vbw

Die bayerische Wirtschaft




Position

Automatisiertes Fahren – Datenschutz und Datensicherheit

Stand: März 2018
www.vbw-bayern.de

Vorwort

Rahmenbedingungen für die Zukunft des Autofahrens schaffen

Die Automobil- und Automobilzulieferindustrie befinden sich mitten in der digitalen Transformation. Das automatisierte und schließlich autonome Fahren zeichnen sich klar als Zukunftstrends ab. Angesichts der enormen Bedeutung der Branche für die bayerische Wirtschaft müssen wir dafür sorgen, dass unsere Unternehmen bestmögliche Rahmenbedingungen für die Entwicklung neuer Technologien und Geschäftsmodelle vorfinden.

Beim automatisierten und vernetzten Fahren entstehen in großem Umfang Daten. Diese gilt es einerseits im Interesse der Betroffenen und des Gesamtverkehrssystems effektiv zu schützen und zu sichern, andererseits liegt in ihrer intelligenten Nutzung ein erhebliches Wertschöpfungspotenzial, das gehoben werden muss.

Anknüpfend an unsere Positionspapiere *Zukunft automatisiertes Fahren: Rechtliche Hürden beseitigen* (März 2018), das sich insbesondere mit verkehrs-, zulassungs- und haftungsrechtlichen Fragen befasst, und *Automatisiertes Fahren – Infrastruktur* (Mai 2016) stellen wir daher in unserer vorliegenden, gegenüber der Fassung von August 2016 aktualisierten und überarbeiteten Position dar, was aus Sicht der vbw – Vereinigung der Bayerischen Wirtschaft e. V. zu tun ist, um auch im Bereich des Datenschutzes und der Datensicherheit die richtigen Rahmenbedingungen für die Zukunft des Autofahrens zu schaffen.

Bertram Brossardt
26. März 2018

Inhalt

Hinweis

Diese Information ersetzt keine rechtliche Beratung im Einzelfall. Eine Haftung übernehmen wir mit der Herausgabe dieser Information nicht.

1 Forderungen im Überblick

Privatsphäre schützen, Sicherheit gewährleisten und Innovationen fördern

Der Gesetzgeber steht vor einer doppelten Herausforderung: Auf der einen Seite gilt es, in allen Entwicklungsstufen des automatisierten Fahrens (vgl. Abb. 1) das notwendige Niveau an Datenschutz und IT-Sicherheit zu gewährleisten. Auf der anderen Seite müssen die richtigen Rahmenbedingungen für Innovationen geschaffen werden, die es insbesondere unserer Automobil- und Zuliefererindustrie ermöglichen, ihre Technologieführerschaft auch im internationalen Wettbewerb zu halten und auszubauen.

Dabei sind insbesondere die folgenden Aspekte zu berücksichtigen:

– Um den automatisierten Verkehr sicher zu gestalten, müssen die Fahrzeuge sowohl mit Infrastruktur und Backend kommunizieren als auch mit anderen Fahrzeugen. Insoweit erforderliche Daten müssen auf gesetzlicher Grundlage zur Verfügung gestellt werden, verbunden mit der Vorgabe, sie sicher zu anonymisieren bzw. zu pseudonymisieren.

– Für die Fahrzeugnutzer muss eine möglichst vollständige Transparenz darüber bestehen, welche Daten in dem Fahrzeug entstehen, gespeichert und übermittelt werden, zu welchem Zweck sie genutzt werden und an wen welche Daten letztlich weitergegeben werden. Sie sollten grundsätzlich die Möglichkeit haben, Zugriff auf die Daten zu nehmen und anderen zu gewähren. Über die Konzepte Privacy by Design und Privacy by Default sollte eine Datensouveränität des Fahrzeugnutzers hinsichtlich sämtlicher Daten angestrebt werden, die zumindest perspektivisch personenbeziehbar sind.

– Für die Einwilligung in die (künftige) Nutzung der Daten sind praxisgerechte Lösungen zu entwickeln; Anonymisierung und Pseudonymisierung müssen auch ohne (erneute) Einwilligung des Betroffenen möglich sein.

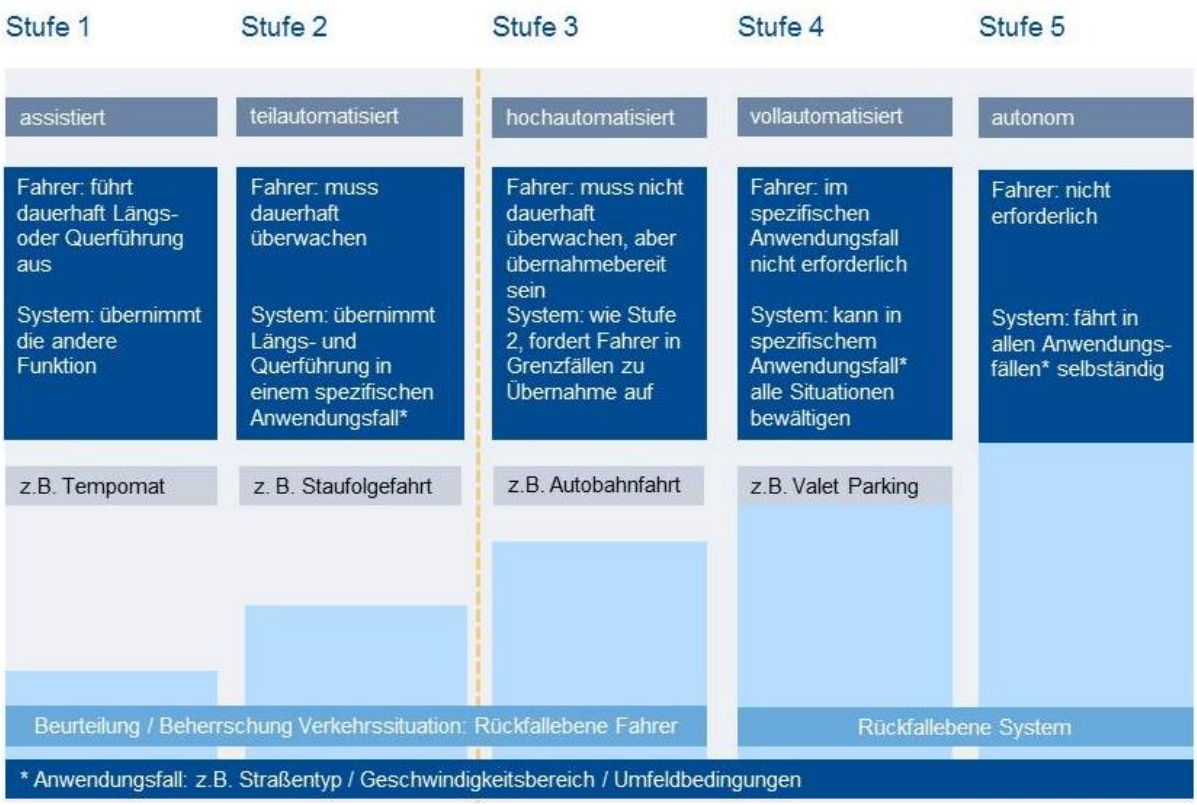
– Alleine durch die technische Möglichkeit dürfen die bewährten prozessualen Grundsätze nicht in Frage gestellt werden. Für die Speicherung und Nutzung der im Zusammenhang mit dem Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System entstandenen Daten sollten datenschutzrechtliche Rahmenbedingungen geschaffen werden.

– Für die IT-Sicherheit müssen angemessene, faire und einheitliche Standards entwickelt werden. Ziel ist die Gewährleistung einer vollständigen Ende-zu-Ende Sicherheit von Daten und Kommunikation durch Hersteller, Zulieferer und Dienstleister. Leitgedanke muss Security by Design sein, die IT-Sicherheit muss also bereits in der Konzeptionsphase berücksichtigt werden. Die Forschung im Bereich der IT-Sicherheit für das automatisierte und vernetzte Fahren muss intensiviert werden.

– Auf die Regelung eines „Dateneigentums“ ist vorerst zu verzichten; Lösungen sind über vertragliche Gestaltungen zwischen den bei der Datenerhebung und Datenverarbeitung Beteiligten anzustreben.

– Datenmonopole sind grundsätzlich zu vermeiden. Es sollte ein Level Playing Field angestrebt werden, verbunden mit einer kostenneutralen Lösung für den Zugriff auf die Nutzerdaten, wenn der Halter / Fahrer eingewilligt hat, bzw. es sich nicht um personenbezogene Daten handelt. Der Staat muss seinerseits Open Data konsequent umsetzen, um auf Basis der von ihm erhobenen Daten neue Geschäftsmodelle zu ermöglichen.

Abbildung 1
Entwicklungsstufen des automatisierten Fahrens



Quelle: vbw

Zu den einzelnen Entwicklungsstufen vgl. näher *Zukunft automatisiertes Fahren: Rechtliche Hürden beseitigen* (vbw, März 2018).

2 Erfasste Daten und Beteiligte

So vielfältig wie die entstehenden Daten sind die daran bestehenden Interessen

Bereits heute werden bei der Nutzung moderner Fahrzeuge in erheblichem Umfang Daten erhoben, gespeichert und teilweise auch übermittelt. Mit zunehmendem Grad an Automatisierung und Vernetzung steigen die Datenmenge und die Datenquellen weiter stark an.

2.1 Arten der anfallenden Daten

Die Daten lassen sich grob nach Bewegungs- und Umfelddaten, Zustands- und Verhaltensdaten sowie Komfortdaten unterteilen. Eine gewisse Sonderrolle kommt dabei den (künftig) gesetzlich vorgegebenen Identifikations-Daten aus dem eCall-Verfahren und der Fahrzeugidentifikationsnummer (FIN) zu, die laufend miterfasst und übermittelt werden.

Abbildung 2
Beim Fahren entstehende Daten

Quelle: vbw

Diese Daten werden einerseits für das automatisierte Fahren selbst benötigt, also beispielsweise für die Orientierung im Raum und als Grundlage für algorithmenbasierte Entscheidungen im Rahmen der Fahrzeugsteuerung (Primärzweck Verkehrssteuerung und Verkehrssicherheit).

Das vernetzte Fahrzeug kommuniziert

– mit anderen Fahrzeugen (C2C)
– mit der Infrastruktur (C2I)
– mit anderen Einrichtungen (C2X)
– mit seinen Insassen, zum Beispiel über die Vernetzung mit deren Mobiltelefonen
– und perspektivisch auch mit weiteren Verkehrsbeteiligten (z. B. Fußgänger).

Mit zunehmendem Grad an Automatisierung nimmt die Bedeutung dieser verschiedenen Kommunikationswege zu, vgl. dazu näher das Positionspapier *Automatisiertes Fahren – Infrastruktur* (vbw, Mai 2016). So sehen heutige Verkehrslagesysteme bspw. eine Vernetzung zum jeweiligen Hersteller vor; mit zunehmender Automatisierung wird ein übergreifender Datenaustausch erforderlich sein, um die Umfeldinformationen auf das notwendige Detaillierungslevel zu bringen.

Andererseits ermöglichen die Daten aber auch eine Nutzung für verschiedenste Geschäftsmodelle und -felder: Dienstleistungen vor, während und nach der Fahrt, aber auch Angebote, die über die eigentliche individuelle Mobilität hinausgehen (Sekundärzwecke).

Eine Unterscheidung nach Primär- und Sekundärzwecken der erhobenen, gespeicherten und übermittelten Daten wird insbesondere dann relevant, wenn es um die vom Gesetzgeber zu treffende Abwägung zwischen der Gewährleistung der Sicherheit im Straßenverkehr und dem Schutz der Privatsphäre der Betroffenen geht (vgl. näher Kapitel 3).

2.2 Möglichkeiten der Datennutzung

Eine Vielfalt an Funktionen ist vorstellbar und teilweise bereits heute im Einsatz:

– Entertainment-Angebote (z. B. Streamen von Videos oder WLAN-Hotspots),
– neue Mobilitätskonzepte, in denen nicht klassische Geschäftsmodelle wie Fahrzeugkauf, -finanzierung und -leasing im Vordergrund stehen, sondern Fahrzeug(mit)benutzung und Bereitstellung von Mobilität, in deren Rahmen das Auto nur ein Baustein ist,
– Mobilitätsmanagement (z. B. hochaktuelle Verkehrsinformationen oder Verbrauchsoptimierung),
– Versicherungs- oder Finanzierungsmodelle, die sich an tatsächlichen Fahrverhalten und / oder Fahrleistung orientieren (z. B. Telematik-Tarife),
– Fahrzeugmanagement (z. B. Fernbedienung oder Wartungsinformationen),
– Sicherheitsfunktionen (z. B. Weiterentwicklung von Assistenzsystemen oder Notruf-Funktionen),
– Marketing (z. B. Hinweis auf Angebote entlang der Fahrtroute, aber auch bzgl. zu wartender Fahrzeugteile oder – unter Berücksichtigung des tatsächlichen Nutzungsverhaltens – der Anschaffung des nächsten Fahrzeugs).

Einige der Nutzungsmöglichkeiten entstehen gerade erst aus einer Zusammenschau der Daten aus einer Vielzahl vernetzter Fahrzeuge und ggf. in Kombination mit weiteren Daten, z. B. die präzise Vorhersage von Verkehrsströmen für die Kalibrierung entsprechender Leitsysteme. Auch außerhalb des eigentlichen Verkehrsbereichs liegende Anwendungen sind aber denkbar. So ist das Auto dank der Vielzahl an Sensoren eine Art rollende Wetterstation; die Gesamtheit der Kraftfahrzeuge ermöglicht ein präzises Ist-Bild. Gleichzeitig können Vorhersagen für Verkehrsdichte etc. in Abhängigkeit von Wetterlagen perfektioniert werden. Hierbei handelt es sich letztlich um Big Data Anwendungen.

Seitens der Kunden besteht durchaus eine Nachfrage nach Geschäftsmodellen, die auf den im Fahrzeug gewonnenen Daten basieren, beispielsweise Telematik-Tarife in der Kfz-Versicherung. Aktuell werden durch verschiedene Versicherungsgesellschaften neue fahrrisikobasierte Tarife (pay as you drive) entwickelt. Neu ist daran allerdings nur die technische Umsetzung: Auch bisher wurden persönliche Daten zur Tarifierung herangezogen, da dies für die Risikobewertung und eine risikogerechte Bepreisung essenziell ist.

2.3 Betroffene und Beteiligte

Mit der zunehmenden Digitalisierung des Fahrzeugs und den möglichen Geschäftsmodellen wächst auch die Anzahl an Betroffenen und Beteiligten neben den eigentlichen Nutzern des Fahrzeugs (Halter, Fahrer, ggf. weitere Insassen), vgl. Abb. 3.

Insbesondere neuen Akteuren auf dem Mobilitätsmarkt (z. B. Google, Apple, Tesla) geht es vorrangig darum, das Auto als Plattform zu erschließen, die ihnen dann neue Interaktions- und Vertriebsmöglichkeiten mit einem größeren Skalierungspotenzial eröffnet. Während der Verkauf eines Autos nur einmalig alle etwa fünf bis sieben Jahre Umsätze erzeugt, können ergänzende Produkte und Dienstleistungen über den gesamten Lebenszyklus des Fahrzeugs hinweg abgesetzt werden.

Auch die etablierten Automobilhersteller entwickeln parallel zu ihrem klassischen Geschäft nutzungsbasierte Geschäftsmodelle und versuchen, eine eigene digitale Beziehung zum Kunden zu entwickeln. Dafür müssen sie ggf. – über die eigenen Produkte oder Dienstleistungen hinweg – mit anderen Unternehmen kooperieren. Ein Beispiel ist etwa das Carsharing-Angebot DriveNow als Joint Venture von Sixt und BMW.

Abbildung 3
Datennutzung und Beteiligte

Quelle: vbw

2.3.1 Interessenlage der Akteure im Überblick

Beim automatisierten Fahren sind viele Akteure beteiligt, die mit Blick auf die Daten unterschiedliche Interessen verfolgen. Im Folgenden werden einige davon skizziert. Diese Interessen gilt es grundsätzlich in einen angemessenen Ausgleich zu bringen.

2.3.1.1 Fahrzeugnutzer (Fahrzeugeigentümer, Halter, Fahrer und Mitfahrer)

Die Betroffenen sind am Schutz ihrer Privatsphäre interessiert und wollen in der Regel selbst entscheiden, welche Daten sie wann und für welche Zwecke preisgeben. Hierzu müssen sie aber über die Datenverarbeitungsprozesse (Erhebung, Speicherung, Übermittlung) möglichst in vollem Umfang informiert werden, damit sie entscheiden können, welche Daten sie „freigeben“. Das gilt grundsätzlich auch für reine Sachdaten (vgl. auch unten Kapitel 3 zur im Einzelfall schwierigen Abgrenzung).

Die Zurverfügungstellung von Daten kann für die Betroffenen mit finanziellen oder immateriellen Vorteilen verbunden sein. So können Versicherungstarife in Anspruch genommen werden, die defensive Fahrweise in Form von Tarifvergünstigungen honorieren, oder der Komfort kann durch maßgeschneiderte Dienstleistungsangebote erhöht werden.

2.3.1.2 Andere Verkehrsteilnehmer

Andere Verkehrsteilnehmer, ob motorisiert oder nicht, können bspw. durch im Fahrzeug installierte Kameras erfasst werden; Sensoren können etwa die Geschwindigkeit des vorausfahrenden Fahrzeugs ermitteln. Auch die Privatsphäre Dritter ist zu schützen.

2.3.1.3 Fahrzeughersteller, Vertragshändler, Werkstätten

Der Hersteller des Fahrzeugs hat ein Interesse daran, die Fahrzeugdaten auszuwerten und die daraus gewonnenen Erkenntnisse bei der zukünftigen Entwicklung, der Wartung und mit Blick auf Garantiefälle zu berücksichtigen. Darüber hinaus können beispielsweise Daten über das Nutzungsverhalten auch Hinweise bezüglich einer Fahrzeugneuanschaffung und entsprechende Dispositionen ermöglichen. Auch Werbemitteilungen können situationsabhängig direkt an das Auto übermittelt werden – sei es im Hinblick auf fahrzeugbezogene Produkte und Dienstleistungen des Herstellers und seiner Vertragspartner oder auf Angebote Dritter, denen der Hersteller den Zugang zum Fahrzeugnutzer vermittelt.

Die Vertragshändler und Werkstätten haben ein Interesse daran, mithilfe der ausgewerteten Daten zusätzliche Serviceverträge bzw. Reparaturangebote zu kreieren und den Kunden auf diese Weise an sich zu binden. Dies kann beispielsweise dadurch erfolgen, dass das Auto im Falle einer Panne bzw. bei Erreichen eines bestimmten Verschleißzustands die für die Reparatur bzw. Inspektion relevanten Daten an eine bestimmte Werkstatt übermittelt und eine Terminanfrage startet.

Der Händler als Vertragspartner des Fahrzeuginhabers hat ein Interesse an Daten für den Fall einer gewährleistungsrechtlichen Haftung, bei der Überprüfung des Fahrzeugzustandes durch eine effektive Fernüberwachung oder mit Blick auf eine Neuanschaffung.

Die skizzierten Interessenlagen gelten auch für freie Händler und Werkstätten, die einen vergleichbaren Nutzen aus den Daten ziehen könnten.

2.3.1.4 Versicherungsgesellschaften

Die Versicherungsgesellschaften bieten Telematikversicherungstarife („pay how you drive“ bzw. „pay as you drive“) an, bei denen das Fahrverhalten ausgewertet wird. Bei vorsichtigem Fahren wird die Versicherungsprämie gesenkt. Hierzu müssen Daten wie Geschwindigkeit, Brems- und Fahrverhalten, Art der befahrenen Straße, gefahrene Strecke, Uhrzeit und Datum ausgewertet und an die Versicherungsgesellschaft bzw. einen Intermediär übermittelt werden. Das letztgenannte Modell wird insbesondere gewählt, um eine Pseudonymisierung sicherstellen zu können (vgl. näher Big Data im Freistaat Bayern – Chancen und Herausforderungen, vbw 2016); zu den datenschutzrechtlichen Aspekten siehe im Übrigen unten Kapitel 3.

Es ist davon auszugehen, dass die Versicherungen versuchen werden, durch eine entsprechende Preis- und Prämienpolitik die Standardtarife sukzessive durch die Telematikversicherungstarife zu ersetzen. Rechtlich ist die Einführung bzw. Umstellung auf Telematiktarife zunächst nicht zu beanstanden (Grundsatz der Vertragsfreiheit); Schwierigkeiten können sich allerdings im Hinblick auf die Versicherungspflicht dann ergeben, wenn die zunehmend granulare Betrachtung im Ergebnis für einzelne zu sehr teuren Versicherungslösungen führt. Das gilt es zu beobachten.

2.3.1.5 Verkehrsleitzentralen, Navigationsdienste, Behörden

Um den vernetzten und automatisierten Verkehr im Ganzen zu organisieren, sind bestimmte Daten sinnvoll oder sogar erforderlich. Das betrifft in erster Linie Bewegungs- und Umfelddaten, die in Echtzeit verfügbar gemacht werden müssen, um beispielsweise eine sichere Steuerung zu gewährleisten.

Auch Daten zur Interaktion zwischen Fahrer und Fahrzeug (z. B. Reaktionen auf „Übernahmeaufforderungen“ in bestimmten Verkehrssituationen) können aber bspw. relevant sein, ebenso wie Daten im Zusammenhang mit Unfallereignissen.

2.3.1.6 Mobilitätsanbieter, Contentanbieter und sonstige Dienstleister

Das Auto entwickelt sich immer mehr zu einem rollenden Computer. Es werden bereits zahlreiche Anwendungen angeboten, mit denen das Autofahren noch bequemer und unterhaltsamer gemacht werden soll. Dabei sind die Daten, die das Fahrzeug über die Bordelektronik generiert, auch für Dienstleister von erheblicher wirtschaftlicher Bedeutung, z. B., um eine genaue Analyse der Nutzung ihrer Angebote durchführen zu können. Damit können individuelle Kundenangebote, etwa in Form von personalisierter Werbung, erstellt werden.

Forderung

Für die Fahrzeugnutzer muss eine möglichst vollständige Transparenz darüber bestehen, welche Daten in dem Fahrzeug entstehen, gespeichert und übermittelt werden, zu welchem Zweck sie genutzt werden und an wen welche Daten letztlich weitergegeben werden. Sie sollten grundsätzlich die Möglichkeit haben, Zugriff auf die Daten zu nehmen und anderen einen Zugriff auf freiwilliger / vertraglicher Basis zu gewähren.

---

3 Datenschutz

Persönlichkeitsrechte schützen, ohne Innovationen auszubremsen

Bei der Gestaltung datenschutzkonformer Lösungen liegt eine grundlegende Herausforderung darin, dass die Produkte im Automobilbereich in der Regel für einen internationalen Markt gestaltet werden, der hinsichtlich der datenschutzrechtlichen Anforderungen heterogen ist. Nachdem aber der Datenschutz in Deutschland und auch in der EU im Ganzen im weltweiten Vergleich auf einem Spitzenniveau liegt, kann davon ausgegangen werden, dass ein den Anforderungen des hiesigen Markts genügendes Fahrzeug oder Geschäftsmodell auch international keinen großen weiteren Hürden mehr begegnet.

Auf europäischer Ebene ist nunmehr eine weitgehende Harmonisierung vollzogen. Mit der EU-Datenschutzgrundverordnung (EU-DSGVO), die ab dem 25. Mai 2018 in allen EU-Mitgliedsstaaten anzuwenden ist, wird nationales Datenschutzrecht jenseits der vereinzelt vorgesehenen Öffnungsklauseln praktisch obsolet, soweit der Anwendungsbereich der EU-DSGVO reicht. Die EU-DSGVO knüpft allerdings an die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten an, so dass sich für den hier relevanten Bereich vergleichsweise wenig ändert. Das vorliegende Positionspapier berücksichtigt in seiner aktualisierten Fassung nur noch die Rechtslage ab dem 25. Mai 2018, also die EU-DSGVO sowie das BDSG 2018, das zeitgleich das bis dahin geltende Bundesdatenschutzgesetz komplett ablöst.

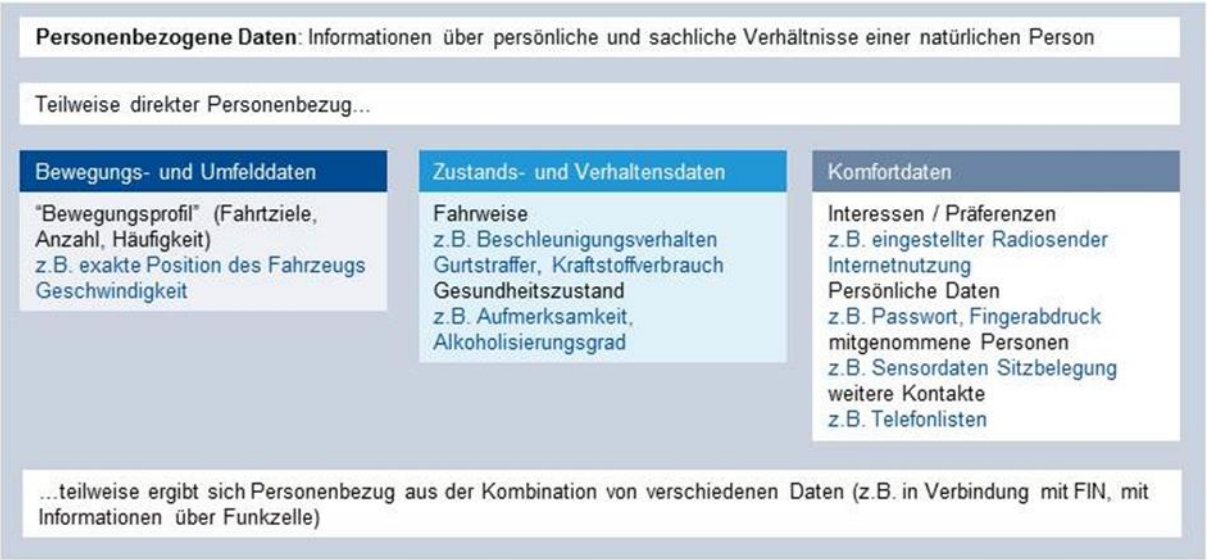
Damit lassen sich zum einen die datenschutzgesetzlichen Anforderungen zumindest innerhalb Europas weitestgehend konvergent abdecken. Zum anderen ist es vorstellbar, dass die Berücksichtigung dieses – insbesondere aus globaler Sicht – ausgesprochen hohen Datenschutzniveaus für die weltweite Vermarktung künftig ein Qualitätsmerkmal darstellen könnte.

3.1 Personenbezug

Entscheidende Vorfrage für die Anwendung des Datenschutzrechts ist, ob es sich bei den Daten um personenbezogene Daten handelt, da nur diese dem Regime der EU-DSGVO unterliegen.

Eine große Anzahl der beim Fahren erzeugten Daten hat einen Personenbezug, weil sie Informationen etwa über die Gewohnheiten des Fahrzeugführers (z. B. Art und Intensität der Kfz-Nutzung) enthalten.

Abbildung 4
Personenbezug der Daten



Quelle: vbw

Der Zusammenhang zu einer bestimmten Person lässt sich teilweise erst im Zusammenhang mit weiteren Informationen herstellen. Ein Personenbezug liegt jedenfalls dann vor, wenn die bei der Kfz-Nutzung anfallenden Daten mit der Fahrzeugidentifikationsnummer (FIN) oder dem Kfz-Kennzeichen verknüpft sind.

Mit steigenden Möglichkeiten der Datenanalyse reichen allerdings immer weniger auch für sich betrachtet noch nicht personenbezogene oder bereits anonymisierte Daten aus, um einen Einzelnen eindeutig zu identifizieren. Das gilt insbesondere im Rahmen von Big-Data-Analysen. Auch bei technischen Messdaten (Fahrzeugfunktion, Servicefunktion o. ä.) kann der Personenbezug beispielsweise beim Auslesen der Daten in der Werkstatt hergestellt werden.

Teilweise wird sogar vertreten, dass sämtliche im Zusammenhang mit der Kfz-Nutzung gewonnenen Daten personenbezogen seien, was zum gegenwärtigen Zeitpunkt aber noch übertrieben erscheint. Sobald allerdings (nahezu) alle Daten auf eine Person bezogen werden können, dürfte das gegenwärtige System nicht mehr geeignet sein, die Lebenswirklichkeit sachgerecht abzubilden.

3.2 Wer ist Betroffener im Sinne von Art. 4 Nr. 1 EU-DSGVO?

Betroffener im Sinne von Art. 4 Nr. 1 EU-DSGVO ist jede identifizierte oder identifizierbare natürliche Person, auf die sich Informationen beziehen („personenbezogene Daten“). Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt,

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

Betroffener ist in der Regel zunächst der Fahrer, von dem die meisten personenbezogenen oder zumindest personenbeziehbaren Daten erfasst werden (z. B. Fahrverhalten, Ortsveränderung, Sitzeinstellungen, Eingaben am Bordcomputer).

Je präziser die Lokalisierung möglich (und für das automatisierte Fahren notwendig) ist, desto genauer werden allerdings z. B. auch Beifahrer mit erfasst. Deren Smartphone ist dann nicht nur in derselben Funkzelle, sondern offensichtlich im selben Fahrzeug. Das gilt erst Recht, wenn auch das Smart Device Dritter in die Kommunikation mit und über das Kfz eingebunden ist. In diesen Fällen sind dann auch die möglichen Abwehrechte Dritter zu beachten.

Neben den Insassen des Fahrzeugs können unter Umständen zusätzlich dem Halter oder auch früheren Nutzern desselben Kfz (deren Informationen – bspw. Komfortdaten – noch gespeichert sind) Abwehrrechte zustehen.

3.3 Wer ist der für den Datenschutz Verantwortliche?

„Verantwortlicher“ ist nach Art. 4 Nr. 7 EU-DSGVO 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.

Das ist regelmäßig derjenige, der die Anwendungen oder Dienste bereitgestellt hat und hierauf – physisch oder mit einem Remotezugang – zugreifen und die Datenherrschaft über die gespeicherten Daten ausüben kann, u. U. auch im Rahmen einer Auftragsverarbeitung (Art. 28 EU-DSGVO):

– bei Daten aus den im Kfz verbauten Steuerungsgeräten, Sicherheitseinrichtungen und ggf. Sensoren derjenige, der sie ausliest, also in der Regel der Hersteller bzw. die Werkstatt
– bei Daten aus Telematikvorrichtungen der für den Einbau verantwortliche Flottenbetreiber bzw. die Versicherung
– bei Daten aus der Kommunikation C2I oder C2X der entsprechende Dienstleister, der die Daten übermittelt bekommt
– beim eCall die im Falle eines Unfalls informierte Leitstelle
– bei Daten aus Servicefunktionen beispielsweise in Infotainment-Systemen z. B. auch der Vermieter oder sonstige Anbieter von Mobilitätsdienstleistungen.

3.4 Wann findet die Datenerhebung statt?

Hier ist danach zu unterscheiden, wo die Daten gespeichert werden:

– (zunächst nur) im Fahrzeug oder
– auf dem Server des Herstellers oder eines Dritten (z. B. Versicherung für Telematik-Tarif) bzw. in einer Cloud.

Wenn die Datenspeicherung lediglich innerhalb des Kfz stattfindet und ein Zugriff Dritter (etwa per Remote-Zugriff) ausgeschlossen ist, kommt es erst dann zu einer datenschutzrechtlich relevanten Erhebung, wenn die Daten – beispielsweise in der Werkstatt – ausgelesen werden.

Erfolgt dagegen eine Datenübermittlung aus dem Fahrzeug heraus, dann findet bereits in diesem Zeitpunkt eine Erhebung im Sinne von Art. 4 Nr. 2 EU-DSGVO statt.

3.5 Transparenz, Privacy by Design

Auch wenn (noch) kein Personenbezug besteht oder dieser gelockert bzw. gelöst wurde (Anonymisierung / Pseudonymisierung), gilt aber, dass zur Wahrung des Rechts auf informationelle Selbstbestimmung für den Betroffenen grundsätzlich Transparenz und Wahlfreiheit hergestellt werden muss. Dazu zählt auch eine Information über Art, Ort und Zweck der Erhebung, Speicherung und Verwendung. Ob die bisherige Praxis dem ausreichend Rechnung trägt, erscheint zumindest sehr fraglich. Art. 12 EU-DSGVO verschärft die bisherige Rechtslage durch explizite Pflichten zur Herstellung von Transparenz. Nach Art. 12 Abs. 1 EU-DSGVO trifft der Verantwortliche „geeignete Maßnahmen, um der betroffenen Person alle Informationen ... die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“. Das ist eine mediendidaktische Herausforderung, auf die die meisten Stellen, die im Kontext Kraftfahrzeug Daten erheben und verarbeiten, kaum vorbereitet sein dürften.

Gerade mit Blick auf die wachsenden Möglichkeiten, einen Personenbezug auch nachträglich noch herzustellen, trifft insbesondere den Hersteller außerdem die Verantwortung, im Rahmen seiner technischen Gestaltungsmöglichkeiten (z. B. Zugriffsmöglichkeiten, Konfigurierung, Schnittstellen) die Daten bestmöglich zu schützen.

Insgesamt spielen bereits in der Konzeptionsphase die Grundsätze der „Privacy by Design“ (Schutz der Privatsphäre als integraler Bestandteil des Geschäftsmodells) sowie „Privacy by Default“ (privatsphärenfreundliche Standard-Einstellungen) eine wichtige Rolle. Diese Grundsätze des Datenschutzes durch Technikgestaltung sind nunmehr in Art. 25 EU-DSGVO verankert.

Nach Art. 25 Abs. 2 EU-DSGVO trifft der Verantwortliche „geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich

nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden."

Eine Möglichkeit wäre es beispielsweise, eine Art Verfallsdatum für zunächst nicht personenbezogene Daten zu definieren, da die Wahrscheinlichkeit der Herstellung eines Personenbezugs mit Menge und Speicherdauer deutlich ansteigt. Damit wird auch den Grundsätzen der Datenvermeidung und Datensparsamkeit Rechnung getragen.

Für den Fahrer muss transparent sein, welche Daten gespeichert bzw. ob aktuell welche übermittelt werden, und er muss die Möglichkeit haben, außerhalb der gesetzlich vorgegebenen Datenverwendung (z. B. eCall, digitaler Tachograph, perspektivisch etwa für Unfallursachenklärung relevante Daten) einer weiteren Verarbeitung und Übermittlung zu widersprechen bzw. die Einwilligung zu widerrufen und dazu das System unkompliziert abschalten können, wenn die Datenverarbeitung nicht für den sicheren Fahrbetrieb erforderlich ist (opt-in / opt-out Funktionalitäten). Damit können allerdings bei Bestehen vertraglicher Beziehungen weitere Konsequenzen verbunden sein: z. B. im Falle von Telematik-Versicherungstarifen eine Kündigung des Tarifs; eine Auffanglösung (klassischer Tarif) muss dementsprechend jedenfalls bei der Haftpflichtversicherung vorhanden sein. Von ihm selbst eingegebene Informationen (insbesondere Komfortdaten) sollte er jederzeit ändern und auch vollständig wieder löschen können.

Forderung

Über die Konzepte Privacy by Design und Privacy by Default sollte eine Datensouveränität des Fahrzeugnutzers hinsichtlich sämtlicher Daten angestrebt werden, die zumindest perspektivisch personenbeziehbar sind.

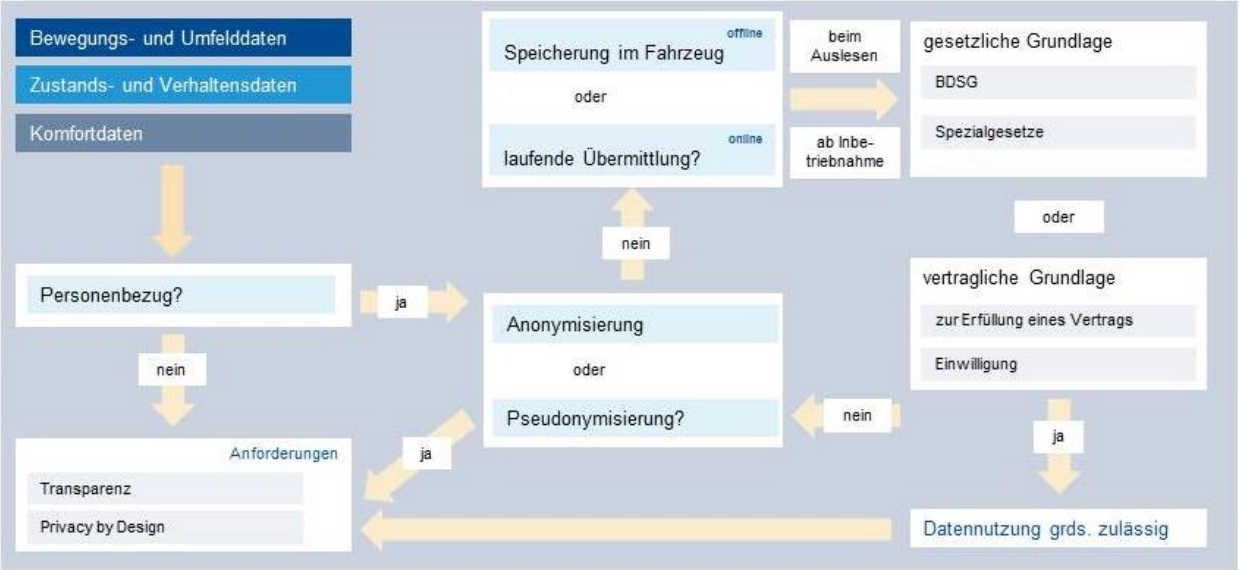
Allgemein kann es sich aus Herstellersicht empfehlen, als vertrauensbildende Maßnahme und ggf. über die bestehenden rechtlichen Beschränkungen hinaus freiwillige Regelungen z. B. zur Zuordnung sämtlicher bei der Kfz-Nutzung entstehenden Daten zum Fahrer / Halter anzubieten. Hier ist die gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) vom 26.01.2016 als erster Schritt anzusehen.

Eine derartige Ausgestaltung ist nicht zuletzt eine Voraussetzung für eine bessere Akzeptanz, da dem Anwender ein ausdrückliches Mitspracherecht eingeräumt wird. Technisch soll die Festlegung der Datenkontrollmechanismen auch durch IT-Laien möglich sein.

3.6 Zulässigkeit der Nutzung

Handelt es sich um personenbezogene Daten, dann ist nach der Systematik von Art. 6 Abs. 1 EU-DSGVO (Verbot mit Erlaubnisvorbehalt) grundsätzlich eine Ermächtigungsgrundlage erforderlich, sofern keine Anonymisierung oder Pseudonymisierung stattgefunden hat.

Abbildung 5
Zulässige Datenerhebung und -speicherung



Quelle: vbw

Die Erhebung, Speicherung und Nutzung personenbezogener Daten sind datenschutzrechtlich gerechtfertigt, wenn hierfür ein Rechtfertigungsgrund besteht oder wenn der Betroffene wirksam eingewilligt hat. Sowohl bei der massenhaften Erhebung als auch bei der automatisierten Verarbeitung personenbezogener Daten sind limitierende Vorgaben (Datensparsamkeit, Scoring nach § 31 BDSG 2018) zu beachten. Für besonders sensible Daten (z. B. Angaben zu Gesundheit oder ethnischer Herkunft, vgl. Art. 9 EU-DSGVO) gelten weitere Restriktionen. Der Erstellung totaler Persönlichkeitsbilder (Profiling) hat das Bundesverfassungsgericht schon vor mehr als vier Jahrzehnten einen Riegel vorgeschoben. Nunmehr regelt Art. 22 Abs. 1 EU-DSGVO, dass die betroffene Person das Recht hat, „nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt." Ausnahmen bestimmt Art. 22 Abs. 2 EU-DSGVO für die Fälle, dass die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist, mit ausdrücklicher Einwilligung der betroffenen Person erfolgt oder aufgrund ausdrücklicher Rechtsvorschriften der Union oder der Mitgliedstaaten zulässig ist.

3.6.1 Spezialgesetzliche Regelungen

Art. 95 EU-DSGVO lässt die auf der Richtlinie 2002/58/EG beruhenden nationalen Regelungen, also auch das *Telekommunikationsgesetz* (TKG), unberührt. Sofern Funktionen des automatisierten Fahrens auf einer Datenübertragung mittels eines Telekommunikationsnetzes basieren, handelt es sich um einen Telekommunikationsdienst im Sinne von § 3 Nr. 24 TKG, so dass auch die spezielleren Datenschutzvorschriften der §§ 91 ff. TKG anzuwenden sind. Eine relevante zusätzliche Ermächtigungsgrundlage etwa im Hinblick auf Standort- oder Verbindungsdaten ist daraus aber nicht ersichtlich. Bei der Übermittlung ist auch der Geheimnisschutz nach § 88 TKG durch jeden Diensteanbieter zu wahren.

Die *eCall-Funktion* ist ab dem 01. April 2018 verpflichtend für alle Neuwagen (EU-Verordnung 2015/758). Es handelt sich dabei um ein bordeigenes Notrufsystem, das im Falle eines Unfalls selbständig einen 112-Notruf an die Rettungsstelle absetzt und unter anderem den genauen Standort des Fahrzeugs übermittelt. Während der normalen Fahrt findet über eCall keine Datenübertragung statt und die Hersteller müssen dafür Sorge tragen, dass keine dauerhafte Verfolgung erfolgt und die Daten im internen Speicher automatisch und kontinuierlich gelöscht werden. Ist die Funktion mobilfunkbasiert, ist der Anwendungsbereich des TKG eröffnet. Beim eCall werden personenbezogene Daten übermittelt, etwa Name, Telefonnummer und Positionsdaten; betroffen können neben dem Fahrer auch weitere Insassen sein. Eine Einwilligung ist hier angesichts der gesetzlichen Verpflichtung jedoch entbehrlich, die Übermittlung gerechtfertigt. Das gilt allerdings nicht für private Notrufdienste und / oder Dienste mit Zusatznutzen, die parallel zum eCall im Fahrzeug installiert sein können.

Fahrassistenzsysteme fallen ggf. auch in den Anwendungsbereich der §§ 11 ff. *Telemediengesetz* (TMG); abweichende bzw. erweitere Befugnisse daraus sind aber nicht ersichtlich. Inwieweit das TMG durch die ePrivacy-Verordnung abgelöst wird, ist derzeit nicht absehbar.

Das *Gesetz über intelligente Verkehrssysteme* (IVSG) ist keine eigenständige Rechtsgrundlage für den Umgang mit personenbezogenen Daten und definiert lediglich bestimmte Daten sowie Zwecke, für die vorrangig intelligente Verkehrssysteme eingeführt werden können:

– Straßendaten (§ 2 Nr. 6 IVSG), d. h. Daten über Merkmale der Straßeninfrastruktur einschließlich fest angebrachter Verkehrszeichen
– Verkehrsdaten (§ 2 Nr. 7 IVSG), d. h. Daten zum tatsächlichen Zustand des Straßenverkehrs (z. B. Glatteis, Staus)
– Reisedaten (§ 2 Nr. 8 IVSG), mit denen Informationen für Planung, Buchung und Anpassung der Reise bereitgestellt werden (z. B. Fahrpläne oder Tarife, vermutlich auch z. B. Mautstrecken).

3.6.2 Zulässigkeit nach Art. 6 Abs. 1 Satz 1 EU-DSGVO

Neben der Einwilligung stellt Art. 6 Abs. 1 Satz 1 EU-DSGVO die wichtigste Ermächtigungsgrundlage für die Datenverarbeitung dar. Ist eine der dort geregelten Varianten einschlägig, ist ein Umgang mit personenbezogenen Daten auch ohne Einwilligung der betroffenen Person zulässig.

3.6.2.1 Vertragsdurchführung, Art. 6 Abs. 1 Satz 1 lit. b EU-DSGVO

Nach Art. 6 Abs. 1 Satz 1 lit. b EU-DSGVO ist der Umgang mit personenbezogenen Daten zur Erfüllung eigener Geschäftszwecke gestattet, wenn dies zur Erfüllung eines Vertrages, also der Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich ist.

Diese Variante dürfte beispielsweise bei *Bewegungsdaten* in Konstellationen relevant sein, in denen Vertragsinhalt eine Mobilitätsdienstleistung ist, wozu dann auch deren automatisierte Durchführung zählt. Besitzt der Fahrer das Auto dagegen – sei es als Eigentum, im Rahmen eines Leasingvertrags o. ä. – jedoch zur dauerhaften Nutzung, dann ist die Nutzung von Bewegungsdaten nicht schon durch Art. 6 Abs. 1 Satz 1 lit. b EU-DSGVO gedeckt, da sie zur Erfüllung des Vertragszwecks nicht erforderlich sind. Im Hinblick auf *Zustands- und Verhaltensdaten* kommt die Tatbestandsalternative z. B. bei Telematik-Tarifen oder für die Einhaltung bestimmter vertraglich vereinbarter Garantieleistungen (Verschleiß von Fahrzeugteilen) in Betracht, wobei sich allerdings – auch mit Blick auf die Möglichkeiten einer Profilbildung und der Erfassung weiterer Personen, die nicht Vertragspartner sind – in der Regel eine Einwilligung empfehlen dürfte. Einige Versicherer wählen sogar den Weg einer zusätzlichen Pseudonymisierung mit einem zwischengeschalteten Vermittler. Auch im Bereich der *Komfortdaten*, beispielsweise für personalisierte Werbung, wird in der Regel nur bei einer vorübergehenden Nutzung (Mietwagen etc.) eine entsprechend klare und nicht überraschende Festlegung im Vertrag (bspw. günstigere Konditionen mit „Werbeeinblendungen“, wie etwa bei Gratis-Apps) in Betracht kommen; ansonsten empfiehlt sich eine ausdrückliche Einwilligung.

3.6.2.2 Berechtigtes Interesse des Verantwortlichen, Art. 6 Abs. 1 Satz 1 lit. f EU-DSGVO

Art. 6 Abs. 1 Satz 1 lit. f EU-DSGVO enthält eine weitreichende Generalklausel. Danach ist der Umgang mit personenbezogenen Daten für die Erfüllung eigener Geschäftszwecke zulässig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Die Zulässigkeit der Datenverarbeitung wird in diesem Fall im Rahmen der Interessenabwägung ermittelt. Diese Variante erfasst z. B. Erkenntnisse aus Bewegungsdaten und einzelnen Zustandsdaten über Unfallursachen zur Verbesserung des Produkts bzw. Gesamtsystems (vgl. auch Unfalldatenspeicher unten).

3.6.2.3 Umgang mit allgemein zugänglichen Daten

Nach der bisher geltenden Rechtslage war die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erlaubt, wenn die Daten allgemein zugänglich sind, die verantwortliche Stelle sie veröffentlichen dürfte und die schutzwürdigen Interessen der betroffenen Person am Ausschluss der Verarbeitung gegenüber dem berechtigten Interesse der verantwortlichen Stelle nicht offensichtlich überwiegen (§ 28 Abs. 1 Nr. 3 BDSG). Diese Variante hat keine Entsprechung in der DSGVO gefunden. Lediglich in einem anderen Kontext findet sich der Begriff der „allgemein zugänglichen Quelle“ (Art. 14 Abs. 2 lit. f EU-DSGVO). Die Literatur geht aber davon aus, dass die Fälle, die unter § 28 Abs. 1 Nr. 3 BDSG fielen, weitgehend von Art. 6 Abs. 1 Satz 1 lit. f EU-DSGVO erfasst sein werden.

Der Tatbestand dürfte im Übrigen für die Gesamtheit der im Fahrzeug erzeugten Daten kaum eine Rolle spielen, sondern ggf. für diejenigen Informationen (Bewegungsdaten), die von außen erfasst werden (z. B. Verkehrsüberwachung).

Um eine möglichst geringe Menge an Daten zu speichern und gleichzeitig neue, datenbasierte Geschäftsmodelle nicht zu behindern, sind unter Einbeziehung von Wirtschaft und Wissenschaft tragfähige *Konzepte zur Qualifizierung von Daten*, die im automatisierten Straßenverkehr erhoben werden, zu entwickeln: Eine Einteilung in solche Daten, die für die Sicherheit und Funktionalität zwingend notwendig sind, und jene, die zusätzlichen Services und der Komforterhöhung dienen, ist dabei wichtig. Sie trägt dazu bei, die Anforderung von Privacy by Design und Privacy by Default für die Fahrzeughersteller zu konkretisieren sowie die Entwicklung von opt-in / opt-out Funktionalitäten, auf deren Basis individuelle Services für die Anwender geschaffen werden können, zu ermöglichen (vgl. oben, 3.5).

Forderung

Um den automatisierten Verkehr sicher zu gestalten, benötigen die Fahrzeuge eine Kommunikation sowohl mit Infrastruktur und Backend als auch mit anderen Fahrzeugen (z. B. zur Meldung entsprechender Gefahren durch vorausfahrende Autos). Es ist daher zwischen Daten zu unterscheiden, die für die Sicherheit und Funktionalität zwingend notwendig sind, und jenen, die zusätzlichen Services und der Komforterhöhung dienen.

Die für Sicherheit und Funktionalität notwendigen Daten müssen auf gesetzlicher Grundlage zur Verfügung gestellt werden. Statt diese von vornherein als nicht personenbezogen zu definieren, empfiehlt es sich, eine Pflicht zur Übermittlung zu statuieren, verbunden mit der Vorgabe, diese Daten sicher zu anonymisieren bzw. pseudonymisieren. Dadurch wird auch ein wirksamerer Schutz weiterer Verkehrsteilnehmer (z. B. Passanten) gewährleistet. Eine Einwilligung ist dann nicht mehr erforderlich.

3.6.3 Einwilligung

Liegt eine Einwilligung des Betroffenen vor, ist die Erhebung und Verarbeitung personenbezogener Daten zulässig. Es gilt der Grundsatz der informierten Einwilligung (Art. 6 Abs. 1 Satz 1 lit. a i.V.m. Art. 7 EU-DSGVO). Der Betroffene muss demzufolge die Tragweite seiner Entscheidung vorhersehen können, also grundsätzlich genau wissen, was mit seinen personenbezogenen Daten geschehen soll. Die Einwilligung muss fundiert, transparent und verständlich gestaltet sein, wie dies Art. 12 EU-DSGVO zum Ausdruck bringt. In der Praxis entstehen dadurch nicht unerhebliche Hürden – zumal, wenn zum Zeitpunkt der Datenerfassung noch nicht genau bekannt ist, wofür die Daten später verwendet werden sollen.

Eine pauschale datenschutzrechtliche Einwilligungserklärung beim Kauf, mit der der Käufer eine Zustimmung zum vollumfänglichen Datenzugriff geben soll, reicht als Grundlage für spätere Eingriffe daher grundsätzlich nicht aus. Zielführender wäre es, wie bei Software (z. B. bei der Aktualisierung von Apps für Smartphones) den Fahrzeugnutzer vom Senden / Empfangen von Daten zu unterrichten und dabei seine Zustimmung einzuholen.

Im Hinblick auf andere Verkehrsteilnehmer (bspw. Passanten) ist es allerdings faktisch unmöglich, eine Einwilligung einzuholen. Insoweit wird die Lösung also regelmäßig nur in einer Anonymisierung liegen können, bzw. in Modellen, bei denen von vornherein keine sensiblen Daten (z. B. Kameraaufnahmen von Gesichtern) gespeichert werden, sondern nur die vom Sensor erfassten Informationen (z. B. Mensch / Größe / Gewicht / Bewegungsrichtung und -geschwindigkeit).

Die Gestaltung und Umsetzung von Einwilligungsprozessen stellen eine große Herausforderung dar; bei guter Umsetzung können sie aber auch zur Vertrauensbildung beitragen (vgl. auch oben, Privacy by Design) und zu einem echten Vorteil des Anbieters im Wettbewerb werden. Grundsätzlich kann die Einwilligung durchaus mit spielerischen Elementen gestaltet sein (Stichwort Gamification).

Die EU-Datenschutz-Grundverordnung enthält aber auch weitergehende Regelungen zur Rechtswirksamkeit einer Einwilligung. Danach gilt eine Einwilligung als nicht freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist (differenzierte Einwilligung, vgl. Art. 7 Abs. 4 und Erwägungsgrund 43). Die Unfreiwilligkeit der Einwilligungserteilung wird ferner vermutet, wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist (Koppelungsverbot).

3.6.3.1 Einwilligung in künftige Nutzung

Bei Datenverarbeitungsvorgängen muss auch der Grundsatz der Zweckbindung beachtet werden. Der Grundsatz besagt, dass die Datenverwendung aufgrund eines Gesetzes oder einer Einwilligung nur zu einem bestimmten *Zweck zulässig ist*, der klar und präzise bestimmt sein muss. Diese Zweckfestsetzung ermöglicht dem Betroffenen bzw. dem Gesetzgeber eine präventive Zulassungskontrolle der Datenverwendung. Problematisch sind daher Einwilligungserklärungen, die eine Rechtsgrundlage für die künftige Nutzung der Daten darstellen sollen. In der Praxis entstehen dadurch nicht unerhebliche Hürden insbesondere für neue Geschäftsmodelle, da im Zeitpunkt der Erteilung der Einwilligung oft noch nicht absehbar sein wird, welche Daten für welche Zwecke genutzt werden sollen. Das gilt insbesondere für Big Data Anwendungen, die im Zusammenhang mit dem automatisierten und vernetzten Fahren stetig an Bedeutung gewinnen werden. Grundsätzlich muss auch eine allgemeine Einwilligung des Betroffenen „in künftige Big-Data-Anwendungen“ rechtlich zulässig sein, wenn ihm nur hinreichend transparent und verständlich vermittelt wird, dass das konkrete Geschäftsmodell sowie Verwendungsart und Methoden noch nicht feststehen. Wer seine Daten – beispielsweise, um im Gegenzug eine kostenlose Anwendung nutzen zu können – in dieser Weise für eine spätere Verwendung freigeben möchte, der muss im Rahmen seiner allgemeinen Handlungsfreiheit grundsätzlich die Möglichkeit haben, dies vertraglich zu regeln. Das sollte erst Recht für die kontinuierliche Datenübermittlung gelten, so dass nicht bei jedem einzelnen Datenübermittlungsvorgang erneut eine Einwilligung erteilt werden muss, solange zu Beginn transparent über die laufende Übermittlung informiert wurde. Sobald allerdings im Vergleich zu der ursprünglich absehbaren Nutzung der Daten eine Änderung vorgenommen werden soll, die aus Sicht des Betroffenen als überraschend zu werten ist, muss er darüber informiert werden, um seine Einwilligung widerrufen bzw. erneuern zu können.

3.6.3.2 Einwilligung bei autonomen Entscheidungen des Kfz

Ein autonom fahrendes Fahrzeug wird nicht nur eigenständig fahren, sondern damit zugleich auch „entscheiden“, welche (auch personenbezogenen) Daten wann erhoben und ggf. übermittelt werden. Automatisierte Einzelfallentscheidungen, d. h. Entscheidungen, die ohne inhaltliche Bewertung durch eine natürliche Person erfolgen, werden bereits heute in vielen Situationen vom Fahrzeug getroffen. Mit zunehmenden Grad an Automatisierung wird die Relevanz dieser Entscheidungen steigen, für die im Einzelfall keine besondere Einwilligung vorliegt. Vielmehr ist bei der Entscheidung für die Aktivierung der Funktion „autonomes Fahren“ davon auszugehen, dass damit zugleich die Einwilligung in die Datenerhebung und ggf. -übertragung erteilt werden soll. Aus Art. 22 EU-DSGVO ergeben sich im Hinblick auf den Primärzweck in aller Regel keine besonderen Einschränkungen, da es hier nur um die automatisierte Datenübermittlung als solche geht, die für sich betrachtet noch keine rechtliche Folge für den Betroffenen auslöst. Anders kann dies zu beurteilen sein, wenn Daten für Sekundärzwecke übermittelt werden und bspw. im Rahmen eines Telematik-Tarifs eine automatisierte Vertragsanpassung auslösen würden.

Forderung

Eine Einwilligung in künftige Nutzung der Daten muss möglich sein. Der Schutz des Persönlichkeitsrechts des Betroffenen kann dadurch gewährleistet werden, dass dem Betroffenen ein Widerrufsrecht eingeräumt wird, wie es auch in Art. 7 Abs. 3 EU-DSGVO geregelt ist. Damit er seine Abwehrrechte ausüben kann, ist er jedenfalls über im Vergleich zum ursprünglichen Verwendungszweck überraschende geplante neue Nutzungen zu informieren.

3.6.3.3 Sonderfall Dienstfahrzeuge

Eine weitere datenschutzrechtliche Besonderheit ergibt sich, wenn der Eigentümer des Fahrzeugs nicht identisch mit dem Halter oder dem tatsächlichen Nutzer des Fahrzeugs ist. Eine solche Fallkonstellation liegt regelmäßig vor, wenn der Arbeitgeber seinen Arbeitnehmern einen Dienstwagen zur Verfügung stellt und dieser das Fahrzeug wie sein eigenes nutzen darf, ohne Eigentümer bzw. Halter zu sein. Das ist insbesondere dann der Fall, wenn das Fahrzeug als Gehaltsbestandteil überlassen wird.

Für das Arbeitsverhältnis gilt: Erfolgt die Fahrzeugnutzung rein dienstlich, so kann die Nutzung der erhobenen Daten für die Durchführung des Arbeitsverhältnisses erforderlich sein. In diesem Fall richtet sich die Zulässigkeit der Datenerhebung und -nutzung nach Art. 88 EU-DSGVO, § 26 BDSG 2018. Eine hiermit verbundene Kontrolle der Arbeitnehmer durch den Arbeitgeber ist im Einzelnen umstritten. Beispielsweise darf die Verwendung von GPS-Ortungssystemen bei Montagefahrzeugen nicht zu einer Totalkontrolle der Arbeitnehmer führen.

Bei zulässiger Privatnutzung kann die Datenerhebung und -nutzung nur aufgrund einer wirksamen Einwilligung erfolgen. Der Arbeitgeber als Eigentümer bzw. Halter des Fahrzeugs kann nicht wirksam in die Nutzung der Daten des Arbeitnehmers einwilligen. In diesem Fall bedarf es entweder einer Einwilligung des Arbeitnehmers oder die Erhebung und Nutzung der Daten muss für die Durchführung eines Vertragsverhältnisses erforderlich sein. Dies ist beispielsweise bei einem Telematik-Versicherungsvertrag vorstellbar, in Bezug auf die hierfür notwendigen Daten.

Denkbar wäre auch eine Lösung, bei der nach jedem Starten des Fahrzeugs der Fahrer durch die Auswahl technischer Einstellungen (z. B. durch Setzen eines Häkchens) in die Erhebung und Nutzung seiner Daten einwilligen könnte. Die EU-DSGVO akzeptiert diese Form der Einwilligung. Grenzen können sich allerdings im Hinblick auf die praktische Umsetzbarkeit bzw. Akzeptanz durch die Fahrer ergeben; derartige Lösungen müssten jedenfalls so ausgestaltet sein, dass der Zeitverlust so gering wie möglich gehalten wird.

3.7 Anonymisierung / Pseudonymisierung

Die Zulässigkeit einer Verwendung personenbezogener Daten kann auch über eine Anonymisierung oder Pseudonymisierung erreicht werden, da die Datenschutzvorschriften der EU-DSGVO auf die – erfolgreich – entsprechend bearbeiteten Daten keine Anwendung mehr findet.

Die EU-DSGVO verlangt anders als noch § 3 Abs. 6 BDSG keine Einwilligung für eine Pseudonymisierung. Art. 4 Nr. 5 EU-DSGVO konkretisiert nur deren Anforderungen, führt aber mit der Bedingung, dass die „Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die die Nichtzuordnung zu einer bestimmten oder bestimmbaren Person gewährleisten“ eine neue Unsicherheit ein: Ob eine gesonderte Aufbewahrung in Zeiten von Cloud Computing und Big Data überhaupt noch vorstellbar ist, ist zweifelhaft.

Es ist daher klarzustellen, dass eine Anonymisierung und Pseudonymisierung bereits erhobener Daten ohne erneute Einwilligung des Betroffenen erfolgen können, da der Zweck gerade in einer Beendigung des Personenbezugs und damit der datenschutzrechtlichen Bindungen besteht. Dadurch wird zugleich ein Anreiz geschaffen, bei Datenbeständen vor Durchführung (weiterer) Analysen oder Übermittlung an Dritte den Personenbezug zu lösen, was per se das Schutzniveau für den Einzelnen erhöht. Das Risiko eines Fehlschlagens der Anonymisierung oder Pseudonymisierung ohne Einwilligung muss allerdings – wie heute auch – der Nutzer der Daten tragen. Selbst dort, wo diese Risiken im Augenblick fernliegend erscheinen, kann sich die Realisierungswahrscheinlichkeit infolge der rasanten Technologieentwicklung – auch durch das Innovationspotenzial von Big-Data-Analysen – in Zukunft ändern, ohne dass die Wiederherstellung des Personenbezugs mit einem „unverhältnismäßig großen Aufwand“ verbunden wäre.

Wer sich dagegen absichern will, was etwa bei Gesundheitsdaten oder anderen sensiblen Informationen, die die Auswertung in Form der Mustererkennung, Kategorisierung oder Erstellung von Profilen ermöglichen, ratsam sein kann, dem steht es auch nach einer gesetzgeberischen Klarstellung frei, eine Einwilligung des Betroffenen einzuholen. Wenn sensible Daten an Dritte für deren Analysen übermittelt werden oder in der Datennutzung eine aus Sicht der Betroffenen fernliegende, überraschende Zweckänderung liegt, empfiehlt sich in jedem Fall eine ausdrückliche Information und Einwilligung.

Forderung

Anonymisierung und Pseudonymisierung müssen ohne (erneute) Einwilligung des Betroffenen möglich sein.

3.8 Grenzen der Datennutzung

Eine Profilbildung durch den Hersteller oder sonstige Dienstleister, die (berechtigt) Zugriff auf Daten erhalten, muss grundsätzlich durch Anonymisierung ausgeschlossen werden, wenn der Fahrer/Halter keiner entsprechenden Nutzung zugestimmt hat.

Teilweise werden auch heute schon gesundheitsbezogene Daten erhoben, wenn das System etwa den Fahrer vor Müdigkeit warnen soll. Mit zunehmendem Einzug von Big Data in die medizinische Diagnose werden auch die daraus ziehbaren Rückschlüsse immer weitreichender. Eine Speicherung kann nicht ohne den ausdrücklichen Willen des Betroffenen in Betracht kommen, von einer automatischen Übertragung etwa in die Cloud ganz zu schweigen (§ 203 I Nr. 1 StGB).

3.9 Autonomes Fahren im Kontext der ePrivacy-Verordnung

Ein wichtiger Bestandteil des autonomen Fahrens ist der Austausch von Informationen zwischen den Fahrzeugen, und zwar durch entsprechende Programmierung ohne menschliches Zutun im Zeitpunkt des Informationsaustauschs („Maschine-zu-Maschine-Kommunikation“). So können etwa Informationen zum Straßenzustand, den der Sensor eines Fahrzeugs erfasst hat, unmittelbar per Funksignal an die Bordcomputer aller in der Nähe befindlichen Fahrzeuge übertragen werden. Ebenso können die Informationen zur Abstandsmessung durch die jeweiligen Sensoren an den Fahrzeugen wechselseitig validiert werden, um jeglichen Kollisionskurs zu vermeiden. Durch den Datenaustausch zwischen Fahrzeugen ist ein autonomes Agieren der Systeme dementsprechend erst möglich.

Mit dem Entwurf der Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG hat die Europäische Kommission eine Diskussion über die Vertraulichkeit der Kommunikation angestoßen. Der vorgelegte Verordnungsvorschlag ePrivacy-VO soll die Richtlinie von 2002 (2002/58/EG) modernisieren. Die ePrivacy-VO ist ergänzend im Licht der im Mai 2018 in Kraft tretenden Datenschutz-Grundverordnung (DS-GVO) zu sehen. Als Verordnung wird sie unmittelbar in den Mitgliedstaaten Anwendung finden.

Zielsetzung der Richtlinie aus dem Jahre 2002 war der Schutz der Privatsphäre und personenbezogener Daten im Bereich der elektronischen Kommunikation. Neben der Vertraulichkeit der Kommunikation (von Endgeräten und Webseiten) sind Sicherheitsaspekte, Berichtspflichten bei Datenschutzverstößen sowie Vorschriften zur Nutzung von Cookies wichtige Regelungsaspekte.

Die ePrivacy-VO soll die bisher geltende Datenschutzrichtlinie für elektronische Kommunikation ablösen. Sie hat somit, ebenso wie die Datenschutz-Grundverordnung, die Achtung des Privatlebens und den Schutz personenbezogener Daten zum Ziel. Allerdings beziehen sich die Vorschriften spezifisch auf die elektronische Kommunikation

und die Verarbeitung elektronischer Kommunikationsdaten durch Betreiber elektronischer Kommunikationsdienste. Diesbezüglich werden die datenschutzrechtlichen Regelungen der ePrivacy-VO der EU-DSGVO wohl vorgehen, vgl. Art. 95 DS-GVO. Dennoch schafft die Verordnung weitere Unklarheiten, zumal eine Abgrenzung zwischen dem Anwendungsbereich der ePrivacy-VO und der EU-DSGVO weitere Konflikte mit sich bringt, insbesondere da beide Verordnungen über eigene Speicher- und Löschvorschriften verfügen.

Darüber hinaus erweitert der Entwurf der ePrivacy-Verordnung den Adressatenkreis in einem nicht mehr vertretbaren Maße. Der Entwurf der ePrivacy-Verordnung erweitert den Schutz auch auf Inhalte einer Maschine-zu-Maschine-Kommunikation (M2M). Die Anwendung der ePrivacy-Verordnung auf Maschine-zu-Maschine-Kommunikation würde den für die Weiterentwicklung und Umsetzung des autonomen Fahrens erforderlichen Datenaustausch erheblich einschränken. Denn der Verordnungsentwurf stellt im Ergebnis eine M2M-Kommunikation mit der Kommunikation zwischen Menschen gleich. So dürften die zwischen Maschinen ausgetauschten Informationen nicht bzw. nur unter den Bedingungen der Art. 5 ff. ePrivacy-VO verarbeitet werden – es gilt das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass Informationen nur dann verarbeitet werden dürfen, wenn die Beteiligten ihre Einwilligung gegeben haben. Wie die Erteilung einer Einwilligung im Bereich des autonomen Fahrens, wo der Datenaustausch zwischen den Fahrzeugen unabdingbar ist, erfolgen soll, ist absolut unklar.

Zudem ist zum Teil völlig unklar, an welchen Stellen die ePrivacy-VO die DS-GVO präzisiert bzw. ergänzt. Verschärft wird diese Abgrenzungsproblematik auch dadurch, dass in vielen Fällen die Unterscheidung von personenbezogenen und nicht personenbezogenen Kommunikationsdaten unmöglich ist.

Die Unübersichtlichkeit der datenschutzrechtlichen Vorschriften im europäischen Raum kann Innovationen behindern. Gleichsam beinhaltet die ePrivacy-VO Spezifizierungsklauseln, so dass die einzelnen Mitgliedstaaten teilweise eigenständige Regelungen im Umfeld der Verordnung regeln dürfen, weswegen die elektronische Kommunikation einem diversifizierten Rechtsrahmen innerhalb der europäischen Union unterliegen wird. Das ist einer abgestimmten Entwicklung des autonomen Fahrens in Europa abträglich.

Darüber hinaus darf nicht außer Acht gelassen werden, dass die ePrivacy-VO teilweise Verunsicherung statt Rechtssicherheit schafft. Insbesondere kann eine mangelnde Verständlichkeit kritisiert werden. Statt eigener Begriffsdefinitionen verweist Art. 4 ePrivacy-VO zur Begriffsbestimmung auf andere europäische Legislativakte. Hierdurch wird die Verordnung intransparent. Gleichsam bleibt der europäische Gesetzgeber bei seinen Begriffsbestimmungen sehr vage, so dass für die Rechtsanwender teilweise nicht ersichtlich ist, ob sie unter den Anwendungsbereich der Verordnung fallen.

Durch die in den Mitgliedstaaten unmittelbar geltenden Verordnungen soll eine Harmonisierung des digitalen Binnenmarktes erreicht werden. Da über die von einer Person besuchten Webseiten ein umfangreiches Persönlichkeitsprofil erstellt werden kann,

enthält die Verordnung ein sehr hohes Schutzniveau (Erwägungsgrund 2 der ePrivacy-VO). Während dieses hohe Schutzniveau partiell gerechtfertigt ist, stellt sich die Frage, warum die Übermittlung von Daten zwischen Maschinen genau dem gleichen Schutzniveau unterfallen sollen, zumal die ausgetauschten Daten zumeist keinen Personenbezug aufweisen.

Die erfolgte Generalisierung im Umgang mit Daten zeigt einen Wandel vom Schutz personenbezogener Daten hin zu einem Schutz von faktisch allen von der Europäischen Union als schutzbedürftig eingestuften Daten. Somit entsteht im Rahmen der elektronischen Kommunikation ein umfassender, buchstäblicher „Daten"schutz, der allerdings partiell über das Ziel hinausschießt. Die ursprüngliche Aufgabe des Datenschutzrechts war der Schutz der Person, die sich hinter den Daten verbirgt und nicht der Schutz von Daten als Selbstzweck.

Es ist selbstverständlich wichtig, dass das Datensicherheitsniveau insoweit abgesichert ist, dass Dritte nicht in eine Datenübermittlung eingreifen und diese verändern können. Dies betrifft auch die Kommunikation unter Maschinen. Allerdings dürfen zu strenge Anforderungen neue Innovationen nicht unterbinden. Deshalb muss eine zielgerichtete Kommunikation unter autonom agierenden Systemen weiterhin möglich sein und es dürfen keine den autonomen Verkehr einschränkenden rechtlichen Hindernisse erzeugt werden.

Es bedarf differenzierter Regelungen, die einerseits den im Einzelfall vorhandenen Gefahren für die Persönlichkeit Rechnung tragen, andererseits aber auch kein „Show-Stopper" der gewollten Digitalisierung und Vernetzung sind.

Die Bayerische Wirtschaft bekennt sich zu den von der DS-GVO geschaffenen Datenschutz- und Vertraulichkeitsstandards in der digitalen Wirtschaft. Die DS-GVO zielt auf einen ausgewogenen Kompromiss zwischen dem Schutz personenbezogener Daten und dem Innovationpotenzial für zukünftige Geschäftsmodelle ab.

Forderung

Aus Sicht der vbw – Vereinigung der Bayerischen Wirtschaft e. V. werden die Sachverhalte, die durch die ePrivacy-VO geregelt werden sollen, bereits durch die DS-GVO erfasst. Eine zusätzliche sektorspezifische Regelung für den Telekommunikationsbereich ist daher überflüssig. Zumindest darf die ePrivacy-VO keine schärferen Regelungen enthalten als die Datenschutz-Grundverordnung. Es darf nicht zur Entstehung von zwei verschiedenen Datenschutzregimes kommen.

---

4 Zivil- und strafprozessuale Verwertung von Daten

Unklarheiten beseitigen und Rechtssicherheit schaffen

Es sind klare Richtlinien dazu erforderlich, inwieweit eine gerichtliche Verwertbarkeit der durch automatisierte Fahrzeuge generierten Daten möglich ist. Dies leistet einen wesentlichen Beitrag zur gesellschaftlichen Akzeptanz automatisierter Verkehrssysteme in der Bevölkerung.

4.1 Sicherstellung und Beschlagnahme von Daten, Verfolgung von Ordnungswidrigkeiten

Verkehrsverstöße bzw. Verkehrsunfälle können strafrechtlich relevantes Verhalten enthalten. Die im Fahrzeug erhobenen Daten könnten aber auch zur Aufklärung von anderen Straftaten genutzt werden, z. B. für die Klärung der Frage, wo oder mit wem sich der einer Straftat Verdächtige zu einem bestimmten Zeitpunkt aufgehalten hat. Mit den Fahrzeugdaten, insbesondere den jeweils gefahrenen Geschwindigkeiten sowie dem Abstand zum vorausfahrenden Fahrzeug, könnten ferner Ordnungswidrigkeiten belegt und geahndet werden.

Freiwillig wird der Fahrer bzw. Halter diese Daten in aller Regel nicht zur Verfügung stellen wollen, so dass eine Einwilligung ausscheidet. Werden Daten beispielsweise für die sichere Durchführung des automatisierten Fahrens laufend aus dem Fahrzeug heraus übermittelt, so ist eine Nutzung für die Verfolgung von Ordnungswidrigkeiten etc. auch nicht von der Zweckbestimmung gedeckt.

Außerdem findet sich auch im novellierten Straßenverkehrsgesetz (StVG) eine Regelung über die Zulässigkeit der Übermittlung von Daten. Gemäß § 63 a Abs. 2 StVG dürfen Positions- und Zeitangaben, die einen Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System protokollieren, an die für die Ahndung von Verkehrsverstößen zuständigen Behörden übermittelt werden.

Auch Daten können allerdings Gegenstand einer Beschlagnahme nach § 94 StPO sein. Die Zulässigkeit der Sicherung und die Herausgabepflicht von Fahrzeugdaten bzw. -datenträgern richtet sich in Strafverfahren nach den §§ 94, 95 und 98 StPO. Diese gelten sinngemäß grundsätzlich auch in Bußgeldverfahren, wobei hier insbesondere der Grundsatz der Verhältnismäßigkeit zu wahren ist.

Fraglich ist allerdings, bei wem (Halter, Hersteller, Diensteanbieter) eine Beschlagnahme erfolgen kann. Da die meisten Hersteller ihre Daten verschlüsseln und in der Regel nicht bereit sein werden, Daten zu entschlüsseln, die ihre Kunden belasten könnten, stellt sich die Frage, ob der Hersteller im Rahmen der Regelungen der StPO

zur Entschlüsselung der Daten verpflichtet werden kann. Zu klären ist ferner, wie Aussageverweigerungsrechte und der Grundsatz der Selbstbelastungsfreiheit dabei zu berücksichtigen sind, beispielsweise auch im Fall einer automatischen Übermittlung von Unfallinformationen.

Grundsätzlich kommt auch eine Bestandsdatenabfrage beim Hersteller nach § 113 TKG und eine TKÜ Maßnahme nach § 100 a StPO in Betracht, ggf. auch eine akustische Überwachung nach § 100 f StPO, wobei dann allerdings immer sämtliche Insassen betroffen sind. Sehr fraglich ist allerdings, ob ein mit einer SIM-Karte ausgestattetes Kfz ein Mobilfunkendgerät nach § 100 i StPO ist.

Forderung

Unklarheiten bei der strafprozessualen Datenverwertung muss der Gesetzgeber beseitigen und Rechtssicherheit schaffen.

Alleine durch die technische Möglichkeit dürfen die bewährten strafprozessualen Grundsätze nicht in Frage gestellt werden. Dies gilt insbesondere für den Grundsatz nemo tenetur.

4.2 Zivilprozessuale Verwertung von Daten

Andere Verkehrsteilnehmer und deren Versicherungsgesellschaften können ein Interesse daran haben, im Falle eines Unfalls die im Fahrzeug gespeicherten oder von diesem an einen Dritten übermittelten Daten in einem Zivilverfahren zu verwenden. So könnte bei einem Verkehrsunfall die Schuldfrage schnell geklärt werden.

Nach geltenden Recht kann ein Unfallbeteiligter die Vorlage entsprechender Daten nur im Rahmen eines entsprechenden zivilrechtlichen Verfahrens gemäß § 142 ZPO verlangen. Vorlagepflichtig ist derjenige, der im Besitz der Daten ist. Die Vorlage der Daten kann nicht nur vom Halter bzw. Eigentümer des Fahrzeugs verlangt werden, sondern auch von einem Dritten. Ein Dritter im Sinne des Gesetzes kann auch der Fahrzeughersteller sein, wenn er diese Daten besitzt. Das Vorlageverlangen darf nicht die Grenzen der unzulässigen Ausforschung überschreiten. Die widerrechtliche Verwendung der Daten führt zu einem Beweisverwertungsverbot.

Eine neue Regelung zur Verwertung von im Rahmen des Betriebs eines automatisierten Fahrzeugs entstandenen Daten hat in § 63a Abs. 3 StVG ihren Eingang gefunden. Gemäß § 63 a Abs. 3 StVG ist der Fahrzeughalter verpflichtet, die Übermittlung von Positions- und Zeitangaben an Dritte zu veranlassen, wenn die Daten zur Geltendmachung, Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit einem Unfall im Sinne von § 7 Abs. 1 StVG erforderlich sind und das entsprechende Kraftfahrzeug mit automatisierter Fahrfunktion an diesem Ereignis beteiligt war.

Forderung

Aus Sicht der vbw darf die Möglichkeit der Datenauswertung nicht zur Verschlechterung der zivilprozessualen Position des Betroffenen führen. Auch wenn die Technik eine schnelle Klärung der Schuldfrage ermöglicht, sollten der Beibringungsgrundsatz sowie die Grundsätze der Beweislastverteilung unangetastet bleiben.

4.3 Sonderfall Unfalldatenspeicherung

Mit Inkrafttreten des achten Gesetzes zur Änderung des Straßenverkehrsgesetzes am 21. Juni 2017 ist das Straßenverkehrsgesetz um Regelungen zum automatisierten Fahren ergänzt worden. Im Mittelpunkt des Gesetzes stehen insbesondere Vorschriften über die Zulässigkeit und Voraussetzungen des automatisierten Fahrens, die Pflichten des Fahrzeugführers und den Schutz personenbezogener Daten.

Das novellierte Straßenverkehrsgesetz sieht vor, dass Fahrzeuge, die mittels hoch- oder vollautomatisierter Fahrfunktion betrieben werden, die durch ein Satellitennavigationssystem ermittelten Positions- und Zeitangaben speichern müssen, wenn ein Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System erfolgt. Die Speicherung von Positions- und Zeitangaben muss auch dann erfolgen, wenn der Fahrzeugführer durch das System aufgefordert wird, die Fahrzeugsteuerung zu übernehmen oder eine technische Störung des Systems auftritt.

In diesem Zusammenhang wird die Frage diskutiert, in welcher Weise und insbesondere an welchem Ort die Speicherung der Daten erfolgen soll. Diese Frage lässt das Gesetz unbeantwortet und enthält in § 63 b StVG lediglich eine Ermächtigungsgrundlage für das Bundesministerium für Verkehr und digitale Infrastruktur zur technischen Ausgestaltung des Speichermediums, zur Regelung des Orts des Speichermediums sowie zur Art und Weise der Datenspeicherung. Denkbar ist die Einführung einer Pflicht zum Einbau eines Datenaufzeichnungsgerätes („Black Box“) im Fahrzeug selbst, oder aber eine Speicherung im Wege der Datenübertragung in einer "Cloud" zum Beispiel auf einem Server des Fahrzeugherstellers oder -händlers.

Der Datenspeicher für die Beweissicherung muss gegen unberechtigten Zugriff geschützt sein, darf nicht manipulierbar sein und muss sämtliche Zugriffe erkennen lassen. Die Protokollierung der Steuerungseingriffe sollte verschlüsselt und gesichert erfolgen. Ein solcher Speicher muss standardisiert sein.

Zur Nutzung der Unfalldaten gehört auch, sie in geeigneter Weise für die Weiterentwicklung der Fahrassistenzsysteme verfügbar zu machen, um die Verkehrssicherheit laufend zu erhöhen. Die Anforderungen müssen – einschließlich des diskriminierungsfreien Zugangs zu den Unfalldaten bei Vorliegen eines berechtigten Interesses – auf europäischer Ebene normiert werden.

Forderung

Für die Speicherung und Nutzung der im Zusammenhang mit dem Wechsel der Fahrzeugsteuerung zwischen Fahrzeugführer und dem hoch- oder vollautomatisierten System entstandenen Daten sollten datenschutzrechtliche Rahmenbedingungen geschaffen werden.

4.4 Sonderfall „Fernabschaltung“ von Fahrzeugen

Diskutiert wird eine – technisch mögliche – Fernabschaltung etwa für den Fall eines Diebstahls des Fahrzeugs oder im Falle ausstehender Nutzungsgebühren / Leasingraten.

Grundsätzlich wird bei der Verfolgung von Eigentumsdelikten die Erforderlichkeit im Sinne von Art. 6 Abs. 1 Satz 1 lit. b EU-DSGVO zu verneinen sein. Die öffentliche Sicherheit und Ordnung ist im Rahmen der ordnungspolizeilichen Vorschriften durchzusetzen.

Eine wirksame vorherige Einwilligung für den Fall einer Nichtzahlung von Leasingraten ist dagegen denkbar; auch Mobiltelefone werden im Falle einer Nichtbegleichung der Rechnung abgeschaltet. Ob das im Zeitpunkt der Abschaltung noch im Interesse des Nutzers ist, dürfte für eine zunächst vertraglich freiwillig erteilte Einwilligung irrelevant sein. Selbstverständlich darf eine solche „Abschaltung“ ausschließlich im ruhenden Verkehr erfolgen, um eine Gefährdung auszuschließen.

5 IT-Sicherheit

Wirksamer Schutz vor Zugriffen, Angriffen und Manipulation

Die Masse und Komplexität der Daten, die hier gespeichert und verarbeitet werden, erfordern Vorkehrungen zum Schutz der Verfügbarkeit und Integrität, ggf. auch der Vertraulichkeit der Datenbestände. Die IT-Sicherheit hat beim automatisierten und vernetzten Fahren im Hinblick auf die potenziell betroffenen Rechtsgüter einen elementaren Stellenwert. Auch mit Blick auf das Vertrauen der Fahrer bzw. Insassen in einen immer stärker automatisierten Verkehr und in die Zuverlässigkeit der Hersteller ist die Gewährleistung der IT-Sicherheit eine Grundvoraussetzung.

Gleichzeitig dürfen keine überzogenen Anforderungen aufgestellt werden, vgl. insoweit auch *Zukunft automatisiertes Fahren: Rechtliche Hürden beseitigen* (vbw, März 2018).

Am 25. Juli 2015 ist das IT-Sicherheitsgesetz in Kraft getreten. Betreiber kritischer Infrastrukturen aus bestimmten Bereichen müssen danach künftig einen Mindeststandard an IT-Sicherheit einhalten und erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Für den Sektor Informationstechnik und Telekommunikation, der ebenfalls für das automatisierte und autonome Fahren von hoher Relevanz ist, definiert die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) bereits den Anwendungsbereich. Auch die Sektoren Transport und Verkehr fallen in den Anwendungsbereich des IT-Sicherheitsgesetzes. Welche Anlagen genau dazu zählen, bestimmt die Erste Verordnung zur Änderung der KRITIS-Verordnung vom 21.6.2017 (BGBl. I, S. 1903). In Teil 3 Anlagenkategorien und Schwellenwerte, Ziff. 1.4 werden genannt:

– Verkehrssteuerungs- und Leitsystem für das Netz der Bundesautobahnen
– Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr für Städte ab 500.000 Einwohner

Auch wenn diese Regelung noch nicht direkt auf ein (hoch-) automatisiertes bzw. autonomes Fahren abzielt, wird bereits deutlich, dass eine entsprechende IT-Infrastruktur unter die erhöhten Anforderungen des IT-Sicherheitsgesetzes fallen wird.

5.1 Funktionale Sicherheit

Hard- und Softwarearchitekturen sollten eine Trennung von Fahrzeugfunktionen und Infotainment-, Telematik- und Navigationsanwendungen vorsehen. Das gilt umso mehr, als Fahrzeugfunktionen zunehmend über Apps ausgelöst werden können, die Anzahl von Schnittstellen des Fahrzeugs mit der Umwelt steigt und zunehmenden Fremdsys-

teme in die Fahrzeuge integriert werden. Diesen Weg einer Trennung von sicherheitskritischen und sonstigen Systemen verfolgen die deutschen Hersteller gegenwärtig; er sollte grundsätzlich Teil eines Security by Design Ansatzes sein.

Gleichzeitig ist eine enge Verzahnung von funktionaler Sicherheit und IT-Sicherheit bei der Systementwicklung anzustreben, um die Wechselwirkung abzubilden (vgl. auch unten 5.2).

Für die Entwicklung sicherer Systeme für das automatisierte Fahren müssen IT-Sicherheitsrisiken schon während der Entwicklung methodisch identifiziert, bewertet, und behandelt werden können. Entsprechende Testverfahren werden ebenso zur Überprüfung der identifizierten Risiken in der praktischen Umsetzung benötigt, um sicherzustellen, dass sowohl einzelne Komponenten als auch die Komponenten im Zusammenspiel den IT-Sicherheitsanforderungen genügen. Hierfür sind sowohl eine Weiterentwicklung bestehender Testverfahren als auch geeignete Testfelder erforderlich (vgl. auch *Zukunft automatisiertes Fahren – Rechtliche Hürden beseitigen* und *Automatisiertes Fahren – Infrastruktur*, vbw 2018 und 2016).

5.2 Zugriffschutz und Manipulationssicherheit

Die Schnittstellen an Fahrzeugen mehren sich und bieten ein potenzielles Einfallstor für Angriffe und Manipulation, auch durch den Fahrer selbst (z. B. Tuning). Gleichzeitig sind Schnittstellen notwendig; so müssen neben dem Hersteller auch beispielsweise freie Werkstätten Zugriff auf Fahrzeugsysteme erhalten können.

Ein Zugriff auf Fahrzeuge ist auf verschiedenen Wegen möglich:

– per Steckverbindung (z. B. Einschleusen von Schadsoftware über Testschnittstellen, SIM, USB)
– via Funk (z. B. Hacken der Herstellerschnittstelle, des Entertainment Systems oder des WLAN Schlüssels)
– mittels Übersteuerung von Signalen (z. B Störsender)
– durch Irritation von Sensoren (z. B. Laserstörung des Lidar)

Bei der Entwicklung der multimedialen Schnittstellen durch die Hersteller sollte auch berücksichtigt werden, dass Drittanbieter, die Anwendungen für das Fahrzeug entwickeln, tendenziell ein schwächeres Bewusstsein für Datensicherheit haben werden. Ein vollständiger Schutz wird dabei nicht möglich sein, wenn eine Kommunikation mit Dritten und Schnittstellen gewollt ist. Von einer vollständigen Absicherung gegen Zugriff und Manipulation kann allerdings auch heute keine Rede sein, so dass hieraus keine überzogenen Anforderungen abgeleitet werden dürfen.

Security (IT-Sicherheit) und Safety (Systemsicherheit) müssen grundsätzlich gemeinsam betrachtet werden, weil fehlende IT-Sicherheit Bedrohungspotenziale durch Hacker bietet, welche damit wiederum die Systemsicherheit beeinträchtigen können. Das

gilt beispielsweise im Hinblick auf Standards für Verschlüsselungsprotokolle oder die IT-Sicherheit bei Synchronisierungsvorgängen.

Für die Installation von Software, die auf den sicherheitsrelevanten Bereich zugreift, ist eine elektronische Signatur vorzusehen, die nur nach Prüfung und Freigabe der Software vergeben werden kann. Der Zugriff und der Austausch von Daten (z. B. mit der Werkstatt oder zwischen Fahrzeugen) darf erst nach erfolgreicher Authentifizierung und Autorisierung der Kommunikationspartner über kryptografisch abgesicherte Wege erfolgen (Gateways, Firewalls).

IT-Sicherheitssiegel oder ähnliche Zertifikate sollten aus der Wirtschaft heraus und möglichst mit maßgeblicher Beteiligung der klassischen Automobilhersteller und -zulieferer für Produkte und Prozesse aus dem Bereich des autonomen Fahrens entwickelt werden, die das gebotene Maß an Vertraulichkeit, Verfügbarkeit und Integrität der Daten gewährleisten.

Seitens der Hersteller wird teilweise vertreten, dass keine Zertifizierung erforderlich sei und die Prüfung durch den OEM ausreiche. Vor dem Hintergrund der extremen Bedeutung der IT-Sicherheit gerade im Hinblick auf die weitergehenden Anwendungen in Stufe 4 und 5 (vollautomatisiertes bzw. autonomes Fahren) empfiehlt es sich aber wohl, eine zusätzliche externe und neutrale Prüfinstanz vorzusehen. Das Interesse der heimischen Hersteller an Sicherheit steht außer Frage, garantiert aber keine vergleichbar konsequente Handhabung durch Wettbewerber, die vielleicht das Interesse an zahlreichen zusätzlichen Features / Apps höher gewichten und die Risiken niedriger einschätzen. Realisiert sich ein solches Risiko, sind Rückwirkungen auf das Gesamtsystem (z. B. Vertrauensverlust in vollautomatisierte Fahrzeuge, Rückgang der gesamten Nachfrage) nicht auszuschließen. In Betracht kommt etwa eine Common Criteria Zertifizierung des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die Möglichkeiten einer Zertifizierung der Daten von den in automatisierten Fahrzeugen enthaltenen Algorithmen müssen von Wirtschaft und Wissenschaft gemeinsam entwickelt werden.

Beim Einsatz von Zertifikaten, Signaturen oder ähnlichen Sicherungssystemen muss sichergestellt sein, dass das System in Notfallsituationen noch handlungsfähig bleibt und ein abgelaufenes Zertifikat beispielsweise nicht den Bremsimpuls verhindert.

Jedenfalls mittelfristig sollte auf Basis der entwickelten Standards auch eine eigene Norm für IT-Sicherheit als Zulassungsvoraussetzung für neue automatisiert bzw. autonom fahrende Kfz-Modelle geschaffen werden.

Im Bereich Datensicherheit besteht noch erheblicher *Forschungsbedarf*. Das Querschnittsthema berührt sämtliche Schlüsseltechnologien, zu denen auch intelligente und vernetzte Verkehrssysteme zählen. Gerade kleinere und mittlere Unternehmen haben oft weder finanzielle Möglichkeiten noch ausreichendes eigenes Know-how, um die notwendige Sicherheit von Anfang an zu berücksichtigen. Der Zukunftsrat der Bayeri-

schen Wirtschaft empfiehlt daher ein (bayerisches) Programm „Sicherheit in Schlüsseltechnologien“ mit einem Schwerpunkt auf der Datensicherheit, das zugleich die individuelle wie auch die systemische Sicherheit adressiert (vgl. *Zukunft digital – Big Data, Analyse und Handlungsempfehlungen*, vbw 2016). Ein Ansatz im Bereich des Schutzes vor Hacker-Angriffen beim automatisierten Fahren kann etwa das Maschinelle Lernen (z. B. zur Erkennung von Manipulationen in einer C2X-Kommunikationsinfrastruktur des automatisierten Fahrens) sein.

Seit Anfang 2018 befasst sich eine Forschergruppe unter der Projektleitung von Prof. Dr. Dirk Heckmann (Lehrstuhl für Öffentliches Recht, Sicherheitsrecht und Internetrecht, Forschungsstelle für IT-Recht und Netzpolitik an der Universität Passau) im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mit einer wissenschaftlichen Studie zur IT-Sicherheitsregulierung. Bis Ende 2019 werden Leitlinien zur Verbesserung der IT-Sicherheit durch Regulierung, Deregulierung und Ko-Regulierung entwickelt. Hierbei ist das autonome Fahren eines von vielen Referenzbereichen. Informationen werden über die Projektseite www.it-sicherheitsregulierung.de bereitgestellt.

Forderungen

Für die IT-Sicherheit müssen angemessene, faire und einheitliche Standards entwickelt werden. Ziel ist die Gewährleistung einer vollständigen Ende-zu-Ende Sicherheit von Daten und Kommunikation durch Hersteller, Zulieferer und Dienstleister. Leitgedanke muss Security by Design sein, die IT-Sicherheit muss also bereits in der Konzeptionsphase berücksichtigt werden.

Die Daten im Fahrzeug und im Backend müssen vertrauenswürdig sein, weil auf dieser Basis vorausschauend die Verkehrssituation berechnet wird. Jeder Zugriff und Steuerungseingriff von außen muss manipulationssicher protokolliert werden; insoweit sind, ebenso wie im Hinblick auf die Verwendung sicherer Verschlüsselungsverfahren durch alle Beteiligte, gesetzliche Regelungen zu entwickeln.

Zertifizierungslösungen für Datenverarbeitungsverfahren beim automatisierten Fahren sind durch Wirtschaft und Wissenschaft zu entwickeln. Entsprechende gesetzliche Vorgaben können auch international betrachtet zur Erhöhung der Sicherheit erforderlich sein.

Die Forschung im Bereich der IT-Sicherheit für das automatisierte und vernetzte Fahren muss intensiviert werden.

Da die Konzipierung von möglichst sicheren Fahrzeugen stets eine Momentaufnahme des aktuellen Stands der Technik ist, müssen auch nach der Auslieferung Sicherheits-Updates / Patches zur Behebung von Fehlern zur Verfügung stehen. Das ist Teil der Produktbeobachtungspflicht des Herstellers, dem es obliegt, sich seinerseits vertraglich

gegenüber seinen (IT-)Zulieferern abzusichern. Über entsprechende Hinweise bei Vertragsschluss und ausdrückliche Regelungen sollte sichergestellt werden, dass der Endanwender bereit ist, ein solches Update in den jeweils erforderlichen Zeitabständen durchzuführen bzw. automatisiert „over the air“ durchführen zu lassen.

Auch die Infrastruktur muss gegen unberechtigte Zugriffe und Manipulation abgesichert sein. Das gilt sowohl für Teile der eigentlichen Verkehrs- und Verkehrsleitinfrastruktur als beispielsweise auch für Werkstätten.

6 Kommerzielle Verwertung von Daten

Innovative Geschäftsmodelle ermöglichen

Bei datenbasierten Geschäftsmodellen stellt sich nicht nur die Frage, mit welchen Schutzrechten und Schutzpositionen sich der Einzelne gegen die Erfassung „seiner" Daten wehren kann (Kapitel 3), und wie diese zu sichern sind (Kapitel 5). Vielmehr ist auch zu klären, wie die Verwertung und Vermarktung dieser Daten gestaltet werden kann.

Die EU-DSGVO enthält Regelungen zum Schutz der Privatsphäre des Betroffenen, trifft selbst allerdings keine Aussage über die Zuordnung von Daten. Zudem regelt das Datenschutzrecht nur den Umgang mit personenbezogenen Daten.

Daten sind als immaterielle Informationen nicht eigentumsfähig im Sinne des § 903 BGB. Eigentum kann nur an Sachen (körperlichen Gegenständen) erworben werden. Es gibt Ansätze eine Eigentumsfähigkeit von Daten über eine Analogie zu § 303 a StGB zu konstruieren. Im Deliktsrecht werden Daten im Rahmen von § 823 Abs. 1 BGB auch teilweise als sonstiges Recht begriffen. Bei diesen Rechtsauffassungen handelt sich jedoch um Mindermeinungen, die sich nicht durchgesetzt haben.

Die Einführung eines Dateneigentums oder eines eigentumsähnlichen Rechts daran würde eine künstliche Datenverknappung bewirken und so die Aussagekraft von Datenanalysen sowie die Nutzungspotenziale insgesamt verschlechtern; sie ist daher abzulehnen. Erst wenn sich zeigt, dass alleine über vertragliche Gestaltungen keine interessengerechte Rechtsgestaltung möglich ist, wäre an eine gesetzliche Regelung zur Datenzuordnung zu denken. Zu diesem Ergebnis kommt auch eine 2017 veröffentlichte Studie des Bundesministeriums für Verkehr und Digitale Infrastruktur („Eigentumsordnung" für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive), die de lege lata ein Dateneigentum ablehnt und die faktische Herrschaft über Mobilitätsdaten besonders von Seiten der Kfz-Hersteller thematisiert:

https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaets-daten.pdf?__blob=publicationFile

„Dies führt zwar im Ergebnis nicht zu einer rechtlichen, aber zu einer faktisch starken Position des Herstellers, weil ohne sein Einverständnis und die durch ihn bestimmte technische Gestaltung der Schnittstellen niemand sonst auf die Daten zugreifen kann. Allerdings determiniert diese faktisch starke Position noch nicht die letztendlichen Nutzungsbefugnisse und die Zuordnung der damit verbundenen Gewinne. Trotz der prima facie starken Ausgangsposition kann es nämlich dazu kommen, dass in den sehr komplexen Marktstrukturen starke Nutzerpräferenzen für bestimmte Dienste oder Geräte (wie Smartphones mit ihren Betriebssystemen) sowie globale, marktmächtige Oligopole den Automobilherstellern letztlich die Bedingungen für die Öffnung des Zugangs

zu den Daten diktieren. Wie diese Entwicklung letztlich ausgeht, ist derzeit als offen zu beurteilen.“ (Seite 62)

Grundsätzlich verbrauchen sich Daten auch nicht und können mit mehrfacher Nutzung sogar wertvoller werden. Neue Geschäftsmodelle sollten über den Zugang zu Daten gefördert werden. Anwendungsszenarien mit breitem gesellschaftlichen Nutzen könnten sich beispielsweise für ländliche Regionen (z. B. medizinische Versorgung) ergeben.

Rohdaten sind überdies weder immaterialgüterrechtlich geschützt noch schutzfähig. Vom Urheberrecht abgesehen entstehen die weiteren Immaterialgüterrechte immer erst nach einem gesetzlich genau vorgeschriebenen Publizitätsakt (Veröffentlichung im Patentblatt, Eintragung ins Markenregister usw.). Die Entstehung und Erfassung eines Datums, die folgende Speicherung und auch das spätere Veredeln sind davon nicht erfasst.

Damit dürften die nicht personenbezogenen bzw. freigegebenen Daten grundsätzlich uneingeschränkt von denjenigen verwendet werden, die darauf Zugriff haben – sie sind öffentliche Güter. Grenzen können sich gleichwohl ergeben:

– faktische Grenze: physischer Zugriff (Verfügungsgewalt über das Kfz / Schnittstellen)
– Einschränkung und Erweiterung über vertragliche Regelungen, mit der bestimmten Kreisen Zugang zu Daten gewährt wird (z. B. der Versicherung für Telematik-Tarif)
– Einschränkungen bzgl. sicherheitsrelevanter Daten (vgl. oben Kapitel 5)

Auch die öffentliche Hand ist aufgefordert, durch *Open Data*, also die Bereitstellung von Daten durch staatliche Stellen, Gründungen und ökonomische Entwicklungen im Bereich Big Data zu unterstützen. Von der öffentlichen Hand und aus Steuermitteln erhobene, nicht personenbezogene Daten sind grundsätzlich öffentlich zugänglich zu machen. Hierzu jüngst *Open Data – Der Rechtsrahmen, vbw 2018*.

Die rechtlichen Rahmenbedingungen (Möglichkeiten und Grenzen der Datenverwertung, Gegenleistung und möglichen Haftungsfolgen) für eine Verwertung der Daten im Rahmen verschiedenster Geschäftsmodelle (vgl. auch oben, Kapitel 2) ist demnach vorrangig Sache der Vertragsgestaltung.

Nachdem Verträge nur inter partes wirken, sollte dabei auch eine Verpflichtung aufgenommen werden, die Vereinbarungen – beispielsweise Nutzungsbeschränkungen – auch in etwaigen späteren Verträgen mit weiteren Beteiligten aufzunehmen, um zumindest einen Regress zu ermöglichen.

Gemeinsam mit der Wissenschaft sollten Muster und Vorlagen für vertragliche Vereinbarungen über Inhaberschaft, Nutzungs-, Verwertungs- und Verfügungsrechte an Daten entwickelt werden. In einem ersten Schritt empfiehlt sich dabei eine Orientierung an

konkreten Anwendungsfällen. Dadurch kann zugleich ein Beitrag dazu geleistet werden, sichere Prozesse und gemeinsame Schnittstellenstandards zu gestalten und gegebenenfalls zu zertifizieren. Wichtig ist auch eine Mitwirkung mittelständischer Unternehmen an derartigen Projekten (vgl. *Zukunft digital – Big Data, Analyse und Handlungsempfehlungen*, vbw 2016).

Forderungen

Auf die Regelung eines „Dateneigentums“ ist vorerst zu verzichten; Lösungen sind über vertragliche Gestaltungen zwischen den bei der Datenerhebung und -verarbeitung Beteiligten anzustreben.

Es ist eine Entwicklung von Musterfällen und entsprechenden Musterverträgen durch Wirtschaft und (Rechts-)Wissenschaft anzustreben, in denen die Datenverwendung und die entsprechenden Gegenleistungen für bestimmte Anwendungsfälle transparent geregelt werden.

Der Staat muss Open Data konsequent umsetzen, um auf Basis der von ihm erhobenen Daten neue Geschäftsmodelle zu ermöglichen.

Datenmonopole sind grundsätzlich zu vermeiden. Es sollte daher ein Level Playing Field angestrebt werden, verbunden mit einer kostenneutralen Lösung für den Zugriff auf die Nutzerdaten, wenn der Halter / Fahrer eingewilligt hat, bzw. es sich nicht um personenbezogene Daten handelt (z. B. für Versicherungen, freie Werkstätten, Pannendienste, sonstige Dienstleister). Dafür bietet sich die Einrichtung einer Telematikplattform an.

Für jedes der möglichen Geschäftsmodelle sollte das rechtliche Risiko im Hinblick auf die Datennutzung bewertet werden. Ein Ansatzpunkt dafür liefert die Matrix Big Data und Recht (vgl. Abb. 6; näher siehe auch die Studie *Big Data im Freistaat Bayern – Chancen und Herausforderungen*, vbw 2016). Bis zu einem Gesamtergebnis von etwa 40 Punkten kann davon ausgegangen werden, dass die (geplante) Datennutzung mit einem vertretbaren Risiko möglich ist, wobei sich eine rein pauschalierende Betrachtung verbietet: Einzelwerte von sieben oder mehr sollten stets eine nähere Prüfung in dem betreffenden Bereich auslösen.

Abbildung 6

Matrix zur Einschätzung der rechtlichen Risiken

Quelle: vbw, Zukunft digital – Big Data, Analyse und Handlungsempfehlungen

7 Autonomes Fahren in ethischer Perspektive

Erkenntnisse der Ethikkommission des BMVI

Ende September 2016 hat der damalige Bundeminister für Verkehr und Digitale Infrastruktur Alexander Dobrindt eine Ethikkommission für automatisiertes und vernetztes Fahren eingesetzt, die sich mit übergeordneten Fragen und Dilemmata befassen sollte. Diese hat im Juni 2017 ihren Abschlussbericht vorgelegt, den man unter dieser Adresse online findet:

https://www.bmvi.de/SharedDocs/DE/Publikationen/G/bericht-der-ethik-kommission.pdf?__blob=publicationFile

In diesem Bericht werden 20 ethische Regeln formuliert, die die Entwicklung zum autonomen Fahren insgesamt positiv bewerten, dabei aber Grenzlinien bei der Ausgestaltung der digitalen Verkehrsinfrastruktur ziehen. Im Hinblick auf Datenschutz und IT-Sicherheit, Verantwortung und Haftung liegt ein besonderes Augenmerk bei den folgenden Regeln:

Teil- und vollautomatisierte Verkehrssysteme dienen zuerst der Verbesserung der Sicherheit aller Beteiligten im Straßenverkehr. Die Einführung höherer automatisierter Fahrsysteme insbesondere mit der Möglichkeit automatisierter Kollisionsvermeidung kann dementsprechend gesellschaftlich und ethisch geboten sein, wenn damit vorhandene Potentiale der Schadensminderung genutzt werden können. Daneben geht es um die Steigerung von Mobilitätschancen und die Ermöglichung weiterer Vorteile. Die Vermeidung von Unfällen ist Leitbild, wobei technisch unvermeidbare Restrisiken einer Einführung des automatisierten Fahrens bei Vorliegen einer grundsätzlich positiven Risikobilanz nicht entgegenstehen.

Die Gewährleistungsverantwortung für die Einführung und Zulassung automatisierter und vernetzter Systeme im öffentlichen Verkehrsraum obliegt der öffentlichen Hand. Fahrsysteme bedürfen deshalb der behördlichen Zulassung und Kontrolle.

Die dem Menschen vorbehaltene Verantwortung verschiebt sich bei automatisierten und vernetzten Fahrsystemen vom Autofahrer auf die Hersteller und Betreiber der technischen Systeme und die infrastrukturellen, politischen und rechtlichen Entscheidungsinstanzen. Gesetzliche Haftungsregelungen und ihre Konkretisierung in der gerichtlichen Entscheidungspraxis müssen diesem Übergang hinreichend Rechnung tragen.

Für die Haftung für Schäden durch aktivierte automatisierte Fahrsysteme gelten die gleichen Grundsätze wie in der übrigen Produkthaftung. Daraus folgt, dass Hersteller

oder Betreiber verpflichtet sind, ihre Systeme fortlaufend zu optimieren und auch bereits ausgelieferte Systeme zu beobachten und zu verbessern, wo dies technisch möglich und zumutbar ist.

Eine vollständige Vernetzung und zentrale Steuerung sämtlicher Fahrzeuge im Kontext einer digitalen Verkehrsinfrastruktur ist ethisch bedenklich, wenn und soweit sie Risiken einer totalen Überwachung der Verkehrsteilnehmer und der Manipulation der Fahrzeugsteuerung nicht sicher auszuschließen vermag.

Automatisiertes Fahren ist nur in dem Maße vertretbar, in dem denkbare Angriffe, insbesondere Manipulationen des IT-Systems oder auch immanente Systemschwächen nicht zu solchen Schäden führen, die das Vertrauen in den Straßenverkehr nachhaltig erschüttern.

Erlaubte Geschäftsmodelle, die sich die durch automatisiertes und vernetztes Fahren entstehenden, für die Fahrzeugsteuerung erheblichen oder unerheblichen Daten zunutze machen, finden ihre Grenze in der Autonomie und Datenhoheit der Verkehrsteilnehmer. Fahrzeughalter oder Fahrzeugnutzer entscheiden grundsätzlich über Weitergabe und Verwendung ihrer anfallenden Fahrzeugdaten.

Auf einer Konferenz am 14./15. September 2017 in Frankfurt wurde der Abschlussbericht durch die europäischen Verkehrsminister positiv aufgenommen und beschlossen, auf dieser Grundlage im Rahmen einer europäischen Task Force Handlungsempfehlungen und Leitlinien für eine abgestimmte Weiterentwicklung der Digitalen Verkehrsinfrastruktur mit dem Ziel einer stufenweisen Entwicklung hin zum autonomen Fahren zu erarbeiten.

Ansprechpartner / Impressum

Christine Völzow
Leiterin Abteilung Wirtschaftspolitik

Telefon 089-551 78-251
Telefax 089-551 78-91251
christine.voelzow@vbw-bayern.de

Oleg Livschits
Grundsatzabteilung Recht

Telefon 089-551 78-238
Telefax 089-551 78-233
oleg.livschits@vbw-bayern.de

Impressum

Alle Angaben dieser Publikation beziehen sich grundsätzlich sowohl auf die weibliche als auch auf die männliche Form. Zur besseren Lesbarkeit wurde meist auf die zusätzliche Bezeichnung in weiblicher Form verzichtet.

Herausgeber

vbw
Vereinigung der Bayerischen
Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.vbw-bayern.de