



Vernetzte und autonome Mobilität

Herausforderungen für Cybersicherheit und Datenschutz sowie Gewährleistungs- und Haftungsrecht

Autoren:

Klaus Brisch LL.M., Dr. Jens Eckhardt, Prof. Dr. Marcus Gelderie,
Daniel Groß, Thorsten Jansen LL.M., Tobias Knoben,
Marco Müller-ter Jung LL.M., Prof. Dr.-Ing. Dr. h.c. Dieter Schramm,
Nils Steffen, Thorsten Stuke, Thomas Weber



Inhalt

1. Vorwort	4
2. Ökosystem Mobilität.	5
2.1 Mobilität 2030 – ein Blick in die Zukunft	5
2.2 Plattformökonomie.	5
2.3 Veränderungen im Ökosystem	6
3. Datenaustausch von vernetzten und automatisierten Fahrzeugen	9
3.1 Erfassung von Daten	9
3.1.1 Erfassung von Daten im Kraftfahrzeug	9
3.1.2 Infrastrukturgestützte Erfassung von Daten	10
3.2 Das Fahrzeug als Teil des Internet of Things	10
3.3 Diagnose und Update von Steuergeräten „over the Air“	11
3.3.1 Konventionelle Fahrzeugdiagnose.	11
3.3.2 Zukünftige Diagnosesysteme	11
3.4 Kooperatives Fahren und Austausch von Sensordaten	12
4. Cybersicherheit vernetzter und autonomer Automobilsysteme.	14
4.1 Herausforderungen für die IT- und Cybersicherheit	14
4.2 Bedrohungsmodelle und redundante Absicherung als Präventivmaßnahme	15
4.3 Lifecycle und Softwareupdates	15
4.4 Verschlüsselung und Protokolle aktuell halten	16
5. Datenschutz	18
5.1 Datenschutzrechtliche Rahmenbedingungen	18
5.2 Anwendungsbereich des Datenschutzrechts	18
5.3 Welches Datenschutzgesetz gilt?	20
5.4 Wer ist verantwortlich für den Datenschutz?	21
5.5 Datenschutzrecht: Anforderungen an die Zulässigkeit und die Dokumentation	22
5.5.1 Zulässigkeit der Verarbeitung	23
5.5.2 Transparenz der Verarbeitung	23
5.5.3 Grundsätze und Dokumentationspflichten.	24
5.6 Wer ist geschützt, wenn Vertragspartner und Nutzer nicht identisch sind?	24
5.7 Privacy by Design und by Default	24
5.8 Sicherheit der Verarbeitung und Folgenabschätzung des Datenschutzes	25
5.8.1 Sicherheit der Verarbeitung	25
5.8.2 Datenschutz-Folgenabschätzung	25
6. Gewährleistungs- und Haftungsregime bei autonomen Fahrzeugen	27
6.1 Status quo der Gewährleistungs- und Garantieansprüche beim Autokauf	27
6.2 Status quo der Gewährleistungs- und Garantieansprüche bei Miet- und Leasingkonstellationen.	28
6.3 Gewährleistungsansprüche bei Übertragung von Daten durch autonome Fahrzeuge	28
6.4 Status quo der Einhaltung der Vorschriftsmäßigkeit durch den Halter	29
6.5 Lebenszyklus des Automobils	29
6.6 Herausforderungen für das Gewährleistungs- und Garantierecht	30
6.7 Herausforderungen für die Haftungsregime	32
7. Ausblick	36
8. Literatur.	37
9. Autoren	39
Impressum	46



Oliver J. Süme

Vorstandsvorsitzender eco – Verband der Internetwirtschaft e. V.

1. Vorwort

Liebe Leserinnen und Leser,

mit der Digitalisierung stehen dem Mobilitätssektor enorme Veränderungen ins Haus. Die deutschen Autobauer haben größere Investitionen angekündigt. Volkswagen plant in den nächsten fünf Jahren Ausgaben in Höhe von 44 Milliarden Euro für die Entwicklung und die Einführung neuer Technologien wie selbstfahrende Autos und Elektromobilität. Das klingt beeindruckend, ist im internationalen Wettbewerb jedoch alternativlos, um bei der rasanten digitalen Transformation der Automobilindustrie und unserer gesamten Mobilität nicht den Anschluss zu verlieren. Internettechnologie ist dabei der Schlüssel zur Zukunft unserer Wirtschaft insgesamt.

Denn nicht nur das Auto selbst verändert sich stark, auch unser Verständnis von Mobilität wandelt sich. Die Fähigkeit, von einem Ort zum anderen zu gelangen, nehmen wir immer stärker als Service wahr, der auf Wunsch verfügbar ist – ob ein eigenes Auto in der Garage steht oder nicht. Car Sharing oder Mobilitäts-Apps helfen uns, unser Ziel zu erreichen. Unsere Fortbewegungsmittel der Zukunft sind nicht länger isolierte Objekte, sondern Bestandteile eines die Welt umspannenden digital verfassten Mobilitäts-Ökosystems.

Das erfordert zuverlässige Datenverarbeitung im großen Stil: Routenplanung, Positionsdaten, Geschwindigkeitsdaten, Umgebungsdaten, Daten zum Fahrverhalten, Entertainment- und Wartungsdaten. Dank der Internetwirtschaft und ihrer digitalen Infrastrukturen ist es möglich, diese Daten sinnvoll zu nutzen. Voraussetzung dafür sind Investitionen in 5G-Technologie, Rechenzentren und Edge Computing, um Mobilität komfortabler, schneller und sicherer zu machen.

Dem letzten Punkt kommt dabei eine zentrale Bedeutung zu: Sicherheit ist der herausragende Aspekt für die Akzeptanz selbstfahrender Autos. Es ist daher unsere vordringlichste Aufgabe, Fahrzeuge und Mobilität vor Angriffen von Cyberkriminellen zu schützen. Die nötigen Standards und Zertifikate für eine durchdachte, verlässliche und vertrauenswürdige Infrastruktur können die Beteiligten nur Hand in Hand schaffen. Deshalb gilt es, die Automobilwirtschaft mit der Internetbranche eng zu vernetzen.

Eine weitere Voraussetzung ist der Datenschutz. Hier haben Deutschland und Europa die Chance, mithilfe der Datenschutz-Grundverordnung (DSGVO) international Maßstäbe zu setzen. Gleichzeitig besteht die Herausforderung, dass Datenschutzauflagen umgekehrt auch digitale Geschäftsmodelle komplizierter – wenn nicht gar unmöglich – machen. Die hohen Anforderungen an den Datenschutz sollten mit den neuen Geschäftsmodellen, ob Ride oder Car Sharing, Reiseportalen oder Versicherungen, in Einklang gebracht werden.

Das vollautonome Fahren wird in naher Zukunft die Straßen erobern. Mit dem vorliegenden Leitfaden möchten wir dazu beitragen, das selbstfahrende Auto mit Cybersicherheit, Datenschutz und wohldefinierten Verantwortungs- und Haftungsbereichen „auf die Straße“ zu bringen. Als Verband der Internetwirtschaft haben wir Analysen und Handlungsempfehlungen für Entscheider bei OEM und Zulieferern, in Forschung, Politik und Verwaltung zusammengestellt. Lassen Sie uns gemeinsam die Mobilität der Zukunft gestalten. Der eco Verband steht dazu als Partner bereit.

Ihr

Oliver J. Süme

Vorstandsvorsitzender eco – Verband der Internetwirtschaft e. V.



2. Ökosystem Mobilität

Die Art und Weise, wie wir uns in Zukunft fortbewegen, wird sich in den kommenden Jahren stark verändern. Das Fortbewegungsmittel steht nicht mehr im Vordergrund; Mobilität wird zur Dienstleistung. Die Zahl autonomer und vernetzter Fahrzeuge wird zunehmen. Um die notwendige digitale Infrastruktur aufzubauen und zu etablieren, bedarf es einer starken Internetwirtschaft, deren Unternehmen zukünftig im Ökosystem Mobilität eine wichtigere Rolle einnehmen werden.

2.1 Mobilität 2030 – ein Blick in die Zukunft

Stellen Sie sich vor, Sie befinden sich im Jahr 2030, leben in Berlin und möchten nach Peking reisen. Ihrem smarten Assistenzsystem, das Sie im Tagesablauf organisatorisch unterstützt, teilen Sie Reiseziel und -zeit mit. Das System hat Zugriff auf ein Mobilitätsportal, das weltweit Informationen über Fortbewegungsmittel und Infrastrukturen wie Straßen, Schienennetze und Flugrouten abrufen kann. Es bucht die optimale Verbindung von Berlin nach Peking: schnell, komfortabel, günstig und Ihren Vorlieben entsprechend.

Zum gewünschten Zeitpunkt starten Sie die Reise: Sie werden zu Hause von einem autonom fahrenden Roboter-Fahrzeug abgeholt, das Sie zum Flughafen bringt. Ein privates Auto besitzen Sie vielleicht gar nicht. Unterwegs nimmt das Fahrzeug noch zwei weitere Fahrgäste aus Ihrem Stadtgebiet mit dem Ziel Flughafen auf, wo Sie in das Flugzeug nach Peking einsteigen. Vom Peking-Mega-Airport fahren Sie mit einem Hochgeschwindigkeitszug in die Stadtmitte. Ein softwaregesteuertes Flugtaxi bringt Sie vom Bahnhof zum Kunden oder ins Hotel.

So wird sie aussehen: Die Mobilität der Zukunft.¹ Wir werden sie als solche vielleicht gar nicht mehr wahrnehmen, weil wir uns ohne eigenes Zutun von A nach B bewegen. Auf keinem Teilstück der oben skizzierten Route müssen wir uns selbst um Komfort, ein Fortbewegungsmittel oder die Abrechnung kümmern, die automatisch über Paymentssysteme und währungsunabhängig erfolgt. Denkbar sind sogar Flatrates, über die man ein monatliches Kilometervolumen bucht. Nirgendwo haben wir überflüssige Wartezeit. Wir können stressfrei reisen, insbesondere, weil wir nicht einen Kilometer das

Steuer übernehmen müssen – dank lückenloser Anbindung und autonom agierender Fortbewegungsmittel.

Durch diese neue Art der Vernetzung von Verkehrsmitteln ist es Menschen möglich, völlig andere Anforderungen an ihre Mobilitätsbedürfnisse zu stellen. Vor allem Stadtbewohner werden nicht mehr zwingend auf ein eigenes Kraftfahrzeug angewiesen sein, da sie auf Angebote wie Car Sharing und Car Pooling zurückgreifen können. Mobilität wird für sie zu einer Dienstleistung, die ständig verfügbar sein muss.

Das automatisierte beziehungsweise autonome Fahren ist nach heutigem Stand nur in Teilen erlaubt. So dürfen autonome Systeme in spezifischen Anwendungsfällen die Längs- und Querverführung übernehmen, zum Beispiel beim Einparken. Für einen höheren Automatisierungsgrad bis hin zur vollständigen Fahrkontrolle durch Software müssen vor allem in puncto technische Sicherheit noch einige wesentliche Schritte unternommen werden – und zwar schnell, denn die Entwicklung schreitet unaufhaltsam voran und das vollautomatisierte Fahren wird kommen.

2.2 Plattformökonomie

Basis dieser „neuen“ Mobilität ist die Plattformwirtschaft. Mobilitätsplattformen ermöglichen dem Kunden eine Fahrt von A nach B dank Berechnung der optimalen Route unter Berücksichtigung aller Verkehrsmittel. Diese Services werden das Zentrum zukünftiger Mobilität sein, nicht das Fortbewegungsmittel.² Das Auto wird Teil eines großen Systems und ist darauf angewiesen, mit anderen Systemkomponenten vernetzt zu sein.

Den Wandel zur Plattformwirtschaft haben einige Branchen bereits erlebt. Dazu zählen Handel (Amazon, E-Commerce), Tourismus (Airbnb) und Musik (Spotify). Aus dem Mobilitätssektor ist Uber ein prominentes Beispiel dafür, dass sich auch diese Branche schon länger im Umbruch befindet. Einige traditionelle Automobilhersteller haben bereits neue Geschäftsbereiche entwickelt, die auf den Grundprinzipien der Plattformökonomie beruhen (zum Beispiel Car2Go, DriveNow und Moia).

Das höchste Gut dieser Ökonomie sind Daten, die durch die Vernetzung digitaler Services generiert werden.³ Im Fall der Mobilität

¹ Vgl. u.a. Heller (2018): Wie wir demnächst von A nach B kommen; Zukunftsinstitut (2017): Die Evolution der Mobilität

² Vgl. ebd.

³ Für 2020 werden Datenmengen von 545 Petabyte pro Jahr prognostiziert – ein Wachstum um 186 Prozent gegenüber 2013. Vgl. Seiberth (2015): Wie verändern digitale Plattformen die Automobilwirtschaft?



Abb. 1

Plattform-Ökonomie vernetzter und autonomer Fahrzeuge



handelt es sich um Daten zum individuellen Verbraucherkomfort, zur Verkehrssituation und Position, zum Wetter, zu Entertainment-Profilen und Daten aus Satellitensystemen. Autonom fahrende Autos bedingen darüber hinaus die Analyse von Umgebungsaufzeichnungen sowie des Verhaltens der anderen Verkehrsteilnehmer.⁴

Diese Daten bilden die Grundlage neuer Geschäftsmodelle, die dem Nutzer individuelle und bestmögliche Mobilitätsangebote zur Verfügung stellen. Von solchen Mobility Services wie von Parking Apps über Reiseportale bis hin zu Verkehrsleitsystemen können noch weitere Akteure profitieren. Auto-Versicherer könnten beispielsweise die Daten, die ein Auto generiert, nutzen, um den Beitrag für die Police dem Fahrstil anzupassen („pay as you drive“). Für die Instandhalter von Verkehrsinfrastruktur können von Sensoren erfasste Daten zur Analyse des Straßenzustands und des Verkehrsflusses über die Notwendigkeit von Belagerneuerung oder Entfernung von Hindernissen informieren.⁵

Das Auto wird zu einer Art offenen und angreifbaren Einheit, die mit vielen Partnern des neuen Ökosystems Daten teilen wird.⁶ Daher sind die Sicherheit und Integrität von Systemen vor unerlaubtem Zugriff auf Funktionen und Daten ein zentraler Faktor. Die Datenschutzgrundverordnung (DSGVO) bietet einen Rechtsrahmen für digitale Geschäftsmodelle und -tätigkeiten. Kapitel 5 analysiert neben der DSGVO noch weitere datenschützende Gesetze hinsichtlich ihrer Anwendbarkeit auf die zukünftigen Geschäftsmodelle des Mobilitätswesens.

2.3 Veränderungen im Ökosystem

Bei der gesellschaftlich so wichtigen Komponente Mobilität ist es von enormer Bedeutung, dass dieses digitalisierte Gesamtsystem dauerhaft funktioniert. Hierfür müssen die beteiligten Player eng vernetzt zusammenarbeiten und es muss eine Art „Systembetreiber“ der digitalen Infrastruktur existieren. Dies gilt sowohl für die Komponenten, die dem Kunden eine optimale Fahrt von A nach B ermöglichen, als auch für diejenigen, die die sichere Bewegung von Fahrzeugen garantieren, die ohne menschliches Zutun gesteuert werden. Denn „moderne Autos sind an sich eine Art Rechenzentrum – sie verfügen über eine Rechenleistung von mehr als 100 CPU und müssen Daten innerhalb von Millisekunden validieren, bevor sie die Ergebnisse nicht nur an ihre internen Antriebssysteme senden können, sondern auch an andere Fahrzeuge auf der Straße zu Kommunikationszwecken“.⁷

War das Auto bisher eine isolierte Kapsel, wird es zukünftig immer mehr Bestandteil eines weit umspannenden Ökosystems sein. Der Datenaustausch in diesem komplexen Ökosystem aus Sensoren, Elektronikkomponenten und On-Board-Entertainmentsystemen im Fahrzeug, bei Funkeinheiten entlang der Straße und in Smart Citys, Werkstattmessgeräten sowie Gateways, Mobilitätsplattformservern und dem Satellitennetz wird gigantisch anwachsen.⁸ Es ist von enormer Bedeutung und eine große Herausforderung, die Chancen für Cyberkriminelle zu minimieren, sich in dieses sensible System einzuhacken, um mutwillig Unfallszenarien herbeizuführen oder Daten zu stehlen.

⁴ Mehr dazu in Kapitel 3.1

⁵ Abbildung 1 zeigt einige Profiteure der Plattform-Ökonomie im Bereich Mobilität.

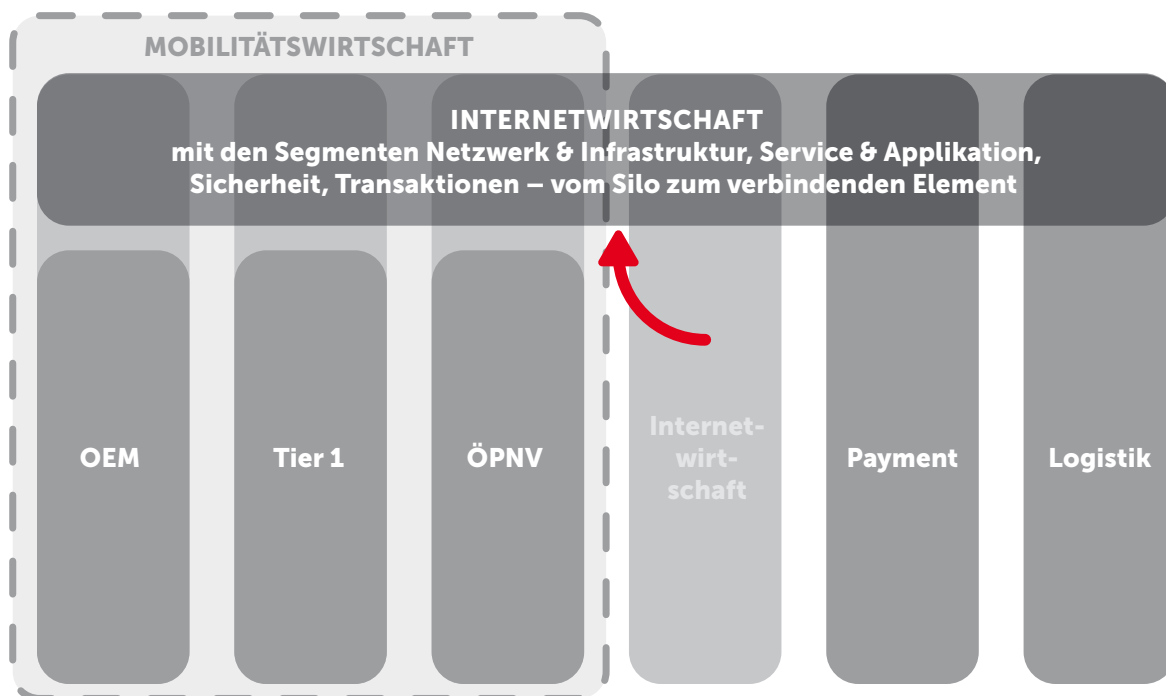
⁶ Vgl. Veronesi/Eibisch (2018): The Car as Connected Platform

⁷ Zachmann (2018): The car as a driver for data growth needing new infrastructure solutions

⁸ Vgl. Comastri (2018): New frontiers for car security: API management



Abb. 2



Das erfordert eine mehrfach redundante digital vernetzte Infrastruktur, die Mobilitätsplattformen und vernetztes beziehungsweise autonomes Fahren realisiert:

- schnelle und permanent verfügbare Netze,
- Rechenzentren zur Verarbeitung der Datenberge,
- Plattformen, die Services steuern,
- maximaler Schutz der Daten und der Infrastruktur,
- Service Provider und Integratoren, die die Systeme am Laufen halten.

Die Leistung dieser Infrastruktur ist schon heute außerordentlich wichtig, um Autos zu fahren und Routen zu planen, denn wir verzeichnen einen stetig wachsenden Bedarf an Sharingangeboten seitens der Konsumenten⁹. Map-gestützte Dienste erleichtern die Navigation und die Suche nach Parkplätzen. Einige On-Board-Angebote wie zum Beispiel Concierge und Entertainment Services sind Standard in Neuwagenmodellen. Die On-Board-Software wird zum Teil durch Over-the-Air-Updates automatisch auf den neuesten Stand gebracht. Nicht mehr wegzudenken sind Systeme, mit denen Werkstätten¹⁰ und Automobilhersteller Diagnosedaten auslesen können.

Wir gelangen mehr und mehr an das Ende der Silowirtschaft und die Automobilindustrie ist im Umbruch.¹¹ Bisher gab es eine klar strukturierte Lieferkette, in der OEM¹², Zulieferer, Softwarehersteller und andere ein Silodasein führten und die Wünsche ihrer

Auftraggeber losgelöst abarbeiteten. Kooperationen mit IT- und Internet-Playern werden aber schon bald unumgänglich sein, um die lückenlose, sichere und latenzfreie Vernetzung der Fahrzeuge und ihrer Komponenten sowie einen steigenden Autonomiegrad zu realisieren.¹³ Christoph Weigler, Deutschland-Chef von UBER, ist überzeugt, dass es nicht auf ein Entweder-oder hinauslaufen wird, sondern auf ein Miteinander. „Das Umfeld wird immer komplexer, Partnerschaften sind schon heute unerlässlich. Klassische Automobilhersteller und Technologieunternehmen werden künftig noch viel enger kooperieren als sie es heute schon tun.“¹⁴ Der verbindende Dreh- und Angelpunkt dieses Ökosystems wird die Internetwirtschaft sein, insbesondere in puncto Sicherheit, Vernetzung und digitale Infrastruktur.¹⁵

Wussten Sie schon? Die deutsche Internetwirtschaft wird die Automobilindustrie im Jahr 2028 in puncto Umsatz überholen und demzufolge auch Geschäftsmodelle dominieren! Somit lohnt es sich, branchenübergreifend zusammenzuarbeiten.¹⁶

9 Vgl. Bundesverband CarSharing e. V. (o.J.): Aktuelle Zahlen und Daten zum CarSharing in Deutschland

10 Vgl. Kapitel 3.3

11 Vgl. Seiberth (2015)

12 Original Equipment Manufacturers

13 Vgl. Abbildung 2: Veränderungen im Ökosystem Mobilität

14 Christoph Weigler äußert sich dazu in einem Artikel des SPIEGEL – vgl. dazu Sommerfeld (2018): Wie sich die Autoindustrie neu erfindet – und unser Leben damit verändert

15 Vgl. Seiberth (2015).

16 Vgl. eco – Verband der Internetwirtschaft e. V./Arthur D. Little (2015): Die deutsche Internetwirtschaft 2015–2019



Interview



Gerrit Pohl,
Chief Digital Officer, ADAC SE

„Ich denke an einen Dienstleister, der die immer zahlreicheren Optionen zur Mobilität intelligent zusammenfasst.“

Interview mit Gerrit Pohl, Chief Digital Officer, ADAC SE

Herr Pohl, was kennzeichnet einen „Mobilitätsdienstleister“?

Das ist natürlich ein breites Bouquet, aber ich denke an einen Dienstleister, der den Kunden die immer zahlreicheren Optionen zur Mobilität unter einer Oberfläche intelligent zusammenfasst. Er macht diese kinderleicht buchbar und bietet zusätzlich verschiedene auf Mobilität basierende Services – also digital perfekt organisierte, aber weitestgehend analoge Leistungen.

Was ist die größte Herausforderung, um das höchste Level autonomen Fahrens auf deutschen und europäischen Straßen zu realisieren?

Die Mathematik wird insbesondere dann reichlich herausgefordert, wenn die Vollautomatisierung auf Teil- oder Nichtautomatisierung trifft, insbesondere im urbanen Umfeld. Die große Herausforderung ist, dass Unvorhersehbare vorherzusehen, denn das vollautonome Fahrzeug muss auf all diese Dinge maximal sicher reagieren können. Wer so etwas beispielsweise in Indien löst, löst es wohl überall. Ansonsten gehen damit natürlich hoch komplexe Zulassungs-, Haftungs- und Versicherungsfragen einher.

Welche Rolle nimmt der ADAC in Zukunft in der autonomen und vernetzten Mobilitätswelt ein?

Unsere Position als Verbraucherschützer und neutraler Berater wird in einer sich immer schneller verändernden Mobilitätswelt an Bedeutung zunehmen. Ansonsten werden wir uns kontinuierlich überlegen, wie wir unseren Mitgliedern die verschiedenen Formen der Mobilität serviceorientiert zugänglich machen können und sie gleichzeitig gegen Risiken möglichst umfassend absichern. Eines ist aber klar: Unsere Services müssen verstärkt eine hohe Bedeutung im Alltag aufweisen. Deswegen beschäftigen wir uns schon heute mit entsprechend relevanten Themen auch abseits der Mobilität.

Top 5

Kernaussagen von Kapitel 2

- Mobilität wird zur permanent verfügbaren Dienstleistung.
- Sie zeichnet sich durch Vernetzung, autonome Fahrzeuge, Sharing Economy und – im Leitfaden nicht näher thematisiert – postfossile Antriebe aus.
- Plattformen werden zum Kern dieser „neuen Mobilität“.
- Es werden neue disruptive Geschäftsmodelle entwickelt.
- Die Internetwirtschaft wird im neu entstehenden Ökosystem Mobilität zum verbindenden Dreh- und Angelpunkt der Player.



3. Datenaustausch von vernetzten und automatisierten Fahrzeugen

Durch die Vernetzung und Autonomisierung wird das Auto zunehmend Teil des Internet of Things. Die Fahrzeuge tauschen gewaltige Datenmengen aus, sei es untereinander oder im Zusammenspiel mit Komponenten der Verkehrsinfrastruktur, beispielsweise über Sensoren an Ampeln oder im Asphalt.

3.1 Erfassung von Daten

Die Datenerfassung erfolgt einerseits fahrzeugbasiert und andererseits infrastrukturbasiert. Die fahrzeugbasierte Erfassung ist bereits seit vielen Jahren etabliert, während eine infrastrukturbasierte Erfassung bisher (Stand 2018) nur im Rahmen von Bewirtschaftungen, zum Beispiel bei Mautsystemen oder allgemeinen Überwachungsmaßnahmen, erfolgt. Das wird sich ändern, je autonomer die Fahrzeuge und je smarter die Städte werden.

Der Verband der Automobilwirtschaft (VDA) unterscheidet zwischen folgenden Datenkategorien beim vernetzten Fahrzeug:¹⁷

- durch ein Gesetz geregelte Zweckbindung, zum Beispiel OBD II¹⁸ und eCall (EU),
- moderne Datendienste, zum Beispiel anonymisierte und pseudonymisierte Car-to-X-Dienste und prädiktive Diagnose,
- kundeneigene/eingebrachte Daten, zum Beispiel Infotainment- und Komforteinstellungen, Navigationsziele, Adressbuch,
- im Fahrzeug erzeugte, dem Fahrer angezeigte Kraftfahrzeug-Betriebswerte, zum Beispiel Füllstände und Verbrauch,
- im Fahrzeug erzeugte aggregierte Fahrzeugdaten, zum Beispiel Fehlerspeicher, Anzahl Fehlfunktionen, Durchschnittsgeschwindigkeit und -verbrauch,
- im Fahrzeug erzeugte technische Daten, zum Beispiel Sensordaten, Aktuatordaten, Einspritzverhalten des Motors, Schaltverhalten des Automatikgetriebes.

3.1.1 Erfassung von Daten im Kraftfahrzeug

Zunächst ist zu unterscheiden zwischen der Erfassung der Eigenbewegung und anderer Zustandsgrößen des Fahrzeugs und zukünftig auch der Erfassung des Fahrers durch propriozeptive¹⁹ Sensoren und der Umwelt durch extrapriozeptive²⁰ Sensoren.

Propriozeptive Sensoren erfassen die Eigenbewegung, die internen Funktionen sowie den Zustand des Fahrzeugs durch eine Vielzahl von Sensoren, die es zum Beispiel gestatten, die Fahrzeugbewegungsdaten, Temperaturen, Schaltstellungen, aber auch Bedienelemente, wie die Pedalerie und das Lenkrad zu erfassen. Derartige Sensoren sind bereits seit dem Aufkommen von Bremssystem- und Fahrdynamikregelungen²¹ verbreitet im Einsatz. Hinzu kommen Sensoren, die Diagnosedaten erfassen, um diese gegebenenfalls an eine Werkstatt, den Hersteller (über einen zusätzlichen OBD-Dongle und GSM oder Smartphones) oder an andere Dienstleister weiterzuleiten. Derartige Systeme sind darüber hinaus imstande, Lokalisierungs- und Bewegungsdaten weiterzugeben. Beispiele hierfür sind im OEM-Bereich Mercedes Me²² und im Drittanbieterbereich RYD²³. Weitere Erfassungen und Übermittlungen von Bewegungsdaten erfolgen durch vernetzte Navigationssysteme, gegebenenfalls ergänzt durch die Einbeziehung von Smartphone-Daten, ebenfalls durch OEM und Drittanbieter. Dies bedeutet, dass propriozeptive Fahrzeugdaten nicht zwingend eine Ausstattung mit speziellen Sensoren erfordern, sondern dass bereits das bloße Mitführen eines Smartphones eine Datenerfassung des „Fahrer-Fahrzeug-Verbunds“ möglich macht.

Extrapriozeptive Sensoren erfassen die Umwelt des eigenen Kraftfahrzeugs, das heißt andere Verkehrsteilnehmer, die Infrastruktur, Wetterdaten etc. Auch hier kommt seit der Einführung von Adaptive Cruise Control (ACC), das zur Differenzgeschwindigkeits-Abstandsmessung einen Radarsensor benötigt, eine Vielzahl von Sensoren zum Einsatz, wie zum Beispiel Radar- und Lidarsensoren, Kameras, Ultraschall- und Infrarotsensoren. Die Ausstattung eines Fahrzeugs der neuesten Generation mit extrapriozeptiven Sensoren zeigt Abbildung 3.

¹⁷ Vgl. Verband der Automobilindustrie e.V. (2014): Datenschutz-Prinzipien für vernetzte Fahrzeuge

¹⁸ On-Board-Diagnose II

¹⁹ Wahrnehmungen aus dem eigenen Körper (beziehungsweise hier „Fahrzeug“); von lat. proprius „eigen“ und recipere „aufnehmen“.

²⁰ Wahrnehmung von außen (hier außerhalb des Fahrzeugs); von lat. extra „außerhalb“ und recipere „aufnehmen“.

²¹ Hierzu gehören beispielsweise Systeme wie ABS, ASR, ESP etc.

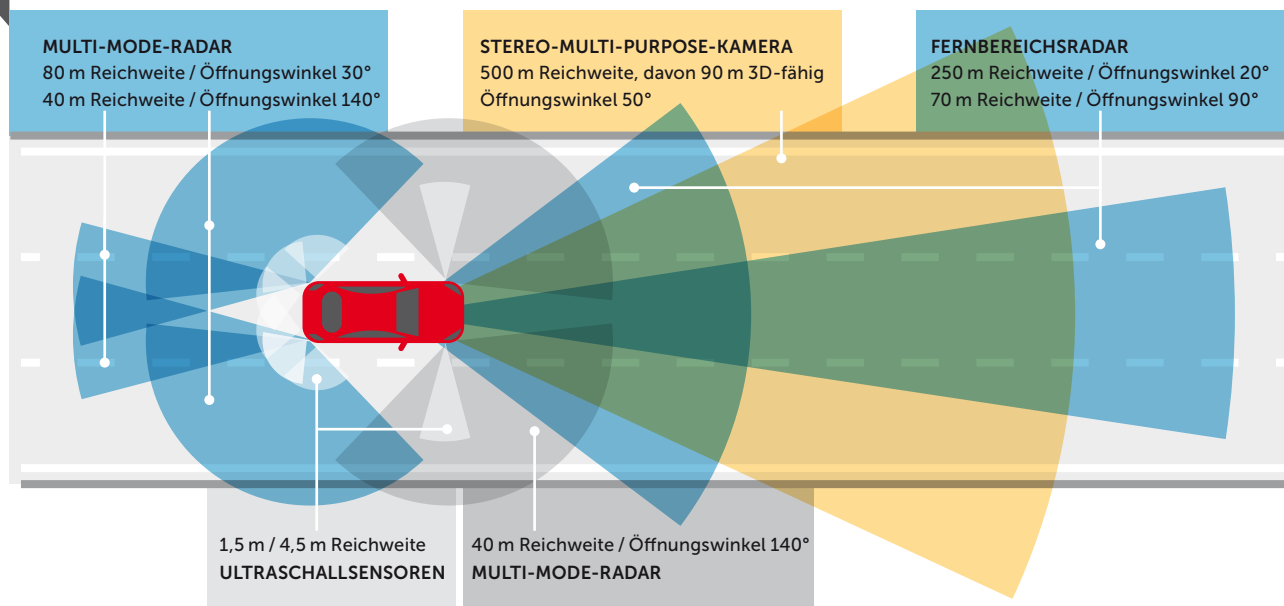
²² Vgl. <https://www.mercedes-benz.com/de/mercedes-me>

²³ Vgl. <https://ryd.one>



Abb. 3

Ausstattung eines Fahrzeugs mit extrapriozeptiven Sensoren



3.1.2 Infrastrukturgestützte Erfassung von Daten

Car-to-Infrastructure (C2I)-Communication ist ein Konzept zur drahtlosen Kommunikation zwischen Kraftfahrzeugen und Infrastruktureinrichtungen. Die Infrastrukturkomponenten können intelligente Verkehrszeichen, Lichtsignalanlagen, Verkehrsleitrechner, Funkbaken, mit Funkmasten ausgestattete Kreuzungen oder Intelligent Roadside Stations (IRS) sein, über die eine Verbindung zum Beispiel zu internetbasierten Diensten, zu Notfallstationen, zum Fahrzeughalter selbst oder auch zum Autohersteller aufgebaut werden kann. In vielen Städten sind diese Installationen Teil eines Smart-City-Konzepts. Systeme, die Diagnose- oder Notfalldaten direkt zum Fahrzeughersteller oder an Werkstätten übermitteln, sind heute bereits im Einsatz. Die Kommunikation kann auch über so genannte Roadside Units (RSU) erfolgen, die an den Verkehrswegen positioniert und über Access Router (AR) miteinander verbunden sind.

Der „Physical Layer“ für derartige Konzepte ist in aller Regel drahtlos und umfasst insbesondere Mobilfunksysteme, wie GSM, UMTS,

HSPA, LTE, WLAN oder WiMAX²⁴. Darüber hinaus können andere Einrichtungen wie Rundfunksysteme mit den Verkehrsinformationen, DAB+ etc. eingebunden werden. Mittlerweile ist außerdem der Standard Cellular V2X als Teil von 5G für den Automobilssektor freigegeben.

Die Netzübergänge funktionieren nach heutigem Stand noch nicht einwandfrei und können in der juristischen Nachbearbeitung von Unfällen durchaus zu Schwierigkeiten führen. Möglicherweise ist dann eine Schnittstellenanalyse erforderlich, um zu untersuchen, ob die Ursache eines Unfalls nicht aus einer solchen Lücke resultiert, die beim Auto zu einem kurzzeitigen Netzausfall und damit einer fehlerhaften Reaktion geführt hat.

3.2 Das Fahrzeug als Teil des Internet of Things

Unter dem Begriff Car-to-X-Kommunikation wird sowohl die funktechnische Vernetzung von Fahrzeugen untereinander (Car-to-Car, Car2C) als auch die Einbindung der Infrastruktur (Car-to-Infrastructure, Car2I) beziehungsweise weiterer Verkehrsteilnehmer

²⁴ WiMAX (Worldwide Interoperability for Microwave Access) ist eine drahtlose Zugangstechnik zum Breitbandinternet und wird häufig als Synonym für Funksysteme nach dem IEEE-Standard 802.16 verwendet, ähnlich wie WLAN, das auf dem IEEE-Standard 802.11 beruht.

Kommunikationskonzepte für Connected Cars

Car to X Konzepte	Beschreibung	Beispiele für übertragene Daten
Car to Car	Kommunikation zwischen zwei Fahrzeugen	Bewegungsdaten, Zustandsdaten
Car to Infrastructure	Kommunikation zwischen dem Fahrzeug und Systemen der Infrastruktur	Informationen von Lichtsignalanlagen, Verkehrszeichen
Car to Mobile	Kommunikation zwischen dem Fahrzeug und dem Mobilfunknetz	Daten von Infotainment, Smart Services



Abb. 4

Gesamtkonzept eines Intelligenten Transport Systems (ITS) i.S.d. ETSI



verstanden. Sie bildet einen Teil des Intelligenten Transport-Systems (ITS), das in Abbildung 4 als Gesamtkonzept dargestellt ist. Es handelt sich dabei um das Verständnis des European Telecommunications Standards Institute (ETSI), das neben dem European Committee for Standardization (CEN) in Europa und bei internationalen Harmonisierungsbemühungen eine führende Rolle einnimmt.

Ziel dieser Standardisierungsbemühungen ist insbesondere, die Netzwerkarchitektur sowie die Zugriffswege, Sicherheitsprotokolle und Datenformate zu vereinheitlichen. Dies soll sicherstellen, dass die Kommunikation zwischen den verschiedenen Verkehrsteilnehmern unterschiedlichster Interessensgruppen gewährleistet werden kann. Hierzu zählen die zahlreichen Automobilhersteller, aber auch die Telekommunikationsanbieter, Zulieferer, Infrastrukturanbieter, Mobilitätsdienstleister, ÖPNV etc. Der Begriff Car-to-X/Car2X beinhaltet also konkrete technische Lösungsansätze und Standards für die Vernetzung von Verkehrssystemen.

3.3 Diagnose und Update von Steuergeräten „over the Air“

3.3.1 Konventionelle Fahrzeugdiagnose

Bei bisher gebräuchlichen Diagnosefunktionen werden die Daten über eine bereits große Anzahl von Sensoren erfasst, die entweder separat platziert oder in Steuergeräten verbaut sind. Die Überwachung erfolgt hierbei entweder nur bei Motorstart oder kontinuierlich

während des Fahrzeugbetriebs. Abgespeichert werden in der Regel nur die während der Überwachung erfassten Unregelmäßigkeiten. Diese werden dann bei einem Werkstattaufenthalt in der Regel über die OBD-II-Schnittstelle mit speziellen Testern ausgelesen und gegebenenfalls durch ein integriertes „Expertensystem“ verknüpft und interpretiert, um eine Fehlerursache zu finden. Dabei kommen sowohl im Fahrzeug als auch bei den Werkstattprüfern standardisierte Beschreibungsformate zum Einsatz.

Eine Onlinediagnose ist bei einem derartigen Vorgehen nicht möglich, aber bei konventionellen Fahrzeugen auch nicht notwendig. Die Verantwortung für die erfassten Daten liegt hier bei der jeweiligen Werkstatt und gegebenenfalls beim Hersteller. Da es sich dabei um Momentaufnahmen im Augenblick des Tests handelt, kann in der Regel keine Historie angelegt werden.

3.3.2 Zukünftige Diagnosesysteme

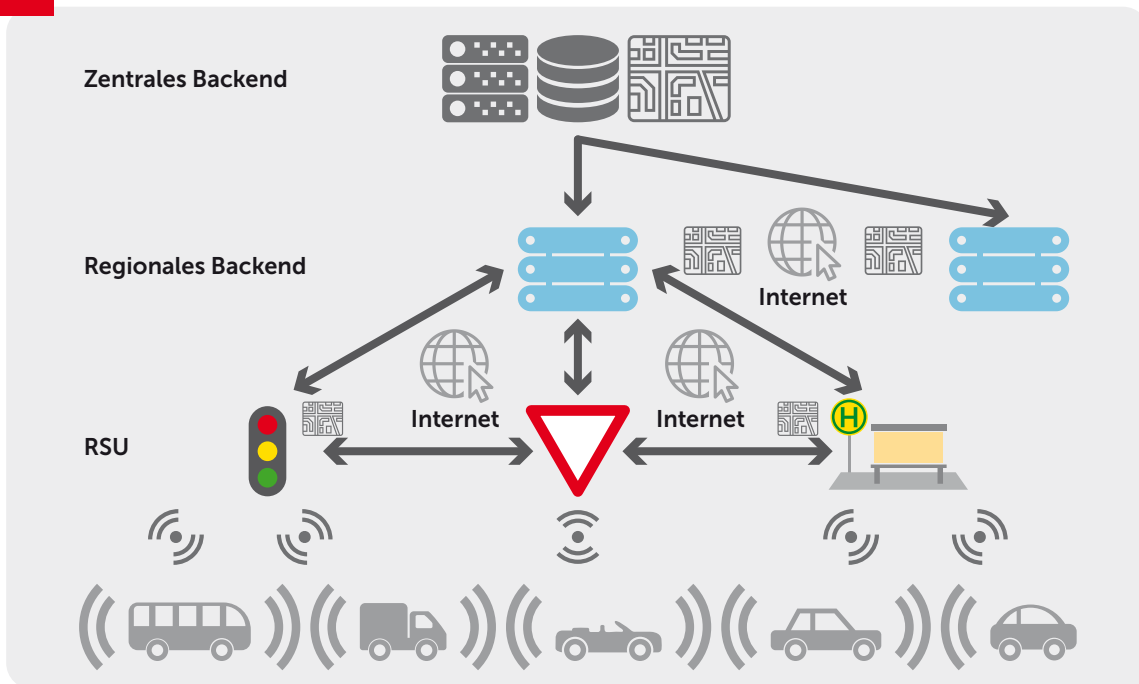
Bei zukünftigen Anwendungsfällen wie autonom fahrenden Fahrzeugen ist das konventionelle Vorgehen nicht mehr ausreichend. In diesem Fall müssen die Daten online erfasst werden, was auch eine Speicherung dieser Daten in einer Cloud ermöglicht. Eine derartige Erfassung kann beispielsweise zur vorausschauenden Wartung („Predictive Maintenance“) dienen, etwa um ein Versagen von Bauteilen aufgrund von Materialermüdung vorherzusagen.²⁵

²⁵ Vgl. Kong et. al. (2017): Mission profiling of road data measurement for coil spring fatigue life



Abb. 5

Kommunikationsebenen vernetzter Verkehrssysteme



Systeme der Fahrzeughersteller werden zukünftig in der Lage sein, durch die Erfassung von Lastkollektiven auf die Nutzung und den Verschleiß von Fahrzeugen zurückzuschließen. Derartige Systeme sind auch dazu geeignet, einen nicht bestimmungsgemäßen Gebrauch nachzuweisen. Zudem können die so erfassten Daten als Belastungsinformationen genutzt werden – etwa zur Auslegung zukünftiger Fahrzeuge oder um Qualitätskosten vorherzusagen, indem das Kundennutzungsverhalten im Realverkehr erfasst wird.

Eine weitere Anwendung ist das Aufspielen neuer Softwarestände (SOTA: Software-over-the-Air). Das Verfahren bietet das Potenzial, fortlaufend und schnell mit Patches Schwachstellen auszubessern, Fehler zu beseitigen sowie neue Funktionen zu installieren oder freizuschalten. Dies erfolgt in der Regel automatisch über die oben genannten Funksysteme. Ein On-Board-Steuergerät nimmt die Softwarepakete entgegen und verteilt sie über Ethernetsysteme oder CAN-Bus an die Zielgeräte im Auto. Bei Tesla können beispielsweise ohne Werkstattaufenthalt Funktionen freigeschaltet werden, wenn ein Aufpreis gezahlt wurde. Ein weiteres Beispiel ist das Aufspielen von Updates – ebenfalls ohne Werkstattbesuch – wie es bereits Stand der Technik bei Navigations- und Entertainmentfunktionen ist.

Diese Art der Wartung und Diagnose ermöglicht einerseits eine zeitnahe Beseitigung von Fehlern ohne Werkstattaufenthalt, verhindert umfassende Rückrufaktionen und spielt beim Aufbau neuer Geschäftsmodelle eine wesentliche Rolle (siehe Tesla). Sie birgt aber andererseits die Gefahr des Missbrauchs durch Dritte oder den Fahrzeughersteller selbst. Möglich wäre zum Beispiel eine Erfassung des Kundennutzungsverhaltens, um eine nicht bestimmungsgemäße Verwendung nachzuweisen. Für den Updateprozess an sich ist ein Höchstmaß an Absicherung der „Luftschnittstelle“ notwendig, um das Aufspielen manipulierter Software zu verhindern. Ein gehacktes autonomes Auto mit ferngesteuerter Kontrol-

leinheit wäre ein Super-GAU mit unvorhersehbaren Folgen für alle Verkehrsteilnehmer.

3.4 Kooperatives Fahren und Austausch von Sensordaten

Nach heutigem Stand der Technik werden die im Fahrzeug erfassten Sensordaten ausschließlich für Funktionen im eigenen Fahrzeug verwendet. Erste Forschungsergebnisse, wie zum Beispiel durch das Projekt Ko-FAS²⁶, haben gezeigt, dass die Übermittlung relevanter Daten ermöglicht, kritische Verkehrssituationen frühzeitig zu erkennen und somit Konfliktsituationen zu vermeiden und Unfälle zu verhindern. Dies kann zum einen durch eine frühzeitige Warnung des Fahrers vor möglichen Gefahren erfolgen und zum anderen durch direkten Eingriff in dafür vorgesehene Assistenz- und Notfallsysteme. Dies ist vor dem Hintergrund zukünftiger Anwendungen im Bereich des hochautomatisierten oder autonomen Fahrens von besonderem Interesse.

Im Projekt SEEROAD²⁷ soll ein fahrzeugbasiertes Sensorsystem zur Erfassung des Fahrbahnzustands entwickelt werden, um zukünftige hochautomatisierte Systeme zu befähigen, die Fahrzeugdynamik – das heißt Geschwindigkeiten und Trajektorien – sicher den Umweltbedingungen anzupassen. Ein weiteres Ziel ist darüber hinaus, die gesammelten Informationen auch anderen Verkehrsteilnehmern, beispielsweise in Form einer dynamischen Fahrbahnzustandskarte, zur Verfügung zu stellen. Abbildung 5 zeigt die möglichen Stufen und Wege bei der Verteilung von fahrzeugspezifischen Daten.

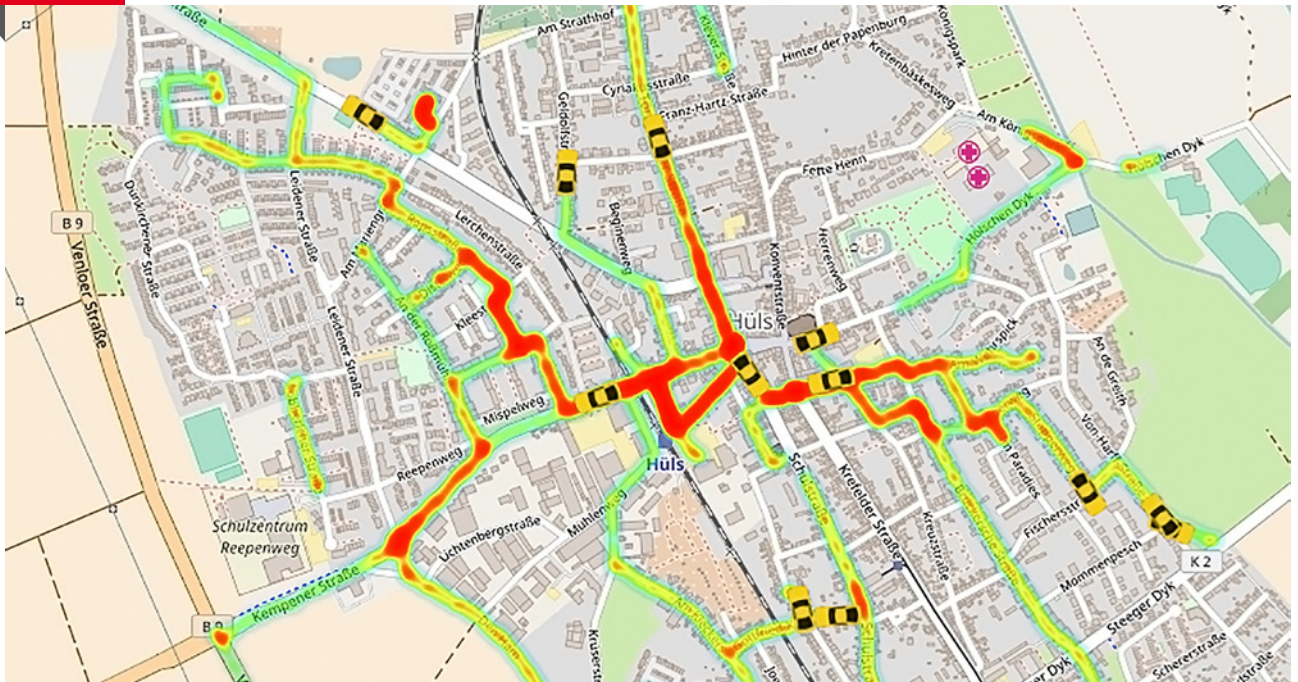
Die grundsätzliche technische Machbarkeit ist bereits vorhanden. Abbildung 6 demonstriert eine mögliche Darstellungsart von

²⁶ Forschungsinitiative Ko-FAS (<http://www.ko-fas.de>)

²⁷ Vgl. <https://seeroad.uni-bremen.de>



Darstellung übermittelter Sensordaten auf einem Backend



- **Datensicherheit:** Wie wirken sich fehlerhafte Daten, falsche Daten und möglicherweise manipulierte Daten auf die Fahrzeugsysteme aus?
- **Datenhoheit:** Wer trägt die Verantwortung für die erhobenen Daten – vor, während und nach einer Übermittlung?

Top 5

Kernaussagen von Kapitel 3

- Kern der neuen Mobilität sind Daten. Ihre Erfassung erfolgt einerseits fahrzeug- und andererseits infrastrukturbasiert.
- Die infrastrukturbasierte Erfassung wird durch Smart Citys und autonome Fahrzeuge stark zunehmen.
- Bei der Datenübertragung wird nach drei Car-to-X-Konzepten unterschieden: Car-to-Car, Car-to-Infrastructure und Car-to-Mobile.
- Prominente Beispiele für den Datenaustausch vernetzter Fahrzeuge sind Over-the-Air-Updates und -Diagnosen sowie das kooperative Fahren, um anderen Fahrzeugen kritische Verkehrssituationen zu übermitteln.
- Durch die vielen Schnittstellen und Funkübertragungen werden immer mehr Autos zum Bestandteil des Internet of Things.



4. Cybersicherheit vernetzter und autonomer Automobilsysteme

Die Vernetzung des Automobils birgt enormes Potenzial für neue technische Features. Sie eröffnet neue Geschäftsmodelle, etwa beim Ride oder Car Sharing. Andere Geschäftsmodelle entwickeln sich weiter. So kann zum Beispiel Funktionalität für bereits verkaufte Autos gegen Bezahlung über das Netz freigeschaltet werden.

Die Vernetzung konfrontiert das Ökosystem „Automobil“ aber auch mit einer Reihe von Bedrohungen, denen es bisher nicht ausgesetzt war. Fahrzeuge werden plötzlich anfällig für Angriffe über das Internet. Die technischen Herausforderungen, die im Bereich autonomes und vernetztes Fahren für die IT- und Cybersicherheit existieren, unterscheiden sich häufig nicht wesentlich von denen aus anderen IT-Landschaften, also beispielsweise von Smartphones oder Desktop-PCs. Ein Softwareupdate kann zwar ein potenzielles Einfallstor für Angreifer sein und muss, etwa durch digitale Signaturen, abgesichert werden. Allerdings sind regelmäßige Updates unerlässlich, um auf neue Bedrohungen zu reagieren und die Sicherheit eines Systems fortlaufend zu gewährleisten. Dabei stellt die Automobilindustrie die IT-Sicherheit vor einige Herausforderungen, die in anderen Marktsegmenten so nicht auftreten.

4.1 Herausforderungen für die IT- und Cybersicherheit

Ein modernes Fahrzeug enthält eine Vielzahl an Steuergeräten (Electronical Control Units; kurz ECU). Die einzelnen Steuergeräte unterscheiden sich stark hinsichtlich Software und Hardware. Die ECU werden über diverse Netzwerktechnologien miteinander verbunden und kommunizieren über diverse, oft für den Automobilbereich spezifische Protokolle.

Ein gutes Beispiel ist die im vorherigen Kapitel beschriebene Diagnose. Steuergeräte im Automobil offerieren Diagnoseschnittstellen, auf die eine Servicekraft oder der Kunde, potenziell auch ohne physischen Zugang zum Fahrzeug, zugreifen kann. Dabei kann es vorkommen, dass ECU die Diagnosedaten anderer ECU empfangen und auswerten, um zum Beispiel eine Warnung im Gesichtsfeld des Fahrers anzuzeigen, eine akustische Warnung auszugeben oder eine Aktion der Kontrolleinheit eines autonomen Fahrzeugs zu veranlassen. Beim Fernzugriff werden die Diagnosedaten über ein Steuergerät mit Internetkonnektivität geroutet, damit sie das Fahrzeug überhaupt verlassen können.

Typischerweise sieht die Fahrzeugarchitektur für ein Steuergerät eine fest definierte Menge von Aufgaben vor – etwa die Motorsteuerung oder das Empfangen von Signalen eines Funkschlüssels. Viele Steuergeräte erfüllen mehrere Aufgaben zugleich, etwa das Infotainmentsystem, das oft auch Informationen über den Reifendruck und andere diagnostische Daten grafisch darstellt. Auf diese Weise entsteht eine Gesamtarchitektur des Fahrzeugs, in der die Funktionalität an konkrete ECU gekoppelt ist. Daraus ergibt sich, dass verschiedene Modelle und Baureihen ein und desselben Modells über eine ähnliche Anzahl und Art von ECU verfügen.

Dennoch ist es aus Sicht der IT-Sicherheit ein Trugschluss, dass die ECU über die verschiedenen Baureihen oder Modelle hinweg so gleich oder mindestens ähnlich sind, dass sie wie in einem Baukasten in Folgevarianten eingebaut werden können, um eine Fahrzeugfunktion auf das neue Produkt zu übertragen. ECU werden in verschiedenen Projekten häufig von unterschiedlichen Zulieferern gefertigt und programmiert. Nicht zuletzt dadurch verändern sich ihre Fähigkeiten und Funktionen hinsichtlich Hardware und Software, auch wenn die kundensichtbare Funktionalität erhalten bleibt. Zudem werden in neuen Fahrzeugen in der Regel neue Funktionen auf den Markt gebracht. Diese Funktionen werden durch neue ECU oder durch das Weiterentwickeln bestehender ECU erreicht.

Ein Konzept zur Absicherung des Fahrzeugs, das Annahmen über die zu verbauenden ECU trifft, kann daher schnell hinfällig werden und ist nicht mehr auf neue Baureihen übertragbar. Beispielsweise könnten die Entwickler einer ECU davon ausgehen, dass die von der ECU verarbeiteten Sensordaten aus Datenschutzsicht unkritisch sind und deswegen auf eine Verschlüsselung dieser Daten verzichten oder die Daten gar freimütig in Fehlerprotokollen abspeichern. Wird nun in einer neuen Baureihe diesen Sensordaten ein GPS-Stempel hinzugefügt, ist die Annahme hinfällig und existierende



Lösungen sind plötzlich unsicher, obwohl sie in vorigen Kontexten ein akzeptables Schutzniveau hatten. Es kann zum ungesicherten Speichern von personenbezogenen Daten kommen, ohne dass dies bemerkt würde. Folglich kann auch der Kunde nicht einwilligen. Die eingangs erwähnte, stark heterogene Organisationsstruktur der Automobilindustrie reduziert die Kommunikation der Entwickler untereinander und verdeckt auf diese Weise solche Probleme. Im Gegensatz zu funktionalen Fehlern, die beim Testen der Fahrzeuge gefunden werden, kann ein solcher Fehler ohne erkennbare Konsequenz bleiben – jedenfalls bis ein Angreifer die Probleme ausnutzt oder diese publiziert werden.

4.2 Bedrohungsmodelle und redundante Absicherung als Präventivmaßnahme

Dieser Art von Problem kann durch eine Kombination von Maßnahmen begegnet werden. Zunächst sollten Bedrohungsmodelle (engl. Threat Models) gepflegt werden, die Bedrohungen und deren Gegenmaßnahmen aufzählen. Basieren diese Gegenmaßnahmen auf Annahmen über die Netzwerktopologie oder die Hardwareausstattung einer ECU, treffen diese Annahmen nicht mehr zu. Bedrohungsmodelle sind ein unerlässliches Werkzeug, um ein sicheres System zu entwickeln und zu pflegen. In der Automobilindustrie haben sie wegen der beschriebenen heterogenen Projektstrukturen ein ganz besonders großes Potenzial, um Fehler systematisch und früh zu erkennen. Wird in einem Bedrohungsmodell etwa explizit dargelegt, dass die Bedrohung des unbefugten Auslesens von Daten nicht berücksichtigt wird, da die Daten als unkritisch vorausgesetzt werden, kann das bei einer Änderung der Anforderungen erkannt werden.

So essenziell Bedrohungsmodelle auch sind, sie erfordern eine aktive Auseinandersetzung mit dem System und mit sich ändernden Anforderungen. Aufgrund der Anzahl an ECU und Entwicklern wird dies wiederum zu einer schwer zu stemmenden Aufgabe, vor allem weil bei jeder kleinen Änderung der Anforderungen das gesamte Bedrohungsmodell überarbeitet werden muss. Um hier Abhilfe zu schaffen, ist es hilfreich, möglichst wenige Annahmen zu treffen und stattdessen ein konservatives Design zu pflegen. Anders ausgedrückt: Je mehr Bedrohungen die ECU selbstständig begegnet, desto weniger Einschränkungen bürdet ihre Verwendung dem Gesamtsystem auf. Im obigen Fall kann man etwa auf die Annahme, dass die Daten unkritisch sind, verzichten. Man behandelt dann alle Daten als potenziell schutzbedürftig und ist so gezwungen auf Verschlüsselung und auf starke Authentifizierung zu setzen. In diesem Fall erweisen sich die gespeicherten Daten sogar dann

als sicher, wenn sie plötzlich über Netzwerke übertragen werden. Analog zur funktionalen Sicherheit bietet ein konservatives Design mit redundanten Sicherheitsmaßnahmen die beste Absicherung gegen sich wandelnde Architektur und Technologie.

Im Zusammenhang mit autonom fahrenden, vernetzten Autos wird die oben beschriebene Landschaft noch heterogener. Das bereits beschriebene, kooperative Fahren (vgl. Kapitel 3.4) erfordert einen Austausch von Daten, insbesondere Sensordaten, über das eigene Fahrzeug hinaus. Daten kommen jetzt nicht nur aus dem eigenen Bordnetz und sie werden auch nicht mehr nur im eigenen Bordnetz verarbeitet. Spätestens diese Form der Vernetzung der Automobile sorgt also dafür, dass das Bedrohungsmodell des Fahrzeugs grundsätzlich von unsicheren Übertragungskanälen ausgehen sollte. Die Herkunft von Daten muss geprüft und der prospektive Empfänger der Daten authentifiziert werden. Im Sinne der Kryptografie ist es geboten, nicht mehr zwischen bordnetzeigenen und bordnetz-fremden Daten zu unterscheiden. Alle Daten sollten mit der gleichen Vorsicht und der gleichen Sorgfalt authentifiziert, validiert und gegebenenfalls geschützt werden.

4.3 Lifecycle und Softwareupdates

Neben der stark heterogenen Natur der Automobilindustrie existiert noch ein zweiter Unterschied zur klassischen IT-Wirtschaft: Während moderne Geräte im Bereich Consumer Electronics, wie zum Beispiel Smartphones, Smartwatches, Tablets und Laptops, eine übliche Lebensdauer im Bereich von wenigen Jahren haben, ist die Lebensdauer eines Automobils deutlich höher. Nicht selten ist ein Fahrzeug über 20 Jahre im Gebrauch. Hersteller garantieren die Verfügbarkeit von Ersatzteilen über einen Zeitraum von etwa zehn Jahren. In der Regel werden die Automobile innerhalb dieser Zeit nicht substanziell weiterentwickelt, was auch dem Geschäftsmodell geschuldet ist, das die Kosten des Herstellers auf die Entwicklungszeit und die Fertigung beschränkt. Bisher schloss dies auch die Software ein. Die lange Lebensdauer und das Entwicklungsende bei Fertigungsbeginn haben profunde Auswirkungen auf die IT-Sicherheit.

Zunächst wird kein modernes Softwareprodukt dauerhaft in dem Zustand belassen, in dem es initial auf den Markt gebracht wurde. Viele Geschäftsmodelle setzen auf Diensten auf, die immer wieder an neue Anforderungen und Gegebenheiten, aber auch Funktionen angepasst werden. Updates sind damit ein vertrauter Teil der Nutzung nahezu jedes digitalen Produkts. Sie können, gegebenenfalls



gegen Bezahlung, neue Funktionalität verfügbar machen. Häufiger aber beheben Updates Probleme und Fehler in der Software – viele davon IT-Sicherheitsfehler. Einige sind rein funktionale Probleme.

Man kann die enorme Bedeutung, die Softwareupdates für die IT-Sicherheit haben, nicht genug unterstreichen. Software enthält oft sicherheitskritische Fehler, die behoben werden müssen. Diese Fehler entstehen, im Gegensatz zu funktionalen Fehlern, nicht nur durch Unachtsamkeit oder mangelndes Testen. Sie entstehen auch durch eine immer weiter fortschreitende Entwicklung der Angriffsmethoden. Ein jüngeres Beispiel für diese Art Fehler sind die Sicherheitslücken moderner Prozessoren, die Anfang 2018 als Meltdown und Spectre bekannt wurden. Vor dem Bekanntwerden dieser Lücken konnte keine Verteidigungsstrategie umgesetzt werden, da diese Art der Bedrohung unbekannt war. Schnelle Updates sind der einzige Weg, um solchen Bedrohungen zu begegnen.

4.4 Verschlüsselung und Protokolle aktuell halten

Ein eng verwandtes Problem ist das der veralteten Kryptografie. In vielen Bereichen der IT-Sicherheit wird mit Methoden der Kryptografie gearbeitet. Auf diese Weise wird Netzwerkverkehr verschlüsselt und mittels kryptografischer Protokolle werden die Kommunikationspartner authentifiziert. Im bereits angesprochenen Beispiel der Softwareupdates ist Kryptografie ein unersetzlicher Bestandteil. Sie dient in der Form von Signaturen als Manipulationsschutz und stellt sicher, dass das Update nachweisbar vom Hersteller stammt. Wird diese Signatur von einem Angreifer umgangen, etwa weil das Signaturverfahren nicht länger sicher ist, kann der Angreifer unter Umständen beliebige Software auf dem Steuergerät ausführen – mit teils gravierenden Konsequenzen.

Kryptografie und Protokolle, die darauf aufbauen, werden stets überarbeitet und an neue Gegebenheiten angepasst. So ist das weit verbreitete TLS-Protokoll, mit dem zum Beispiel Verbindungen zwischen Browser und Bankwebseiten, aber auch zwischen Fahrzeug und Backend, abgesichert werden, inzwischen in der Version 1.3 verfügbar. Ältere Versionen, wie 1.0, gelten heute als überholt und unsicher. Zwischen diesen beiden Versionen liegen 19 Jahre – es fahren noch Autos, die älter sind, auf unseren Straßen. Solche Versionssprünge müssen vom Hersteller auch für Altfahrzeuge mitgegangen werden, um die Sicherheit des Systems über einen langen Zeitraum zu gewährleisten.

Zusammenfassend ist die Automobilindustrie durch ihr Netzwerk an Zulieferern und deren unterbeauftragten Firmen enorm komplex. Diese Komplexität wird durch die Vielzahl an Modellen und Baureihen der Hersteller noch erhöht. Für die IT-Sicherheit stellt das eine enorme Herausforderung dar, der sich nur durch systematische Bedrohungsmodelle seitens der OEM sowie durch eine konsequent konservative Sicherheitsarchitektur begegnen lässt. Da hierbei unweigerlich Fehler passieren und sich die Angriffsmethoden immer weiterentwickeln, sind Softwareupdates für alle ECU ein unerlässlicher Baustein eines tragfähigen Sicherheitskonzepts.

In diesem Kapitel wurde bewusst nicht auf die konkreten technischen Herausforderungen des Connected Cars eingegangen. Hierzu zählen unter anderem die Absicherung des Datenverkehrs zwischen Fahrzeug und Backend, der Manipulationsschutz von Software im Auto oder bei der Übertragung dorthin, etwa beim Update. Diese Probleme unterscheiden sich auf technischer Ebene kaum von ihren Pendants aus verwandten Disziplinen wie der Bereitstellung von Clouddiensten, die auf ständige und sichere Verbindungen angewiesen sind, beispielsweise in der Telemedizin oder in der vernetzten Produktionssteuerung. Die Absicherung von Geräten und Updates ist auf Smartphones bereits gelöst und diese Lösungen sind übertragbar. Ebenso ist die Internetwirtschaft sich der Methoden der Absicherung einer Netzwerkkommunikation bewusst. Diese Themen sind gleichwohl zentrale Aufgaben der Automobilindustrie. Die besondere Herausforderung wird sein, die bestehenden Lösungen in das, wie oben beschrieben, nicht immer zur IT-Industrie kompatible Ökosystem „Automobil“ zu übertragen.



Interview



„Cyberkriminelle sind bei Fahrzeugen aus Gewissensgründen nicht zurückhaltender als in anderen Bereichen.“

Interview mit Prof. Dr. Norbert Pohlmann, Vorstand IT-Sicherheit, eco – Verband der Internetwirtschaft e.V.

Autos kommunizieren immer stärker untereinander und mit ihrer Umwelt. Damit geraten sie auch ins Visier von Cyberkriminellen. Prof. Dr. Norbert Pohlmann, Vorstand für IT-Sicherheit im eco Verband, fordert von der Branche mehr Zusammenarbeit, um gemeinsam die größtmögliche Sicherheit zu schaffen.

Welche Herausforderungen gibt es für die IT-Sicherheit im vernetzten Auto?

In der Vergangenheit war die IT in Autos von der Außenwelt abgekapselt. Dadurch waren unerwünschte Zugriffe von außen ausgeschlossen. Inzwischen sind in Autos immer mehr Systeme vernetzt, etwa für die Navigation oder den automatischen Notruf eCall. Hinzu kommen Systeme für das Infotainment, das automatische Bezahlen von Parkgebühren und Maut oder die Car-to-Car-Kommunikation. Zukünftig werden Autos autonom fahren. Sie sind dann auf noch viel mehr Informationen von außen angewiesen – von Steuersystemen für den Verkehrsfluss bis hin zu Ampeln.

Welche Gefahren gibt es konkret?

Durch die umfassende Vernetzung entstehen komplexe IT-Ökosysteme, in denen Hacker nach Angriffsmöglichkeiten suchen. Sobald sie eine Sicherheitslücke entdecken, werden sie diese auch ausnutzen. Beispielsweise könnten sie versuchen, einen Erpressungstrojaner zu platzieren und damit drohen, das Fahrzeug stillzulegen, wenn kein Lösegeld gezahlt wird. Die Liste der möglichen Angriffsvektoren ist lang und es ist nicht zu erwarten, dass Cyberkriminelle bei Fahrzeugen aus Gewissensgründen zurückhaltender sind als in anderen Bereichen.

Sollten wir aufgrund dieser Gefahren nicht eher auf die Vernetzung der Autos verzichten?

Das autonome Fahren bietet die Chance, die Zahl der Verkehrstoten sehr stark zu reduzieren. Diese Chance aus Angst vor dem Scheitern gar nicht erst zu nutzen, ist sicher der falsche Weg. Die vernetzten Autos werden sicher sein, wenn wir uns dieser Auf-

Prof. Dr. Norbert Pohlmann,
Vorstand IT-Sicherheit, eco – Verband der Internetwirtschaft e.V.

gabe heute schon stellen. Es gibt hohe Erwartungen an die deutsche Automobilindustrie, was die Verlässlichkeit und Sicherheit der vernetzten Autos betrifft. Damit die Hersteller diese erfüllen können, müssen sie jetzt etwas dafür tun.

Was erwarten Sie konkret von der Automobilwirtschaft?

Die Automobilindustrie braucht eine gemeinsame Strategie für die Infrastruktur im vernetzten Auto. Nur so lässt sich ein sicherer und vertrauenswürdiger Datenaustausch für alle garantieren. Kern dieser Strategie müssen unternehmensübergreifende Standards sein – sei es für die Assistenzsysteme, für das Stromtanken oder die Authentifikation, um ein Auto zu öffnen und zu starten. Momentan arbeitet jeder Autohersteller an einer eigenen Infrastruktur. Dadurch steigt die Komplexität und damit auch das Risiko für Sicherheitslücken. Nur mittels allgemeiner Standards und Zertifikate, die eine durchdachte, verlässliche, vertrauenswürdige und sichere Infrastruktur belegen, lässt sich die Sicherheit der vernetzten Autos langfristig gewährleisten – eine Grundvoraussetzung dafür, dass die Menschen selbstfahrende Autos akzeptieren werden.

Top 5

Kernaussagen von Kapitel 4

- Durch die umfassende Vernetzung der Autos entstehen komplexe IT-Ökosysteme, in denen Hacker neue Angriffsmöglichkeiten finden. Die Komplexität wird durch die Vielzahl an Modellen und Baureihen der Hersteller erhöht.
- Eine große Herausforderung im Bereich der Cybersicherheit ist die Veränderung einzelner elektronischer Bausteine durch Austausch oder Softwareupdates. Dem kann durch Bedrohungsmodelle und eine innovative und globale IT-Sicherheitsinfrastruktur begegnet werden.
- Die Unterscheidung zwischen bordnetz eigenen und bordnetz fremden Daten bedeutet eine Einschränkung der IT-Sicherheit. Datenschutz wird zur umfassenden Aufgabe.
- Dauerhafte Verfügbarkeit von Softwareupdates ist zwingend notwendig, denn der Lifecycle eines Autos beträgt oft mehrere Dekaden.
- Verschlüsselungstechnologien und -protokolle müssen hochaktuell gehalten werden.



5. Datenschutz

Durch den wachsenden Grad der Autonomisierung und Vernetzung von Fahrzeugen nimmt der Austausch von Daten zwischen Autos und Infrastruktur zu. Das ist notwendig, um die informationsbasierten Systeme am Laufen zu halten. Allerdings unterliegen der Datenaustausch und das Recht zur Datenverarbeitung klaren Regeln, die mit Inkrafttreten der DSGVO internationale Geltung besitzen. Die DSGVO ist allerdings nicht die einzige Regelung für den Schutz der Daten, und sie gilt nicht unter jeder Bedingung.

5.1 Datenschutzrechtliche Rahmenbedingungen

Das Datenschutzrecht dient dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 1 DSGVO). Es ist von dem Ziel geprägt, dass betroffene Personen entscheiden können, wer welche Daten wozu und warum über sie verarbeitet. Das gilt auch im Bereich der Mobilität.

Die DSGVO ist seit dem 25. Mai 2018 in allen EU-Mitgliedstaaten als EU-Verordnung unmittelbar anwendbares Recht zur Regelung des Schutzes personenbezogener Daten. Sie hat grundsätzlich Vorrang vor nationalen Regelungen, die denselben Anwendungsbereich haben. Das gleichzeitig in Kraft getretene Bundesdatenschutzgesetz in der seit dem 25. Mai 2018 geltenden Fassung (BDSG) ist darauf beschränkt, Themen zu regeln, für die die DSGVO eine Regelung durch nationales Recht fordert oder ausnahmsweise zulässt.

Daneben bestehen für den vorliegenden Kontext auch datenschutzrechtliche Spezialregelungen im Telekommunikationsgesetz (§§ 91 ff. TKG) und im Telemediengesetz (§§ 11 ff. TMG). Derzeit geht man davon aus, dass die §§ 11 ff. TMG vollständig durch die DSGVO verdrängt werden und bestimmte Regelungen der §§ 91 ff. TKG nach Maßgabe des Art. 95 DSGVO fortgelten. Diese unklare Rechtslage hat ihre Ursache darin, dass der deutsche Gesetzgeber bislang nicht für die gebotene Rechtsklarheit sorgte, indem er die telemedien- und telekommunikationsrechtlichen Regelungen aufhob oder an die Vorgaben der DSGVO anpasste.

Ferner könnte zukünftig vor allem die derzeit diskutierte ePrivacy-Verordnung²⁸ für Connected Cars anwendbar sein, soweit elektronisch Daten übertragen werden. Die ePrivacy-Verordnung zielt primär auf den Schutz von personenbezogenen Daten bei der Kommunikation in öffentlichen Kommunikationsnetzen.

5.2 Anwendungsbereich des Datenschutzrechts

Die DSGVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1 DSGVO).

Im vorliegenden Kontext ist typischerweise von einer automatisierten Verarbeitung auszugehen. Entscheidend ist damit, ob personenbezogene Daten verarbeitet werden. Als „personenbezogene Daten“ definiert Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Diese Person wird in der DSGVO als „betroffene Person“ bezeichnet. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Nr. 1 DSGVO). Erwägungsgrund 26 DSGVO gibt weitere Anhaltspunkte, wie der Personenbezug zu verstehen ist:

„[...] Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche

28 Die Electronic Communications Code Directive beschäftigt sich mit den rechtlichen und technischen Rahmenbedingungen zur Erbringung von elektronischen Kommunikationsdiensten und elektronischen Kommunikationsnetzen und soll innerhalb der EU einheitliche Standards schaffen. Die datenschutzrechtlichen Aspekte sollen – nach dem Stand zum Zeitpunkt der Drucklegung – primär durch die ePrivacy-Verordnung geregelt werden.



Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind. [...]

In Deutschland ist seit vielen Jahren umstritten, wann eine Identifizierbarkeit gegeben ist. Nach einer Entscheidung des EuGH in der Sache Breyer ²⁹ BRD liegt es nahe, die Identifizierbarkeit danach zu bestimmen, ob der Datenverarbeiter – auch unter Heranziehung weiterer Informationen von Dritten – die Daten einer natürlichen Person zuordnen kann (so genannter subjektiver Ansatz). Entgegen dem so genannten objektiven Ansatz werden ihm aber nicht alle beliebigen Erkenntnisse zugerechnet, sondern nur die, auf die er unter Berücksichtigung der vorgenannten Kriterien tatsächlich zugreifen kann. Die Frage ist aber nach wie vor rechtlich umstritten.

Im Umkehrschluss wird allerdings auch deutlich, dass für die Anonymisierung beziehungsweise die Anonymität von Daten, die die Anwendbarkeit des Datenschutzrechts ausschließen, hohe Anforderungen gelten. Erwägungsgrund 26 DSGVO enthält hierzu (im Anschluss an vorstehendes Zitat) folgende Aussage:

„[...] Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, das heißt für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymen Daten, auch für statistische oder für Forschungszwecke.“

Von der Anonymisierung, die endgültig keinen Rückschluss auf eine natürliche Person zulässt, ist die Pseudonymisierung zu unterscheiden. Pseudonymisierung wird durch Art. 4 Nr. 5 DSGVO definiert als:

„[...] die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.“

Pseudonyme Daten sind ein Unterfall personenbezogener Daten und unterliegen daher dem Schutz der DSGVO. Allerdings können sie juristisch relevante Sonderkonstellationen hervorrufen: Speichert beispielsweise der Betreiber einer Fahrzeugflotte die Bewegungsdaten seiner Fahrzeuge, um Laufleistungsdaten zur Überwachung und Kontrolle von Verschleiß an einen Wartungsbetrieb weiterzuleiten, können die Daten für den Flottenbetreiber und den Wartungsbetrieb mitunter völlig verschiedene datenschutzrechtliche Qualitäten haben. Der Flottenbetreiber weiß, welchen Personen welche Fahrzeuge zugeordnet sind. Die Laufleistungsdaten sind für ihn in jedem Fall personenbezogen. Der Wartungsbetrieb hingegen erhält nur die reinen Laufleistungsdaten aller Fahrzeug der Flotte. Welchen Personen die Fahrzeuge zugeordnet sind, erfährt er jedoch nicht. Daher kann es mitunter möglich sein, dass Daten für einen Empfänger personenbezogen sind und für einen anderen nicht. Diesem Umstand muss Rechnung getragen werden, wenn Datenverarbeitungssysteme erstellt werden.

Damit wird deutlich, dass der Anwendungsbereich des Datenschutzrechts weit gefasst ist und keine hohen Anforderungen an die Anwendung gestellt werden.

Für die Anwendung der DSGVO ist es nicht entscheidend, ob die betroffene Person ein Verbraucher oder Unternehmer ist.²⁹ Datenschutzrecht ist kein Verbraucherschutzrecht. Hingegen sind Daten, die sich ausschließlich auf juristische Personen beziehen, vom Schutzbereich der DSGVO ausgenommen. Das sind beispielsweise Daten über eine GmbH, eine AG oder einen Verein.³⁰ Eine Besonderheit besteht jedoch: Die Datenschutzbestimmungen des TKG (siehe ausführlicher unten) und voraussichtlich auch der ePrivacy-Verordnung gelten auch für juristische Personen.

Der Schutz der DSGVO greift danach also auch nicht für reine Maschinendaten. Können solche Daten allerdings auf eine natürliche Person bezogen werden und enthalten sie eine Aussage in Bezug auf diese natürliche Person, sind sie ebenfalls personenbezogene Daten:

- Beispielsweise sind Daten über die „Abnutzung“ des Fahrzeugs beim vollautonomen Fahren auf den ersten Blick reine Sachinformationen für das Wartungsintervall und damit nicht personenbezogen. Sobald diese Daten einem Menschen zugeordnet werden können (beispielsweise dem Vertragspartner, Lea-

²⁹ Der eingetragene Kaufmann (e. K.) ist eine natürliche Person und damit vom Schutz der DSGVO erfasst.

³⁰ Bei den so genannten Personengesellschaften – also beispielsweise GbR, OHG und KG – ist es umstritten, ob und in welchen Fällen die DSGVO gilt.



sing- oder Versicherungsnehmer), kann es sich dabei insoweit (auch) um personenbezogene Daten handeln und das Datenschutzrecht ist zu beachten. Wichtig ist allerdings, dass sich die Zuordnung nicht nur aus einem solchen direkten Bezug, sondern auch indirekt ergeben kann, wenn der Zusammenhang aufgrund anderer, weiterer Informationen des Datenverarbeiters hergestellt werden kann. Dies könnte beispielsweise der Fall sein, wenn dem Datenverarbeiter zwar nicht originär bekannt ist, wem das Fahrzeug zur Nutzung zugeordnet ist (beispielsweise wenn der Leasingnehmer eine juristische Person ist), er aber aufgrund einer Bezahlung, einer persönlichen Abgabe im Kundenservice oder einer Anmeldung feststellen kann, wer das Fahrzeug tatsächlich nutzt.

Die Reichweite der Personenbeziehbarkeit solcher Fahrverlaufsdaten wurde bereits in der Vergangenheit deutlich: 2016 wurde ein Fahrer eines Autos aus einer Vermietflotte anhand seiner Anmeldedaten identifiziert und ihm anhand einer Analyse des durch das Fahrzeug erfassten und gespeicherten Fahrverlaufs die Schuld an einem Verkehrsunfall nachgewiesen.

- Ähnlich wie bei Maschinendaten muss auch bei juristischen Personen hinterfragt werden, ob nicht doch Daten in Bezug auf Menschen verarbeitet werden. Das kann beispielsweise der Fall sein, wenn formal eine juristische Person (beispielsweise eine GmbH) der Vertragspartner ist, aber dem Anbieter die nutzende Person (beispielsweise der Geschäftsführer) bekannt ist. Selbst wenn dies für den Anbieter nicht der Fall sein sollte, kann im Binnenverhältnis beispielsweise zwischen der anmietenden GmbH und dem Beschäftigten, dem sie das Auto zur Nutzung überlässt, das Datenschutzrecht zum Tragen kommen.

Ob Maschinendaten personenbezogen sind oder Daten in Bezug auf „hinter“ der juristischen Person stehende Menschen betroffen sind, muss im konkreten Einzelfall bewertet werden. Deutlich werden soll aber, dass keine pauschalen „Ausblendungen“ des Datenschutzrechts erfolgen können.

5.3 Welches Datenschutzgesetz gilt?

Die DSGVO ist nicht das einzige in Deutschland geltende Gesetz, das Datenschutzbestimmungen enthält. Zwar werden nach überwiegender Ansicht die Datenschutzbestimmungen des TMG – wie oben bereits erläutert – durch die DSGVO verdrängt. Sie bleiben jedoch ebenso wie die Datenschutzbestimmungen der geplanten ePrivacy-Verordnung anwendbar.

Die Datenschutzbestimmungen des TKG sowie der geplanten ePrivacy-Verordnung enthalten Spezialregelungen für die Verarbeitung von Daten, die im Rahmen und aufgrund einer Übertragung über Kommunikationsnetze anfallen (insbesondere für Standortdaten). In Bezug auf die Zulässigkeit der Verarbeitung sind diese Datenschutzbestimmungen „strenger“ als die DSGVO, da sie insbesondere keine Zulässigkeit aufgrund einer Interessenabwägung vorsehen, sondern nur in den explizit durch die Datenschutzbestimmungen geregelten Fällen. Diese Zulässigkeitsregelungen sind aber nicht auf Connected Car oder IoT zugeschnitten. Damit müsste im praktischen Ergebnis für Connected Car oder IoT ein (zu) enger Rechtsrahmen beachtet werden.

Im Art. 95 legt die DSGVO „in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen“. Nach überwiegender Ansicht gelten danach die Regelungen in den Datenschutzbestimmungen des TKG für Erbringer öffentlich zugänglicher Kommunikationsdienste fort, soweit die Regelungen in den §§ 91 ff. TKG auf der Richtlinie 2002/58/EG beruhen.

Für die Anwendbarkeit der Datenschutzbestimmungen des TKG statt der DSGVO sind damit – vereinfacht zusammengefasst – folgende Aspekte zu prüfen:

- Die Datenerhebung muss im Rahmen eines öffentlich zugänglichen Kommunikationsdienstes innerhalb eines öffentlichen Kommunikationsnetzes erfolgen.
Für Fahrzeugdiagnosesysteme wird die Anwendung des TKG eher zu verneinen sein. Das kann unter Umständen für Fahrzeughersteller zutreffen, die dem Nutzer eine Telekommunikationsverbindung zur Verfügung stellen, um über diese zu kommunizieren oder um Anwendungen im Internet aufzurufen. Für die Bewertung von Softwareaktualisierung „over the Air“ (SOTA) und den Austausch von Sensordaten wird es auf die Art des Updates und die Vertragsgestaltung gegenüber dem Kunden ankommen. Entscheidend wird damit, ob die Vernetzung des Fahrzeugs nur für eigene Zwecke des Anbieters erfolgt oder ob sie (auch) zur Kommunikation des Nutzers dient.



- Die Datenschutzbestimmungen des TKG gelten dann in Bezug auf die mit dem Angebot des öffentlich zugänglichen Kommunikationsdienstes verbundenen Bestands-, Verkehrs- und Standortdaten.

Im Übrigen gelten die Regelungen der DSGVO. Die Einzelheiten dieser Abgrenzung sind rechtlich komplex und – natürlich – auch umstritten, sodass der jeweilige Einzelfall geprüft werden muss. Der Gesetzgeber hat die gebotene Anpassung des Anwendungsbereichs der Datenschutzbestimmungen des TKG auf den Anwendungsbereich der öffentlichen Netze bis zur Drucklegung unterlassen.

Ob, wann und mit welchem Anwendungsbereich die ePrivacy-Verordnung in Kraft treten wird, ist derzeit unklar. Sie soll die ePrivacy-Richtlinie 2002/58/EG, die in Deutschland in den Datenschutzbestimmungen des TKG umgesetzt wurde, ablösen. Die Datenschutzbestimmungen des TKG würden durch diese dann verdrängt und müssten durch den deutschen Gesetzgeber aufgehoben werden. Die Diskussion über das anzuwendende Recht spielt daher weiterhin eine Rolle.

5.4 Wer ist verantwortlich für den Datenschutz?

Die DSGVO bezeichnet den für den Datenschutz verantwortlichen als „Verantwortlichen“. Das führt – wie der vorstehende Satz zeigt – zuweilen zu sprachlich unschönen Formulierungen und zu Missverständnissen.

Die DSGVO definiert den Verantwortlichen in Art. 4 Nr. 7 DSGVO wie folgt:

„[...] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet [...]“.

Ausschlaggebend ist damit, wer über die Zwecke und Mittel der Verarbeitung entscheidet. Auch wenn zwei Personen oder Stellen gemeinsam die Zwecke und Mittel bestimmen, bleibt jeder für die Einhaltung der Pflichten der DSGVO verantwortlich. Der EuGH hat in der Entscheidung zu Facebook-Fanpages anhand der Vorgängerregelung in der Datenschutzrichtlinie 95/46/EG Kriterien benannt, bei denen eine gemeinsame Verantwortlichkeit (Joint Controllership) angenommen werden muss.

Der EuGH hat in dieser Entscheidung auch klargestellt, dass ein Joint-Controllership-Agreement keine gleichmäßige Mitbestimmung der Zwecke und Mittel der Datenverarbeitung erfordert. Es kann in diesem Zusammenhang bereits genügen, dass ein Verantwortlicher die Verarbeitung durch den anderen Verantwortlichen „veranlasst“. Die Anforderungen an eine solche Veranlassung sind im Einzelfall noch nicht abschließend geklärt. Ein weiteres Kriterium ist, dass der eine von der Datenverarbeitung des anderen profitiert. Die Bedeutung und Anwendung dieser Kriterien werden derzeit kontrovers diskutiert, da es nicht leicht ist, eine Grenze zur getrennten, alleinigen Verantwortlichkeit zu ziehen.

Eine wesentliche Neuerung in der DSGVO ist aus deutscher Sicht, dass weitere datenschutzrechtliche Regelungen greifen, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel der Datenverarbeitung bestimmen. Sie sind insofern gemeinsame Verantwortliche.

Diese Neuerung dürfte im Bereich von Connected Cars, insbesondere aber auch bei autonom fahrenden Autos, hohe Bedeutung haben, denn in den Fahrzeugen fallen – wie in Kapitel 3 dargelegt – eine Vielzahl von Sensor- und sonstigen Nutzungsdaten an, die nicht zwangsläufig ausschließlich durch den Fahrzeughersteller erhoben und verarbeitet werden müssen. Vielmehr ist denkbar, dass auch andere Unternehmen, wie etwa Wartungs- und Reparaturbetriebe, Versicherungen oder Anbieter von On-Board-Entertainment-Programmen, die im oder durch das Fahrzeug generierten Daten für ihre eigenen Zwecke verarbeiten. Deshalb liegt es nahe, dass diese Stellen hinsichtlich der zu verarbeitenden Daten als gemeinsame Verantwortliche agieren werden. Eine gemeinsame Verantwortlichkeit (Joint Controllership) hat für die Beteiligten weitreichende Folgen:

- Die gemeinsam Verantwortlichen müssen nach Maßgabe des Art. 26 DSGVO untereinander regeln, wer auf welche Weise die Betroffenenrechte (Auskunft, Berichtigung, Löschung, Datenübertragbarkeit, Recht auf Vergessen etc.) erfüllt und die wesentlichen Bestandteile dieser Vereinbarung der betroffenen Person bekannt machen.
- Sie können nach Maßgabe des Art. 82 DSGVO im Außenverhältnis gesamtschuldnerisch auf Schadensersatz haftbar sein,

Joint Controllership darf aber nicht dahingehend verstanden werden, dass dadurch die gemeinsame Verarbeitung personenbezogener Daten irgendwie erleichtert wird. Jeder der Verantwortlichen wird datenschutzrechtlich als eigenständiger Verantwortlicher behandelt und muss selbst im Sinne des Art. 6 DSGVO zur Datenverarbeitung



berechtigt sein. Die gemeinsame Verantwortlichkeit ist kein Rechtsgrund für eine Datenverarbeitung.

Die DSGVO kennt als weiteren Datenverarbeiter den Auftragsverarbeiter. Das ist nach Art. 4 Nr. 8 DSGVO „[...] eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“. Aus Art. 28 DSGVO ergibt sich, dass ein Auftragsverarbeiter nicht über den Zweck und die Mittel der Verarbeitung entscheiden darf. Er ist weisungsabhängig tätig.

Zusammenfassend lässt sich feststellen: Die DSGVO kennt verschiedene Datenverarbeiter mit unterschiedlichen Anforderungen und unterschiedlichem Verhältnis zueinander. Bei der Gestaltung der Zusammenarbeit von Datenverarbeitung und bei dem Angebot von Leistungen gegenüber den betroffenen Personen ist konkret zu prüfen, wer im Sinne der DSGVO über die Zwecke und Mittel der Verarbeitung allein (Verantwortlicher), gemeinsam mit (einem) anderen (Joint Controller) oder gegenüber einem weisungsgebundenen handelnden Auftragnehmer (Auftragsverarbeitung) entscheidet.

Im Kontext der Entwicklung und Implementierung von Connected-Car-Anwendungen muss daher frühzeitig konkret bewertet werden, ob in Folge der Veranlassung einer Datenverarbeitung oder aus anderen Gründen eine Joint Controllership vorliegt, denn hieraus ergeben sich weitere Anforderungen für die Verarbeitung der Daten. Beispielsweise können Hersteller, Versicherer und Carsharing-Anbieter Joint Controller sein, wenn diese gemeinsam die Mittel und Zwecke der Verarbeitung personenbezogener Daten festlegen.

Der Vollständigkeit halber ist darauf hinzuweisen, dass in bestimmten Konstellationen auch die besonderen Bestimmungen des Beschäftigtendatenschutzes nach § 26 BDSG in Verbindung mit Art. 88 DSGVO zur Anwendung kommen können. Dies kann insbesondere der Fall sein, wenn der Vertragspartner nicht direkt der Nutzer selbst ist, sondern etwa der Arbeitgeber das Fahrzeug zur Verfügung stellt und (auch) personenbezogene Daten aus den Connected-Car-Anwendungen verarbeitet. Das bedeutet: Während zwischen dem Anbieter und dem Arbeitgeber die allgemeinen Datenschutzregelungen der DSGVO angewendet werden, kommen zwischen Arbeitgeber und der konkret betroffenen Person die Regelungen zum Beschäftigtendatenschutz zur Anwendung. Der Arbeitgeber ist dann Verantwortlicher im Verhältnis zum Beschäftigten.

Maßstab für die Rechtmäßigkeit der Datenverarbeitung ist in diesen Konstellationen grundsätzlich die Erforderlichkeit der Datenverarbeitung für die Durchführung des Beschäftigungsverhältnisses. Insofern gilt es genau zu prüfen, ob und wenn ja, inwieweit die Analyse der Fahrzeugdaten dem Beschäftigungsverhältnis zuzuordnen ist und zu Zwecken des Beschäftigungsverhältnisses verarbeitet wird. Die Voraussetzungen im Beschäftigtendatenschutz werden eng ausgelegt und Tatbestandsmerkmal der Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses in § 26 BDSG wird nicht in jeder Konstellation vorliegen. Ob und inwieweit daneben die Zulässigkeitsregelungen der DSGVO (insbesondere der Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO) zur Anwendung kommen können, ist umstritten und wird im konkreten Einzelfall zu bewerten sein. Die wirksame Einwilligung des Beschäftigten wird typischerweise an der vorausgesetzten Freiwilligkeit scheitern. Jedenfalls verneint die Rechtspraxis häufig aufgrund der Abhängigkeitsfähigkeit im Beschäftigungsverhältnis die freie Entscheidungsfähigkeit und damit die Freiwilligkeit.

5.5 Datenschutzrecht: Anforderungen an die Zulässigkeit und die Dokumentation

Mit dem Anwendungsbeginn der DSGVO sind neben die Zulässigkeitsbewertung (nachfolgend Kapitel 5.5.1) stark ausgeprägte Regelungen über die Dokumentation und die Organisation der Einhaltung des Datenschutzes getreten (nachfolgend Kapitel 5.5.2 und 5.5.3). Das ist der eigentliche Paradigmenwechsel im Datenschutzrecht infolge der DSGVO.

Diese Anforderungen entstehen nicht spezifisch für Connected-Car-Anwendungen, sondern gelten allgemein für jede Verarbeitung personenbezogener Daten. Die Vorgaben zur Dokumentation werden auch für sich nicht dazu führen, dass Datenverarbeitungen unzulässig sind. Aber ihre Nichtbeachtung ist gleichwohl bußgeldbewehrt.

Eine abschließende Darstellung dieser neuen Anforderungen infolge der DSGVO ist in diesem Leitfaden nicht möglich und würde den inhaltlichen Schwerpunkt verschieben. Zur Verdeutlichung des Umfangs wird nachfolgend exemplarisch auf einzelne Aspekte eingegangen.



5.5.1 Zulässigkeit der Verarbeitung

Das Datenschutzrecht ist von dem Grundsatz geprägt, dass jede Verarbeitung personenbezogener Daten unzulässig ist, es sei denn, die betroffene Person hat eingewilligt, ein Gesetz gestattet es oder ordnet die Verarbeitung in Übereinstimmung mit der DSGVO an (so genanntes Verbot mit Erlaubnisvorbehalt; Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 DSGVO). Hinzu kommt der Grundsatz der Zweckbindung, wonach die Zulässigkeit für den jeweiligen Verarbeitungszweck zu prüfen ist (beispielsweise sind Vertragsabwicklung und Werbung zwei verschiedene Zwecke) (Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4 DSGVO).

Im Rahmen von Connected-Car-Anwendungen kommen vor allem folgende Faktoren in Betracht:

- die Erfüllung eines Vertrags gegenüber der Person, deren Daten verarbeitet werden (Art. 6 Abs. 1 lit. b DSGVO),
- die Interessenabwägung (Art. 6 Abs. 1 lit. f DSGVO) und
- die Einwilligung, wobei sorgfältig die Freiwilligkeit zu prüfen ist (Art. 6 Abs. 1 lit. a DSGVO).

Bei dem weiter oben aufgeführten Beispiel des Over-the-Air-Updates ist wahrscheinlich auch die Verarbeitung personenbezogener Daten erforderlich, um das Update dem richtigen Fahrzeug zuordnen zu können. Dies ist insbesondere dann der Fall, wenn Updates oder Zusatzfunktionen gegen Zahlung eines Aufpreises angeboten werden. Da das Update entweder aufgrund einer (kostenpflichtigen) Zusatzvereinbarung aufgespielt wird oder für den Betrieb des Fahrzeugs notwendig ist (und damit zumindest Teil der Herstellergarantie, wenn nicht sogar des Kaufvertrags), wird hier in der Regel die Verarbeitung erfolgen, um einen Vertrag zu erfüllen.

5.5.2 Transparenz der Verarbeitung

Die Transparenz der Datenverarbeitung ist ein wesentliches Element der Selbstbestimmung der betroffenen Person, weshalb die Einhaltung der entsprechenden Vorgaben seit jeher die besondere Aufmerksamkeit der Datenschutzaufsichtsbehörden genießt. Die DSGVO sieht in den Art. 13 und 14 Informationspflichten vor, die proaktiv ausgestaltet sind. Diese sind inhaltlich umfassend (unter anderem Verarbeiter, Zweck der Verarbeitung, Rechtsgrundlage, Löschregelungen, Drittlandübermittlung, Empfänger beziehungsweise Quellen der Daten) und können durch verschiedene Vorgänge ausgelöst werden:

- bei der Erhebung der Daten,
- bei einer zweckändernden Verarbeitung,
- bei der Absicht, die Daten an einen Dritten zu übermitteln sowie
- wenn Daten nicht direkt bei der betroffenen Person selbst

(beispielsweise von anderen Datenverarbeitern oder aus dem Internet) erhoben werden.

Insbesondere in komplexen Datenverarbeitungen werden diese Informationspflicht und die Informationserteilung zum richtigen Zeitpunkt eine Herausforderung.

Im Zusammenhang mit Connected Cars werden personenbezogene Daten von Teilnehmern (also beispielsweise Fahrern), aber auch außenstehenden Dritten erfasst, die in keiner Beziehung zu dem Verantwortlichen stehen. Beide Personenkreise sind jedoch nach Art. 13 und 14 DSGVO zu informieren. Als Möglichkeit ist beispielsweise in Betracht zu ziehen, dass die Personen – ähnlich wie bei Einzelverbindungen im Telekommunikationsbereich – durch den Anbieter informiert werden und dadurch keine zusätzlichen Informationen durch die weiteren Beteiligten notwendig sind.

Die Herausforderung ist nicht nur, wie der Informationspflicht nachgekommen werden soll, sondern auch, wer informieren soll. Diese Aufgabe obliegt dem Verantwortlichen (vgl. Kapitel 5.4). An dem Betrieb eines autonom fahrenden Autos gibt es stets mehrere Beteiligte, die eine Informationspflicht treffen kann. Die Praxis zeigt, dass sich die Verantwortlichen koordinieren müssen, um einen praktikablen und dennoch datenschutzkonformen Weg zu finden, um die Transparenzpflichten zu erfüllen.

Oftmals werden die Verantwortlichen als gemeinsame Verantwortliche (siehe Kapitel 5.4) auftreten. In diesem Fall sind sie sogar verpflichtet, die Erfüllung der Pflichten gegenüber der betroffenen Person festzulegen.

Diese rechtlichen Fragen und ihre praktische Umsetzung gilt es bereits in der Entwurfsphase für ein Connected Car zu berücksichtigen.

Eine weitere Frage stellt sich auch im Rahmen des Anwendungsbeispiels „Kooperatives Fahren“ (vgl. Kapitel 3.4). Werden bei dem Austausch der Sensordaten weitere Daten übermittelt, die zumindest mittelbar einen Rückschluss auf eine natürliche Person zulassen, und werden deshalb personenbezogene Daten übermittelt, dann ist die betroffene Person grundsätzlich nach Art. 13 und 14 DSGVO zu informieren. Ob die Art der Übermittlung in einer Weise geschieht, dass die Erteilung der Pflichtinformation einen unverhältnismäßigen Aufwand gemäß Art. 14 Abs. 5 lit. b DSGVO erfordern würde, kann erst abschließend bewertet werden, wenn der Use Case endgültig feststeht und der Datenaustausch vollends analysiert werden kann.



5.5.3 Grundsätze und Dokumentationspflichten

Die Grundsätze der Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO geregelt. Diese müssen in Bezug auf jede Verarbeitung personenbezogener Daten beachtet werden. Besondere Bedeutung erlangen diese Grundsätze, weil sie nach Art. 5 Abs. 2 DSGVO der so genannten Rechenschaftspflicht unterliegen: Der Verantwortliche hat die Einhaltung der datenschutzrechtlichen Anforderungen sicherzustellen und muss deren Einhaltung nachweisen können. Mit dieser Nachweispflicht ist die zentrale Regelung der Dokumentation – neben dem Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) und den Transparenzregelungen (Art. 13 und 14 DSGVO) – angesprochen.

Die Regelungen erfordern eine grundlegende, einzelfallbezogene datenschutzrechtliche Bewertung jeder Verarbeitung personenbezogener Daten und deren Dokumentation. Ein zentraler Anknüpfungspunkt ist hierbei die Bestimmung der Person des Verantwortlichen, denn jeder Verantwortliche ist für sich hierzu verpflichtet. Auch bei einer Joint-Controllership-Vereinbarung muss die Dokumentationspflicht durch jeden Verantwortlichen erfüllt werden.

5.6 Wer ist geschützt, wenn Vertragspartner und Nutzer nicht identisch sind?

Die DSGVO schützt die so genannte betroffene Person, also gemäß Art. 4 Nr. 1 DSGVO jede natürliche Person, in Bezug darauf, welche Daten verarbeitet werden (vgl. Kapitel 5.2). Insofern ist der Schutzbereich der DSGVO weit gespannt. Im Bereich der Connected-Car-Anwendungen sind alle betroffenen Person geschützt, unabhängig davon, ob sie Halter, Fahrer oder von der Verarbeitung betroffene Dritte sind.

Ein Vergleich mit den TKG-Datenschutzbestimmungen eröffnet ein „Denkmodell“: Bei Connected-Car-Anwendungen zeigt sich eine Rollenverteilung, die die Datenschutzbestimmungen des TKG kennen. Das TKG unterscheidet zwischen „Teilnehmer“ und „Nutzer“. Der Teilnehmer ist der Vertragspartner des Datenverarbeiters (vgl. § 3 Nr. 20 TKG). Nutzer ist, wer eine solche Anwendung nutzt, aber nicht der Vertragspartner ist (vgl. § 3 Nr. 14 TKG). Interessant ist diese Unterscheidung zum einen, weil die Begrifflichkeiten eine Differenzierung der Rollen ermöglicht. Zum anderen differenziert das Gesetz auch aufgrund der Rollen in den Zulässigkeits- und Transparenzregelungen. Diese Konstellation ist gerade bei Connected-Car-Anwendungen vergleichbar. Unterschieden werden könnte

einerseits der Vertragspartner in Bezug auf das Fahrzeug oder die Connected-Car-Anwendung und andererseits die sonstigen Nutzer.

Eine solche Rollendifferenzierung sollte auch bei Connected-Car-Anwendungen umgesetzt werden. Die Einführung der Differenzierung in die DSGVO wird nicht in Betracht kommen. Aber für die Zulässigkeitsbewertung und die Umsetzung der Transparenzvorgaben verdeutlicht sie die Unterschiede zwischen den Rollen, denn die Betroffenheit eines Vertragspartners ist eine andere als die eines bloßen Nutzers, den der Anbieter selbst häufig nicht identifizieren kann. Darüber hinaus lassen sich auch im Rahmen der DSGVO aufgrund der Identifikation der Unterschiedlichkeit der verschiedenen Rollen abgestufte Informationsgestaltungen entwerfen, indem beispielsweise der Vertragspartner verpflichtet wird, jeden Nutzer, dem er das Fahrzeug überlässt, zu informieren.

In jedem Fall zeigen die TKG-Datenschutzbestimmungen, dass eine begriffliche Unterscheidung der Rollen zur Klarheit in der Bewertung und Gestaltung führt.

5.7 Privacy by Design und by Default

Die DSGVO regelt unter der Überschrift „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung“ in Art. 25 Anforderungen an die Verarbeitung personenbezogener Daten. Die Regelung adressiert jeden Verantwortlichen, mithin auch die Hersteller von Fahrzeugen und Sensortechnik.

Der in Art. 25 Abs. 1 DSGVO angelegte „Datenschutz durch Technikgestaltung“ fordert geeignete technische und organisatorische Maßnahmen – wie zum Beispiel Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. Dabei sollen berücksichtigt werden: Stand der Technik; Implementierungskosten; Art, Umfang, Umstände und Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung.



Die Connected-Car-Anwendung muss daher von Beginn an so gestaltet werden, dass möglichst wenige Daten für das gesteckte Ziel verarbeitet werden. Beispielsweise bedeutet dies Folgendes für Systeme in Connected Cars, die Kollisionen mit Fahrradfahrern oder Fußgängern vermeiden sollen: In Anbetracht der zuvor beschriebenen Grundsätze sind die Systeme technisch so auszugestalten, dass sie zwar zuverlässig sowohl Fußgänger und Fahrradfahrer als auch andere Verkehrsteilnehmer erkennen, sie aber nicht persönlich identifizieren können. Dies kann etwa bereits dadurch erreicht werden, dass nur niedrigauflösende bildgebende Systeme eingesetzt werden, die aus sich heraus die Identifizierbarkeit eines Individuums ausschließen. Alternativ kann auch erwogen werden, die fraglichen Systeme technisch so auszugestalten, dass sie die zur Kollisionsvermeidung erhobenen Daten bereits im Zeitpunkt der Erhebung anonymisieren.

Ferner erfordert der Datenschutz gemäß Art. 25 Abs. 2 DSGVO, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen für die jeweilige Datenverarbeitung ergreift, die sicherstellen, dass durch datenschutzfreundliche Voreinstellung grundsätzlich nur personenbezogene Daten verarbeitet werden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Der zweite Ansatz konzentriert sich auf die bereitgestellte Anwendung. Danach sind nicht Datenverarbeitungen per se verboten, aber die bereitgestellten Anwendungen sind bei der Auslieferung so einzustellen, dass nicht notwendige Verarbeitungen deaktiviert sind und durch die betroffene Person aktiviert werden müssen.

5.8 Sicherheit der Verarbeitung und Folgenabschätzung des Datenschutzes

Die so genannte Sicherheit der Verarbeitung ist Teil des Schutzes der personenbezogenen Daten. Trotz der begrifflichen Nähe zur IT-Sicherheit ist das Schutzziel nicht dasselbe, denn die IT-Sicherheit zielt auf eine grundsätzliche Absicherung von IT-Systemen ab.

5.8.1 Sicherheit der Verarbeitung

Die Anforderungen an die Sicherheit der Verarbeitung sind durch die DSGVO gegenüber dem bisherigen Datenschutzrecht (vgl. § 9 BDSG-alt) grundlegend und signifikant erweitert worden. Der Grundsatz ist wie folgt in Art. 32 Abs. 1 DSGVO festgelegt und

wird in den weiteren Absätzen des Art. 32 DSGVO ausgestaltet: *„Unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.“*

Art. 32 DSGVO legt hiervon ausgehend fest, dass und wie Maßnahmen bestimmt und dokumentiert werden. Entgegen dem bisherigen Datenschutzrecht nach dem BDSG-alt sind Verstöße gegen die Sicherheit der Verarbeitung bußgeldbewehrt. Auch dadurch wird der neue Stellenwert deutlich.

5.8.2 Datenschutz-Folgenabschätzung

Die Anforderungen an die Sicherheit der Verarbeitung werden in der durch die DSGVO neu eingeführten Datenschutz-Folgenabschätzung in Art. 35 DSGVO „fortgesetzt“: Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Die detaillierte Ausgestaltung erfolgt durch die weiteren Absätze des Art. 35 DSGVO.

Das bedeutet: Jede Verarbeitung muss zunächst darauf geprüft werden, ob voraussichtlich ein solches hohes Risiko besteht. Falls dies bejaht wird, muss eine umfassende Bewertung der Risiken stattfinden. Dieses Risiko kann bei Over-the-Air-Updates noch gering sein, allerdings ist ein hohes Risiko spätestens dann anzunehmen, wenn eine umfangreiche Verarbeitung personenbezogener Daten über den Aufenthalt von natürlichen Personen anhand von Standortdaten stattfindet. Im Bereich des autonomen Fahrens wird so die Durchführung von Datenschutz-Folgenabschätzungen unumgänglich sein.

Die DSGVO zwingt damit dazu, vor Beginn der Verarbeitung die Risiken für den Datenschutz der betroffenen Personen zu ermitteln. Auch wenn Art. 35 DSGVO als Ergebnis nicht die unmittelbare (Un-) Zulässigkeit einer Verarbeitung zur Folge hat, muss das Ergebnis doch bei der Zulässigkeitsprüfung nach Art. 6 DSGVO (insbesondere



bei einer Interessenabwägung) berücksichtigt werden. Außerdem kann das Ergebnis nach Art. 36 DSGVO dazu zwingen, vor der Verarbeitung die Einschätzung der zuständigen Datenschutzaufsichtsbehörde einzuholen (so genannte „Vorherige Konsultation“).

Die Nichtbeachtung dieser Pflichten ist ebenfalls bußgeldbewehrt, womit der Gesetzgeber den Stellenwert dieser Pflicht im Rahmen der DSGVO unterstreicht.

Top 5

Kernaussagen von Kapitel 5

- *Die Datenschutz-Grundverordnung findet im Bereich der autonomen Fahrzeuge dann Anwendung, wenn personenbezogene Daten verarbeitet werden. Diesem Umstand muss bei Erstellung der Datenverarbeitungssysteme Rechnung getragen werden. Zukünftig können außerdem die derzeit diskutierte ePrivacy-Verordnung sowie die Electronic Communications Code Directive für Connected Cars anwendbar sein, sofern elektronisch Daten übermittelt werden.*
- *Im Anwendungsbereich der DSGVO sind neben dem Erfordernis einer Rechtsgrundlage bei der Verarbeitung personenbezogener Daten insbesondere auch die stark ausgeprägten Regelungen über die Dokumentation und die Organisation der Einhaltung des Datenschutzes zu beachten.*
- *Die Connected-Car-Anwendung muss von Beginn an so gestaltet werden, dass möglichst wenige personenbezogene Daten für das gewählte Ziel verarbeitet werden.*
- *Durch datenschutzfreundliche Voreinstellung ist sicherzustellen, dass nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang der Verarbeitung, die Aufbewahrungsdauer sowie die Zugänglichkeit.*
- *Jede Datenverarbeitung im Bereich der autonomen Fahrzeuge muss darauf geprüft werden, ob voraussichtlich ein hohes Risiko besteht. Falls dies bejaht wird, muss eine umfassende Bewertung der Risiken stattfinden, etwa wenn eine umfangreiche Verarbeitung personenbezogener Daten über den Aufenthalt von natürlichen Personen anhand von Standortdaten stattfindet.*



6. Gewährleistungs- und Haftungsregime bei autonomen Fahrzeugen

Autonome Fahrzeuge stellen das Gewährleistungs- und Haftungsrecht im Automobilsektor vor neue Herausforderungen. Ihre Teilnahme am Straßenverkehr und die damit einhergehende mögliche Gefährdung von Leib und Leben ihrer Insassen und der übrigen Verkehrsteilnehmer bringen hohe Anforderungen an Sicherheit und Funktionsfähigkeit im Betrieb solcher Fahrzeuge mit sich. Insbesondere erfordert es die Sicherheit des Straßenverkehrs, dass Risiken von Fehlfunktionen in autonomen Fahrzeugen adressiert werden, möglichst bevor sie sich manifestieren. Insofern spricht vieles dafür, einen präventiven Wartungs- und Instandhaltungsansatz für autonome Fahrzeuge im Betrieb zu verfolgen. Es ist jedoch fraglich, ob sich dieser aus dem geltenden Recht herleiten lässt oder ob das bestehende Rechtsregime angepasst und erweitert werden sollte.

6.1 Status quo der Gewährleistungs- und Garantieansprüche beim Autokauf

Nach derzeitiger in Deutschland geltender Rechtslage ist der Kauf eines Autos nicht anders zu behandeln als der jeder anderen beweglichen Sache. Dies bedeutet, dass von Gesetzes wegen beim Kauf eines Neuwagens eine zweijährige Gewährleistungsfrist besteht, innerhalb derer ein Händler für Mängel am Auto haftet (§ 438 Abs. 1 Nr. 3 BGB), die bereits bei der Übergabe („Gefahrübergang“) vorhanden waren. Durch die verbraucherschutzrechtliche Sonderregelung des § 476 BGB besteht eine Beweislastumkehr hinsichtlich Mängeln, die in den ersten sechs Monaten ab Erwerb des Kraftfahrzeugs auftreten. Zugunsten von Verbrauchern wird innerhalb dieses Zeitraums vermutet, dass das gekaufte Kraftfahrzeug bereits im Zeitpunkt des Erwerbs mangelhaft war, sofern nicht die Art des vom Verbraucher geltend gemachten Mangels mit dieser Vermutung unvereinbar ist. Das Gewährleistungsrecht eignet sich daher insbesondere für Mängel, die sich bereits in einem Schaden manifestiert haben. Mängel hingegen, die nur in anderen Fällen, aber (noch) nicht beim eigenen Kaufgegenstand, zu Schäden geführt haben, können Käufern einen höheren Begründungsaufwand aufbürden.

Seinem Umfang nach umfasst das Mängelgewährleistungsrecht sowohl die mechanischen Komponenten eines Kraftfahrzeugs als auch dessen Software. Auch Softwarefehler können Sachmängel darstellen. Allerdings treten im Falle von Software besonders das Problem der Unsicherheit eines mangelverursachten Schadens sowie bereits die Frage auf, ob ein Mangel vorliegt. Gerade im Bereich der IT-Sicherheitsarchitektur muss nicht notwendigerweise jeder Fehler eine Angriffsmöglichkeit eröffnen, selbst wenn der jeweilige Angriffsvektor bereits im Grundsatz bekannt ist. Darüber hinaus werden mit der Zeit neue Angriffsmöglichkeiten bekannt, die bei der Übergabe beziehungsweise bei „Gefahrübergang“ nach dem Stand der Technik noch nicht vorhersehbar waren (siehe Informationen zu Spectre und Meltdown sowie zu Verschlüsselungstechniken in den Kapiteln 4.3 und 4.4). In diesen vorgenannten Fällen ist fraglich, ob überhaupt ein Mangel, das notwendige Verschulden und letztlich ein Gewährleistungsanspruch vorliegen.

Gewährleistungsrechte wirken nicht präventiv, indem sie den Verkäufer verpflichten, einem Mangel, der nach dem Verkauf in Erscheinung treten kann, vorbeugend in eigener Initiative entgegenzuwirken. Vielmehr verschaffen die gesetzlichen Mängelgewährleistungsrechte dem Erwerber eines Kraftfahrzeugs nur Ansprüche auf Beseitigung eines bereits manifesten Mangels und der verursachten Schäden.

Gewährleistungsrechte setzen ferner voraus, dass sie proaktiv durch ihren Inhaber, in der Regel den Fahrzeugkäufer, zunächst erkannt und dann auch geltend gemacht werden. Es besteht hingegen keine gesetzliche Pflicht für den Verkäufer, vorbeugend Nachrüstbauteile oder Softwareupdates zur Behebung von Produktionsfehlern anzubieten. Erst recht begründen Gewährleistungsrechte keine Pflicht, ein verkauftes und funktionsfähiges Produkt weiter zu verbessern, indem Updates oder Upgrades in Funktions- oder Leistungsfähigkeit angeboten werden.

Im Ergebnis ist das Gewährleistungsrecht somit strukturell auf den Schutz des Austauschverhältnisses im Kaufzeitpunkt ausgelegt: „Der Käufer soll das bekommen, was er gekauft und bezahlt hat.“ Weitergehende (IT-)sicherheitspolitische Erwägungen oder die Prävention von Schäden spielen hingegen beim Gewährleistungsrecht derzeit keine Rolle.

Die verbraucherschützenden Regelungen des Produkthaftungsgesetzes führen zu keinen anderen Ergebnissen. Das Produkthaftungsgesetz begründet Schadensersatzpflichten des Herstellers eines fehlerhaften Produkts. Eine Schadensersatzpflicht verlangt



jedoch einerseits den Eintritt eines Schadens und ist andererseits darauf gerichtet, diesen entstandenen Schaden zu ersetzen. Dies bedeutet, dass das Gesetz auch durch die Schadensersatzpflichten den Hersteller eines Produkts nicht verpflichtet, vorbeugend Nachbesserungen für das Produkt anzubieten.

Auch die Möglichkeit Garantieansprüche einzuräumen, sei es durch den Verkäufer oder durch den Hersteller eines Kraftfahrzeugs, ändert an dieser Bestandsaufnahme nichts. Garantieansprüche zielen ebenfalls auf eine nachträgliche Beseitigung von Mängeln an mechanischen Bauteilen, an Software und hieraus entstandenen Schäden ab. Der einzige Unterschied zur Mängelgewährleistung besteht darin, dass der Garantiegeber verschuldensunabhängig für die Mängelfreiheit seines Produkts einstehen muss, wodurch der Anspruchsinhaber seine Ansprüche leichter geltend machen kann.

Nach derzeitiger Gesetzeslage besteht durch die gesetzlichen Mängelgewährleistungsrechte, das Produkthaftungsrecht und durch vertraglich eingeräumte Garantien grundsätzlich keine Pflicht für Hersteller oder Verkäufer von Kraftfahrzeugen, vorbeugend Softwareupdates für Fahrzeuge bereitzustellen. Die Entscheidung, ob und in welcher Form diese vorbeugend ausgerollt werden, ist eine wirtschaftliche Entscheidung, die allein bei dem Hersteller oder Verkäufer liegt.

6.2 Status quo der Gewährleistungs- und Garantieansprüche bei Miet- und Leasingkonstellationen

Jedenfalls in zeitlicher Hinsicht weicht die Rechtslage bei der reinen Fahrzeugmiete ab. Durch § 535 Abs. 1 S. 2 BGB ist der Vermieter einer Sache grundsätzlich dazu verpflichtet, die Mietsache für die Dauer der Mietzeit in einem zum vertragsgemäßen Gebrauch geeigneten Zustand zu halten. Dies bedeutet, dass bei entsprechend langfristig ausgelegten Mietverträgen der Vermieter eines Kraftfahrzeugs mehr als zwei Jahre für eine Erhaltung der Funktionsfähigkeit des Fahrzeugs Sorge tragen muss.

Gleichwohl gilt es zu beachten, dass sich zu dieser grundsätzlichen Wertung, insbesondere im Bereich des Kraftfahrzeugleasings, einzelvertraglich zahlreiche abweichende Regelungen etabliert haben, die den Leasingnehmer zur Erhaltung der Gebrauchsfähigkeit des Fahrzeugs verpflichten. Zudem ist fraglich, in welchem Umfang die mietvertragliche Instandhaltungspflicht auch die Beseitigung von Sicherheitslücken in Softwarekomponenten beziehungsweise

die Bereitstellung von Softwareupdates zur Aufrechterhaltung der gebotenen IT-Sicherheit umfasst.

Daher besteht auch im Miet- und Leasingvertragsrecht keine grundsätzliche und vorbeugende Verpflichtung für Leasinggeber oder Kraftfahrzeughersteller, Softwareupdates für Fahrzeuge anzubieten.

6.3 Gewährleistungsansprüche bei Übertragung von Daten durch autonome Fahrzeuge

Das zuvor beschriebene Szenario berücksichtigt nur die Lage, dass relevante Software fahrzeugintern eingesetzt wird. Wie in Kapitel 3 erläutert, werden viele Anwendungsfälle für autonome Fahrzeuge erfordern, dass Daten zwischen Fahrzeugen ausgetauscht und sogar online, etwa über Cloudanwendungen, erfasst und verarbeitet werden. In diesem Fall kommt durch die Softwareschnittstellen der erforderlichen Kommunikationsinfrastruktur ein weiterer sicherheitsrelevanter Aspekt hinzu: Die Kommunikationsschnittstellen müssen gegen Angriffe von außen abgesichert werden, damit der Betrieb autonomer Fahrzeuge nicht durch Angreifer gestört werden kann. Überdies tritt, sofern die cloudbasierte Datenverarbeitung nicht durch den jeweiligen Fahrzeughersteller selbst erfolgt, möglicherweise ein weiterer Anspruchsgegner hinzu. Hinsichtlich etwaiger Mängelgewährleistungsansprüche ist, in Anbetracht der vorstehenden Ausführungen, vieles davon abhängig, wie das Nutzungsverhältnis der Onlineinfrastruktur konkret ausgestaltet ist.

Auch hier besteht aus dem allgemeinen Gewährleistungsrecht kein grundsätzlicher Anspruch auf Softwareupdates. Vielmehr ergibt sich eine Updatepflicht (jedoch ohne einen Anspruch des Nutzers auf Durchführung der Updates zu begründen) im Falle von öffentlich zugänglichen Clouddiensten für die Infrastruktur dieser Dienste aus dem Telemediengesetz (§ 13 Abs. 7 TMG). Dieses statuiert in Umsetzung der Europäischen NIS-Richtlinie eine öffentlich-rechtliche Pflicht zur Absicherung solcher Dienste. Verstöße werden jedoch im Wesentlichen durch die zuständigen Aufsichtsbehörden verfolgt und eröffnen kein Klagerecht der Nutzer, sofern diesen kein Schaden entstanden ist. Ferner ist noch nicht abschließend geklärt, ob diese Verpflichtung zur Installation von sicherheitsrelevanten Updates überhaupt über den eigentlichen Clouddienst hinaus auch die Fahrzeuge selbst umfassen kann. Daher lässt sich diese Updatepflicht aus § 13 Abs. 7 TMG nur in Einzelfällen von den Haltern beziehungsweise Eigentümern der Fahrzeuge gegen den Fahrzeughersteller anführen.



Überdies gilt es in Konstellationen, denen eine Datenübertragung zum Betrieb autonomer Fahrzeuge zu Grunde liegt, zu beachten, dass unter derzeitiger Rechtslage der Umfang der Anwendbarkeit des Telekommunikationsrechts ungeklärt ist. Die Datenübertragung zwischen Fahrzeugen und/oder die Datenübertragung vom Fahrzeug zur Cloudanwendung wird zwar regelmäßig eine Datenübertragung über das Internet oder eine vergleichbare offene Telekommunikationsinfrastruktur erfordern. Der Zugang zu dieser dürfte jedoch regelmäßig über die im Auto vorhandene Software ermöglicht werden. In diesen Fällen ist bislang ungeklärt³¹, ob die Anwendung als sogenannter Telekommunikationsdienst zu qualifizieren ist und damit dem Regelungsregime des TKG unterliegt. Nur in diesem Fall würden die telekommunikationsrechtlichen Sonderregelungen greifen, die Vorschriften zur fortwährenden Einhaltung technischer Standards enthalten, die den Dienst gegen Angriffe absichern.

6.4 Status quo der Einhaltung der Vorschriftsmäßigkeit durch den Halter

Straßenverkehrsrechtlich ist grundsätzlich der Halter eines Kraftfahrzeugs zu dessen Instandhaltung und zur Einhaltung der vorschriftsgemäßen Betriebsfähigkeit verpflichtet. Die Einhaltung wird im regelmäßigen Turnus durch amtlich anerkannte Stellen überprüft (§ 29 StVZO). Die durchzuführende Prüfung umfasst insbesondere auch die Funktionsfähigkeit des Motormanagements, der Brems- und der Lenkanlage (Anlage VIII a zu § 29 StVZO).

Dies ist im Hinblick auf autonom fahrende Fahrzeuge ein relevanter Punkt. Die Steuerungssoftware eines Automobils dürfte zwar zu den Bestandteilen des Motormanagements, der Brems- und der Lenkanlage gehören. Dadurch wäre grundsätzlich der Halter eines Fahrzeugs verpflichtet, Fehler in den entsprechenden Softwarekomponenten zu beheben beziehungsweise beheben zu lassen. Allerdings beschränkt sich der derzeitige verpflichtende Prüfkatalog in der Regel auf die Funktionsfähigkeit und die Einhaltung von festgelegten Vorgaben. Nur in Ausnahmefällen werden neben dem allgemeinen Zustand auch bestimmte Risiken betrachtet, die zu späteren Schäden führen können, insbesondere zur Undichtigkeit von Leitungen. Für die Prüfung der IT-Sicherheit der im Fahrzeug verwendeten Software müssten hingegen die Prüf- beziehungsweise Anforderungskataloge entsprechend ergänzt sowie entsprechende Prüfprozesse bei den Prüfstellen etabliert werden.

Sollte eine dahingehend erweiterte Prüfung Sicherheitsmängel an der Software feststellen, bevor die Gewährleistungsfrist abgelaufen ist oder solange der Fahrzeughersteller selbst noch Softwareupdates für sein Fahrzeug bereitstellt, wird der Fahrzeughalter seinen gesetzlichen Pflichten nachkommen können. Weitaus komplizierter wird die Situation, wenn der Fahrzeughersteller sich entschließt, den Support für die Software einzustellen. In diesem Fall ist der Fahrzeughalter mit dem Problem konfrontiert, dass er am freien Markt unter Umständen keine Leistungen beziehen kann, um Fehler in der defekten Steuerungssoftware zu beheben.

Ausgehend vom heutigen Regelfall ist anzunehmen, dass auch in Zukunft in Fahrzeugen eingesetzte Software herstellerspezifisch und proprietär, also nicht quelloffen, sein wird. Daher dürfte für Drittanbieter der notwendige Zugang zum Quellcode fehlen. Das Recht des Fahrzeughalters aus § 69 d Abs. 1 UrhG zum Dekompilieren der Steuerungssoftware dürfte bereits aufgrund des großen Aufwands und geringen Nutzens des Quellcodes ohne Kommentierung keine Hilfe sein. Der Fahrzeughalter wäre mithin praktisch gehindert, sein Fahrzeug in einen vorschriftsmäßigen Zustand zu versetzen. Diese Situation wäre inakzeptabel, da eine kritische Störung in IT-Systemen in den wichtigen Bestandteilen des Kraftfahrzeugs dazu führen kann, dass es nicht mehr verkehrssicher betrieben werden kann und somit eine Gefahr für Leib und Leben seiner Insassen, aber auch für andere Verkehrsteilnehmer darstellt.

6.5 Lebenszyklus des Automobils

Wie in Kapitel 4.3 erläutert sollte IT-Sicherheit bei einem autonomen Fahrzeug keine auf den Zeitpunkt der Auslieferung beschränkte Aufgabe sein. Vielmehr erfordert es die Sicherheit im Straßenverkehr, die hierzu relevante IT-Sicherheit als eine sich auf den Lebenszyklus eines Fahrzeugs erstreckende Daueraufgabe anzusehen. Insofern ist zu hinterfragen, ob es Automobilherstellern selbst überlassen bleiben sollte, den IT-Support für autonom fahrende Fahrzeuge auch hinsichtlich des sicherheitsrelevanten Bereichs einstellen zu können. Derzeit besteht keine solche gesetzliche Verpflichtung, aber ohne Updates zur Aufrechterhaltung des sicheren Betriebs würden die Fahrzeuge für ihre Eigentümer praktisch unbenutzbar.

Hintergrund dieser Erwägungen ist die bereits in anderem Kontext diskutierte Frage der geplanten Obsoleszenz, also der Auslegung bestimmter oder aller Teile für eine vordefinierte Lebensdauer, die unter der üblichen Nutzungsdauer liegt. Bei autonomen Fahrzeugen ist es denkbar, die übliche Nutzungsdauer entweder anhand der langen

³¹ Und überdies dem Europäischen Gerichtshof zur Entscheidung vorgelegt, vgl. OVG NRW, Beschluss vom 26.02.2018 - 13 A 17/16.



Lebenszyklen des Automobilsektors oder der im Vergleich extrem kurzen Lebenszyklen des Hochtechnologiebereichs zu bestimmen. Im ersten Fall wären die Hersteller gezwungen, eine Vielzahl von IT-Altsystemen („legacy“) zu betreiben, die noch während des Lebenszyklus des Fahrzeugs von den sich schnell entwickelnden Anforderungen an IT-Sicherheit hoffnungslos überfordert würden. Im zweiten Fall würde die Nutzbarkeit des gesamten Fahrzeugs in Frage gestellt, sobald die erste sicherheitsrelevante IT-Komponente die Anforderungen nicht länger erfüllen kann – egal, ob wegen zu schwacher Hardware, veralteter Software oder gestiegenen Anforderungen der Software, die die Hardware nicht mehr erfüllt.

Das derzeitige Haftungs- und Gewährleistungsregime ist – wie bereits beschrieben – auf den Schutz des Austauschverhältnisses im Zeitpunkt der Übergabe („Gefahrübergang“) ausgelegt, befasst sich jedoch gerade nicht ausdrücklich mit der Haltbarkeit eines Produkts (egal, ob Hardware oder Software). Daher sind es derzeit nicht rechtliche, sondern vornehmlich kaufmännische Interessen, die Einfluss auf die Planung des Lebenszyklus und der Haltbarkeit haben. Der Makel einer (zu) geringen Haltbarkeit der Produkte kann die Reputation eines Unternehmens schädigen und nachhaltig noch über Jahre fortwirken. Darüber hinaus ist der Support über einen langen Lebenszyklus bereits seit Langem ein anerkanntes Geschäftsmodell, sowohl hinsichtlich der Hardware (zum Beispiel Ersatzteilgeschäft) als auch der Software (zum Beispiel „Software as a Service“), sodass auch in der Automobilbranche zumindest ein gewisses Interesse beispielsweise der Hersteller an längeren Lebenszyklen bestehen dürfte.

Allerdings müssen zudem der Verbraucherschutz und der Ressourcenverbrauch eines voreiligen Austauschs ganzer Fahrzeugflotten berücksichtigt werden. Aus verbraucherschutzrechtlicher Sicht dürfte vor allem Transparenz hinsichtlich der Haltbarkeit, Nutzungsmöglichkeit und Folgekosten im Vordergrund stehen. Da Verbraucher nachvollziehbar von der Annahme des langen üblichen Lebenszyklus eines Kraftfahrzeugs ausgehen dürften, sollten Einschränkungen und Folgekosten bereits zum Kaufzeitpunkt (soweit der Kauf weiterhin das dominierende Vertragsmodell bleiben sollte) offen und transparent im Vertrag festgelegt werden.

Aus ökologischer Sicht und zur Verringerung des Ressourcenverbrauchs ist es ferner wünschenswert, die Aufrechterhaltung der Betriebssicherheit durch Drittanbieter am Markt zu ermöglichen, zumindest für den Fall der Abkündigung des Supports durch den Hersteller. Hierzu wäre jedoch eine Offenlegung der Schnittstellen,

gegebenenfalls sogar des Quellcodes der eingesetzten Software notwendig, die derzeit (vgl. Kapitel 6.4) gesetzlich nicht vorgesehen ist.

Hinsichtlich der Transparenz von Einschränkungen der Nutzungsmöglichkeit und Folgekosten bestehen zwar bereits einige Informationspflichten aus verbraucherschutzrechtlichen Regelungen. Es überwiegt jedoch derzeit noch das Ansinnen, durch (im Vergleich zum Lebenszyklus eines Fahrzeugs) kurze Fristen schnell Rechtsfrieden zu schaffen. Außerdem wären Unwägbarkeiten hinsichtlich der Preiskalkulation über mehrere Jahre dabei kaum vermeidbar. Ein Vorgehen gegen Hersteller wegen falscher Angaben oder einer erst viel später geänderten Produkt- und Supportpolitik ist im derzeitigen Haftungsrecht nicht vorgesehen.

Hinsichtlich der zwangsweisen Öffnung hin zu einem Drittanbietermarkt für langfristigen Support steht derzeit allein das Kartellrecht zur Verfügung, das jedoch hohe Hürden für einen Zugriff Dritter, insbesondere von Wettbewerbern, auf rechtlich geschützte Produktbestandteile (zum Beispiel urheberrechtlich geschützte Software) vorsieht. Solange zumindest vernünftige wirtschaftliche Gründe eine Abkündigung der jeweiligen Supportangebote stützen, dürfte eine Verpflichtung zur Offenlegung gegenüber Wettbewerbern – jedenfalls nachzeitigem Stand – sehr geringe Erfolgsaussichten haben.

6.6 Herausforderungen für das Gewährleistungs- und Garantierecht

Die vorstehenden Erwägungen und Erkenntnisse ergeben, dass

- erstens der Halter in der Regel selbst weder tatsächlich noch (nach Ablauf der kurzen Gewährleistungs- beziehungsweise Haftungsfristen) rechtlich in der Lage ist, die IT-Sicherheit und damit gegebenenfalls die Betriebssicherheit aufrechtzuerhalten,
- zweitens die Hersteller nicht zum Support über die gesamte tatsächliche Nutzungsdauer eines Fahrzeugs verpflichtet sind und
- drittens Drittanbieter regelmäßig keine Einsicht in geschützte Hardware- oder Softwarebestandteile erhalten werden.

Das legt die Schlussfolgerung nahe, dass das (kaufrechtliche) Gewährleistungs- und Haftungsrecht in seiner derzeitigen Form die Anforderungen an IT-Sicherheit zum Schutz aller Verkehrsteilnehmer nicht zufriedenstellend umsetzen kann.



Daher sollte die Durchsetzung von Verpflichtungen des Herstellers zur Nachbesserung beziehungsweise Lieferung von entsprechenden Sicherheitsupdates gegenüber der Alternative einer Stilllegungsverpflichtung des Halters diskutiert werden. Insoweit kann eine Stilllegungsverfügung der zuständigen Aufsichtsbehörde, die bei fehlender Betriebssicherheit des Fahrzeugs und einer Gefährdung anderer Verkehrsteilnehmer zu erlassen wäre, zu einem Entzug jeglicher Nutzungsmöglichkeit des Fahrzeugs durch den Eigentümer führen, ohne dass Ausgleichsansprüche gegen den Hersteller beziehungsweise Verkäufer bestehen, wenn nach wenigen Jahren die letzten Verjährungsfristen abgelaufen sind.

Im Hinblick auf die derzeit in § 29 StVZO verankerten Untersuchungspflichten ergeben sich weitere rechtliche Herausforderungen. Einerseits ist dem Umstand Rechnung zu tragen, dass ein autonom fahrendes Fahrzeug ohne kontinuierliche Sicherheitsupdates und ohne eine gesicherte, fortlaufend verfügbare Pflege der Steuer- software nicht verkehrssicher betrieben werden kann. Es wäre daher denkbar, den straßenverkehrsrechtlichen Pflichtenkatalog für Fahrzeughalter um eine Pflicht zum Betrieb des Kraftfahrzeugs unter Nutzung der jeweils aktuellsten Softwareversion zu erweitern. Verstöße dagegen könnten mit Verlust der straßenverkehrsrechtlichen Zulassung sanktioniert werden. Hierdurch könnte ein gleichmäßig hohes Sicherheitsniveau aller am Straßenverkehr teilnehmenden Fahrzeuge sichergestellt werden. Umgekehrt entspricht es der staatlichen Schutz- und Fürsorgepflicht, unsichere Fahrzeuge wie bislang auch zukünftig bei IT-Sicherheitsrisiken aus dem Verkehr zu ziehen.

Andererseits kann der Halter eines autonom fahrenden Fahrzeugs für die Einhaltung der IT-Sicherheit – anders als bei den bislang verkehrsrechtlich geschuldeten Maßnahmen zur Aufrechterhaltung eines verkehrssicheren Zustands – nicht durch Aufsuchen einer nahezu beliebigen Werkstatt selbst Sorge tragen. Sollen die Käufer der Fahrzeuge davor bewahrt werden, bereits nach wenigen Jahren ausgleichlos einzelne oder sämtliche Nutzungsmöglichkeiten des Fahrzeugs zu verlieren, gäbe es mehrere Varianten, den rechtlichen Rahmen anzupassen. Auf der Ebene des Vertragsrechts wäre es denkbar, eine bestimmte Nutzungsdauer beziehungsweise Haltbarkeit gesetzlich als Teil der so genannten „Soll-Beschaffenheit“, also der Gesamtheit der Anforderungen, die das Fahrzeug erfüllen muss, um dem Vertrag zu entsprechen, zu statuieren. Kombiniert mit einer Anpassung der Verjährungsfristen würde dies bei einem späteren Wegfall der Nutzungsmöglichkeit dem Käufer jedenfalls einen finanziellen Ausgleich, wenn nicht sogar einen Nachbesserungs-

anspruch geben. Dieser wäre jedoch weiterhin einzeln oder im Rahmen einer Musterfeststellungsklage – jeweils mit allen Prozessrisiken und üblichen Laufzeiten zivilrechtlicher Verfahren – durchzusetzen.

Weitergehende Überlegungen sollten jedoch berücksichtigen, dass im Falle von Sicherheitslücken zumeist nicht nur einzelne Fahrzeuge, sondern ganze Baureihen betroffen sein dürften. Daher könnte es sinnvoll sein, die Durchsetzung einer Nutzungsmöglichkeit zu zentralisieren. Neben einer rein staatlichen Überwachung durch die zuständigen (Verkehrs-) Aufsichtsbehörden könnte ein Verbandsklagerecht hinsichtlich eines (ebenfalls neu zu schaffenden) Anspruchs auf Durchführung von Maßnahmen zur Aufrechterhaltung der (sicheren) Nutzungsmöglichkeit aller betroffenen Baureihen geschaffen werden. Ebenso wäre es denkbar, eine Hinterlegungspflicht für sämtlichen Software Quellcode und die Hardwarepläne zu statuieren, um im Falle einer widerrechtlichen Weigerung oder einer Insolvenz des Herstellers die Möglichkeit einer Ersatzvornahme der notwendigen Maßnahmen (zum Beispiel Erstellung von Updates) durch einen anderen Marktteilnehmer zu ermöglichen. Da es sich dabei jedoch um einen Eingriff in das Eigentumsrecht des Herstellers (insbesondere in die Urheberrechte und gewerblichen Schutzrechte) handelt, müssten bei der Ausgestaltung einer solchen Hinterlegungspflicht die jeweiligen verfassungsrechtlich geschützten Positionen sorgfältig abgewogen werden.

Schließlich kann in Anbetracht der technischen Möglichkeiten autonomer Fahrzeuge, insbesondere in Verbindung mit Sensorik und IoT- oder auch Blockchain-Anwendungen, die Frage aufgeworfen werden, ob die bislang durch § 29 StVZO vorgesehene turnusmäßige Sicherheitsprüfung von Kraftfahrzeugen nicht gänzlich obsolet wird. Durch zunehmend ausgefeilte und immer weiter verbreitete Sensortechnologie ist jedenfalls aus technischer Sicht nicht ausgeschlossen, dass sich ein autonomes Fahrzeug in einem solchen Umfang selbst testet und gegebenenfalls kontinuierlich, transparent und manipulationssicher seine straßenverkehrsrechtliche Konformität prüft. Hierdurch werden turnusmäßige Überprüfungen, die aus einer Zeit stammen, in der eine ständige Datenverbindung in und zwischen Fahrzeugen und Kommunikation zwischen Maschinen noch in weiter Ferne lag, möglicherweise eines Tages überflüssig.



6.7 Herausforderungen für die Haftungsregime

Bei Connected Cars und voll automatisierten Fahrzeugen verlagern sich die möglichen Schadensursachen zunehmend von menschlichem Fehlverhalten hin zu einem Versagen von IT-Systemen mit ihren Software- und Hardwarekomponenten. Dies führt dazu, dass die Klärung der Verantwortlichkeit und Haftung zunehmend (technisch) komplexer wird, etwa wenn, wie in Kapitel 3.4 beschrieben, die im Fahrzeug erfassten Sensordaten, um kritische Verkehrssituationen frühzeitig zu erkennen und Konfliktsituationen zu vermeiden, an andere Verkehrsteilnehmer übermittelt werden. Bei der Übermittlung von einem Verkehrsteilnehmer zum anderen müssen die Daten möglicherweise auf unterschiedlichsten Kanälen durch mehrere Netzwerke geleitet werden. Diese Übergänge stellen nicht nur ein Sicherheitsrisiko dar. In der Praxis führen all diese Facetten und die stetig steigende technische Komplexität dazu, dass die Rechtsverfolgung schnell an die Grenzen der Justiziabilität und Wirtschaftlichkeit kommen kann.

Dies führt zu der Überlegung, dass das bestehende System der Haftung und Pflichtversicherung sowie die etablierten Mechanismen des Beweisrechts bei Verkehrsunfällen und die Einführung der relevanten Datensätze in den Zivilprozess, um das Unfallgeschehen aufzuklären, bei autonom fahrenden Fahrzeugen auf den rechtlichen Prüfstand zu stellen sind. Schließlich steigt im Internet der Dinge, bei dem unzählige Gegenstände miteinander in Sekundenbruchteilen kommunizieren und operieren, die Komplexität der Abläufe erheblich.

Eine vollständige Analyse sämtlicher Daten, die vor einem Unfallereignis von den am Geschehen beteiligten Fahrzeugen erhoben wurden, könnte jedoch am ehesten die Verantwortlichkeit klären. Es stellt sich daher die Frage, ob zivilprozessual eine Pflicht zur Herausgabe (lediglich) der für die Analyse des Unfallhergangs und die Schadensursachen relevanten Daten durchgesetzt werden kann, und wenn ja, gegenüber wem? Selbstverständlich müssten dabei etwa das Datenschutzrecht und die spezifischen Regelungen zum Know-how-Schutz beziehungsweise zum Schutz von Geschäftsgeheimnissen berücksichtigt werden.

Die Vorschrift des § 142 ZPO dürfte hier vielfach nicht weiterhelfen, um die im vernetzten Automobil gespeicherten Daten nutzbar zu machen. Denn es dürfte sich bei den Daten, die im selbstfahrenden Auto gespeichert werden, weder um Urkunden im Sinne von

§ 415 ZPO noch um Unterlagen im Sinne des § 142 ZPO handeln³². Zudem ermächtigt § 142 ZPO nur das zuständige Gericht, eine Anordnung zur Vorlage von Urkunden oder sonstigen Unterlagen gegenüber den Parteien oder Dritten auszusprechen. Es besteht jedoch grundsätzlich kein Anspruch der Parteien auf eine solche gerichtliche Anordnung. Sofern die Aufklärung eines Unfallgeschehens selbstfahrender Autos nur unter Hinzuziehung der Daten aus dem Auto der Gegenseite in Betracht kommt, könnten außerdem die Vorschriften der §§ 371, 144 ZPO eine Rolle spielen. Hierbei gilt es aber zu beachten, dass die im selbstfahrenden Auto generierten Millionen Daten teils flüchtig, teils dauerhaft in einem Daten- oder Cloudspeicher gespeichert und zugleich qualifiziert elektronisch signiert und vor Veränderung geschützt werden müssten. Ist dies nicht der Fall, scheidet eine Anwendung des § 371 Abs. 1 S. 2, 144 Abs. 1 S. 2, 371 a Abs. 1 ZPO ebenfalls als Regelung für den Zugriff auf die Daten der am Unfallgeschehen beteiligten selbstfahrenden Autos aus. Eine Verwertbarkeit bliebe nur im Rahmen des Anscheinsbeweises eröffnet. Damit die Beweiskraft eines elektronischen Dokuments dem einer privaten Urkunde gleichgestellt ist, muss das elektronische Dokument jedoch ebenfalls mit einer qualifizierten elektronischen Signatur im Sinne des Signaturgesetzes versehen sein (§ 371 a Abs. 1 ZPO).

Um die im Automobil gespeicherten Daten in einen Zivilprozess einzubeziehen, könnten zudem möglicherweise Ermittlungsergebnisse beziehungsweise -akten der Ermittlungsbehörden, die denselben Verkehrsunfall betreffen, in den Zivilprozess eingeführt werden. Stellt die Staatsanwaltschaft Ermittlungen bezüglich des Verkehrsunfalls an, liegt es nahe, dass sie dazu gemäß § 94 StPO die gespeicherten Daten als nichtkörperliche Gegenstände sicherstellen beziehungsweise beschlagnahmen wird, da diese Daten mit hoher Wahrscheinlichkeit zur Aufklärung des Unfallgeschehens beitragen könnten und damit potenzielle Beweismittel darstellen. Die von den Ermittlungsbehörden sichergestellten und ausgewerteten Daten könnten dann in einen späteren Zivilprozess im Wege des Urkundenbeweises eingeführt werden. Allerdings liegt die Entscheidung, die im Automobil gespeicherten Daten sicherzustellen, jeweils im Ermessen der Ermittlungsbehörden, sodass auch hierauf kein Anspruch des Einzelnen besteht. Nichts anderes folgt zudem mit Blick auf die jüngere Rechtsprechung zur zivilprozessualen Verwertung von Dashcam-Aufnahmen, deren Zulässigkeit als Beweismittel von der Rechtsprechung lediglich in Einzelfällen nach sorgfältiger Interessensabwägung zugelassen wird.

³² Vgl. Eichele (2017): Vorb. zu § 415 Rz. 1, 2; Von Selle (2018): § 142, Rz. 7, § 131 Rz. 4



Die vorangegangenen Ausführungen zeigen, dass ein Zugriff auf die gespeicherten Daten der an einem Unfallgeschehen beteiligten selbstfahrenden Autos allenfalls nur in begrenztem Umfang prozessual in Betracht kommen dürfte. Hinzu kommen die oben beschriebenen datenschutzrechtlichen Hürden.

Der mögliche Erkenntnisgewinn ist in Anbetracht der immensen „Datensammlung“ jedoch höher als beim menschlichen Beobachter, denn es ist objektiv feststellbar, was die „Dinge“ im Internet der Dinge unmittelbar vor dem Unfallereignis wahrgenommen haben. Beim Menschen ist die Wahrnehmung hingegen subjektiv. Daher sollten die Möglichkeiten des höheren Erkenntnisgewinns genutzt werden können, einerseits um Ansprüche effektiv durchsetzen zu können und andererseits, um – ähnlich wie in der Luftfahrt – zur Verhütung zukünftiger Unfallszenarien eine umfassende Ursachenforschung betreiben zu können. Richten Connected Cars einen Schaden an, besteht ein öffentliches Interesse an rückhaltloser Aufklärung, insbesondere wenn es sich um Unfälle und Störungen von besonderer Bedeutung für die Sicherheit im Straßenverkehr handelt. Die Prämisse muss sein, gerade im Hinblick auf die Komplexität möglicher Schadensereignisse, entsprechende Wiederholungen künftig zu vermeiden.

Ein Blick auf das Recht der Flugunfalluntersuchung zeigt, dass gemäß § 3 Abs. 1 des Gesetzes über die Untersuchung von Unfällen und Störungen bei dem Betrieb ziviler Luftfahrzeuge (FIUUG) Unfälle und Störungen mit dem ausschließlichen Zweck untersucht werden, möglichst die Ursachen aufzuklären. Ziel ist es, künftige Unfälle und Störungen zu verhüten.

Zwar wird ausdrücklich klargestellt, dass die Untersuchungen nicht dazu dienen, das Verschulden, die Haftung oder Ansprüche festzustellen (§ 3 Abs. 2 FIUUG). Der § 21 Abs. 1 FIUUG sieht jedoch, mit einer Anzahl von Ausnahmen (§ 21 Abs. 2 FIUUG), vor, dass die Bundesstelle für Flugunfalluntersuchung³³ den von dem Ereignis Betroffenen oder deren Rechtsbeiständen Auskünfte aus den Akten des Untersuchungsverfahrens erteilen oder Akteneinsicht gewähren kann (§ 21 Abs. 3 FIUUG), soweit dies erforderlich ist, um Rechtsansprüche im Zusammenhang mit dem Unfall oder der Störung festzustellen, durchzusetzen oder abzuwehren. Der Ansatz, dass ein Dritter, der über erforderliche technische Auswertungen verfügt, um einen Anspruch zu substantiieren, auf Auskunft in Anspruch

genommen werden kann, ist dem Zivilrecht grundsätzlich nicht fremd. So sieht zum Beispiel § 101 Abs. 9 UrhG vor, dass ein im urheberrechtlichen Sinne Verletzter von einem Telekommunikationsunternehmen Auskunft über die Verwendung von Verkehrsdaten (§ 3 Nr. 30 TKG) auf vorherige richterliche Anordnung verlangen kann.

³³ Zur Untersuchung von Unfällen und Störungen in der zivilen Luftfahrt wurde im Geschäftsbereich des Bundesministeriums für Verkehr und digitale Infrastruktur die Bundesstelle für Flugunfalluntersuchung errichtet (§ 4 Abs. 1 S. 1 FIUUG).



Interview



„Assistenzsysteme haben auf viele Schäden gar keinen Einfluss.“

Interview mit Dr. Tibor Pataki. Leiter Kraftfahrtversicherung, Kfz-Technik und Statistik beim Gesamtverband der Deutschen Versicherungswirtschaft (GDV) e.V.

Dr. Pataki, welche Bedeutung haben die Daten aus vernetzten Fahrzeugen für die Versicherungswirtschaft?

Die Daten aus dem vernetzten Auto haben das Potenzial, Verbrauchern mehr und bessere Dienstleistungen zu ermöglichen, zum Beispiel eine schnellere Pannenhilfe, den Weg zur günstigsten Tankstelle oder ein direktes Feedback zum Fahrstil – ein neuer Markt mit innovativen, datenbasierten Geschäftsmodellen entsteht. Auf diesem Markt wollen nicht nur die Automobilhersteller, sondern auch Automobilclubs, Werkstätten und Versicherer ihren Kunden im Auto neue Angebote machen. Aktuell haben aber nur Automobilhersteller Zugriff auf diese Daten. Wir sind der Meinung: Die Daten gehören in die Hände der Verbraucher. Nur diese sollten entscheiden, ob, wann und wem sie welche Daten überlassen. Anderenfalls können Autohersteller den gerade entstehenden Markt abschotten, andere Anbieter ausschließen und Monopolgewinne einstreichen – zum Nachteil der Autofahrer, die ein beschränkteres Angebot zu einem höheren Preis bekämen.

Nach heutigem Stand übernehmen Versicherungen im Straßenverkehr die Haftung für den Fahrer eines Fahrzeugs. Wie sieht das bei einem autonom fahrenden Fahrzeug aus?

Die Kraftfahrzeug-Versicherung ist technikneutral. Auch bei Unfällen durch automatisierte Fahrsysteme entschädigt somit die Kraftfahrzeug-Versicherung das Opfer. Schon jetzt ist es für das Verkehrsoffer unerheblich, ob den Fahrer ein Verschulden trifft oder der Unfall beispielsweise durch einen defekten Reifen verursacht wird – das Unfallopfer hat mit der Kraftfahrzeug-Haftpflichtversicherung einen direkten und solventen Ansprechpartner. Wir können es einem Unfallopfer nicht zumuten, dem Autohersteller einen eventuellen Produktfehler nachweisen zu müssen, bevor es eine Entschädigung erhält. Das Produkthaftungsrecht ist auf diesen Fall nicht ausgelegt. Für etwaige Regressansprüche im Falle eines Fehlers des automatisierten Fahrsystems werden die Versicherer praktikable Lösungen mit den Automobilherstellern finden.

Dr. Tibor Pataki

Leiter Kraftfahrtversicherung, Kfz-Technik und Statistik beim Gesamtverband der Deutschen Versicherungswirtschaft (GDV) e.V.

Wie verändern sich Schadensgeschehen und -aufwand bei automatisierten Fahrsystemen?

Assistenzsysteme haben auf viele Schäden gar keinen Einfluss. Ein Autobahnpiлот schützt gegen Autodiebe ebenso wenig wie eine Einparkhilfe vor Steinschlag, Hagel oder Marderbissen. Auch der beste Notbremsassistent ändert nichts an den physikalischen Gesetzen für den Bremsweg eines Autos. Zudem werden wir nun eine sehr langsame Verbreitung von automatisierten oder autonomen Systemen und steigende Reparaturpreise im Schadensfall sehen. Laut unserer Prognose wird der Schadensaufwand der Kraftfahrzeug-Versicherer bis 2035 im Vergleich zu 2015 durch die neuen Systeme um sieben bis maximal 15 Prozent sinken. Auf absehbare Zeit hat der technologische Fortschritt also nur geringen Einfluss auf das Schadensgeschehen.



Top 5

Kernaussagen von Kapitel 6

- Eine gesetzliche Verpflichtung des Herstellers/Verkäufers, vorbeugend Softwareupdates oder Upgrades zur Prävention möglicher Schadensszenarien bereitzustellen, besteht derzeit grundsätzlich nicht. Auch aus dem TMG und TKG folgt eine Verpflichtung des Herstellers zur Installation von sicherheitsrelevanten Updates, anders als für Clouddienstanbieter, nicht ohne Weiteres.
- Die Pflicht nach § 29 StVZO zur turnusgemäßen Sicherheitsüberprüfung von Kraftfahrzeugen lässt sich in Anbetracht der als Daueraufgabe zu begreifenden IT-Sicherheit nicht ohne Weiteres auf autonom fahrende Fahrzeuge übertragen.
- Die Aufrechterhaltung der IT-Sicherheit bei autonomen Fahrzeugen sollte keine auf den Zeitpunkt der Auslieferung beschränkte Aufgabe des Herstellers sein, da andernfalls der Halter/Eigentümer daran gehindert ist, sein Fahrzeug in einen vorschriftsmäßigen Zustand zu versetzen und es stilllegen müsste, sofern der Hersteller den Support für die Software einstellt.
- Es gilt daher eine Durchsetzung von Verpflichtungen des Herstellers zur Nachbesserung bzw. Lieferung von Sicherheitsupdates gegenüber der Alternative einer Stilllegungsverpflichtung des Halters unter Berücksichtigung des zu erwartenden oder bestimmten Lebenszyklus eines autonom fahrenden Fahrzeugs zu diskutieren.
- Das bestehende System der Haftung und Pflichtversicherung sowie die etablierten Mechanismen des Beweisrechts bei Verkehrsunfällen und die Einführung relevanter Datensätze in den Zivilprozess zur Aufklärung des Unfallgeschehens sind bei autonom fahrenden Fahrzeugen auf den rechtlichen Prüfstand zu stellen, da die technische Komplexität bei wirtschaftlicher Betrachtung der Unfallaufklärung entgegenstehen kann, wenngleich jedoch eine vollständige Aufklärung der Ursache und der Verantwortlichkeit für einen von autonom fahrenden Fahrzeugen verursachten Unfall unter Ausschöpfung aller verfügbaren Erkenntnisquellen (insbesondere sämtlicher Daten aus dem Zusammenhang mit dem Unfallereignis) im Allgemeininteresse geboten sein kann.



7. Ausblick

Autos bzw. Kraftfahrzeuge sind schon heute über diverse Schnittstellen Bestandteil digitaler Netzwerke. Denken wir etwas weiter als eine Dekade in die Zukunft, werden viele Fahrzeuge nicht nur vernetzt, sondern auch vollautonom sein. Für die Gesellschaft bedeutet das einen Wandel, denn Mobilität hängt immer weniger vom Autobesitz oder einem bestimmten Verkehrsmittel ab, sondern kann jederzeit als Service gebucht und in Anspruch genommen werden.

Die Automobilwirtschaft steht dementsprechend vor enormen Veränderungen, da ihr bisheriges Kernprodukt nicht mehr im Zentrum der Mobilität steht, sondern das Fortbewegungsangebot von A nach B für den Kunden.

Die Internetwirtschaft stellt mit Rechenzentren, Cloudangeboten und Netzverbindungen die notwendige digitale Infrastruktur. Ihre Technologien werden für die Automobilindustrie von so großer Bedeutung sein, dass eine enge Zusammenarbeit unbedingt notwendig ist. Die Automobilbranche ist zwingend auf die Infrastruktur und Kompetenz der Internetwirtschaft angewiesen, die zum verbindenden Dreh- und Angelpunkt von OEM, Zulieferern, Bahn und ÖPNV wird.

Und die Internetwirtschaft ist technisch gerüstet: Schon jetzt bieten Rechenzentren ausreichend Kapazitäten an, um die enormen Datenmengen aus vernetzten und autonomen Fahrzeugen zu verarbeiten. Mit der Einführung von 5G wird außerdem ein Meilenstein der notwendigen Netzgeschwindigkeit und -stabilität erreicht sein.

In einigen Jahren werden autonom fahrende und immer stärker vernetzte Autos auf den Straßen zu sehen sein. Es geht von jetzt an zwingend darum, die Funktionalität und Sicherheit des Gesamtsystems „Autonomes Fahren“ und die rechtlichen Rahmenbedingungen umzusetzen. Ein Ziel muss es sein, ein Maximum an Cybersicherheit zu erreichen, damit Fahrzeuge und Netzwerke vor Angriffen sicher sind. Auch hier wird der Automobilsektor nicht ohne die Expertise der Internetwirtschaft auskommen, um die komplexen IT-Ökosysteme vor Hackern zu schützen: Protokolle müssen aktuell gehalten werden und Autos nahezu in Echtzeit Updates erhalten, während ihres gesamten Lebenszyklusses. Die einzelnen elektronischen Komponenten benötigen standardisierte Modelle für Sicherheitsbedrohungen. Ansonsten droht der Kollaps der essenziellen digitalen Infrastruktur.

Datenschutz wird zu einer zentralen Aufgabe, um dem Fahrer und dem Halter einen ausreichenden Schutz seiner Persönlichkeit zu gewähren und ihn vor den unberechtigten Interessen Dritter zu bewahren. Die Sicherung der Daten muss bereits in der Softwareentwicklung berücksichtigt werden (Privacy by Design/Security by Design).

Zwar definiert die DSGVO umfassend Regelungen. Dennoch ist es in manchen Fällen nicht eindeutig, ob eine andere Datenschutzbestimmung (beispielsweise aus dem TKG) anzuwenden ist und welche Instanz letztlich für den Datenschutz verantwortlich ist. Eine Möglichkeit wäre eine Joint Controllershship bestehend aus diversen Beteiligten des Ökosystems. Wer auch immer diese Verantwortung trägt: Er ist beziehungsweise sie sind angehalten, diverse Grundsätze von Dokumentationspflichten, über Verarbeitungstransparenz bis hin zur Sicherheit der Datenverarbeitung umzusetzen. Aufgrund der Komplexität des entstehenden Ökosystems und der Vielzahl der beteiligten Player stellt dies zukünftig eine nicht zu unterschätzende Aufgabe dar.

In diesem Ökosystem stehen auch Gewährleistungsregime vor neuen Herausforderungen, denn hier sind einige Regelungen noch nicht eindeutig, die beispielsweise die Verpflichtung betreffen, Softwareupdates bereitzustellen. Diese sind allerdings essenziell für die Sicherheit autonomer Fahrzeuge, da sie Sicherheitslücken zeitnah schließen und dem Fahrzeughalter die Einhaltung der Vorschriften ermöglichen. Besonders schwerwiegend ist die unklare Situation nach einer möglichen Einstellung von Softwareupdates seitens des Herstellers beispielsweise für einen bestimmten Autotyp. Diese Fahrzeuge könnten dann nicht mehr verkehrssicher betrieben werden, ohne dass der Halter etwas dagegen tun kann. Die zugehörigen Erwägungen und Erkenntnisse legen die Schlussfolgerung nahe, dass das (kaufrechtliche) Gewährleistungs- und Haftungsrecht in seiner derzeitigen Form die Anforderungen an IT-Sicherheit zum Schutz aller Verkehrsteilnehmer nicht zufriedenstellend umsetzen kann.



8. Literatur

Bundesverband CarSharing e. V. (o.J.):

Aktuelle Zahlen und Daten zum CarSharing in Deutschland, in: <https://carsharing.de/alles-ueber-carsharing/carsharing-zahlen>, abgerufen am 11.12.2018.

Comastri, Marco (2018):

New frontiers for car security: API management, in: dotmagazine, 06/2018. Online verfügbar unter <https://www.dotmagazine.online/issues/mobility-and-connected-car/connected-car-security/car-security-api-management>, abgerufen am 04.02.2019.

eco – Verband der Internetwirtschaft e. V./Arthur D. Little (2015):

Die deutsche Internetwirtschaft 2015–2019, Köln. Online verfügbar unter: https://www.eco.de/wp-content/blogs.dir/studie_internetwirtschaft_2015-2019.pdf, abgerufen am 13.03.2019.

Eichele Hans (2017):

Vorb. zu § 415 Rz. 1, 2, in: Saenger, Ingo (Hrsg.): Zivilprozessordnung, 7. Aufl., Baden-Baden.

Gasser, Tom M. et al. (2012):

Rechtsfolgen zunehmender Fahrzeugautomatisierung. Gemeinsamer Schlussbericht der Projektgruppe, in: Berichte der Bundesanstalt für Straßenwesen, H. F 83.

Grünweg, Tom (2017):

Audi ist ein Level weiter, 27.09.2017, in: <http://www.spiegel.de/auto/aktuell/audi-a8-audi-ist-beim-autonomen-fahren-ein-level-weiter-a-1169062.html>, abgerufen am 03.02.2019.

Heller, Piotr (2018):

Wie wir demnächst von A nach B kommen, 16.09.2018, in: https://www.deutschlandfunk.de/zukunft-der-mobilitaet-wie-wir-demnaechst-von-a-nach-b-740.de.html?dram:article_id=427850, abgerufen am 14.03.2019.

Kong, Yat Sheng et al. (2017):

Mission profiling of road data measurement for coil spring fatigue life, in: Measurement. Journal of the International Measurement Confederation, Jg. 107, S. 99–110.

SAE International On-Road Automated Vehicle Standards Committee (2014):

Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, SAE J3016. Online verfügbar unter: https://www.sae.org/standards/content/j3016_201401/, abgerufen am 14.03.2019.

Seiberth, Gabriel (2015):

Wie verändern digitale Plattformen die Automobilwirtschaft?, in: Baums, Ansgar et al. (Hrsg.): Kompendium Industrie 4.0. Wie digitale Plattformen die Wirtschaft verändern – und wie die Politik gestalten kann, Berlin. Online verfügbar unter: <http://plattform-maerkte.de/wp-content/uploads/2015/11/Kompendium-High.pdf>, abgerufen am 11.12.2018.

Sommerfeld, Felix (2018):

Wie sich die Autoindustrie neu erfindet – und unser Leben damit verändert, 15.10.2018, in: <http://www.spiegel.de/wirtschaft/unternehmen/autoindustrie-wie-sich-vw-bmw-und-daimler-neu-erfinden-a-1229415.html>, abgerufen am 11.12.2018.

Verband der Automobilindustrie e. V. (2015):

Von Fahrerassistenzsystemen zum automatisierten Fahren, Berlin. Online verfügbar unter: <https://www.vda.de/dam/vda/publications/2015/automatisierung.pdf>, abgerufen am 14.03.2019.

Verband der Automobilindustrie e. V. (2014):

Datenschutz-Prinzipien für vernetzte Fahrzeuge, Berlin. Online verfügbar unter: <https://www.vda.de/de/themen/innovation-und-technik/vernetzung/datenschutz-prinzipien-fuer-vernetzte-fahrzeuge.html>, abgerufen am 14.03.2018.

Veronesi, Lorenzo/Eibisch, James (2018):

The Car as Connected Platform – Interconnection Needs in the Automotive Industry, IDC Mini Market Spotlight, in: <https://www.de-cix.net/de/about-de-cix/academy/white-papers/The-Car-as-Connected-Platform-Interconnection-Needs-in-the-Automotive-Industry>, abgerufen am 03.02.2019.



Von Selle, Dirk (2018):

§ 142, Rz. 7, § 131 Rz. 4, in: Vorwerk, Volker/Wolf, Christian
(Hrsg.): Beck'scher Online-Kommentar ZPO, Stand 15.09.2018.

Zachmann, Frank (2018):

The car as a driver for data growth needing new infrastructure
solutions, in: dotmagazine, 06/2018. Online verfügbar unter:
[https://www.dotmagazine.online/issues/mobility-and-connect-
ed-car/connected-car-market/car-as-driver-for-data-growth](https://www.dotmagazine.online/issues/mobility-and-connected-car/connected-car-market/car-as-driver-for-data-growth),
abgerufen am 03.02.2019.

Zukunftsinstitut (2017):

Die Evolution der Mobilität, hg. von ADAC e. V., München.
Online verfügbar unter: [https://www.zukunftsinstitut.de/fil-
eadmin/user_upload/Publikationen/Auftragsstudien/ADAC_
Mobilitaet2040_Zukunftsinstitut.pdf](https://www.zukunftsinstitut.de/fileadmin/user_upload/Publikationen/Auftragsstudien/ADAC_Mobilitaet2040_Zukunftsinstitut.pdf), abgerufen am 01.02.2019.



9. Autoren



Klaus Brisch LL.M.

Fachanwalt für Informationstechnologierecht sowie Partner und Global Head of Technology, DWF Germany Rechtsanwaltsgesellschaft mbH

Klaus Brisch, Partner und Global Head of Technology bei DWF, ist einer der ersten Fachanwälte für IT-Recht. Sein Studium absolvierte er in Köln, Bonn und Lausanne und bekam den Master von der University San Diego verliehen. Des Weiteren ist er u. a. Mitglied des Ausschusses Datenschutzrecht der Bundesrechtsanwaltskammer, im Advisory Board der German American Business Association (GABA) und im Fachbereichsbeirat „Additive Fertigung“ des Deutschen Instituts für Normung (DIN).

Klaus Brisch berät bei komplexen, nationalen und internationalen IT-Projekten, u.a. zu Fragen im Outsourcing und der Migration von Technologien, bei technologiebasierten Transaktionen, Compliance-Fragen, der Cyber-Sicherheit und Smart Grid-Technologien. Er unterstützt Mandanten verschiedener Branchen bei der Strukturierung ihrer IT-Infrastruktur und sorgt somit für sichere Produktions- und Vertriebsprozesse. Des Weiteren berät Klaus Brisch im Zusammenhang mit eCommerce-Möglichkeiten und sämtlichen Fragen zum Internetrecht. Seine Beratungsschwerpunkte liegen in der Identifizierung und Bearbeitung rechtlicher Fragestellungen im Zusammenhang mit disruptiven Technologien wie etwa Industrie 4.0, autonomes Fahren und künstliche Intelligenz.



Dr. Jens Eckhardt

Fachanwalt für Informationstechnologierecht und Datenschutz-Auditor (TÜV) sowie Compliance-Officer (TÜV) und ECSA Legal Auditor, Derra, Meyer & Partner Rechtsanwälte PartGmbH

Dr. Jens Eckhardt ist Fachanwalt für Informationstechnologierecht sowie ECSA Legal Auditor, Datenschutz-Auditor (TÜV) und Compliance-Officer (TÜV). Er ist für Derra, Meyer & Partner Rechtsanwälte PartGmbH tätig und berät seit 2001 bundesweit nationale und internationale Unternehmen zu den Themen Datenschutz, Informationstechnologie, Telekommunikation und Marketing. Die Beratung umfasst die gerichtliche Vertretung, Vertretung gegenüber Aufsichtsbehörden, insbesondere im Datenschutz, die strategische Beratung bei der Einführung neuer Systeme, die Bewertung von bestehenden Systemen, das Outsourcing sowie die Vertragsgestaltung.

Dr. Jens Eckhardt hält regelmäßig Vorträge, verfasst Veröffentlichungen und doziert u.a. an der udis Ulmer Akademie für Datenschutz und IT-Sicherheit – gemeinnützige Gesellschaft mbH, an der der DeutscheAnwaltAkademie Gesellschaft für Aus- und Fortbildung sowie Serviceleistungen mbH sowie an der SRH Fernhochschule Riedlingen. Bei EuroCloud Deutschland_eco e. V. ist er im Vorstand für das Ressort Recht & Compliance zuständig und fungiert als Head of Legal Advisory Board, EuroCloud Star Audit.



Prof. Dr. Marcus Gelderie

Professor, Hochschule Aalen

Nach seiner Promotion in der theoretischen Informatik und formalen Logik arbeitete Herr Gelderie bei der BMW Car IT. Dort beschäftigte er sich vor allem mit der IT Sicherheit von On-Board Systemen in der Serienentwicklung. Seit 2018 ist er Professor an der Hochschule Aalen im Studiengang „Internet der Dinge“, wo er zur Sicherheit von IoT Devices lehrt und forscht.



Daniel Groß

Associate, DWF Germany Rechtsanwaltsgesellschaft mbH

Daniel Groß ist Associate bei DWF und sitzt im Kölner Büro. Er verfügt über umfassende Erfahrung im Bereich des IT-Rechts und versteht sich besonders auf dem Gebiet der Projektberatung bezüglich Software- und Technologieentwicklung. Daniel Groß absolvierte sein Studium der Rechtswissenschaft in Münster und Bochum. Vor seinem Wechsel zu DWF und seiner Zulassung als Anwalt 2016 war er Syndikusanwalt bei der FinTech Group AG und beriet insbesondere im Bereich des IT-Rechts mit Schwerpunkt auf Finanztechnologien.

Daniel Groß berät Software- und FinTech-Unternehmen, IT-Systemhäuser und Telekommunikationsanbieter bei der Erstellung von Verträgen mit Schwerpunkt auf Softwareentwicklungsprojekten, Lizenzverträgen sowie zu den Themen Datenschutz und Open-Source-Software. Außerdem berät er bei Projekten mit Bezug zur Blockchain-Technologie und ist Teil unseres hausinternen Blockchain Kompetenzteams.

Aufgrund seiner Erfahrung in der Softwareentwicklung ist er in der Lage, sich mit Softwareentwicklern auf Augenhöhe zu unterhalten, rechtliche Lösungen für technische Fragen zu finden und zwischen den technischen Abteilungen und anderen Projektteilnehmern zu vermitteln.



Thorsten Jansen LL.M.

Senior Associate, DWF Germany Rechtsanwaltsgesellschaft mbH

Thorsten Jansen ist Senior Associate im Kölner Büro des DWF. Er hat tiefe Kenntnisse im Bereich des IT-Rechts, Datenschutzes und in der IT-Sicherheits-Compliance. Sein Studium der Rechtswissenschaft absolvierte er in Freiburg und Sydney (LL.M.) und wurde 2011 als Rechtsanwalt zugelassen.

Thorsten Jansen berät Mandanten des Technologiesektors bei zahlreichen IT-rechtlichen Fragestellungen. Er verfügt über umfangreiche Erfahrung bei der Erstellung von IT-Verträgen und in Vertragsverhandlungen, in der Datenschutz- und IT-Sicherheits-Compliance sowie im Urheberrecht und benachbarten Rechtsgebieten.

Des Weiteren hat Thorsten Jansen ein hohes Technologieverständnis, insbesondere von IT-Systemen, die in Mandantenprojekten verwendet werden. Aufgrund seiner Erfahrungen, die er während seiner Arbeit im Rechenzentrum eines Finanzinstituts sammeln konnte, ist Thorsten Jansen vertraut mit den Abläufen eines komplexen Unternehmensnetzwerks einer IT-Umgebung mit höchsten Sicherheitsanforderungen. Vor dieser Tätigkeit verwaltete Thorsten Jansen das Client IT-System eines Lehrstuhls an der rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg.



Tobias Knoben

Projektmanager, eco – Verband der Internetwirtschaft e.V.

Tobias Knoben arbeitet seit 2017 als Projektleiter bei eco – Verband der Internetwirtschaft e.V. Dort ist er für die Aktivitäten im Kontext Internet of Things, Mobility, Smart City und Smart Home zuständig und betreut die Kompetenzgruppe IoT.

2009 schloss er sein Studium als Magister Artium in Kommunikationsforschung und Neuere Geschichte an der Rheinischen Friedrich-Wilhelms-Universität Bonn ab. Vor seinem Wechsel zu eco arbeitete er als Senior Konferenzmanager und Projektleiter bei Euroforum Deutschland SE (heute: Handelsblatt). Dort war er für Kongresse und Tagungen rund um die Themen Digitalisierung, IT und Mobility verantwortlich. In dem Kontext erwarb er umfassendes Know-How in neuen Technologien, ökonomischem Wandel und Digitalisierung des Automobilsektors.



Marco Müller-ter Jung LL.M.

Partner und Fachanwalt für Informationstechnologierecht,
DWF Germany Rechtsanwälts-gesellschaft mbH

Marco Müller-ter Jung, Partner und Fachanwalt für IT-Recht, arbeitet in Köln. Seine Beratungsschwerpunkte liegen im IT-Recht, Recht des geistigen Eigentums sowie Datenschutz.

Nach seinem Studium der Rechtswissenschaften in Düsseldorf erwarb Marco Müller-ter Jung 2008 den Master of Laws (LL.M., Informationsrecht) an der Düsseldorf Law School und wurde 2009 als Rechtsanwalt zugelassen. Vor seinem Wechsel zu DWF war er Rechtsanwalt bei der Wirtschaftskanzlei Wülfig Zeuner Rechel.

Marco Müller-ter Jung berät national und international tätige Unternehmen in den Bereichen Internet-, eCommerce- und Datenschutzrecht sowie bei IT-Verträgen und komplexen IT-Projekten, wie etwa der Beschaffung und Integration neuer Technologien sowie Migration und Outsourcing. Seine Schwerpunkte liegen in der Beratung der rechtlichen Anforderungen disruptiver Technologien, etwa des Industrial Internet, des autonomen Fahrens oder von Sprach-Assistenzsystemen. Des Weiteren ist Marco Müller-ter Jung stellvertretender Vorsitzender des Fachausschusses 105.5 „Rechtliche Aspekte der additiven Fertigung“ beim VDI.



Prof. Dr.-Ing. Dr. h.c. Dieter Schramm

Dieter Schramm schloss 1981 sein Mathematikstudium an der Universität Stuttgart ab, arbeitete dort von 1981-1986 als wissenschaftlicher Mitarbeiter und promovierte 1986 in Ingenieurwissenschaften. Von 1986-1998 arbeitete er bei der Robert Bosch GmbH als Gruppenleiter, Abteilungsleiter der Vorentwicklung und der Serienentwicklung für Fahrzeugsysteme. Er kam 1999 zu Tyco Electronics Ltd. und war bis 2004 als Director Global Automotive Engineering und später als CEO der Tyco Electronics Pretema GmbH tätig. Im Jahr 2004 wurde er zum ordentlichen Professor und Leiter des Lehrstuhls für Mechatronik an der Universität Duisburg-Essen ernannt und seit 2006 zum Dekan der Fakultät für Ingenieurwissenschaften und Leiter des Fachbereichs Maschinenbau gewählt. Seine aktuellen Forschungsinteressen sind elektrifizierte und alternative kraftstoffbetriebene Automobile, Fahrerassistenzsysteme, Fahrdynamik und kabelgebundene Manipulatoren. Im Jahr 2015 wurde er von der Universität Miskolc, Ungarn, mit einem Dr. h.c. ausgezeichnet. Neben seiner Forschungstätigkeit ist er Direktor und Partner mehrerer Unternehmen im Bereich Forschung und Weiterbildung in Deutschland und Malaysia.



Nils Steffen

Rechtsanwalt, Datenschutzbeauftragter (TÜV) und ESCA Legal Auditor, Derra, Meyer & Partner Rechtsanwälte PartGmbH

Nils Steffen berät seit 2016 europaweit nationale und internationale Unternehmen in den Beratungsfeldern Datenschutz, Marketing und Wettbewerbsrecht. Die Beratung umfasst die außergerichtliche und gerichtliche Vertretung, auch gegenüber Aufsichtsbehörden, insbesondere im Datenschutz, sowie Vertragsgestaltungen. Er ist Referent verschiedener Datenschutzveranstaltungen, Autor von Fachbeiträgen zum Datenschutzrecht, Mitautor der Zeitschrift „Datenschutz digital“ und Legal Auditor für EuroCloud StarAudit.



Thorsten Stuke

Experte Mobility, eco – Verband der Internetwirtschaft e.V., Gründer und Geschäftsführer, m2m-Tailors

Thorsten Stuke ist Geschäftsführer und Gründer von m2m Tailors. Nach seiner Ausbildung zum Kaufmann im Luftverkehr durchlief er Stationen als Key Account Manager im Bereich mobile Datenerfassung zur Überwachung des ruhenden Straßenverkehrs. Anschließend fungierte er als Manager Apple Business Unit der Computer 2000 (heutige TechData), bevor er bis 2013 Head of M2M Sales and Solutions bei Telefónica Deutschland war.

Thorsten Stuke verantwortete als Projektleiter die Einführung des Handyparkens in Köln, Düsseldorf und Bremen. Er ist Inhaber diverser Patente im Bereich M2M (Jugendschutz mit dem Handy und sichere Übertragungswege) und Entwickler der transaktionsstärksten M2M Plattform im Vendingmarkt (ca. 1,5 Mio Transaktionen täglich).

Mit seinen umfangreichen Erfahrungen im Automobilsektor fungiert er im eco Verband als Experte Mobility.



Thomas Weber

Thomas Weber studierte Luft- und Raumfahrttechnik an der Universität der Bundeswehr in Neubiberg. Nach seinem Abschluss wurde er bei der Luftwaffe bis zum Ende seiner zwölfjährigen Verpflichtungszeit als Fluglotse eingesetzt. Nach dem Ende seiner Dienstzeit absolvierte er im Rahmen einer beruflichen Weiterbildung das Masterprogramm „Automotive Engineering and Management“ an der Universität Duisburg-Essen, wo er seitdem als wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Mechatronik tätig ist.



VERNETZTE UND
AUTONOME MOBILITÄT



Impressum

Herausgeber:

eco – Verband der Internetwirtschaft e.V.
Lichtstraße 43h
50825 Köln

Drucklegung:

April 2019

Kontakt:

eco – Verband der Internetwirtschaft e.V.
Tel.: +49 221 - 70 00 48-0
E-Mail: iot@eco.de





eco – Verband der Internetwirtschaft e.V.

Lichtstraße 43h, 50825 Köln

fon +49(0)221/700048-0

fax +49(0)221/700048-111

info@eco.de, www.eco.de

 @eco_de,  @ecoverband



WIR GESTALTEN DAS INTERNET.
GESTERN. HEUTE. ÜBER MORGEN.