Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 441

Datenschutz im Fahrzeug der Zukunft: Vernetzt, Autonom, Elektrisch

Meiko Jensen[1], Nils Gruschka[2] und Jens Lüssem[3]

Abstract: Das Fahrzeug der Zukunft wird durch die Trends Vernetzung, autonomes Fahren und Elektromobilität bestimmt. Damit verbunden sind große Hoffnungen für die Aspekte Reisekomfort, Sicherheit im Straßenverkehr und Umweltfreundlichkeit.

Allerdings werden diese Fortschritte auch z. T. durch erhebliche Eingriffe in die Privatsphäre und in das Recht auf informationelle Selbstbestimmung erkauft. In diesem Beitrag beleuchten wir, welche Datenschutzprobleme sich durch technische Neuerungen im Fahrzeug der Zukunft ergeben können, wie diese rechtlich einzuschätzen sind, und welche Lösungswege für die zugrundeliegenden Fragen denkbar sind.

1 Überblick

Bereits heute bauen die großen Automobilhersteller massiv Vernetzungstechnologien in ihre aktuellen Modelle ein. Vom klassischen Automobil über Busse und Lastkraftwagen bis hin zu Einsatzfahrzeugen von Rettungsdienst, Feuerwehr und Polizei wird überall digitale Technologie eingesetzt, um das Fahren in Zukunft zu erleichtern. Dieser Trend der massiven Digitalisierung und Vernetzung wird in den nächsten Jahren noch deutlich verstärkt werden und neben den offensichtlichen Vorteilen zeichnen sich auch schon Probleme dieser Entwicklung ab. Bisher wird dabei primär die Sicherheit von Leben und Besitz betrachtet. Berichte über geknackte [ADA16] oder ferngesteuerte Autos [Gre] erlangen dabei immer wieder große Aufmerksamkeit und Experten gehen davon aus, dass diese Bedrohungen in Zukunft noch deutlich gravierender werden [BFN].

Wenig Beachtung haben bisher hingegen die Nebeneffekte in Bezug auf Datenschutz und informationeller Selbstbestimmung erfahren. So weiß kaum ein Autokäufer heutzutage, ob, wann, welche und wie viele Daten sein Fahrzeug an wen übermittelt. Gleichzeitig sind viele der gesammelten Daten in modernen Fahrzeugen teilweise äußerst sensibel, erlauben sie doch brisante Rückschlüsse auf Fahrverhalten, Bewegungsmuster, Angewohnheiten und sogar medizinisch relevante Umstände von Fahrern und Insassen solcher Automobile.

In diesem Beitrag geben wir einen Überblick über die bekannten und zukünftig zu erwartenden Daten, die im Fahrzeug gesammelt, ausgewertet und gegebenenfalls an Dritte

[1] FH Kiel, meiko.jensen@fh-kiel.de. Die Arbeit von M.J. wurde teilweise am Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein durchgeführt und dort im Rahmen des Projektes iKoPA durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert.
[2] FH Kiel, nils.gruschka@fh-kiel.de
[3] FH Kiel, jens.luessem@fh-kiel.de

übertragen werden, und beleuchten anschließend die in diesem Zusammenhang auftretenden Probleme hinsichtlich des Datenschutzes anhand von zwei ausgewählten Beispielen. Diesen folgt eine kurze datenschutzrechtliche Perspektive, und abschließend zeigen wir Wege auf, wie sich die Datenhaltung im Fahrzeug der Zukunft datenschutzfreundlicher gestalten ließe.

2 Stand der Technik

In der Diskussion der Zukunft des Automobilsektors werden fast schon gebetsmühlenartig drei große Paradigmen wieder und wieder diskutiert. Zunächst ist als sicher anzunehmen, dass das Automobil der Zukunft *vernetzt* sein wird. Dies impliziert eine permanente, mobile Anbindung des Fahrzeugs an das Internet, über die eine bidirektionale Kommunikation zwischen Fahrzeug und entsprechenden Internetdiensten realisiert wird. Schon heute übermitteln moderne Fahrzeuge ihre Sensordaten per Mobilschnittstelle an ihre Hersteller, um etwa den Wartungs- und Inspektions-Prozess in Vertragswerkstätten zu optimieren.

Ein zweites großes Thema in Hinblick auf das Fahrzeug der Zukunft besteht in seiner Fähigkeit, zumindest teilweise *autonom fahren* zu können. Erste Ergebnisse lassen hier einen großen technischen Fortschritt erkennen (vgl. [Gui11, Gom16]), der mit großer Wahrscheinlichkeit in naher Zukunft auch in Deutschland umgesetzt werden dürfte. Zwar ist es noch ein weiter Weg bis die Technik das vollständig autonom fahrende Automobil zuverlässig implementiert hat, teilautonome Fahrassistenzsysteme – etwa beim Einparken oder zur Spurführung auf Autobahnen – sind jedoch bereits heute Teil modern ausgestatteter Fahrzeugmodelle.

Schließlich zeichnet sich ein deutlicher Trend weg von Verbrennungsmotoren hin zur Elektromobilität ab, bei dem Fahrzeuge *elektrisch* angetrieben werden. Diese Entwicklung geht jedoch mit veränderten Anforderungen an Verkehrsinfrastruktur und Fahrverhalten einher, da sich Fahrzeugbatterien nicht wie Verbrennungsmotoren binnen kurzer Zeit an beliebigen Tankstellen neu befüllen lassen. Auch die aktuellen Reichweitenbegrenzungen von Elektrofahrzeugen, vorgegeben durch die Maximalkapazität der Bordbatterie, dürften in naher Zukunft massiven Einfluss auf die Art und Weise haben, wie Elektrofahrzeuge in Deutschland genutzt werden.

Alle diese drei großen Neuerungen haben ihre jeweils eigenen, speziellen Anforderungen an Automobil, Fahrer, Hersteller und Verkehrsinfrastruktur, aber allen gemeinsam ist zu eigen, dass sie ihre Vorzüge nur dann ausspielen können, wenn die hierfür notwendigen technischen und infrastrukturellen Neuerungen geeignet realisiert werden. Ein Kernmerkmal ist hierbei die Nutzung gesammelter Sensordaten aus dem Fahrzeug zur Optimierung der jeweils benötigten Infrastrukturen. So steht beispielsweise zu erwarten, dass Navigationssysteme direkt mit Batteriesensoren und internetbasierten Batterie-Lade-Diensten gekoppelt werden, um die optimale Kombination von Fahrt, Batterieladung und ggfs. Batterietausch zu errechnen. Hierfür werden auch das Fahrverhalten des Fahrers, das Fahrzeuggewicht, der Grad der Abnutzung von Batterie und anderen Fahrzeugteilen, sowie weitere Sensordaten mit einbezogen.

3 Daten im Fahrzeug der Zukunft

Bereits heute fallen in gängigen Fahrzeugmodellen umfassende Messdaten verschiedenster Sensoren an, die oft fortlaufend erhoben, an entsprechende Steuergeräte im Fahrzeug übermittelt, dort aggregiert und ausgewertet und zur Regelung bzw. Steuerung der einzelnen Fahrzeugsysteme verwendet werden. Eine umfassende Auflistung verschiedener gängiger Sensoriksysteme in Fahrzeugen findet sich etwa bei Konrad Reif [Rei11]; eine (unvollständige) Übersicht relevanter Sensoren wird im Folgenden gegeben:

Sensorik zu Antrieb, Motorik und Fahrzeugzustand

- Raddrehzahlsensoren
- Beschleunigungssensoren
- Sensorik im Antrieb (Drucksensoren, Klopfsensoren, Drehzahlsensoren etc.)
- Lambdasonde (zur Steuerung der Kraftstoff-Luft-Mischung)
- Reifendrucksensoren
- Tankstands- und Tankdrucksensoren, bzw. Batterie-Ladestandssensorik
- Scheinwerfer-Neigungssensoren
- Fahrzeugneigungssensoren
- Überrollsensoren

Sensorik zur Fahrzeugsteuerung

- Lenkradwinkelsensoren
- Lenkrad-Drehmomentsensoren (Servolenkung)
- Pedalwegsensorik

Sensorik zur Überwachung von Innenraum und direkter Fahrzeugumgebung

- Sitzbelegungssensoren
- Sensorik der Zentralverriegelung und der Türschlösser
- Luftgütesensoren
- Feuchte- und Temperatursensoren
- Regensensor
- Abstandssensoren (Ultraschall, Radar, Lidar etc.)
- Kameras (Rückfahrkamera, Dashcam etc.)

Sensorik zur Navigation

- GPS-Sensoren
- Radio Data System (RDS-Sensor)
- Car2X-Sensoren (z.B. IEEE802.11p)
- Mobilfunkkommunikation

Wie sich unschwer erkennen lässt, erfasst die Sensorik im Fahrzeug der Zukunft umfassende Messdaten über das Fahrzeug und seine Umgebung. Insbesondere werden dabei vielfach auch personenbezogene Daten gesammelt. So hängen Daten zu Antrieb, Motorik und Fahrzeugzustand direkt vom Fahrer und seinem Fahrverhalten ab, ebenso wie die Sensorik zur Fahrzeugsteuerung. Die Navigationssensorik verarbeitet Daten über die Bewegungsmuster des Fahrzeugs – und damit die seiner Insassen. Schließlich verarbeiten vielfältige Überwachungssensoren sowohl personenbezogene Daten zu Fahrzeuginsassen als auch zu anderen Verkehrsteilnehmern im Umfeld des Fahrzeugs. Somit besteht ein klares datenschutzstechnisches Interesse daran, die Art der jeweiligen Messdaten bezüglich ihres Verwendungszweckes und ihres Personenbezuges näher zu analysieren.

4 Datenschutzprobleme im Fahrzeug der Zukunft

Ein kurzer Blick auf die Liste der Sensordaten, die in modernen Fahrzeugen verarbeitet werden, offenbart bereits eine Fülle potentiell datenschutzrechtlich bedenklicher Datenverarbeitungsprozesse. So sind etwa GPS-Position und Car2X-Sensoren offensichtlich zur Erstellung von Bewegungsprofilen des Fahrzeugs – und damit des Fahrers – nutzbar, und folglich datenschutztechnisch hochgradig sensibel. Auch die Verbrauchsdaten zu Tankfüllung bzw. Batterieladestand bergen das Potential, gefahrene Strecken über die Änderungen des Füll- bzw. Ladestands zu erkennen.

Darüber hinaus gibt es in modernen Fahrzeugen aber auch Sensorik, deren Relevanz in Hinblick auf den Datenschutz nicht sofort offensichtlich wird. Im Folgenden werden hierfür zwei Beispiele gegeben, die aufzeigen, wie sich aus vermeintlich harmlosen Sensoren hochgradig sensitive Informationen ablesen lassen. Daran anschließend wird die aktuelle rechtliche Lage rund um Datenschutz in Fahrzeugen skizziert.

4.1 Erstes Szenario: Reifendruck

Neben der potentiellen Überwachung der Position und Bewegungsmuster eines Fahrzeugs – und damit einhergehend seines Fahrers bzw. der Mitfahrer – gibt es noch andere Arten personenbezogener Informationen, die sich mehr oder weniger direkt aus den Sensordaten des Fahrzeugs der Zukunft ableiten lassen. In diesem Szenario betrachten wir eine zunächst relativ harmlos wirkende Datenquelle: den Reifendrucksensor.

In modernen Fahrzeugen muss jeder Reifen gemäß EU-Verordnung 661/2009 Art. 9 Abs. 2 [EU609] mit einem entsprechenden Reifendrucksensor ausgestattet sein. Technischer Hintergrund hier ist die frühzeitige Erkennung von Über- oder Unterdruck während der Fahrt. Dadurch können beispielsweise Unfälle aufgrund akuten Druckverlustes in voller Fahrt vermieden werden, wenn der Fahrer sofort eine Warnmeldung erhält und zeitgleich das Lenksystem des Fahrzeugs auf den reduzierten Luftdruck in einem der Fahrzeugreifen reagieren kann. Gleichermaßen können dem Fahrer Warnmeldungen angezeigt werden, wenn der Luftdruck in den Reifen insgesamt zu hoch oder zu niedrig wird, oder wenn signifikante Druckunterschiede zwischen den verschiedenen Reifen des Fahrzeugs bestehen. Auch hängt der Verbrauch eines Fahrzeugs stark vom Reifendruck ab, so dass ein korrekter Reifendruck im Fahrbetrieb hilft, Kraftstoff bzw. Batteriekapazität zu sparen.

Aufgrund der Natur eines Reifendrucksensors wird die Datenübermittlung an das Fahrzeug über eine kabellose Kommunikationsschnittstelle realisiert. Gängige Verfahren nutzen hier Techniken auf Basis von Funkwellen (z.B. Bluetooth), um die Reifendruckdaten des (rotierenden) Reifens an einen entsprechenden Empfänger am Fahrzeuggestell zu übermitteln. Moderne Reifendrucksensoren beziehen zudem bei ihren Messungen auch Temperaturunterschiede der Außenwelt über einen eingebauten Temperatursensor direkt mit ein. Ein weiterer, optionaler Bewegungssensor kann zudem ermitteln, ob ein Reifen sich gerade in Bewegung befindet oder nicht. Dies dient zum einen der präziseren Kalkulation des Reifendrucks im Stand bzw. in Fahrt, zum anderen kann der Reifendrucksensor aus Energieeffizienzgründen auf eine reduzierte Abtastrate schalten, wenn das Fahrzeug steht. Hierdurch verlängert sich die Funktionszeit der (häufig batteriebetriebenen) Reifendrucksensoren erheblich.

Die Historie der Reifendrucksensordaten wird üblicherweise in den Steuereinheiten des Fahrzeugs gespeichert, und lässt sich dort relativ leicht auslesen (vgl. etwa [Spa16]). Spätestens bei einer Übermittlung der Reifendrucksensordaten an Hersteller oder Werkstatt ist davon auszugehen, dass externe Organisationen relativ leicht direkten Zugriff auf die Reifendruckhistorie eines Fahrzeugs erlangen können.

4.1.1 Problemstellungen

Ein naheliegender Schwachpunkt in der Reifendruck-Messarchitektur besteht in der Verwendung einer drahtlosen Schnittstelle zur Datenübertragung vom Reifen an das Fahrzeug. Wie von Rouf et al. [RMM+10] nachgewiesen wurde, lässt sich eine solche Datenkommunikation im Fahrzeugbetrieb (d.h. auch während der Fahrt) erfolgreich angreifen, um etwa einen platten Reifen vorzugaukeln. Entsprechende Folgen eines solchen Angriffs reichen von einer akuten Warnmeldung an den Fahrer bis hin zu automatischen Ausweich- und Bremsmanövern, die jedoch von falschen Reifendruckwerten ausgehen und daher inkorrekte Fahrmanöver ausführen. Je größer hierbei die Autonomie des Fahrzeugs in Bezug auf sein Fahrverhalten ist, desto gravierender können die Folgen eines solchen Angriffs sein.

Ein anderer, datenschutzrechtlich wesentlich relevanterer Aspekt besteht in der Auswertung der Reifendruckhistorie. Abbildung 1 zeigt ein (konstruiertes) Beispiel für einen möglichen Druckverlauf in den Reifendrucksensoren eines Fahrzeugs über Zeit. Es ist deutlich zu erkennen, dass sich der Reifendruck mit der Zeit signifikant verändert. Stets folgt auf eine akute Erhöhung des Reifendrucks (Druckspitze) eine lange Phase geringfügig, aber signifikant höheren Luftdrucks. Dieser Unterschied lässt sich wie folgt interpretieren. Geht man von einem gewöhnlichen Fahrzeug mit vier Rädern aus, ergibt sich der tatsächliche Reifendruck hauptsächlich aus zwei Faktoren: der Luftmenge im Reifen selbst und dem Gewicht des Fahrzeugs, das darauf lastet. Bei einer angenommenen Gleichverteilung des Gewichtes auf vier Räder trägt folglich jedes Rad ein Viertel des Gesamtgewichtes des Fahrzeugs. Erhöht sich nun schlagartig der Reifendruck aller vier Reifen, so wurde entweder allen vier Reifen gleichzeitig mehr Luft zugeführt, oder das Gewicht des Fahrzeugs hat sich erhöht. Ein solches Muster ist also typischerweise stets dann zu beobachten, wenn das Fahrzeug beladen wird, bzw. wenn Personen in das Fahrzeug einsteigen – wobei ihr Körpergewicht das Gesamtgewicht des Fahrzeugs erhöht. Die Druckspitzen entstehen durch den akuten Beschleunigungsfaktor, der entsteht, wenn sich eine Person auf einen Fahrzeugsitz setzt. Anzumerken ist, dass die Messung von Druckspitzen nur in Abhängigkeit von der Abtastrate der Drucksensoren erfolgt, daher wird nicht jede Druckspitze auch aufgezeichnet. Der Übergang von einem Drucklevel zum nächsten ist aber stets ablesbar. Analog lassen sich entsprechende Reduktionen des Reifendrucks auf das Aussteigen von Personen zurückführen.

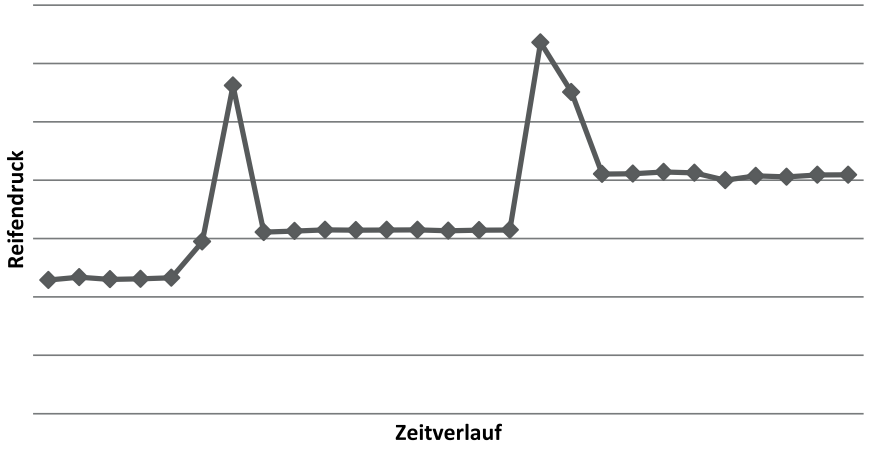

Abbildung 1: Beispiel eines Reifendruckverlaufs beim Einsteigen

Wie sich unschwer erkennen lässt, gibt die Reifendruckhistorie direkten Aufschluss darüber, zu welchen Zeitpunkten Personen das Fahrzeug bestiegen oder verlassen haben. Auch die Anzahl der Personen lässt sich leicht ableiten, entweder anhand der Zahl der Druckspitzen oder aus der Anzahl verschiedener Drucklevel im Verlauf. Rechnet man nun noch die Skaleneinheiten der Drucksensoren hinzu, lässt sich sogar das Gewicht der einzelnen Personen errechnen, indem die Differenz zwischen dem Druck vor Besteigen des Fahrzeugs und dem Druck nach Besteigen des Fahrzeugs gebildet wird. Sogar die Sitzplatzverteilung der Personen im Fahrzeug kann theoretisch ermittelt werden, wenn man annimmt, dass die Druckspitzen üblicherweise an der Fahrzeugecke am höchsten ausfallen, an der die Person

beim Einsteigen die meiste beschleunigte Masseeinwirkung ausgeübt hat. Folglich lassen sich aus den Reifendruckdaten mit relativ geringem Aufwand Profile erstellen, welche Person(en), identifiziert durch ihr Gewicht, zu welchen Zeitpunkten das Fahrzeug bestiegen oder verlassen haben.

Je nach Präzision der Gewichtsbestimmung der einzelnen Be- und Entladungen im Fahrzeug lassen sich sogar noch weitere Informationen ableiten, unter anderem zu folgenden Aspekten:

- Dauer der Fahrten (über Zeiträume zwischen Ein- und Ausstieg),
- Essgewohnheiten der wiederkehrenden Fahrzeuginsassen (über Gewichtsveränderungen),
- Schwangerschaften (über 9 Monate langsame Gewichtszunahme, gefolgt von akuter Gewichtsabnahme)
- Wachstumsverlauf und Alter von Kindern (über Gewichtsverlauf, Wechsel auf Vordersitz/Fahrersitz),
- Fahrverhalten (über Differenzen des Reifendrucks verschiedener Räder während der Fahrt, etwa bei Kurven und Brems- bzw. Beschleunigungsvorgängen), sowie
- Fahrziele (über Fahrtdauer insgesamt und zeitliche Abstände von Kurven und Brems-/Beschleunigungsmanövern).

Wie unschwer zu erkennen ist, geben Reifendrucksensordaten eine Fülle zusätzlicher Informationen preis, wenn sie längerfristig aufgezeichnet werden. Einige dieser Informationen sind dabei sogar besonders sensibler Natur (siehe Schwangerschaften), sodass hier ein hoher Schutzbedarf für derartige Daten abgeleitet werden muss. Die Übertragung dieser Daten im Rohzustand an die Steuerungseinheiten des Fahrzeugs oder gar an externe Parteien (über Mobilschnittstelle oder Auslesen in der Werkstatt) ist somit als hochgradig bedenklich einzustufen.

Es bleibt anzumerken, dass viele der genannten Informationen sich in ähnlicher Form auch aus anderen Sensordaten im Fahrzeug der Zukunft ermitteln lassen. So sind Autositze bereits heute mit Gewichtssensoren ausgestattet, um ggfs. zu warnen, wenn ein Insasse des Fahrzeugs nicht angeschnallt ist. Auch die Auszugweite eines Anschnallgurtes oder die Einstellungen von Sitz-und Lehnenpositionen erlauben Rückschlüsse auf die Insassen.

4.1.2 Lösungswege

Für die genannten Einsatzzwecke des Reifendrucksensors wäre es technisch hinreichend, die Einhaltung der relevanten Grenzen für den Reifendruck direkt im Sensor abzuprüfen, und nur bei Überschreiten einer solchen Grenze eine Kommunikation nach außen (d.h. zum Fahrzeug, zum Fahrer oder zu anderen Sensoren bzw. Steuergeräten) aufzubauen. Bei einer solchen Architektur würden die Informationen, die den einzelnen Reifendrucksensor

verlassen, kaum noch in realistischem Maße für die oben beschriebenen datenschutztechnisch bedenklichen Auswertungen nutzbar sein. Die relevanten Nutzinformationen (Reifendruck zu hoch oder zu niedrig) blieben erhalten, das Signal selbst würde jedoch verborgen bleiben. Entsprechend würde dem Datenschutzprinzip der Datensparsamkeit durch eine solche Architektur am ehesten entsprochen werden, ohne die legitimen Anwendungszwecke für Reifendrucksensoren zu verbauen.

Im Zuge der Vollvernetzung des Fahrzeugs findet sich heutzutage allerdings die gegenteilige Entwicklung: Reifendruckdaten werden im Original an die Steuereinheiten des Fahrzeugs übermittelt, dort aufgezeichnet und ausgewertet, und ggfs. an Hersteller, Werkstätten und andere Organisationen weitergegeben. Die Annahme hierbei ist, dass sich Reifendruckdaten auch für andere nützliche Anwendungszwecke einbeziehen lassen (ABS-Steuerung, Klimaanlagensteuerung, Überladungswarnungen etc.). Hier muss folglich eine umfassende Abwägung zwischen den verschiedenen legitimen und illegitimen Anwendungszwecken der Reifendruckdaten erfolgen. Zum gegenwärtigen Zeitpunkt ist hier aber nicht von einer datenschutzseitig vorteilhaften Ausgestaltung der Informationsflüsse im Fahrzeug der Zukunft auszugehen.

4.2 Zweites Szenario: Bewegungsprofile anderer Verkehrsteilnehmer

Damit sich Fahrzeuge autonom im Straßenverkehr bewegen können, müssen fortlaufend Informationen über die jeweilige Umgebung und damit auch über die eigene Position gesammelt werden. Diese Informationen über die Umgebung werden in der Regel in sogenannten SLAM-Algorithmen (Simultanous Localization and Mapping) verarbeitet, um eine genaue Umgebungskarte zu generieren und gleichzeitig eine möglichst exakte Bestimmung der eigenen Lokation vorzunehmen.

Abbildung 2 zeigt die Einbindung der Kartographierung in die Gesamtarchitektur eines autononem Fahrzeugs. Hindernisse werden dabei mit Hilfe von Sensoren (Ultraschall, Radar, Laser, ...) detektiert [TMD+06]. Die Existenz oder die Nicht-Existenz von Hindernissen kann allerdings nur mit einer gewissen Wahrscheinlichkeit angegeben werden. Dies liegt beispielsweise an Artefakten wie Schattenwurf oder auch an Fehlfunktionen von Sensoren. Um diese Wahrscheinlichkeiten zu erhöhen, werden fortlaufend Umgebungskarten erstellt, mit bereits generierten Karten abgeglichen und auf diese Weise aktualisiert wie auch detailliert. De facto gelingt dies durch Verwendung bedingter Wahrscheinlichkeiten. So wird die Wahrscheinlichkeit der Existenz eines Hindernisses erhöht, wenn die nachfolgende Auswertung der Sensoren wiederum ergibt, dass sich an der bezeichneten Stelle ein Hindernis befindet.

Das oben beschriebene Vorgehen funktioniert zunächst nur für unbewegliche Hindernisse, kann aber auf bewegliche Objekte ausgeweitet werden. Hierzu müssen weitere Informationen wie beispielsweise Bewegungsrichtung und Objektgeschwindigkeit erfasst werden. Dennoch ist eine Detektion beweglicher Objekte mit größeren Unsicherheiten verbunden. Eine mangelhafte bzw. zu späte Detektion beweglicher Objekte (z.B. Ball, Mensch) kann problematisch werden, da hier – in Abhängigkeit von der Geschwindigkeit der bewegli-

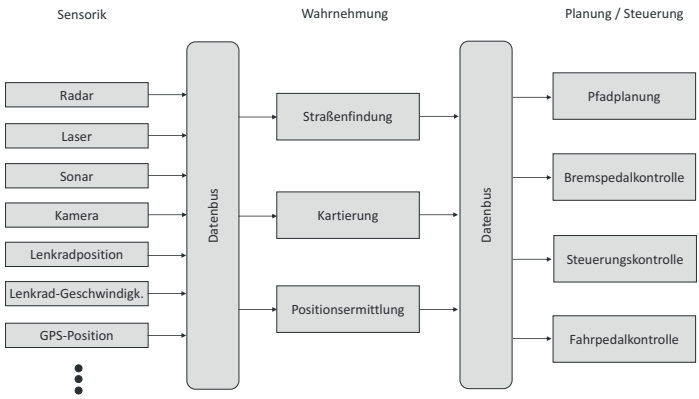

Abbildung 2: IT-Architektur eines autonomen Fahrzeugs (Ausschnitt, vereinfacht)

chen Objekte – ggf. zu hohe Anforderungen an die Reaktionszeiten von autonomen Fahrzeugen gestellt werden könnten.

In Abbildung 3 ist eine derartige Situation dargestellt. Die unterschiedlichen Grautöne geben das Maß an Sicherheit wider, mit der ein autonomes Fahrzeug ein Hindernis erkannt hat (hellgrau: Hindernis mit noch recht geringer Gewissheit erkannt, schwarz: Hindernis mit sehr hoher Gewissheit erkannt). In dieser Darstellung ist ebenfalls angedeutet, dass eine sichere Detektion beweglicher Objekte in der Regel mehr Sensordaten erfordert und damit zeitaufwändiger ist.

Um die Geschwindigkeit der oben skizzierten Kartierung zu erhöhen, könnten bereits existierende – aktuelle – Karten genutzt werden. Als Quellen derartiger Umgebungskarten kommen stationäre Objekte (z.B. Straßenlaternen) wie auch bewegliche Objekte (z.B. andere autonome Fahrzeuge) in Frage. So trägt beispielsweise eine Vernetzung von autonomen Fahrzeugen mit dem Ziel der Weitergabe bereits erstellter Karten dazu bei, dass sich die Güte der von den autonomen Fahrzeugen verwendeten Karten erhöht und damit auch die Grundlage für Entscheidungen verbessert.

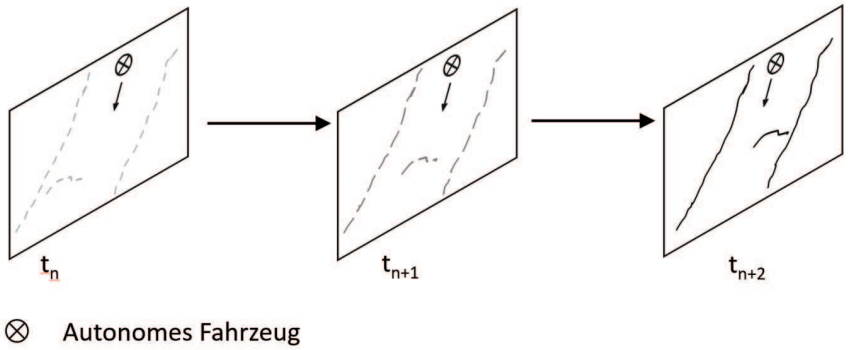

Abbildung 3: Kartierung mittels SLAM-Agorithmen (Prinzipskizze)

4.2.1 Problemstellungen

Die sich aus diesem Szenario ergebenden datenschutzrelevanten Problemstellungen sind mannigfaltig. Eine detaillierte Beschreibung sprengt den gesetzten Rahmen. An dieser Stelle soll daher nur auf die Möglichkeit der Generierung von Bewegungsprofilen anderer Verkehrsteilnehmer eingegangen werden.

Es werden in diesem Szenario Daten zwischen autonomen Fahrzeugen drahtlos übermittelt. Diese Daten sind keine Sensor-Rohdaten, sondern – in Form von Karten – bereits vorverarbeitete Daten. Die übermittelten Karten enthalten neben Informationen zu stationären Hindernissen oder Straßen auch Informationen über bewegliche Objekte, sofern diese eine Relevanz für die Exploration der Umgebung eines autonomen Fahrzeugs besitzen. Aus diesen – ggf. von mehreren autonomen Fahrzeugen – übermittelten Karten lassen sich zumindest über begrenzte Zeiträume Bewegungsprofile von Fußgängern erstellen, aus denen sich gegebenenfalls sogar die Identität dieser Verkehrsteilnehmer ableiten lässt.

Nicht nur autonome Fahrzeuge können solche Karten generieren. Auch stationäre Objekte wie z.B. mit entsprechenden Sensoren ausgerüsteten Straßenlaternen sind in der Lage eine Kartierung ihrer jeweiligen Umgebung vorzunehmen, um diese Informationen an autonome Fahrzeuge drahtlos zu übermitteln. Hier ist die Gefahr der Erstellung von Bewegungsprofilen anderer Verkehrsteilnehmer (z.B. Fußgänger) ungleich größer.

4.2.2 Lösungsszenarien

Da das Erkennen von Hindernissen (inkl. Fußgänger) und das Erstellen von (möglichst genauen) Karten ein integraler Bestandteil des autonomen Fahrens ist, lässt sich die dabei automatisch abfallende Erstellung von Bewegungsprofilen nicht einfach verhindern. Eine Möglichkeit zur Minderung dieser Gefahr wäre eine rein lokal Generierung von Karten ohne die Weitergabe an andere Teilnehmer. Allerdings verbessert die Verwendung von Karten anderer Provenienz die Genauigkeit der von einem autonomen Fahrzeug verwendeten Kartierung seiner Umgebung und erhöht damit auch die Sicherheit aller Verkehrsteilnehmer.

So verbleibt die Frage, ob insbesondere zu der Ausrüstung stationärer Objekte mit Sensoren Alternativen existieren, mit denen es nicht so einfach möglich ist, Bewegungsprofile von Verkehrsteilnehmern aufzuzeichnen.

4.3 Rechtliche Lage

Unabhängig von den konkreten einzelnen Datentypen lässt sich festhalten, dass das Fahrzeug der Zukunft umfassende personenbeziehbare und teils hochsensible Daten und Informationen verarbeitet. Entsprechend besteht nach BDSG §4 Abs. 1 (Verbot mit Erlaubnisvorbehalt) die Notwendigkeit einer geeigneten Rechtsgrundlage für die Erhebung und Verarbeitung dieser Daten. Zwar existieren hier teilweise entsprechende Regularien

(vgl. [EU609]), diese sind allerdings stets zweckgebunden und daher nicht ohne Weiteres auf die hier geschilderten Verarbeitungsvorgänge übertragbar. Insoweit bleibt für eine Rechtsgrundlage meist nur der populäre Weg der Einwilligung der Betroffenen (vgl. BDSG §4 Abs. 1 bzw. BDSG §4a). Allerdings ergeben sich im Kontext vernetzter Fahrzeuge hier große Herausforderungen: Wie sieht eine informierte, freiwillige Einwilligung in die Datenverarbeitung im Fahrzeug aus? Den Fahrer könnte man über die (nicht sehr ausdrucksstarken) Kommunikationsmöglichkeiten von Display und Bedienelementen im Armaturenbrett des Fahrzeugs erreichen, um eine Information und eine Einwilligung zu erhalten. Der Fahrzeughalter könnte möglicherweise bereits beim Kauf des Fahrzeugs über die Datenerhebung und -verarbeitung informiert und um Einwilligung gebeten werden.

Schwieriger wird die Einwilligung aber schon in Bezug auf Beifahrer, die ggf. nicht über ein eigenes Fahrzeug-Bedienelement verfügen. Wie in Abschnitt 4.1 ausgeführt werden auch personenbeziehbare Daten dieser Beifahrer umfassend Teil der fahrzeuginternen Datenerfassung, -verarbeitung und -weitergabe. Für häufig wiederkehrende Mitfahrer, etwa Familienmitglieder, ließe sich hier möglicherweise ein Konstrukt ähnlich der Haltereinwilligung zum Zeitpunkt des Fahrzeugkaufes realisieren. Dies dürfte jedoch für seltenere oder gar spontan aufgenommene Beifahrer nicht praktikabel sein.

Gänzlich unbrauchbar wird das Instrument der Einwilligung in Bezug auf Daten über andere Verkehrsteilnehmer. So kann ein Fußgänger an einem Zebrastreifen wohl kaum vorab um Erlaubnis gebeten werden, wenn er von den Kameras bzw. den hochauflösenden Laser- oder Radar-basierten Umgebungssensoren eines (teil-)autonomen Fahrzeugs erfasst und gescannt wird. Nichtsdestotrotz werden Daten über solche Verkehrsteilnehmer zweifelsohne erhoben und verarbeitet, ohne Einwilligung, und häufig ohne Kenntnis der Betroffenen.

Dass eine derartige Datenerhebung unbeteiligter Dritter rechtlich vermutlich unzulässig ist, lässt sich bereits aus der Urteilsbegründung des berühmten Dashcam-Urteils herauslesen (vgl. VG Ansbach in seinem Urteil vom 12.08.2014, Az: AN 4 K 13.01634), bei dem die Rechtmäßigkeit von Videoaufzeichnungen der direkten Umgebung eines Fahrzeugs zum Zwecke der Beweisdokumentation im Unfallfall deutlich angezweifelt wurde. Diese Einschätzung dürfte auf bildgebende Laser- oder Radarabtastungen ähnlich übertragbar sein, die zwar weniger Bildinformation liefern als eine vollwertige Kamera, aber dennoch hinreichend präzise Daten für eine Profilbildung und damit eine potentielle spätere Identifizierung von Personen erheben.

Es bedarf hier folglich einer Abwägung durch den Gesetzgeber: ist der Zweck der (teil-) autonomen Fahrzeugführung mit all ihren Vor- und Nachteilen ein überwiegendes Gut gegenüber den Beeinträchtigungen der Betroffenen? Ist hier ggfs. eine entsprechende Rechtsgrundlage zu schaffen? Zur Beantwortung dieser juristischen Kernfrage des autonomen Fahrzeugs der Zukunft bedarf es sicherlich zunächst weiterer technischer Forschungsdaten, um die tatsächlichen Vor- und Nachteile des autonomen Fahrens gegeneinander abwägen zu können. Rein juristisch ist vermutlich ein Großteil der vernetzt und (teil-) autonom fahrenden Fahrzeuge nach heutigem Rechtsstand nicht völlig rechtskonform im deutschen Straßenverkehr einsetzbar.

5 Lösungswege

5.1 Technische Lösungen

Zur Verbesserung der Privatsphäre können zum großen Teil bekannte Techniken des Datenschutzes verwendet werden. Allerdings können diese auch nur wirksam eingesetzt werden, wenn das komplexe Ökosystem rund um das Fahrzeug der Zukunft in Gänze analysiert wird und alle Bestandteile aufeinander abgestimmt sind. Da dies noch nicht der Fall ist, wird im Folgenden nur angedeutet, wie die jeweiligen Techniken zu einer Gesamtlösung beitragen könnten.

5.1.1 Zugriffskontrolle

Ein wichtiges Werkzeug zum Schutz von Daten (vor Auslesen aber auch vor Veränderung) ist die Zugriffskontrolle. Dabei wird an den Schnittstellen bzw. Diensten, über die auf die Daten zugegriffen wird, überprüft, ob das Subjekt die erforderlichen Privilegien besitzt. Dies erfordert detaillierte Richtlinien (engl. *Policies*), in denen die Zugriffsrechte festgelegt sind.

Während bei netzwerkbasierten Softwaresystemen (beispielsweise bei Web-Diensten) diese Technik standardmäßig verwendet wird, so ist dies bei intelligenten Fahrzeuge offensichtlich nicht der Fall. Dies zeigt auch der Fall des „gekaperten“ Chryslers [Gre].

Ein elaboriertes Zugriffskontroll-System könnte hier sowohl die Sicherheit als auch den Datenschutz verbessern. Man könnte damit den Zugriffe für Aussenstehende unterbinden und für Berechtigte zumindest einschränken. So ist es beispielsweise nicht notwendig, dass ein Mechaniker in der Werkstatt vollen Zugriff auf alle Daten erhält, sondern nur auf diejenigen, die für die momentane Tätigkeit notwendig ist. Weiterhin könnten auch bestimmte Datenzugriffe von außen die (temporäre) Freischaltung durch den Fahrer bzw. Halter erfordern.

5.1.2 Datensparsamkeit

Datensparsamkeit wird explizit im BDSG als Mittel zur Verbesserung des Datenschutzes erwähnt. Es sollten nur so wenig personenbezogene Daten wie möglich erhoben werden. Wie in diesem Artikel dargelegt, sind viele der im Fahrzeug der Zukunft gespeicherten oder kommunizierten Daten personenbezogen oder zumindest personenbeziehbar. Bei vielen der erhobenen Daten stellt sich auch die Frage nach dem Zweck der Speicherung (siehe beispielsweise [Spa16]). Hier sollte eine strenge Auswahl der relevanten Daten erfolgen.

5.1.3 Anonymisierung

Auch Anonymisierung wird bereits im BDGS aufgegriffen. Werden Daten so verändert, dass der Personenbezug nicht mehr enthalten ist, so sind sie für die Einzelperson unkritisch und fallen auch nicht mehr unter das BDSG. Bei vielen Daten rund um das Fahrzeug

der Zukunft ist der Bezug zu einer Person (oder einem Automobil) gar nicht relevant. Beispielsweise ist es zur Verkehrssteuerung typischerweise unwichtig, welche Fahrzeuge an einem Ort sind, nur die Anzahl der Fahrzeuge (und weitere Eigenschaften wie Geschwindigkeit, die keine Zuordnung erlauben) ist nötig.

Allerdings lässt sich Anonymisierung bei ungeschickter Umsetzung oder durch Erlangungen von zusätzlichen Informationen auch wieder aufheben. So kann beispielsweise die Information „silbergrauer Golf“ als anonym angesehen werden, während die Information „pinkfarbener Ferrari“ höchstwahrscheinlich genau ein Fahrzeug beschreibt (zumindest in einer Stadt). Ein anderes Beispiel wurde bereits im Abschnitt 4.2 beschrieben: das Bewegungsprofil einer (anonymen) Person ist unkritisch. Allerdings kann durch genaue Analyse und weitere Informationen (in welchen Hauseingang geht diese Person und wer wohnt in diesem Haus) auch hier die Anonymität wieder aufgehoben werden.

Anonymisierung ist also ein sehr mächtiges Werkzeug, welches die Weiterverarbeitung von Daten unter Beibehaltung der Privatsphäre ermöglicht. Allerdings müssen auch die Randbedingungen genau beachtet werden.

5.2 Rechtliche Lösungen

Wie bereits oben erwähnt, widersprechen wahrscheinlich ein Großteil der aktuellen oder geplanten Datenverwendungen den gesetzlichen Bestimmungen. Hier sollte die Einhaltung der Normen, z.B. von Datenschutzbeauftragten, verstärkt überprüft werden.

Weiterhin stellt sich aber auch die Frage, ob neuartige technische Systeme wie das Fahrzeug der Zukunft noch hinreichend vom BDSG abgedeckt werden können und nicht neue Datenschutzbestimmungen erforderlich sind. Hier wird interessant zu analysieren sein, wie sich die neue Datenschutz-Grundverordnung (vgl. [DSG16]) auf die Datenerhebung und -verarbeitung im Fahrzeug der Zukunft auswirken wird.

6 Zusammenfassung und Ausblick

Der vorliegende Artikel hat dargelegt, welche Datenschutzprobleme beim Fahrzeug der Zukunft auftreten können. Kritisch ist dabei die Kombination aus einer Vielzahl von Sensoren, exzessiver Speicherung von Sensordaten und der Vernetzung des Fahrzeugs mit vielen anderen Instanzen. Betrachtet man die aktuell bereits existierenden Systeme, so scheint zusätzlich beim Entwurf sowohl Sicherheit als auch Datenschutz nicht besonders beachtet worden zu sein.

Hier lassen sich in Zukunft durch verbessertes Systemdesign und Berücksichtigung von IT-Sicherheits- und Datenschutz-Mechanismen noch deutliche Fortschritte erzielen. Zusätzlich muss verstärkt auf die Einhaltung der gesetzlichen Bestimmungen geachtet werden, und diese sind gegebenenfalls an die neuartigen Anforderungen anzupassen.

Literatur

[ADA16] ADAC. Autos mit Keyless leichter zu klauen. `https://www.adac.de/keyless`, 2016.

[BFN] Manuel Bewarder, Florian Flade und Lars-Marten Nagel. BSI-Chef warnt vor Hackerangriffen auf Autos und Flugzeugen. *DIE WELT*, 26.04.2016.

[DSG16] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), April 2016.

[EU609] Verordnung (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates über die Typgenehmigung von Kraftfahrzeugen, Kraftfahrzeuganhängern und von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge hinsichtlich ihrer allgemeinen Sicherheit, 2009.

[Gom16] Lee Gomes. When will Google's self-driving car really be ready? It depends on where you live and what you mean by "ready". *IEEE Spectrum*, 53(5):13–14, 2016.

[Gre] Andy Greenberg. Hackers Remotely Kill a Jeep on the Highway—With Me in It. *WIRED*, 21.07.2015.

[Gui11] Erico Guizzo. How google's self-driving car works. *IEEE Spectrum Online, October*, 18, 2011.

[Rei11] Konrad Reif. *Bosch Autoelektrik und Autoelektronik*. Springer, ISBN: 978-3-8348-1274-2 (Print) 978-3-8348-9902-6 (Online), 2011.

[RMM+10] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe und Ivan Seskar. Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study. In *Proceedings of the 19th USENIX Conference on Security*, USENIX Security'10, Seite 21 ff., Berkeley, CA, USA, 2010. USENIX Association.

[Spa16] Dieter Spaar. Daten auf Rädern: Was moderne Autos speichern und wie man an die Informationen herankommt. In *c't Magazin 09/2016, Heise-Verlag, ISSN 0724-8679*, Seite 170 ff., 2016.

[TMD+06] Sebastian Thrun, Mike Montemerlo, Hendrik Dahlkamp, David Stavens, Andrei Aron, James Diebel, Philip Fong, John Gale, Morgan Halpenny, Gabriel Hoffmann, Kenny Lau, Celia Oakley, Mark Palatucci, Vaughan Pratt, Pascal Stang, Sven Strohband, Cedric Dupont, Lars-Erik Jendrossek, Christian Koelen, Charles Markey, Carlo Rummel, Joe van Niekerk, Eric Jensen, Philippe Alessandrini, Gary Bradski, Bob Davies, Scott Ettinger, Adrian Kaehler, Ara Nefian und Pamela Mahoney. Stanley: The robot that won the DARPA Grand Challenge. *Journal of Field Robotics*, 23(9):661–692, September 2006.