Informationelle Selbstbestimmung auch auf der Straße?

Steffen Kroschwald

Dr. Ing. h.c. F. Porsche Aktiengesellschaft
steffen.kroschwald@porsche.de

Zusammenfassung

Mit der digitalen Vernetzung von Fahrzeugen öffnet sich die Tür zu einer neuen Ära der Mobilität. Nicht nur der Fahrzeugindustrie stehen grundlegende Veränderungen bevor. Auch die Verkehrsinfrastruktur, wenn nicht sogar ganze Mobilitätskonzepte, werden langfristig hinterfragt werden, zur Disposition stehen oder neu zu gestalten sein. Die Vernetzung im Bereich der Mobilität könnte damit zum Grundstein und zur Blaupause für eine Zukunft der ubiquitären Informationstechnologie werden. Damit einher geht aber eine neue Dimension der Informationsverarbeitung und es entstehen neue Möglichkeiten der Datensammlung, -analyse und -verwertung. Die neue Informationstechnologie könnte dabei grundlegende Prinzipien des Datenschutzrechts herausfordern. Der vorliegende Beitrag unternimmt eine Analyse der derzeitigen und absehbaren Ansätze zur Fahrzeugvernetzung und stellt die Frage, inwiefern diese mit dem geltenden Datenschutzrecht vereinbar sind und wo die Technik aber auch das Recht den Entwicklungen begegnen können, ohne das Grundrecht auf informationelle Selbstbestimmung langfristig auszuhöhlen.

1 Auf der Straße in eine vernetzte Welt

In heutigen Fahrzeugen beschränkt sich die Informationsverarbeitung bereits nicht mehr nur auf die lokale elektronische Steuerung von Fahrzeugfunktionen und die Aufzeichnung von Protokollen. Schon heute stehen in Fahrzeugen zunehmend online-Anbindungen zur Verfügung. Mittels dieser Anbindungen können Nutzer von anderen Endgeräten aus Funktionalitäten wie Sicherheits- und Assistenzsysteme verwalten, Fahrzeuginformationen abrufen und Fehler diagnostizieren und beheben [ReMe14, 368]. Auch bieten Fahrzeughersteller für bestimmte Fahrzeugsegmente vermehrt Online-Dienste im sogenannten „Infotainment-Bereich“ an. So können etwa Fahrzeuginsassen über fahrzeuginterne Multimediamodule Online-Karten und -Navigationsdienste nutzen, auf Online-Dienste zur Information und Kommunikation zuzugreifen sowie sich direkt aus dem Fahrzeug heraus mit sozialen Netzwerken verbinden [ReMe14, 371]. Das Fahrzeug selbst wird gewissermaßen zu einem Smart-Device [Weic14a, 201].

Allein hierbei wird es jedoch nicht bleiben. Als nächster Schritt zeichnet sich die Vernetzung des Fahrzeugs mit seiner Umgebung, also der Verkehrsinfrastruktur und anderen Verkehrsteilnehmern ab. Diese als „Car2Car“ beziehungsweise „Car2X“ bezeichneten Ansätze sollen selbst

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 86-97.

mittelfristig wiederum Grundlagen für das Ziel des automatisierten Fahrens und schließlich eines sich vollständig automatisiert steuernden Verkehrs sein.[1] Hierdurch soll Mobilität nicht nur effizienter werden, sondern auch umweltfreundlicher und weniger gefährlich [Sche14, 353].

1.1 Vom Fahrzeughersteller zum IT-Dienstleister

Mit der Vernetzung der Mobilität gehen erhebliche Marktveränderungen einher. Die Unternehmen der Fahrzeugindustrie wandeln sich rasant von bloßen Fahrzeugentwicklern, -produzenten und -distributoren hin zu IT-Herstellern und, noch wesentlicher, auch IT-Anbietern [Weic14, 201]. Wo früher die Fahrzeug-IT im Wesentlichen Bestandteil der eigentlichen Fahrzeugprodukte war oder Hard- und Software gegebenenfalls ergänzend zu Fahrzeugen vertrieben wurden, könnten zukünftige Geschäfts- und Vertriebsmodelle online-basierte Dienste mit Bezug zum Fahrzeug oder der Mobilität im Allgemeinen in den Fokus rücken. Für die Fahrzeugindustrie könnte es somit zukünftig möglich sein, mit ihren Produkten auch völlig neue Kundengruppen – etwa Nutzer von Carsharing-Angeboten oder sonstigen alternativen Mobilitätskonzepten – zu gewinnen.

Wo Geschäfts- und Vertriebsmodelle entstehen, betreten regelmäßig auch neue Anbieter den Markt – Apples iCar, die selbstfahrenden Google-Autos und Dienste der Firma Uber sollen hier nur exemplarisch für Angebote stehen, die bestehende Marktkonstellationen tiefgreifend verändern könnten. Hierauf werden nicht nur die Entwicklungs- und Vertriebsabteilungen der Fahrzeugindustrie und weiterer Mobilitätsanbieter reagieren müssen. Auch die Politik und der Gesetzgeber benötigen Antworten auf sich durch solche Marktveränderungen neu aufwerfende, gesellschaftliche und wirtschaftspolitische Fragestellungen.

1.2 Die Fahrzeug-Cloud

Mit den neuen technischen Möglichkeiten, den neuen Angeboten und den neuen Anbietern gehen jedoch auch erhebliche Veränderungen in der Wertschöpfung der Fahrzeugindustrie einher. Vernetzte Fahrzeug- und Verkehrskonzepte benötigen riesige Datenmengen, die es zu erheben und zu verarbeiten gilt. Gleichzeitig beinhalten diese Datenmengen einen unfassbaren Informationswert. Das Fahrzeug, der Fahrer, die Insassen und die Fahrzeugumgebung werden langfristig zur nicht versiegenden Quelle von Informationen. Mithilfe moderner und ebenfalls vernetzter Datenverarbeitungstechniken, etwa durch das Cloud Computing und Big Data-Anwendungen, lässt sich dieser Informationsschatz heben und analysieren. Vernetzte Fahrzeugsysteme bergen damit den Rohstoff für unzählige Geschäftskonzepte und weitere Verwendungen. Sie ermöglichen die Auswertung von Vorgängen und Geschehnissen, etwa zur Analyse von Verkehrsflüssen oder Unfällen, zur genauen Detektion von Fehlern, etwa im Rahmen der Produktverbesserung an Fahrzeugen und der Infrastruktur, aber auch zur Erstellung von präzisen Profilen über Verkehrsteilnehmer bis hin zur Vorhersage ihres Verhaltens. Wer Zugang zu Standort- und Bewegungsinformationen, Daten über Fahrzeugzustände, deren Insassen und deren Umgebung hat und diese geschickt zu kombinieren weiß, verfügt über ein beinahe umfas-

[1] Siehe hierzu die Diskussion um erste Autobahn-Teststrecken zum autonomen Fahren o.A., Dobrindt plant Teststrecke für selbstfahrende Autos auf A9, FAZ-Online vom 26.01.2015 http://www.faz.net/agenturmeldungen/unternehmensnachrichten/roundup-dobrindt-plant-teststrecke-fuer-selbstfahrende-autos-auf-a9-13391422.html

sendes Bild über das Leben des Einzelnen. Wer diese Informationen mit denen weiterer Verkehrsteilnehmer verknüpft und über einen bestimmten Zeitraum analysiert, vermag darüber hinaus Aussagen über Regelmäßigkeiten und auch zukünftige Geschehnisse abzuleiten.

Die Vernetzung der Mobilität als Ausgangspunkt des Ubiquitous Computing ist damit nicht nur für die Fahrzeugindustrie und das Verkehrswesen von Bedeutung [Roßn06, 281] [Roßn14, 281 f.] [KiKü14, 3060]. Die generierten und abgeleiteten Informationen wecken vielmehr schon heute Begehrlichkeiten für die Nutzung zu Überwachungs-, Kontroll- und Vorhersagezwecken – etwa auf Seiten privater Unternehmen wie Versicherungen und großer „Datenkonzerne“ [Weic14a, 245f.]. Aber auch staatliche Stellen versprechen sich Vorteile, beispielsweise in der Ermittlung und Verhinderung von Straftaten wie terroristischen Handlungen ebenso wie der Abschreckung vor und Ahndung von kleineren Delikten.

2 Schutzbereich Informationelle Selbstbestimmung

Vernetzte Fahrzeuge könnten langfristig nicht nur Vorteile und Annehmlichkeiten und Freiheiten mit sich bringen sowie Gefahren vermeiden und Belastungen verringern. Die Generierung, Verarbeitung und Verteilung von Daten im Rahmen der Fahrzeugvernetzung könnte in Verbindung mit neuen technischen Möglichkeiten der Analyse auch die Menschen der Gefahr einer umfassenden Überwachung aussetzen [Mark15, 10 ff.] [Spaa15, 86]. Die Analyse und Vorhersage ihres Verhaltens könnte Menschen stigmatisieren und in ihrem Handeln einschränken oder dieses sogar steuern. Darin begründet sich ein erheblicher Eingriff in die Freiheit und Grundrechte des Einzelnen.

2.1 Grundrechtsgewährleistung

Nach dem Bundesverfassungsgericht ist es mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar, wenn „Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“. Hierdurch könne die „Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“ Gerade der Missbrauch von Informationssystemen, die zur Erstellung von Persönlichkeitsprofilen geeignet sind, kann nach dem Bundesverfassungsgericht die Selbstbestimmung des einzelnen, aber auch das freiheitlich demokratische Gemeinwesen an sich gefährden. Das vom Bundesverfassungsgericht angesichts dieser Gefahren vom allgemeinen Persönlichkeitsrecht abgeleitete „Recht auf informationelle Selbstbestimmung“ soll deshalb den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten sichern. Es zwingt die Beteiligten, die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, zu respektieren [BVerf83, 43].

Für die Welt einer ubiquitären Datenverarbeitung und vornean für die Welt der vernetzten Mobilität stellt sich aber die Frage, wie sich das Recht auf informationelle Selbstbestimmung und die hieraus abgeleiteten Grundsätze wie die Datensparsamkeit, Erforderlichkeit, Transparenz, Zweckbindung und Datensicherheit auch zukünftig wahren lassen [Roßn07, 128 f.]. Wie können Fahrzeugsysteme zukünftig datensparsam sein, wenn ein mehr an Daten grundsätzlich auch die Verbesserung von Diensten für die Nutzer bedeutet? Wie kann der Datenumgang auf das erforderliche Maß beschränkt werden, wenn sich zukünftige Verwendungsmöglichkeiten noch gar nicht abschätzen lassen? Wie lässt sich die Zweckbindung realisieren, wenn die Verarbeitung der Daten in unterschiedlichsten Anwendungen starke Begehrlichkeiten weckt und das

Schicksal einmal erhobener Daten kaum nachvollziehbar ist? Wie kann der Betroffene Transparenz über den Umgang mit personenbezogenen Daten erhalten und selbstbestimmt über ihren Umgang entscheiden, wenn sich weder genau definieren lässt, welche Daten Rückschlüsse auf wen zulassen, noch sich Datenverarbeitungsprozesse und Verantwortlichkeiten für den Einzelnen überblicken geschweige denn verständlich darstellen lassen [Weic14a, 205]? Und schließlich: Wie lässt sich garantieren, dass technische Mechanismen, die dem Schutz der informationellen Selbstbestimmung dienen, nicht überwunden oder bereits in ihrem Entwicklungsprozess unterwandert werden?[2]

2.2 Personenbezogene Fahrzeugdaten

Ausgangspunkt jeder datenschutzrechtlichen Diskussion ist das personenbezogene Datum. Durch den Umgang mit personenbezogenen Daten eröffnet sich der Anwendungsbereich des Datenschutzrechts. Im Bundesdatenschutzgesetz sind personenbezogene Daten nach § 3 Abs. 1 BDSG als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ definiert. Für einen Personenbezug muss eine Information demnach nicht unmittelbar einer Person anhaften – etwa über die Verknüpfung mit ihrem Namen und ihrer Anschrift. Es genügt, wenn Angaben, unter Umständen durch Einsatz weiterer Informationen, mit verhältnismäßigen Mitteln einer Person zumindest mittelbar zugeordnet werden können. Eine solche Person ist zwar nicht bestimmt, aber bestimmbar und das betreffende Datum somit personenbezogen. Auch Angaben, die für sich genommen keinen Bezug zu einer Person aufweisen, etwa Kennnummern, können – sofern die jeweilige Stelle über entsprechende Zusatzinformationen verfügt – personenbezogen und ihre Erhebung, Verarbeitung und Nutzung im Sinne des § 1 Abs. 1 BDSG datenschutzrechtlich reguliert sein.

Die Frage nach dem Personenbezug stellt sich für den Umgang mit Daten im und rund um das Fahrzeug im besonderen Maße. So weisen beispielsweise Signale und Messwerte, die in Steuergeräten des Fahrzeugs anfallen, an sich keinen Bezug zu einer bestimmten Person auf. Selbst wenn diese Informationen, wie bei der Fahrzeugvernetzung häufig der Fall, mit der sogenannten Fahrzeug-Identifikationsnummer (FIN) verbunden werden, ist kein direkter Bezug zu einer natürlich Person vorhanden. Die Daten könnten folglich als nicht personenbezogen eingeordnet werden und der Umgang mit ihnen – beispielsweise die Erhebung und Verarbeitung durch Fahrzeughersteller oder Behörden – datenschutzrechtlich folgenlos bleiben. Fraglich ist aber, ob sich ein solcher Bezug zu einer Person möglicherweise mittelbar herstellen lässt. So ist die FIN dem Fahrzeug in der Regel einmalig und exklusiv zugeordnet. Fahrzeughersteller erfassen in der Regel zumindest beim Neuwagenverkauf die FIN zusammen mit dem Namen des Fahrzeugkäufers. Auch bei späteren Werkstattbesuchen oder im Gebrauchtwagenhandel wird die FIN in Verbindung mit einer Person – dem Kunden, dem Auftraggeber oder dem Fahrzeughalter – erfasst. Für diese Stellen ist die FIN problemlos zumindest irgendeiner Person zuordenbar. Angesichts der weiten Verbreitung von FIN-Nummern bei Unternehmen und Behörden wird die FIN mittlerweile überwiegend als personenbezogenes Datum betrachtet [ReMe14, 372] [Roßn06, 283]. Dies umso mehr, als die FIN auch zunehmend im Rahmen von fahrzeugbezogenen Online-Diensten als Identifikationsmerkmal eingesetzt und damit von unzähligen Stellen erfasst wird, die wiederum mit weiteren Informationen einen Bezug zu einer Person herstellen

[2] Exemplarisch seien hier Berichte über mutmaßliche Interventionen US-amerikanischer Geheimdienste bei der Entwicklung von Verschlüsselungen und Standards hingewiesen, hierzu etwa o.A., NSA zahlte 10 Millionen US-Dollar für Krypto-Backdoor, Heise Online vom 21.12.2013, http://www.heise.de/security/meldung/NSA-zahlte-10-Millionen-US-Dollar-fuer-Krypto-Backdoor-2071567.html, abgerufen am 16.03.2015.

können. Damit werden für diese Stellen aber auch Informationen, die zusammen mit der FIN erhoben, verarbeitet und genutzt werden (möglicherweise auch sehr technisch anmutende Daten wie die aktuelle Öltemperatur eines Fahrzeugs), zu personenbezogenen Daten, die Rückschlüsse über eine bestimmbare Person wie etwa den Halter, den Fahrer, den Vorbesitzer oder andere Betroffene zulassen – beispielsweise deren aktuelles oder historisches Fahrverhalten. Wenngleich also zahlreiche Informationen im Rahmen der Fahrzeugvernetzung als „technische Daten“ zunächst keinen Personenbezug aufweisen mögen, werden sie durch Verknüpfung mit weiteren Informationen wie die FIN oder andere zuordenbare Kennzeichen personenbezogen, damit datenschutzrechtlich relevant und – je nach Verwendung zu einem bestimmten Zweck oder Einbringung in einen bestimmten Kontext – auch brisant [KiKü14, 3058] [ReMe14, 373] [RaHo14, 353] [ScRD12, 512].

2.3 Schutzbereich oder: Wem die Daten gehören

Die Vielzahl unterschiedlicher Informationen, die sich aus der Fahrzeugvernetzung gewinnen lassen und die neuen technischen Möglichkeiten der Kombination und Analyse bescheren demjenigen, der über die Daten und die technischen Mittel verfügt nicht nur wirtschaftliches Potential, sondern möglicherweise auch Einfluss. Fahrzeughersteller könnten die anfallenden Daten nutzen, um ihre Fahrzeuge zu verbessern, aber auch den Kunden individuellere Angebote maßzuschneidern. Erste Versicherungen bieten anhand der netzbasierten Auswertung des Fahrverhaltens bereits spezielle Policen an – zukünftig wäre vorstellbar, dass Versicherungsnehmer mit auffälligen Werten mit höheren Versicherungsbeiträgen belegt werden oder erst gar nicht versichert werden. Staatliche Stellen könnten die Daten zur Optimierung der Infrastruktur aber auch mit der Begründung einer „Effektivierung der Gefahrenabwehr und Strafverfolgung“ zu Beobachtungs- und Ermittlungszwecken nutzen. Daten aus der Fahrzeugvernetzung können folglich für bestimmte Stellen einen hohen Nutzen und Wert haben, die exklusive Verfügung darüber und der Ausschluss anderer von diesen Daten möglicherweise für einige erstrebenswert sein. Damit drängt sich automatisch die Frage auf, ob auf personenbezogene Daten, vergleichbar mit materiellen Gütern, auch ein exklusiver Verfügungsanspruch begründet werden, ob also über personenbezogene Daten eine Art Eigentums- oder Besitzposition erworben werden kann – oder kurz: Können Daten einer Person oder Stelle „gehören“?

Das Datenschutzrecht schützt nach § 1 Abs. 1 BDSG den Einzelnen vor der Beeinträchtigung seines Persönlichkeitsrechts bei der Erhebung, Verarbeitung und Nutzung „seiner“ personenbezogenen Daten. Wenngleich durch die Verwendung des Possessivpronomens ein Besitzverhältnis ausgedrückt wird, bezieht sich der Schutz aus dem BDSG keineswegs nur auf das Verhältnis eines bestimmten, einzelnen Betroffenen zu „seinem“ Datum. Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Die in dem jeweiligen Datum enthaltenen Einzelangaben müssen jedoch nicht zwingend ausschließlich die persönlichen und sachlichen Verhältnisse einer einzelnen Person beschreiben. Möglich ist vielmehr, dass sich mit den Angaben auch Verhältnisse anderer Betroffener beschreiben lassen. So werden Angaben zur Entwicklung des Spritverbrauchs zunächst einmal einen potentiellen Rückschluss auf das Fahrverhalten eines bestimmten Fahrers zulassen. Es lassen sich – gegebenenfalls in Verbindung mit weiteren Werten – aber möglicherweise auch Aussagen über mögliche Fahrerwechsel sowie den Einsatzort des Fahrzeuges und damit über andere Fahrzeugnutzer und gegebenenfalls auch über den Halter treffen. Andere Werte wiederum lassen gegebenenfalls Rückschlüsse zu anderen Verkehrsteilnehmern, Fahrzeuginsassen bis hin zu Mitarbeitern in Werkstätten zu. Vom

Datenschutzrecht geschützt ist folglich jeder Betroffene, also jede Person, auf deren Verhältnisse anhand des Datums geschlossen werden kann. Das personenbezogene Datum des einen kann gleichzeitig auch das personenbezogene Datum eines anderen sein. [Krau14, 377]

Das Datenschutzrecht kennt folglich auch kein Dateneigentum, das einer Person etwa dem betroffenen Fahrzeuginhaber oder dem Fahrzeughersteller ein individuelles Verfügungsrecht an dem Datum und die Möglichkeit zum Ausschluss anderer gäbe. Vielmehr setzt das Datenschutzrecht an der Frage an, ob der Umgang, also die Erhebung, Verarbeitung und Nutzung eines Datums zu einem bestimmten Zweck zulässig ist oder nicht. Nicht das Datum ist somit entscheidend, sondern der Umgang damit und der Kontext, in dem dies geschieht. Die durch Sensorik und Fahrzeugvernetzung ermittelten Werte über den Zustand eines Fahrzeugs gehören in der Folge weder dem Fahrzeuginhaber, noch dem Fahrer, der Werkstatt oder dem Hersteller. Soweit die Daten, beispielsweise durch den Hersteller des Fahrzeugs, abgerufen, gespeichert und mit weiteren Informationen kombiniert werden sollen und der Hersteller hierdurch einen Rückschluss auf irgendeine bestimmte oder bestimmbare Person ziehen kann, muss jeder Datenumgang im Sinne des § 4 Abs. 1 BDSG für den konkreten Zweck legitimiert sein. Er muss den gesetzlich normierten Anforderungen der Datensicherheit entsprechen und begründet gleichzeitig Rechte dieser betroffenen Person wie etwa auf Transparenz und Auskunft [Roßn14, 283 ff.] [ReMe14, 32], [Krau14, 377].

2.4 Datenschutz-Verantwortung in ubiquitären Systemen

Das Datenschutzrecht knüpft Rechte und Pflichten an die sogenannte „verantwortliche Stelle“ an. Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Die der Regelung zugrundeliegende europäische Datenschutzrichtlinie definiert die verantwortliche Stelle unter Art. 2 lit. d RL 95/46/EG noch konkreter als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für die Fahrzeugvernetzung stellt sich somit die Frage, welche Person oder Stelle über Zwecke und Mittel des Datenumgangs entscheidet und wer damit als verantwortliche Stelle Regelungsadressat des Datenschutzrechts ist. Anders als vom Gesetzgeber möglicherweise ursprünglich angedacht, lässt sich gerade bei der Vernetzung von Alltagssystemen eine solche Zuordnung immer schwieriger vornehmen [Roßn07]. Wer entscheidet beispielsweise, über den Zweck, der einer Aufzeichnung von technischen Daten aus dem Fahrzeug und die Übermittlung an zentrale Server zugrunde liegt, wenn die Daten dort dem Fahrer zur Auswertung seines Fahrverhaltens über eine App aber auch dem Hersteller zur Analyse seiner Produkte und womöglich sogar unzähligen weiteren Verkehrsteilnehmern im Rahmen der „Car2Car“-Dienste zur Verfügung gestellt werden?

Ein Fahrzeughalter, der seinen Fahrzeugzustand über eine App auswertet oder online-Dienste aus dem Fahrzeug nutzt, bestimmt damit für sich den Zweck der Verarbeitung seiner „eigenen“ Daten. Da sich Informationen, wie festgestellt, gerade aber nicht nur auf ihn selbst beziehen, wird der Fahrer durch Nutzung solcher Dienste möglicherweise auch datenschutzrechtlich verantwortlich für den Umgang mit personenbezogenen Daten weiterer Fahrer des Fahrzeugs, mögliche Insassen oder Personen, die sich im Umfeld des Fahrzeugs befinden und auf die mithilfe des Datums ebenfalls ein Rückschluss möglich ist. Ein Fahrzeughalter, der beispielsweise den Standort seines Fahrzeugs über eine App ermitteln lässt, kann möglicherweise nicht nur erfahren, ob und wo der jeweilige Fahrer sich gerade mit dem Fahrzeug befindet, sondern dies

auch für mögliche Mitfahrer erfahren, sofern er von diesen Kenntnis hat. Die Nutzung der App führt folglich zu einer vom App-Nutzer zu verantworteten Erhebung und Verarbeitung personenbezogener Daten.

Soweit überdies der Anbieter der App – etwa der Fahrzeughersteller – die Daten netzbasiert an zentrale Server übermittelt, dort verarbeitet, auswertet oder an Dritte weitergibt wird auch diesem Anbieter eine datenschutzrechtliche Verantwortung zufallen. Wenngleich dem App-anbietenden Fahrzeughersteller der konkrete Fahrer oder die Insassen im Einzelfall unbekannt sein mögen, so sind die im Rahmen der Nutzung übertragenen Daten doch zumindest regelmäßig – etwa über die FIN – dem Fahrzeuginhaber oder einem angemeldeten Dienstnutzer zuzuordnen. Mit Blick auf den Hersteller erhebt, verarbeitet und nutzt dieser zumindest personenbezogene Daten derjenigen Person, der in den Listen der Hersteller dem Fahrzeug (beispielsweise als Erstkäufer oder als Werkstattkunde) zugeordnet ist oder der sich als Nutzer eines Online-Dienstes hierzu registriert hat.

Die datenschutzrechtliche Verantwortlichkeit und die Fragen der Zulässigkeit und der Folgen einer Datenverarbeitung lassen sich somit nicht pauschal für ein bestimmtes Datum oder ein bestimmtes System beantworten. Für die Nutzung von Diensten in der Fahrzeugvernetzung sind datenschutzrechtlich in der Regel mehrere Stellen „kollektiv“ verantwortlich. Die Verantwortung und in der Folge die Zulässigkeit lässt sich konkret immer nur mit Blick auf den einzelnen Datenumgang und vor allen Dingen den Verwendungszweck, also den Kontext des Datenumgangs bestimmen. Die Erhebung und Verarbeitung von Daten, beispielsweise die Bildaufnahme der Umgebung zur Bereitstellung im „Car2Car“-Kontext, mag für den Fahrzeugnutzer und mögliche weitere Verkehrsteilnehmer zu einer bestimmten Situation und zu einem bestimmten Zweck zulässig sein – etwa um auf eine Gefahr adäquat reagieren zu können, jedoch nicht zwingend für den Hersteller der dem Fahrer interessante Angebote in der Umgebung machen will oder die Polizei, die potentielle Verkehrssünder beweissicher identifizieren möchte [Kros13, 388 ff.].

3 Datenschutz als „Showstopper“?

Soweit nach dem vorangehenden Kapitel festzustellen ist, dass ein bestimmtes Datum personenbezogen und eine Stelle für die Erhebung, Verarbeitung und Nutzung dieser Daten in einem bestimmten Kontext verantwortlich ist, stellt sich die Frage, ob der jeweilige Datenumgang nach dem geltenden Datenschutzrecht zulässig ist oder ob das Datenschutzrecht dem Datenumgang hier entgegensteht und damit – zumindest für den konkreten Fall – zum „Showstopper“ der Fahrzeugvernetzung wird. Dieser Frage soll im Folgenden anhand ausgewählter Szenarien nachgegangen werden.

3.1 Zulässigkeit der Erhebung von Fahrzeugdaten

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nach § 4 Abs. 1 BDSG nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Ist der konkrete Datenumgang folglich nicht durch eine Vorschrift – im BDSG oder in einem anderen Gesetz – ausdrücklich zugelassen und hat der Betroffene alternativ auch nicht oder nicht wirksam seine Einwilligung erklärt, ist der Datenumgang untersagt.

Zunächst könnte in der Praxis beispielsweise die Frage im Raum stehen, ob ein Fahrzeuginhaber den Zustand und Standort seines Fahrzeugs über einen entsprechenden App-basierten

Dienst ermitteln dürfte. Soweit sich über das Fahrzeug kein Bezug zu anderen Personen herstellen lässt – etwa weil nur der Fahrzeuginhaber als Nutzer des Dienstes Zugang zum Fahrzeug hat – steht das Datenschutzrecht dieser Person für die Nutzung der App zunächst nicht entgegen. Der Nutzer des Dienstes erhebt allenfalls Daten zu seinem eigenen Standort in eigener Verantwortung. Fraglich ist aber, ob solch eine Standortermittlung für den App-Nutzer auch zulässig ist, wenn nicht der Nutzer des Dienstes selbst, sondern ein Dritter, etwa ein Fahrzeugmieter oder ein Familienmitglied, das Fahrzeug führt und gegebenenfalls weitere Insassen im Fahrzeug befindlich sind. Durch Ermittlung des Standortes kommt es zu einer Erhebung personenbezogener Daten dieser Fahrzeuginsassen durch den Nutzer des Dienstes. Eine solche Datenerhebung müsste gesetzlich erlaubt oder durch eine Einwilligung legitimiert sein. Eine gesetzliche Erlaubnis, etwa aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG, wird zwar in Einzelfällen vorliegen – etwa wenn sich das Fahrzeug in einer Notfallsituation befindet und nicht nur der Erhebende, sondern auch die Fahrzeuginsassen ein Interesse an der Ortung haben. Gleichwohl hängt die Zulässigkeit hier stets von einer einzelfallbasierten Abwägung zwischen den Interessen der verantwortlichen Stelle (in diesem Fall des Dienstnutzers) und der Betroffenen ab. Pauschal ergibt sich eine Zulässigkeit für die Standortdatenerhebung gesetzlich aber nicht – sie bleibt allenfalls besonderen Fällen vorbehalten, für die dann gegebenenfalls (so etwa zur Standortermittlung im Rahmen des EU e-Calls) auch gesetzliche Regelungen geschaffen werden.

Für eine zulässige Erhebung von Standortdaten wird sich der Nutzer somit regelmäßig eine Einwilligung des Fahrzeugführers und – falls diese ihm bekannt sind – möglicherweise sogar auch aller Insassen einholen müssen. Eine solche Einwilligung muss bei wortgenauer Anwendung des § 4a BDSG nicht nur freiwillig, transparent und bestimmt erfolgen. Sie bedarf nach dem Gesetzeswortlaut sogar der Schriftform. Dass eine solche Anforderung in der Praxis schwer zu erfüllen ist, ist offensichtlich [KiKü14, 3058 ff.] [ReMe14, 373]. Die Nutzung von bestimmten Online-Diensten, die auch eine Ortung des Fahrzeugs möglich machen, könnte folglich beispielsweise bei der gewerblichen Fahrzeugüberlassung für die Dienstnutzer datenschutzrechtlich unzulässig sein und sogar zu Folgen wie Schadensersatzforderungen und Bußgeldern führen. Für diese und vergleichbare Nutzungen von Fahrzeugdiensten verbleiben folglich rechtliche Unsicherheiten, die sich mit zukünftigen Anwendungen – etwa im Bereich Car2Car – noch potenzieren könnten.

3.2 Zentralisierte Datenverarbeitung und Dienstanbindung

Die Vernetzung der Mobilität beruht auf dem Ausbau schneller Netzinfrastruktur und der Möglichkeit, auch kleine und mobile Einheiten an das Internet anzubinden. Das Angebot von komplexen Informations- und Multimediadiensten im Fahrzeug wäre undenkbar ohne den Zugriff auf riesige und stets aktuell verfügbare Ressourcen im Internet. Auch der Zugriff auf Fahrzeuginformationen und die Auswertung über standardisierte Apps ist vielfach nur über eine internetbasierte Verbindung und die Verarbeitung der Daten auf hochleistungsfähigen Servern in der „Cloud“ möglich. Die dem Nutzer zur Verfügung gestellte Information selbst bedarf häufig nicht nur der Einzeldaten aus dem Fahrzeug, sondern muss in leistungsstarken Servern durch Kombination mit anderen Informationen – vielfach auch Daten anderer Verkehrsteilnehmer – erst generiert werden. Das Angebot von Diensten für die Fahrzeugvernetzung ist somit erst durch eine netzbasierte, zumindest virtuell zentralisierte Datenverarbeitung möglich [RaHo14, 354].

Um Dienste anbieten zu können, müssen Anbieter somit zunächst Daten (etwa aus dem Fahrzeug) erheben, diese an ihre Server oder Drittanbieter übermitteln, dort weiterverarbeiten, um

sie dann den Kunden oder wiederum anderen Abnehmern anzubieten. Damit ist bereits fraglich, ob die Erhebung von personenbezogenen Daten (beispielsweise aus dem Fahrzeug) und ihre Übermittlung an einen Server für die Anbieter zulässig sind. Wie festgestellt umfassen die Dienste häufig die Erhebung von Daten durch den Dienstanbieter (etwa den Hersteller), die, beispielsweise über die FIN, einen Rückschluss zulassen, sodass der Anbieter hierdurch für den Umgang mit personenbezogenen Daten verantwortlich ist. Für die Erhebung und Verarbeitung von sogenannten Bestands- und Nutzungsdaten kann sich der Anbieter möglicherweise auf §§ 14 und 15 TMG berufen [ScRD12, 512]. Die Erhebung von Bestandsdaten, also etwa der Anschrift, der Telefonnummer und der Zahlungsinformationen ist nach § 14 TMG zulässig, soweit diese Bestandsdaten für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Dienstanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind – beispielsweise also, wenn der Anbieter den Nutzer als Kunden seines App-Dienstes führt und ihm über die Anschrift Rechnungen zusenden will. Nach § 15 TMG kann der Anbieter außerdem Nutzungsdaten, also Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen, erheben und verwenden. Zulässig ist deshalb häufig die Erhebung der IP-Adresse und der Zeitdauer, in dem ein bestimmter Dienst genutzt wurde, wenn dieser später beispielsweise zeitabhängig abgerechnet wird. Auch wenn die Erhebung und Verarbeitung von weiteren Informationen erforderlich ist, um den Dienst anzubieten – die Steuerung der Klimaanlage über eine App wäre nicht möglich, wenn die Innentemperatur nicht im Fahrzeug erhoben und verarbeitet würde – ist der Datenumgang auf Basis des TMG oder des § 28 Abs. 1 Satz 1 Nr. 1 BDSG regelmäßig zulässig.

Fraglich ist aber, ob der Anbieter die einmal erhobenen Daten neben dem Nutzer auch an Dritte weitergeben geben darf. So wird der Anbieter beispielsweise häufig Serverinfrastrukturen – zum Teil auch die darauf betriebene Anwendung – nicht selbst bereitstellen. Die Bereitstellung entsprechender Ressourcen erfolgt häufig über Dienstleister wie etwa Rechenzentrumsbetreiber oder Cloud-Anbieter. Die einmal (beispielsweise im Fahrzeug) erhobenen Daten müssen folglich an diese Dienstleister übertragen und von diesen verarbeitet werden. Eine solche Datenübermittlung müsste wiederum legitimiert werden. Dies gilt sogar, wenn der Server von einem rechtlich selbstständigen Konzernunternehmen betrieben wird. Unwahrscheinlich ist aber, dass jeder Betroffene in eine solche Übermittlung einwilligt und völlig unklar ist, was die Folge eines unerwarteten Widerrufs einer solchen Einwilligung wäre. Auch kann sich der Anbieter, für die Datenübermittlung praktisch nicht auf die vom Einzelfall und von einer Abwägung abhängigen gesetzlichen Erlaubnisse stützen.

Für einen solchen Fall kann sich der Anbieter allenfalls der sogenannten Auftragsdatenverarbeitung nach § 11 BDSG bedienen. Hierbei nutzt er einen Dienstleister lediglich zur Ausführung der technischen Datenverarbeitung (also beispielsweise zum Hosting oder der Verarbeitung von Daten in Servern), behält aber die Verwendungshoheit über die Daten. Der Dienstleister darf die Daten nur streng nach dem Auftrag des Auftraggebers verarbeiten. Der Anbieter des Fahrzeugdienstes ist in der Folge als Auftraggeber auch verantwortlich für die sichere Datenverarbeitung beim Dienstleister und muss dies auch kontrollieren. Unter diesen Bedingungen darf der Auftraggeber nach § 3 Abs. 8 i.V.m. § 11 BDSG die Daten beim Dienstleister zwar in der Weise verarbeiten und weitergeben, als würde er die Datenverarbeitung selbstständig durchführen.

Als verantwortliche Stelle hat der Dienstanbieter aber auch sicherzustellen, dass der Datenweg – beispielsweise vom Fahrzeug über den Anbieter an einen Server und zurück – sowie die Datenverarbeitung in den Servern an sich sicher sind. Gerade hinsichtlich der Sicherheit der Fahrzeugsysteme sowie der Übertragungswege haben sich vereinzelt bereits Sicherheitslücken in

der Praxis offenbart. Überdies ermöglicht die Auftragsdatenverarbeitung, soweit sie nicht als Datenübermittlung legitimationspflichtig sein soll, aus Sicht des europäischen Datenschutzrechts bislang in der Regel ausschließlich die Nutzung europäischer Serveranbieter und Server. Gerade für weltweite Angebote und solche, die über ortsungebundene Cloud-Server betrieben werden, ergeben sich hier hohe, teils schwer überwindbare Hürden.

3.3 Zweckbindung

Die Möglichkeit, auf Basis einer Datenverarbeitung im Auftrag Daten bei Dritten zu verarbeiten findet aber auch dort ihre Grenze, wo der Dritte die Daten zu anderen als den ihm aufgetragenen Zwecken verarbeitet [KiKü14, 3060]. Nutzt beispielsweise ein Serveranbieter die ihm übertragenen Informationen, um dem Kunden des Fahrzeugdienstes selbstständig Werbung anzubieten oder gibt der Anbieter des Fahrzeugdienstes Daten an Dienstleister weiter, die die Daten mit eigenen Informationen anreichern – etwa an einen Dienstleister, der aus den Bewegungsdaten aller Fahrzeugnutzer einen eigenen Verkehrskartendienst erstellt – muss diese Datenweitergabe als Datenübermittlung wieder datenschutzrechtlich legitimiert sein. Auch wenn der Dienstnutzer ursprünglich in die Verarbeitung seiner Daten eingewilligt hat oder der Dienstanbieter die Daten zur Bereitstellung des Dienstes erheben und verarbeiten musste, ist der Datenumgang ausschließlich für die hierbei definierten Zwecke zulässig. Werden beispielsweise von einem Anbieter eines personalisierten Multimediadienstes Daten zu Hörgewohnheiten erhoben, um dem Nutzer im Fahrzeug die persönliche „Playlist“ zu erstellen, so läge eine unzulässige Zweckänderung vor, wenn die Informationen zu Hörgewohnheiten auch dafür verwendet würden, dem Nutzer individuelle Kaufangebote zu machen oder an entsprechende Werbetreibende weiterzuverkaufen. Ein solcher Datenumgang müsste wieder – beispielsweise durch die ausdrückliche Einwilligung des Nutzers – legitimiert werden.

Das Gebot der Zweckbindung steht aber auch einem möglichen Verlangen – staatlicher wie privater Stellen – entgegen, den im Rahmen der Fahrzeugvernetzung entstehenden Datenschatz zur unbegrenzten Ausforschung, Profilbildung oder Verhaltens- und Persönlichkeitsauswertung zu verwenden [Roßn06, 284 f.]. Für die Verwendung von Fahrzeugdaten bedürfte es in den entsprechenden Strafermittlungs- oder Polizeigesetzen Ermächtigungen, die durch die Erlaubnis zur zweckändernden Datenübermittlung durch Dienstanbieter an Behörden ergänzt werden müssten. Zwar sind bereits heute etwa mit § 102 ff. StPO Eingriffsbefugnisse und mit § 28 Abs. 2 Nr. 2 lit. b BDSG Übermittlungsbefugnisse geschaffen. Auch diese Befugnisse sind jedoch eng auf bestimmte Anlässe begrenzt und müssen sich am Erforderlichkeits- beziehungsweise Verhältnismäßigkeitsprinzip messen lassen. Zukünftige Technik in der Fahrzeugvernetzung wird aber gerade darauf aus sein, die Daten zunächst einmal zu erheben und erst später – sei es für private, sei es für staatliche Anlässe – den Zweck der Datenverarbeitung flexibel zu bestimmen. Die Anforderungen der Zweckbindung stehen zukünftigen Nutzungsszenarien damit zum Teil diametral gegenüber.

4 Zukünftige Herausforderungen

Was sich bereits seit Etablierung des Internet und umso mehr im Zuge des Web 2.0 und zuletzt mit dem Cloud Computing abgezeichnet hat, findet mit der Fahrzeugvernetzung erneut Bestätigung: Neue Technologien verschieben grundsätzliche Annahmen des geltenden Datenschutzrechts und stellen sie teilweise infrage. Insbesondere die Regelungen des Bundesdatenschutzgesetzes finden nur bedingt Antworten auf eine zunehmende Vernetzung, bei der die Grenze zwischen Betroffenen und Datenverarbeitern verschwimmt, bei der Verantwortlichkeiten

schwer abzugrenzen sind und zu Rechtsunsicherheiten führen, bei der Datenwege nicht mehr vorgezeichnet werden können und die Verdatung des Alltags das Prinzip der Datensparsamkeit konterkariert.

Mit der Fahrzeugvernetzung könnte die Verwirklichung des Rechts auf informationelle Selbstbestimmung besonders bedroht sein: Gerade das Fahrzeug wird von Betroffenen häufig in verschiedenen Rollen genutzt – zu Fahrten mit der Familie, mit Freunden oder zu Geschäftszwecken [Weic14a]. Die Möglichkeit, diese Rollen zu trennen ist Kern der informationellen Selbstbestimmung: Betroffene sollen wissen „wer was wann und bei welcher Gelegenheit über sie weiß". Durch die Vernetzung des Fahrzeugs könnte die vom Betroffenen selbstbestimmte Rollentrennung aber aufgehoben werden. Das Ziel sollte zukünftig aber nicht sein, resigniert das Grundrecht auf informationelle Selbstbestimmung zur Disposition zu stellen. Vielmehr sollte die Verwirklichung des Grundrechts bei der Gestaltung der Technik in den Mittelpunkt gerückt werden.

Beispielhaft für eine solche „datenschutzfördernde Technikgestaltung" können Verfahren zur Anonymisierung, Pseudonymisierung und Verschlüsselung genannt werden. Wenn zwar nicht verhinderbar ist, dass Daten im und um das Fahrzeug sowie von weiteren Endgeräten der Nutzer erhoben werden, könnten diese zumindest derart aggregiert, zerstückelt oder verzerrt werden, dass ein Rückschluss auf eine natürliche Person ausgeschlossen ist. Zum Schutz vor Zugriffen Unbefugter können Daten verschlüsselt übermittelt oder gespeichert werden [Kros14, 77 ff.]. Je früher die Daten dabei in der Prozesskette gelöscht oder nicht mehr zuordenbar sind, desto eher kann dem Prinzip der Datensparsamkeit entsprochen werden – auch wenn die Daten zunächst einmal erhoben wurden. Auch die Transparenz und Selbstbestimmung der Betroffenen kann durch technische Gestaltung unterstützt werden. So könnten Piktogramme in Fahrzeugdisplays eine bestimmte Einstellung oder Datenverarbeitungsvorgänge, etwa die Übertragung von Standortdaten, anzeigen und den Betroffenen somit klar und situationsadäquat auf die Erhebung und Verarbeitung von personenbezogenen Daten hinweisen. Ebenso mit dem Ziel des situationsadäquaten Datenschutzes ist es vorstellbar, dem Nutzer die Möglichkeit zu geben, Datenflüsse durch entsprechende Voreinstellungen oder Wahltasten ganz zu unterbinden oder durch nutzerfreundliche Konfigurationsmöglichkeiten anzupassen. Vergleichbar könnte dem Betroffenen auch über Internetportale oder leicht bedienbare Menüelemente im Fahrzeug die Möglichkeit gegeben werden, seinen Betroffenenrechten auf Auskunft, gegebenenfalls sogar Löschung, nachzukommen.

Gleichwohl bleiben viele technische Gestaltungsansätze wirkungslos, wenn sie nicht durch das Recht begleitet werden. Dieses kann Grenzen setzen aber auch Datenschutztechnik fördern, indem es beispielsweise Planungssicherheit für die Entwicklung und den Einsatz technischer Mittel schafft. So könnten gesetzliche Regelungen die Berücksichtigung datenschutzrechtlicher Anforderungen und datenschutzfreundlicher Voreinstellungen bereits in der Entwicklung der Technik einfordern. Die Einhaltung dieser Anforderungen könnte unabhängig kontrolliert und etwa durch Zertifikate rechtssicher bestätigt werden. Nur so kann der Nutzer auch ohne weitere Expertise und ständige Prüfung sich auf den Schutz seiner Daten verlassen und damit Vertrauen in den Datenumgang gewinnen. Der Fahrzeugindustrie könnte durch Anreize wie die Einführung verlässlicher Datenschutz-Gütesiegel überdies die Möglichkeit gegeben werden, sich im Wettbewerb als datenschutzfreundliche Hersteller zu präsentieren. Gerade für europäische Automobilhersteller könnte sich so der Datenschutz zu einem Wettbewerbsvorteil entwickeln. Bemühungen, das geltende Datenschutzrecht auf europäischer Ebene zu vereinheitlichen, sind vor diesem Hintergrund begrüßenswert [RoKr14]. Gerade im Hinblick auf aufkommende Möglichkeiten des Big Data und des sogenannten „Predictive Analysing" sollte aber auch bei einem

zukünftigen europäischen Datenschutzrecht an Grundpfeilern der Informationellen Selbstbestimmung – wie etwa dem Grundrechtsschutz, der Zweckbindung und dem sogenannten „Verbot mit Erlaubnisvorbehalt“– nicht gerüttelt werden.

Literatur

[BVerf83] Bundesverfassungsgericht. Urteil vom 15.12.1983 – Volkszählung. In: BVerfGE 65, 1. Karlsruhe (1983).

[KiKü14] K. Kinast, C. Kühnel: Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten. In: NJW (2014) 3057.

[Konf14] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Entschließung der 88. Konferenz am 8. und 9. Oktober 2014. Hamburg (2014).

[Krau14] M. Kraus: Telematik – Wem gehören Fahrzeugdaten? In: J. Taeger: BIG DATA & Co – Neue Herausforderungen, Oldenburg (2014) 377.

[Kros13] S. Kroschwald: Kollektive Verantwortung für den Datenschutz in der Cloud - Datenschutzrechtliche Folgen einer geteilten Verantwortlichkeit beim Cloud Computing. In: ZD (2013) 388.

[Kros14] S. Kroschwald: Verschlüsseltes Cloud Computing - Auswirkung der Kryptografie auf den Personenbezug in der Cloud. In: ZD (2014) 75.

[Mark15] E. Markey: Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk. Boston (2015).

[RaHo 14] K. Rammo, S. Holzgräfe: Datenschutz bei vernetzten Autos – Elektronische Fahrtenbücher. In: In: J. Taeger (Hrsg.): BIG DATA & Co – Neue Herausforderungen für das Informationsrecht. Oldenburg (2014) 351.

[ReMe14] J. Reiter, O. Methner: Datenschutz im Fahrzeug. In: J. Taeger: BIG DATA & Co – Neue Herausforderungen für das Informationsrecht. Oldenburg (2014) 368.

[RoKr14] A. Roßnagel, S. Kroschwald: Was wird aus der Datenschutzgrundverordnung? – Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument. In: ZD (2014) 495.

[Roßn07] A. Roßnagel: Datenschutz in einem informatisierten Alltag. Berlin (2007).

[Roßn06] A. Roßnagel: Datenschutz in der Verkehrstelematik. In: NVZ (2006) 281.

[Roßn14] A. Roßnagel: Fahrzeugdaten – wer darf über sie entscheiden? Zuordnungen – Ansprüche – Haftung. In: SVR (2014) 281.

[Sche14] J. Scherrer: eCall: Ein Lehrstück für Politik, Regulierung und Datenschutz. In: MMR (2014) 353.

[ScRD12] T. Schulz, A. Roßnagel, K. David: Datenschutz bei kommunizierenden Assistenzsystemen – Wird die informationelle Selbstbestimmung von der Technik überrollt? In: ZD (2012) 510.

[Spaa15] D. Spaar: Auto öffne dich – Sicherheitslücken bei BMWs Connected Drive. In: c’t (5/2015) 86.

[Weic14a] T. Weichert: Datenschutz im Auto – Teil 1. In: SVR (2014) 201.

[Weic14b] T. Weichert: Datenschutz im Auto – Teil 2. In: SVR (2014) 241.