisierten Fahrt – Straßenverkehrsregelungen einhalten muss. Dabei muss der anzulegende Maßstab für die einzuhaltenden (unbestimmten) Sorgfalts- und Verhaltensgrundsätze den durch die Rechtsprechung für menschliche Fahrer*innen entwickelten Maßstäben entsprechen.[331]

Bei bestimmungswidriger Verwendung muss nach § 1a Abs. 2 Nr. 6 StVG ein Systemhinweis erscheinen. Dabei ist jedoch zu beachten, dass ein solcher Hinweis nicht genügt, wenn die bestimmungswidrige Verwendung auch mit technischen Mitteln gesperrt werden kann.[332] Der geforderte Hinweis hat insofern auch Relevanz, da eine bestimmungswidrige Verwendung unzulässig ist (§ 1a Abs. 1 StVG) und sich daraus Folgen für den Sorgfaltsmaßstab ergeben (§ 1b StVG greift nicht), weshalb das System notwendigerweise die bestimmungsmäßige Verwendung zuverlässig erkennen muss (§ 1a Abs. 2 Nr. 4, 6 StVG).[333]

Die Übernahmeaufforderung nach § 1a Abs. 2 Nr. 5 StVG ist speziell vor dem Hintergrund der Mensch-Maschine-Interaktion beachtlich. Die Anforderungen an die konkrete Ausgestaltung von derartigen Interface-Gestaltungen, die unmittelbar mit der Kraftfahrzeugsteuerung zusammenhängen und damit sicherheitsrelevant sind, müssen besonders hoch sein.[334] Beispielsweise macht die bereits oben erwähnte UNECE Regelung 79 weit-

[331] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 117.

[332] Ebd.; *Berndt,* Der Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes – ein Überblick, SVR 2017, 121 (S. 123).

[333] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 118.

[334] *von Bodungen/Hoffmann*, Autonomes Fahren – Haftungsverschiebung entlang der Supply Chain?, NZV 2016, 503 (S. 505); *Franke*, Rechtsprobleme beim automatisierten Fahren – ein Überblick, DAR 2016, 61 (S. 63).

gehend alternativlose Vorgaben für die Ausgestaltung der Interaktion bei Assistenzsystemen, insbesondere bezüglich akustischer, visueller und haptischer Warnhinweise.[335] Bezüglich automatisierter Fahrfunktionen wird dies in mindestens gleichem Maß umgesetzt werden müssen.[336]

Zusammenfassend ist zu sagen, dass ein Produktfehler eines automatisierten Fahrzeugs alle drei Fehlerarten betreffen kann. Die Vorgaben des § 1a StVG sind für automatisierte Kraftfahrzeuge dahingehend von besonderer Bedeutung, dass diese als Beurteilungsmaßstab für etwaige Konstruktionsfehler herangezogen werden können. Ursächlich dafür ist, dass § 1a StVG für den Hersteller zwingend einzuhaltende technische Vorgaben macht, aufgrund derer ein Haftungsanspruch entstehen kann. Es liegt demnach in der Verantwortung des Herstellers, dass bei der automatisierten Fahrt den in § 1a Abs. 2 StVG genannten Grundsätzen in jeder Verkehrssituation entsprochen wird.

4.3.2.5 Technische Aufsicht § 1d Abs. 3 StVG-Neu

Die mit der Gesetzesnovelle 2021 neu eingeführte sogenannte Technische Aufsicht kann haftungsrechtlich nicht als klassische Kraftfahrzeugführer*in eingeordnet werden, da diese sich nicht im Kraftfahrzeug befindet und dieses gemäß § 18 Abs. 1 StVG führt. Die im Kraftfahrzeug beförderten Personen haben auch keinen Einfluss auf die von der Technischen Aufsicht freigegebenen Fahrmanöver, wobei die Technische Aufsicht wiederum lediglich im Rahmen der vom System vorgeschlagenen Parameter handeln kann.[337] Während der autonomen Fahrt ist die Technische Aufsicht jedoch die einzige (zwingend natürlich) Person, die unmittelbar und individuell eine menschliche Entscheidung in der konkreten Fahrsituation treffen kann, womit angenommen werden könnte, dass hier eine Ausgestaltung als Verschuldenshaftung in Frage kommt.[338] Ein Fehlverhalten der Technischen Aufsicht wäre also wie ein vermutetes Verschulden der kraftfahrzeugführenden Person anzusehen. Diese Sichtweise wurde jedoch nicht in die Neuregelungen des StVG übernommen. Da die Fahrer*innenhaftung nicht auf die Technische Aufsicht übertragen werden kann, haftet die als Technische Aufsicht eingesetzte Person nur nach allgemeinen deliktischen Grundsätzen, also gemäß § 823 Abs. 1 BGB.

[335] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 118.

[336] Ebd.

[337] *Schrader*, Neujustierung der Gefährdungs- und Verschuldenshaftung bei der Fahrzeugautomatisierung, DAR 2022, 9, (S. 12).

[338] *Schrader*, Neujustierung der Gefährdungs- und Verschuldenshaftung bei der Fahrzeugautomatisierung, DAR 2022, 9, (S. 12).

Zu berücksichtigen ist hierbei jedoch auch, dass der Gesetzgeber festgelegt hat, dass die Technische Aufsicht zwingend in die Haftpflichtversicherung der Halter*innen aufzunehmen ist (vgl. § 1 S. 2 Pflichtversicherungsgesetz). Letztlich bleibt die Halter*innenhaftung als reine Gefährdungshaftung bestehen und bietet damit einen, für alle beim Betrieb des Kraftfahrzeugs entstanden Personen- und Sachschäden, umfassenden Opferschutz.[339]

Hinsichtlich der Cybersicherheit ist mit der Schaffung der Technischen Aufsicht und der dadurch notwendigen Kommunikationsschnittstelle, über welche Fahrmanöver freigegeben werden können, womöglich ein neues Einfallstor für Hacker geschaffen worden.[340] Da wie beschrieben kein neuer Haftungstatbestand für die Technische Aufsicht vorgesehen ist, kommen hier nur die Regelungen des allgemeinen Deliktsrechts in Betracht. Ein solcher Haftungsfall läge vor, wenn die Technische Aufsicht gemäß § 823 Abs. 1 BGB schuldhaft einen Cyberangriff ermöglichte.[341] Durch die Übernahme der Aufsicht über eine Gefahrenquelle übernimmt die Technische Aufsicht auch die Pflicht mit angemessenen Mitteln dafür zu sorgen, dass nicht in den Betrieb eingegriffen wird. Eine solche Pflicht zum Treffen von Sicherheitsvorkehrungen gegen Cyberangriffe ergibt sich zwar nicht direkt aus § 1d Abs. 3 oder § 1 f Abs. 2 StVG, da dort nur die Pflichten für den Normalbetrieb geregelt sind, erscheint aber aus der beschriebenen Übernahme der Aufsicht über eine potenziell erhebliche Gefahrenquelle geboten.[342] Die Technische Aufsicht muss demnach ihre Systeme warten und dafür sorgen, dass beispielsweise keine Zugangsdaten missbräuchlich verwendet werden oder über Sicherheitslücken in der Software der Technischen Aufsicht Angriffe erfolgen.

Hier wird deutlich, dass es künftig noch weiterer intensiver Forschung und Beobachtung der Praxis unter dem neu geschaffenen Rechtsrahmen bedarf.

4.3.3 Spezieller Fall Software-Fehler

Der spezielle Fall von Produkthaftung und Software spielt im Rahmen automatisierter Kraftfahrzeuge eine wichtige Rolle. Grundsätzlich war und ist umstritten, ob Software ohne weiteres als Produkt im Sinne des ProdHaftG anzusehen ist.[343] Einfacher ist es, wenn es sich zweifelsfrei um sogenannte Kombinationsprodukte handelt, bei denen physische

[339] *Schrader*, Wohin steuert das autonome Fahrzeug – vorübergehend?, ZRP 2021, 109, S. 111.

[340] *Schwartz,* Virtuelle Schwarzfahrer – Haftung für Cyberangriffe auf selbstfahrende Fahrzeuge, DSRITB 2021, 305 (S. 309).

[341] A.a.O., S. 316.

[342] Ebd.

[343] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 2 Rn. 16 ff.; *Lehmann*, Produkt- und Produzentenhaftung für Software, NJW 1992, 1721 (S. 1722 ff.).

Gegenstände eine eingebettete Software besitzen. Diese sind als Produkt iSd. § 2 ProdHaftG anzusehen.[344]

Um Software prinzipiell einzuordnen, bedarf es der Auslegung von § 2 ProdHaftG. Wie oben dargestellt, ist ein Produkt eine bewegliche Sache. Es bietet sich daher an, hilfsweise § 90 BGB heranzuziehen, in dem Sachen als körperliche Gegenstände definiert werden. Das ProdHaftG beruht zwar auf einer europäischen Richtlinie[345] und ist daher autonom auszulegen, allerdings kann auch bei einer solchen eigenständigen Betrachtung jedenfalls davon ausgegangen werden, dass ein körperlicher Gegenstand als Sache anzusehen ist,[346] womit das Kraftfahrzeug an sich und diverse einzelne Teile als Produkt anzusehen sind.

Im Fall von Software ist indes davon auszugehen, dass diese nicht körperlich ist, sondern ein Programm, welches einer Maschine mit Hilfe von Daten, Anweisungen erteilt.[347] Software war zwar in der Vergangenheit klassischerweise auf einem Datenträger gespeichert, weshalb man die erforderliche Körperlichkeit diesem zusprach,[348] allerdings scheint diese Auslegung vor dem Hintergrund neuer Entwicklungen nicht mehr überzeugend. Insbesondere vor dem Hintergrund von sogenannten Streamingdiensten, bei welchen die Anweisungen extern ausgeführt werden und lediglich das Ergebnis übertragen wird, erscheint das Abstellen auf einen Datenträger nicht praktikabel. Eine beim Nutzer gleichwie verkörperte Form der Software liegt dabei zu keiner Zeit vor.[349] Das führt letztlich dazu, dass es bei einer solchen Sichtweise zu Situationen kommen kann, bei denen ein Hersteller fehlerhafte Software beispielsweise einerseits auf einem USB-Stick vertreibt und damit durch ein Produkt im Sinne des ProdHaftG verantwortlich ist und andererseits die gleiche Software mit den gleichen Fehlern, die zu einer Rechtsgutverletzung führen kann, über einen Streamingdienst vertreibt und es sich dann um kein Produkt handelt, für welches er haften muss.[350] Noch willkürlicher erscheint, an der Körperlichkeit festzuhalten, wenn die Software überhaupt nicht mehr heruntergeladen wird, sondern lediglich über das Internet genutzt wird und damit das Programm vollständig in der Cloud verbleibt. In

[344] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 2 Rn. 21.

[345] Richtlinie 85/374/EWG des Rates vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, ABIEG Nr. L 210/29 v. 7. 8. 1985.

[346] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 2 Rn. 2; *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Straßenverkehr, Springer Gabler, 2019, S. 119.

[347] *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Straßenverkehr, Springer Gabler, 2019, S. 119.

[348] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 2 Rn. 17 ff.

[349] *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Straßenverkehr, Springer Gabler, 2019, S. 119.

[350] A.a.O., S. 119 f. m.w.N.

einem solchen Fall wäre nach bisheriger Auslegung das ProdHaftG nicht anwendbar.[351] Das frühere Abstellen auf die Verkörperung einer Sache ist demnach nicht mehr überzeugend.

Die Europäische Kommission antwortete bereits 1989 auf die Frage,[352] ob die Produkthaftungs-Richtlinie, auf der das ProdHaftG beruht, auch Computer-Software umfasst, kurz und pauschal indem sie es ohne weitere Angabe von Gründen bejahte.[353] In der Literatur wird darüber hinaus auch vertreten, dass im Sinne des grundsätzlichen Zwecks des ProdHaftG – dem Opferschutz – § 2 ProdHaftG weit auszulegen sei und damit Software als Produkt im produkthaftungsrechtlichen Sinne anzusehen ist.[354] Das herkömmliche Kraftfahrzeug, das geradezu symbolisch für ein Produkt steht und auf welches eine Software übertragen wird, bleibt selbstverständlich weiterhin eine körperliche Sache, von der eine Gefahr ausgeht, die sich ursächlich in der Softwaresteuerung verwirklichen und damit die Gefährlichkeit des Produkts begründen kann.[355] Mit Blick auf automatisierte Kraftfahrzeuge, bei welchen die Steuerung (je nach Automatisierungsgrad) ganz überwiegend durch Software vollzogen wird, erscheint es nur konsequent, diese Software auch als Produkt anzuerkennen. Darüber hinaus ist es gerade in den höheren Level der Automatisierung schlicht kaum mehr möglich, die Steuerungssoftware von der Hardware zu trennen, weshalb ein Softwarefehler ebenfalls als Produktfehler erachtet werden sollte. Damit würde der vom Gesetzgeber verfolgte Schutz auch für automatisierte Kraftfahrzeuge aufrechterhalten werden.[356]

4.3.4 Produktbeobachtungspflicht

Im Zusammenhang von Fahrzeugautomatisierung und der Frage nach den Möglichkeiten der (Softwaregestützten) Steuerung von Kraftfahrzeugen ist weiterhin die Produktbeobachtungspflicht näher zu betrachten. Im bisherigen System von Verschuldens- und Gefährdungshaftung wurde ein weitgehender Gleichlauf beider Haftungssysteme vor Inverkehrbringen des Produkts angenommen.[357] Nachdem das Produkt in Verkehr gebracht

[351] MüKo-BGB/*Wagner*, 8. Auflage 2020, ProdHaftG § 2 Rn. 17

[352] Amtsblatt der Europäischen Gemeinschaften, Frage Nr. 706/88, ABl. C 114 v. 8.5.1989, S. 42.

[353] A.a.O., Antwort 89/C 114/76, S. 42.

[354] MüKo-BGB/*Wagner*, 8. Auflage 2020, ProdHaftG § 2 Rn. 22 ff.; ähnlich *Redeker*, IT-Recht, 7. Auflage 2020, Rn. 878.

[355] Vgl. *Wagner*, Produkthaftung für autonome Systeme AcP 217, S. 714 f.

[356] *Hey*, Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Straßenverkehr, Springer Gabler, 2019, S. 120.

[357] *Schrader*, Neujustierung der Gefährdungs- und Verschuldenshaftung bei der Fahrzeugautomatisierung, DAR 2022, 9 (S. 10).

wurde, greift lediglich die Verschuldenshaftung. Es kommt also maßgeblich auf den Zeitpunkt der Inverkehrgabe an.[358] Begründet wurde dies damit, dass die Hersteller ab Verlassen des Werkstores („Werktorprinzip") keinen Einfluss mehr auf das Produkt und den davon ausgehenden Gefahren haben.[359] Diese Ansicht hat trotz einiger Kritik[360] im Schrifttum größtenteils Anklang gefunden, kann jedoch durch technische Entwicklungen und Möglichkeiten der softwarebasierten Steuerung eines Produkts und der damit einhergehenden Einflussnahme seitens der Hersteller auf die vom Produkt ausgehenden Gefahren auch nach Inverkehrgabe nicht mehr ohne weiteres überzeugen.[361] Der Umstand, dass sich Software nie vollständig fehlerfrei programmieren lassen kann, wirkt nicht haftungsbefreiend, weshalb insbesondere im Rahmen automatisierter und vernetzter Kraftfahrzeuge ein hohes Risikopotenzial mit außerordentlichem Kontrollaufwand einhergeht.[362] Daher kommt der Produktbeobachtungspflicht hier eine wichtige Rolle zu. Da das ProdHaftG keine Produktbeobachtungspflichten kennt, ist hier auf den bereits erwähnten § 823 Abs. 1 BGB zu verweisen. Demnach sind Hersteller verpflichtet, Produkte hinsichtlich drohender Gefahren nach Inverkehrgabe zu beobachten und sofern diese Gefahren erkannt wurden, sind die Endabnehmer darüber zu informieren.[363]

Hinsichtlich vernetzter und automatisierter Kraftfahrzeuge könnte eine Möglichkeit der Produktbeobachtung (vorausgesetzt in datenschutzkonformer Weise durchgeführt) in der Erhebung und Auswertung von Kraftfahrzeugdaten gesehen werden. Sofern der Hersteller Drittanbietern die Möglichkeit eröffnet hat, Software auf das Kraftfahrzeug aufzuspielen, trifft ihn ebenfalls die Pflicht zur Kontrolle und Beobachtung dieser Drittsoftware.[364] Da mit Einführung der AFGBV ebenfalls die Kommunikation von Kraftfahrzeugen untereinander geregelt ist und dafür Mindestanforderungen definiert wurden,[365] ist auch eine Beobachtungspflicht seitens der Hersteller für die Interaktion mit anderen Kraftfahrzeugen zu bejahen. Hieraus ergibt sich ein hoher Aufwand für die Hersteller, der

[358] *Schrader*, Neujustierung der Gefährdungs- und Verschuldenshaftung bei der Fahrzeugautomatisierung, DAR 2022, 9 (S. 10).

[359] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 1 Rn. 24 f.

[360] BeckOK BGB/*Förster*, 62. Ed. 1.5.2022, ProdHaftG § 1 Rn. 39; BeckOK BGB/*Förster*, 62. Ed. 1.5.2022, BGB § 823 Abs. 1 Rn. 678.

[361] *Schrader*, Neujustierung der Gefährdungs- und Verschuldenshaftung bei der Fahrzeugautomatisierung, DAR 2022, 9 (S. 10).

[362] *Ebers*, Haftung für fehlerhafte Daten beim autonomen Fahren, in: *Specht-Riemenschneider/Werry/Werry* (Hrsg.), Datenrecht in der Digitalisierung § 9.2 Rn. 51.

[363] BGH Urt. v. 27.9.1994 – VI ZR 150/93, NJW 1994, 3349 (S. 3350); BGH Urt. v. 16.12.2008 – VI ZR 170/07, NJW 2009, 1080 (S. 1081).

[364] *Ebers*, Haftung für fehlerhafte Daten beim autonomen Fahren, in: *Specht-Riemenschneider/Werry/Werry* (Hrsg.), Datenrecht in der Digitalisierung § 9.2 Rn. 59.

[365] Vgl. Ausführungen unter Abschnitt 4.1.2.2.

jedoch aufgrund des hohen Gefahren- und Risikopotenzials, welches von dem in Verkehr gebrachten Produkt ausgeht, gerechtfertigt ist.

Eine datenschutzkonforme Produktbeobachtung mittels Zugriff auf Daten aus dem Kraftfahrzeug könnte einerseits dadurch realisiert werden, dass die Daten lediglich in anonymisierter Form ausgewertet werden und damit das Datenschutzrecht in diesem Fall keine Anwendung findet. Andererseits wird eine solche anonyme Verarbeitung, wie in Abschnitt 1.2 erörtert, nur in begrenztem Maß erfolgen können. Da sich wie zuvor beschrieben die Produktbeobachtungspflicht nicht aus dem Produkthaftungsrecht, sondern aus einer von der Rechtsprechung entwickelten Pflicht, die aus der Produzentenhaftung gemäß § 823 BGB entwickelt wurde, ergibt, mangelt es hier an einer Rechtsgrundlage (Art. 6 Abs. 1 lit. c DSGVO)[366] für die Datenverarbeitung. Möglich erscheint jedoch ein Rückgriff auf die Interessenabwägungsklausel nach Art. 6 Abs. 1 lit. f DSGVO.[367] Da die Anforderungen an den Hersteller, die sich aus seiner Produktbeobachtungspflicht ergeben hoch sind, wird er sich für die Datenverarbeitung in diesem Zusammenhang auf ein berechtigtes Interesse berufen können.[368] Die Datenverarbeitung darf in diesem Fall nur für den Zweck der Produktbeobachtung erfolgen und hat sich an dem Grundsatz der Datenminimierung zu orientieren. Neben der auf das notwendigste Maß zu reduzierenden Verarbeitung und strengen Zweckbindung an die Beobachtungspflicht, hat der Hersteller dann auch seine Informationspflichten nach Art. 13 und 14 DSGVO zu wahren.[369]

4.3.5 Herstellerseitige Haftung für Schäden durch Cyberangriffe

Die mit der Vernetzung einhergehenden Risiken automatisierter Kraftfahrzeuge begründen einerseits die rechtmäßige Erwartung an eine datenschutzkonforme Ausgestaltung des Kraftfahrzeugs, andererseits ist auch im Datenschutzrecht bereits die Anforderung nach Datensicherheit angelegt. Muss der Hersteller gemäß Art. 25 DSGVO (*data protection by design* und *default*)[370] das Kraftfahrzeugsystem durch geeignete technische und organisatorische Maßnahmen datenschutzkonform absichern, so muss dieser auch im Rahmen der Datensicherheit, den ordnungsgemäßen Ablauf der Datenverarbeitung sicherstellen und die Daten vor Missbrauch, Beschädigung und Verlust schützen (Art. 32 DSGVO). Die Endnutzer können im Rahmen der Datensicherheit nach Art. 32 DSGVO die berechtigte Erwartung geltend machen, dass das Kraftfahrzeug gegen Cyberangriffe

[366] Vgl. Ausführungen unter Abschnitt 2.7.3.

[367] Vgl. Ausführungen unter Abschnitt 2.7.4.

[368] *Preuß,* Haftungsrecht beim Einsatz hoch- und vollautomatisierter sowie vollautonomer Fahrzeuge, 2021, S. 217 f.

[369] A.a.O., S. 218.

[370] Ausführungen unter Abschnitt 2.8.

geschützt ist.[371] Konkrete Maßnahmen und Umsetzungsmöglichkeiten solcher Anforderungen können konstruktiver Art sein oder auch durch gezielte Aufteilung von Befugnissen der für die Datenverarbeitung Verantwortlichen oder durch Protokollierungen umgesetzt werden.[372] Auch der Nachweis eines Cybersicherheitszertifikats kann eine Maßnahme sein, um im Kontext der Haftung für Rechtssicherheit zu sorgen. Damit könnte bescheinigt werden, dass das Kraftfahrzeug zum Zeitpunkt der Inverkehrgabe keine potenzielle Cybergefahr dargestellt hat. Die konkrete Ausgestaltung eines solchen Mechanismus und die Anforderungen daran, wie beispielsweise die Bescheinigung, dass das Kraftfahrzeug technisch in der Lage ist Angriffe auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Verarbeiteten Daten zu gewährleisten und Angriffe abzuwehren, also die Gewährleistung von Cybersicherheit sicherzustellen, ist in den Abschnitten 4.1 und den dazugehörigen Unterabschnitten beschrieben.

4.3.6 Ausschluss Produktfehlerhaftung

§ 1 Abs. 2 ProdHaftG schließt unter den dort genannten Umständen die Haftung des Herstellers aus. Für die Fahrzeugautomatisierung und speziell für den in diesem Beitrag interessierenden Kontext sind insbesondere § 1 Abs. 2 Nr. 4 und 5 ProdHaftG von Belang. § 1 Abs. 2 Nr. 4 ProdHaftG schließt die Haftung aus, wenn der Fehler darauf beruht, dass das System bei Inverkehrbringen den geltenden zwingenden Rechtsvorschriften entsprochen hat. Dieser Ausschlussgrund soll den Hersteller aus der Zwangslage befreien, in die er lediglich aufgrund der Befolgung rechtlicher Vorschriften gerät.[373] Dabei ist nur auf die tatsächlich rechtlich bindenden Vorschriften abzustellen. Der Hersteller soll sich also nicht auf einen Haftungsausschluss aufgrund der Einhaltung von Normen privater Normungsinstitute (DIN, VDI, VDE etc.) berufen können.[374] Die Normen müssen vielmehr rechtlich bindende Wirkung haben, welche eine abweichende Konstruktion ausschließt und die technischen Vorgaben so präzise sein, dass kein Ausgestaltungsspielraum besteht.[375]

Mit Blick auf automatisierte Kraftfahrzeuge hat beispielsweise § 1a Abs. 3 StVG Relevanz, da dieser auf verbindliche technische Anforderungen verweist, welche das automatisierte

[371] *Preuß,* Haftungsrecht beim Einsatz hoch- und vollautomatisierter sowie vollautonomer Fahrzeuge, 2021, S. 174 f.

[372] A.a.O., S. 175.

[373] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 1 Rn. 43

[374] A.a.O., Rn. 44.

[375] A.a.O., Rn. 44 ff.

System einhalten muss.[376] Damit ist § 1a Abs. 3 StVG eine solche rechtlich zwingende Vorschrift.[377] Die dort genannten Verweise beziehen sich auf die technischen Anforderungen, welche sich aus den entsprechenden UNECE-Regelungen ergeben beziehungsweise nach Art. 39 Abs. 2 bzw. Art. 57 VO (EU) 2018/858[378] einzuhalten sind.

Zweiter relevanter Haftungsausschlussgrund im vorliegenden Kontext ist gemäß § 1 Abs. 2 Nr. 5 ProdHaftG, dass der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte. Die Beweislast dafür trägt insoweit der Hersteller selbst.[379] Die Einhaltung technischer Normen kann dabei zwar den Beweis erleichtern,[380] allerdings genügt dies nicht automatisch, wenn die technische Entwicklung tatsächlich bereits darüber hinaus gegangen ist.[381] Da § 1a Abs. 3 StVG allerdings vorschreibt, dass automatisierte Kraftfahrzeuge zwingenden technischen Normen entsprechen müssen, wird es auf den § 1 Abs. 2 Nr. 5 ProdHaftG regelmäßig nicht ankommen.[382] Damit liegt die Verantwortung für die Sicherheit automatisierter Kraftfahrzeugsysteme letztlich beim Normgeber, welcher dem einzelnen Geschädigten jedoch nicht haftet.

Bezüglich autonomer Systeme, welche durch lernfähige Algorithmen gesteuert werden, wird zudem die Ansicht vertreten, dass das Verhalten eines solchen Systems in einer konkreten Gefahrensituation für den Hersteller nicht vorhersehbar sei und daher als Entwicklungsrisiko einzustufen wäre.[383] Dieser Ansicht ist jedoch nicht zu folgen, da es bei dem Begriff des Entwicklungsrisikos nicht darum geht, dass der Hersteller das Verhalten des autonomen Systems in der konkreten Gefahrensituation hätte vorhersehen können,

[376] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 124.

[377] *Greger*, Haftungsfragen beim automatisierten Fahren, NZV 2018, 1 (S. 4).

[378] Verordnung (EU) 2018/858 des Europäischen Parlaments und des Rates vom 30.5.18 über die Genehmigung und die Marktüberwachung von Kraftfahrzeugen und Kraftfahrzeuganhängern sowie von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge, zur Änderung der Verordnungen (EG) Nr. 715/2007 und (EG) Nr. 595/2009 und zur Aufhebung der Richtlinie 2007/46/EG.

[379] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 1 Rn. 86.

[380] Ebd.

[381] *Ensthaler/Gollrad*, Rechtsgrundlagen des automatisierten Fahrens – Standardessentielle Patente und Fahrzeugvernetzung, Zulässigkeit und Zulassung, Haftungsrecht, Datenschutz, Datensicherheit und Datenhoheit, Deutscher Fachverlag, Fachmedien Recht und Wirtschaft, 2019, S. 125.

[382] *Greger*, Haftungsfragen beim automatisierten Fahren, NZV 2018, 1 (S. 4).

[383] So jedenfalls *Droste*, Intelligente Medizinprodukte: Verantwortlichkeiten des Herstellers und ärztliche Sorgfaltspflichten, MPR 2018, 109 (S.111).

sondern vielmehr ob das Autonomierisiko erkennbar war.[384] Die dafür nötigen Kenntnisse liegen zweifelsfrei beim Hersteller solcher Produkte und eine pauschale Entlastung mit Rücksicht auf § 1 Abs. 2 Nr. 5 ProdHaftG ist daher nicht in Betracht zu ziehen.[385]

[384] MüKoBGB/*Wagner*, 8. Aufl. 2020, ProdHaftG § 1 Rn. 61.

[385] Ebd.

5. Zusammenfassung: Rechtliche Anforderungen an eine vertrauenswürdige IT im Kraftfahrzeug

Wie die Ausführungen in Kapitel 1 bis 4 gezeigt haben, sind die rechtlichen Anforderungen an automatisierte und vernetzte Kraftfahrzeuge – analog zur technischen Entwicklung – kontinuierlich im Wandel. Rechtliche und technische Vorgaben bedingen und überholen sich teilweise gegenseitig. Dies hat zur Folge, dass es einer ständigen Beobachtung, aber auch eines kontinuierlichen Mitdenkens der verschiedenen Disziplinen bedarf. Zur datenschutzkonformen Ausgestaltung von automatisierten Kraftfahrzeugen gehört die Beachtung der in den Kapiteln 2 bis 4 beschriebenen rechtlichen Anforderungen.

Es kann festgehalten werden, dass Daten, die im Zusammenhang mit automatisierten Kraftfahrzeugen generiert und verarbeitet werden, in der Regel als personenbezogene Daten im Sinne des Art. 4 DSGVO anzusehen sind. Obgleich es auf den konkreten Anwendungsfall ankommt und das Kraftfahrzeug und dessen Steuerung insgesamt zu betrachten sind, hat sich die Sichtweise dahingehend entwickelt, dass Kraftfahrzeugdaten regelmäßig als personenbezogene Daten nach Art. 4 Nr. 1 Hs. 1 DSGVO anzusehen sind.[386] Bei der Beurteilung, ob ein Datum Datenschutzrelevanz hat oder nicht, spielen Aspekte wie Datenart, Format oder Speichermedium keine Rolle. Entscheidend ist einzig der Personenbezug, also ob der Bezug zu einer natürliche Person hergestellt werden kann oder diese nur identifizierbar ist.[387] Die damit einhergehende Einordnung als personenbezogenes Datum hat die konsequente Anwendung des Datenschutzrechts als Abwehrrecht der betroffenen Person gegenüber der verantwortlichen Stelle zur Folge.[388] Dementsprechend wichtig ist es, dass bisher wenig aussagekräftige Schlagworte wie *data protection by design* mit konkreten Vorschlägen und technischen Maßnahmen gefüllt werden und beispielsweise Methoden bezüglich sinnvoller und wirksamer Pseudonymisierung tatsächlich erarbeitet werden.

Mit dieser Erkenntnis, des anzunehmenden Personenbezugs (Art. 4 DSGVO) einerseits und der eigentlichen Wichtigkeit der Konkretisierung und Ausarbeitung von tatsächlichen Maßnahmen andererseits, sind im hier interessierenden Kontext Art. 5, 24, 32 DSGVO und vor allen Dingen Art. 25 DSGVO anwendbar, welcher die Vorgaben zum

[386] *Reiter*, Verbraucher sitzen vorne: Für einen fairen Zugang zu Fahrzeugdaten, DAR 2022, 123, S. 123; *Brockmeyer*, Teil 15.5 Big Data im vernetzten Verkehr, in: *Hoeren/Sieber/Holznagel* (Hrsg.) Handbuch Multimedia-Recht, Werkstand: 57. EL September 2021, Rn. 22 ff.

[387] *Brockmeyer,* Teil 15.5 Big Data im vernetzten Verkehr, in: *Hoeren/Sieber/Holznagel* (Hrsg.) Handbuch Multimedia-Recht, Werkstand: 57. EL September 2021, Rn. 22.

[388] *Reiter*, Verbraucher sitzen vorne: Für einen fairen Zugang zu Fahrzeugdaten, DAR 2022, 123, S. 123.

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen beinhaltet. Rechtliche Anforderungen an die IT- und Cybersicherheit finden sich in den Neuregelungen des StVG, der dazugehörigen AFGBV und den entsprechenden UNECE-Regelungen 155 und 156. Die dort identifizierten Vorgaben gilt es, in technische Anforderungen zu übersetzen und technische Maßnahmen daraus abzuleiten.[389] So ist es möglich, die Technik anhand der rechtlichen Vorgaben zu entwickeln. Dadurch kann den Vorgaben *data protection by design* und *data protection by default* in einem Maße Rechnung getragen werden, welches über die sonst in der Literatur eher generischen und wiederholten Forderungen diesbezüglich, hinausgeht. Das Forschungsprojekt VITAF konnte hier einen entscheidenden Beitrag leisten und eine Momentaufnahme des Stands der Technik und des Stands des Rechts liefern. Gleichzeitig wurden bereits die Vorgaben für zukünftig zu entwickelnde Kraftfahrzeuge analysiert und eingeordnet.

[389] Eine solche konkrete Ausarbeitung findet sich in: *Arzt/Kleemann/Plappert/Rieke/Zelle*, Datenverarbeitung und Cybersicherheit in der Fahrzeugautomatisierung – Rechtliche und technische Anforderungen im Verbund, MMR 2022, 593-614.

6. Ausblick und Forschungsbedarfe

Die Ausführungen haben gezeigt, dass es einen kontinuierlichen Forschungsbedarf bezüglich der Vernetzung und Automatisierung von Kraftfahrzeugen gibt. Die rechtlichen Vorgaben in §§ 1d-1l StVG beinhalten Regelungen für Kraftfahrzeuge, die heute noch nicht auf unseren Straßen unterwegs sind. Hier wird die Technik jedoch vermutlich schnell nachziehen und irgendwann auch darüber hinaus Anwendungen entwickeln, die sodann ebenfalls wieder eines rechtlichen Rahmens bedürfen. Auf der anderen Seite wurden mit der Einführung des TTDSG als letzte Umsetzung der ePrivacy-RL in nationales Recht bereits jetzt neue Regelungen geschaffen, die hier einschlägig sein könnten. Aufgrund der Öffnungsklausel in Art. 95 DSGVO gehen die Regelungen der ePrivacy-RL auch denen der DSGVO vor. Hier gilt es im Anschluss an diese Ausarbeitung zu untersuchen, ob und inwiefern das TTDSG auf automatisierte beziehungsweise vernetzte Kraftfahrzeuge Anwendung findet.[390]

Außerdem werden mit der (vermutlich bald zu erwartenden) Verabschiedung der ePrivacy-VO weitere neue Regelungen in Kraft treten, die im hiesigen Kontext Anwendung finden. Da die ePrivacy-VO ebenfalls *lex specialis* zur DSGVO sein wird,[391] ist es unumgänglich, hier weitere Forschung zu betreiben und diese neuen Entwicklungen künftig zu berücksichtigen. Zudem werden aktuell mit dem Entwurf einer Verordnung zur Regelung von Künstlicher Intelligenz[392] auf EU-Ebene weitere neue Regeln geschaffen, die auch den Bereich des künftigen autonomen Fahrens zum Inhalt haben könnten. Auch hier entstehen Anknüpfungspunkte, die weitere Forschung unumgänglich machen. Es bedarf in diesem Kontext vornehmlich interdisziplinärer Forschung unter künftig wesentlich intensiverer Betrachtung der Kraftfahrzeugarchitektur als ein holistisches Gesamtkonzept. Datenschutz, Cybersicherheit, aber auch *safety* und *security* müssen gemeinsam betrachtet und bewertet werden. Technikentwicklung muss dabei immer auch den Grundrechten und Grundfreiheiten der Bevölkerung dienen, weshalb unterschiedliche wissenschaftliche Disziplinen diese Zukunft gemeinsam gestalten sollten.

[390] Siehe hierzu auch Ausführungen unter 2.1.2.

[391] *Roßnagel*, in: *Simitis/Hornung/Spiecker gen. Döhmann* (Hrsg.), Datenschutzrecht, Art. 98 Rn. 13.

[392] Vorschlag für eine Verordnung der Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM 2021(206) final vom 21.04.2021.

Kleemann & Arzt: Vertrauenswürdige IT für autonomes Fahren

Die Automatisierung und Vernetzung von Kraftfahrzeugen wird seit Jahren in Fachkreisen wie in den Medien breit diskutiert. Nicht selten wird diese insbesondere im ÖPNV als wichtiger Baustein der dringend notwendigen Verkehrswende gesehen. Bei der Umsetzung spielen auch rechtliche Aspekte eine wichtige Rolle. Das vom Bundesministerium für Bildung und Forschung (BMBF) finanzierte Projekt „Vertrauenswürdige IT für autonomes Fahren – VITAF“ (FKZ: 16KIS0839) hat zwischen Januar 2019 und März 2022 intensiv zu verschiedenen Aspekten der Vertrauenswürdigkeit der notwendigen IT geforscht.

Die Autoren des FÖPS Berlin befassten sich im Rahmen des Projekts VITAF mit zentralen Fragen der IT-Sicherheit und Datensicherheit, des Datenschutzes sowie der Produkthaftung in automatisierten Kraftfahrzeugen aus Sicht des deutschen, europäischen und internationalen Rechts. Die Ergebnisse der Untersuchung werden in dieser Publikation zusammengefasst. Die Darstellung geht dabei in einem Schwerpunkt auf die relevanten Änderungen im Straßenverkehrsgesetz ein, insbesondere die 2021 erfolgte Novelle des StVG mit den §§ 1d-l StVG sowie die damit verbundene Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung (AFGBV).

Die Ergebnisse der derzeit auf europäischer Ebene diskutierten Digitalrechtspakete (bspw. KI-VO, ePrivacy-VO, Data Act oder DSA) konnten aufgrund der Projektlaufzeit nicht mehr im Detail berücksichtigt werden, auch wenn sie wichtige Anknüpfungspunkte für die künftige Regulierung automatisierten Fahrens enthalten. Hier besteht demzufolge weiterer Forschungsbedarf.

Herausgeber: Forschungsinstitut für öffentliche und private Sicherheit
(FÖPS Berlin) der Hochschule für Wirtschaft und Recht Berlin
Alt-Friedrichsfelde 60, 10315 Berlin – www.foeps-berlin.org