CASTON

INTERNATIONAL LAW & BUSINESS INFORMATION | PUBLISHED BY HERFURTH & PARTNER | SINCE 1988 | CASTON COMPACT

Daten im Intelligenten Fahrzeug

Marc-André Delp, M.L.E., Rechtsanwalt in Hannover

No 369 | SEPTEMBER 2016 | APRIL 2017

Selbstfahrende (autonome oder automatisierte) Fahrzeuge benötigen einen rechtlichen Rahmen für die Nutzung im Straßenverkehr. Dieser und die dabei resultierenden Haftungsfragen sind im Folgenden zu klären. Daneben sind aber gerade auch die Daten an sich, die in einem intelligenten Fahrzeug gewonnen werden sowie die Fragen zur Datensicherheit von Bedeutung. Denn die zunehmende Vernetzung bietet nicht nur Chancen und Entwicklungspotential bei der Kommunikation der Fahrzeuge, sie birgt auch Risiken und eröffnet die Möglichkeiten von Manipulationen.[1]

Datensicherheit

Bislang bestand bei den zentralen Funktionen des Fahrzeugs wie Bremsen, Gasgeben (Längsfunktion) und Lenken (Querfunktion) keine Verbindung des Fahrzeugs (Systems) nach außen. Von innen konnte eine Manipulation am Fahrzeug aber nur durch Chiptuning erfolgen. Für einen Cyber-Angriff auf ein Fahrzeug musste somit noch eine physische Manipulation vorgenommen werden; eine komplexe und aufwändige Vorarbeit war dazu notwendig.

Die Vernetzung von Fahrzeugen bietet jedoch viele Vorteile, da die Unfallrisiken im Ergebnis minimiert werden können. Allerdings erhöht die Vernetzung auch die Gefahr von Hackerangriffen auf und in die Fahrzeuge. Die Vielschichtigkeit der Automationsprodukte birgt Angriffsflächen für Cyberattacken durch Dritte. Mit zunehmender Vernetzung der Systeme sind die Angriffe von außen auf ein Fahrzeug möglich, auch bei dessen Betrieb des selbigen. Angriffsszenarien über Android- Systeme im Fahrzeug sind ebenso möglich. Angriffspunkte sind dabei zum Beispiel die Sensoren für Fahrassistenzsysteme mit Steuerung über Smartphone. Beispiele hierfür gibt es genug. Im Jahre 2015 beschäftigte die Presse, dass Hacker / Studenten der Zhejiang Universität einen Tesla S hackten und in voller Fahrt Türen und Schiebedach öffneten, die Lampen einschalteten und die Hupe betätigten. Dieses geschah in einem Wettbewerb der Sicherheitskonferenz Syscan in Peking. Der Konzern Fiat Chrysler rief 2015 Millionen Autos wegen mangelndem Schutz vor Hackerangriffen zurück. Zwei IT-Sicherheitsexperten konnten dabei über eine Sicherheitslücke im Jeep Cherokee mittelbar das dortige Infotainment-System bis zur Steuerung des Fahrzeugs vordringen und Bremsen, Geschwindigkeit, Klimaanlage und Radio fernsteuern. Dabei saßen sie in ihrem Wohnzimmer.

Ebenfalls wurde berichtet, dass sich im August 2015 Forscher über das Telematik-Gerät ihrer Versicherung in eine Chevrolet Corvette einhacken und den Wagen abbremsen konnten, der jedoch nur bei geringer Geschwindigkeit fuhr. Diese Tests geschahen, um auf vorliegende Sicherheitslücken aufmerksam zu machen. Die Autohersteller haben schnell auf diese Hinweise reagiert und Abwehrmaßnahmen entwickelt, jedoch zeigt sich hier vor allem die technische Manipulationsmöglichkeit.

Im Jahr 2015 wollte Continental als Systemintegrator in Kooperation mit Cisco sich für Datenaustausch in

[1] Aus der Reihe: Rechtsrahmen für autonomes Fahren, Haftung beim Autonomen Fahren, Daten in intelligenten Fahrzeugen (Juli-September 2016, aktualisiert im April 2017)

der Cloud einsetzen. Dazu wollte Continental Firewalls entwickeln und die Hypervisor- Virtualisierungstechnologie in Fahrzeuge integrieren (wie schon in der Luftfahrt geschehen). Dadurch bekommen vernetzte Funktionen (Android) nur über bestimmte Schnittstellen Zugriff zum System und sind auf bestimmte Funktionen /Rechte beschränkt. Nach einer Studie des ADAC kann fast jede Regung eines modernen Fahrzeugs aufgezeichnet und über Mobilfunk an die Konzerne übermittelt werden, also eine Datenautobahn zum Hersteller. Die Datensicherheit in Fahrzeugen wird, wie auch bei anderen vernetzten Maschinen, Fabriken usw., ein zentrales Thema für die Zukunft sein. Durch Vernetzung bestehen Zugriffsmöglichkeiten von außen und Manipulationen der Systeme sind möglich. Hier gilt es wirksame Schutzmechanismen zu schaffen und vor allem weiter zu entwickeln.

Datenschutz

Im Zusammenhang mit den Daten, die in den Fahrzeugen aufgezeichnet und übermittelt werden, spricht man vom Connected Car. Als Connected Car bezeichnet man Fahrzeuge, die mittels verschiedener Sensoren und Benutzerschnittstellen eine Vielzahl von Daten erfassen und unter Nutzung verschiedener Übertragungstechniken im Kontakt mit ihrer Umwelt (z.B. auch Internet) stehen. Dabei ist zu berücksichtigen, dass auch die Daten aus den Fahrzeugen dem Datenschutz unterliegen können. Das Datenschutzrecht findet auf die Erhebung, Verarbeitung und Nutzung von Daten Anwendung, wenn die betreffenden Daten personenbezogen sind. Personenbezogene Daten sind gemäß § 3 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Bezüglich Fahrzeugdaten ist seitens des VDA und der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder in einer gemeinsamen Erklärung am 26.01.2016 dargelegt worden, dass ein Personenbezug bei Daten, die die Fahrzeugnutzung betreffen, jedenfalls dann anzunehmen sei, wenn die Daten mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen verknüpft sind (*https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html*). Viele Daten, die in einem Fahrzeug anfallen, unterliegen dagegen nicht der Personengebundenheit (z.B. rein technische Daten aus Steuerungssystemen). Diese werden erst durch Verbindung mit den genannten Anknüpfungspunkten oder Fahrer oder Halter zu personenbezogenen Daten. Ein datenschutzrelevantes Erheben wird auch nicht schon im Speichern der Daten im Fahrzeug zu sehen sein. Erst wenn ein Verantwortlicher die Datenverfügungsgewalt erhält (z.B durch online Empfang oder Zugriff auf die Daten), ist von einem datenschutzrechtlichen Erheben auszugehen. Wenn also personenbezogene Daten aus einem Fahrzeug erhoben, verarbeitet oder genutzt werden, ist dazu entweder eine Einwilligung oder eine Rechtsgrundlage (z.B. BDSG, aber auch weitere) notwendig.
Auch in Zukunft wird also eine Art „gläserner Fahrer“ grundsätzlich nicht möglich sein. Gleichwohl haben viele Institutionen ein Interesse an den im Fahrzeug erhobenen Daten, zu denen Hersteller und Systemanbieter, Polizei und Staat sowie Versicherer zählen. Bei den Herstellern und Systemanbietern stellt sich bereits die Frage, wer Herr über die beim Betrieb eines Kraftfahrzeugs erhobenen Daten ist: Zum Beispiel Apple, Google, Facebook, Amazon, Audi, BMW, Mercedes-Benz, Porsche, oder Continental? Wem gehören die Daten aus technischem Betrieb, Bewegungsprofilen, Wartung/Service etc.? Die Fahrer bekommen in den wenigsten Fällen Informationen, was mit ihren Daten geschieht. Hersteller könnten sich bereits beim Autokauf in den AGB ein Zugriffsrecht auf Daten sichern, so dass technische Daten in regelmäßigen Abständen an Hersteller übertragen werden dürfen. Ein mögliches anderes Szenario ist, dass die Person, die nicht will, dass ihre Daten im Auto vom Hersteller ausgelesen werden, ihr Fahrzeug nicht zur Wartung bringen kann.
Der Wert der Daten ist groß, die Folgen ebenso:

Werkstätten / Hersteller können aus Daten zum Beispiel auslesen, ob ein Fahrer bestimmungsgemäß gefahren ist. So verweigerte ein Sportwagenhersteller die Garantie, wenn ein Wagen auf Rennstrecken bewegt wurde und dies an sich untersagt war bzw. einen Ausschlussgrund darstellte. Die Datenerhebung kann auch zu einer Veränderung der Beweislage führen, wenn beispielsweise bei einem Motorschaden das System mitteilt, im Cockpit habe eine Warnlampe ge-

brannt, die der Fahrer übersehen hat. Auch wenn der Fahrer widerspricht, hat er praktisch keine Möglichkeit, einen Fehler im System zu widerlegen. Dabei stellt sich die Frage, wem zur Beweiserleichterung oder im Streitfalle erhobene Daten zur Verfügung zu stellen sind. Könnte in einem derartigen Fall der Fahrer vom Hersteller die Herausgabe oder Offenlegung der Daten vom Hersteller verlangen? Bereits auf dem Verkehrsgerichtstag in Goslar im Jahr 2014 wurde folgende Empfehlung aufgestellt: Die informationelle Selbstbestimmung ist ein Grundrecht. Nur Fahrer / Besitzer haben Rechte daran: im Auto produzierte Daten sind personenbezogen oder zumindest auf eine Person beziehbar. Damit dürfen sie nicht ohne ausdrückliche Zustimmung des Halters oder Fahrers ausgelesen und genutzt werden. Die im Gesetzesentwurf zur Änderung des StVG vorgesehene Blackbox sieht die Herausgabe der Daten bei Verlangen an die zuständigen Behörden vor, aber auch an Dritte, wenn sie glaubhaft machen, dass diese Daten für Geltendmachung oder Abwehr von Rechtsansprüchen benötigt werden und das entsprechende Kraftfahrzeug mit automatisierter Fahrfunktion an dem Ereignis beteiligt war.

Auch die Polizei könnte ein Interesse an den beim Betrieb eines Kraftfahrzeugs erhobenen Daten haben. Die Polizei könnte belastendes Datenmaterial leicht auslesen: Sammlung von Daten über ABS-Steuergerät, Navigationssystem, Motorsteuerung, Daten zu Bremsmanöver, Fahrzeugposition, Geschwindigkeit usw. Diese Daten könnten dann zur Belastung des Fahrers herangezogen werden. Über das Auslesen von Speichereinheiten in Fahrzeugen lässt sich eine Vielzahl an wichtigen Daten beispielsweise für die Unfallrekonstruktion gewinnen. Der vorliegende Gesetzesentwurf sieht allerdings eine Löschung der aufgezeichneten Daten spätestens nach drei Jahren vor. Die Black Box soll dabei aufzeichnen, ob das Fahrzeug durch den Fahrzeugführer oder mittels hoch- oder vollautomatisierter Fahrfunktion gesteuert wird. Ebenso wird aufgezeichnet, ob das System den Fahrzeugführer zur Übernahme der Fahrzeugsteuerung aufgefordert hat oder ob ggf. eine technische Störung des Systems vorgelegen hat.

Die Daten sollen nach dem Gesetzesentwurf gespeichert und genutzt werden können. Die allgemeinen Regeln zur Verarbeitung personenbezogener Daten sollen aber unberührt bleiben.

Das Auslesen zum Zweck der Unfallrekonstruktion betrifft aber personenbezogene Daten. Bei Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) muss daher eine Einwilligung des Betroffenen oder ein gesetzlicher Erlaubnistatbestand vorliegen, wobei dieser nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorliegen.

Könnte die Missachtung des Signals für verschlissene Bremsbeläge bereits eine durch die Polizei zu ahndende Ordnungswidrigkeit darstellen? Was passiert mit Daten, die bei der Auswertung anderer Daten gewonnen werden (Zufallsdatenfund)? Kann ein unmittelbarer Zugriff auf die Daten wegen Gefahr der Löschung der Daten unmittelbar erfolgen? Hier wird dem selbständigen Beweisverfahren zur Sicherung von Daten für die Unfallrekonstruktion eine besondere Bedeutung zugemessen. Mit diesem Verfahren könnten die wichtigen Daten, die jedoch nur kurzzeitig gespeichert sind, gesichert werden.
In manchen Fällen könnten die gewonnenen Daten aber auch zur Entlastung dienen. So wurde ein Popstar wegen eines unerlaubten Rennens und Motorenlärm in einem gemieteten Ferrari verhaftet. Ihm wurde vorgeworfen, ein illegales Rennen in der Stadt gefahren zu sein. Die Auswertung der Daten ergab jedoch lediglich eine Geschwindigkeit von 40 km/h. Hier hat das Problem schlussendlich wohl eher in der fehlenden Beherrschbarkeit der Gangschaltung gelegen. Ohne Datenauswertung wäre diese Entlastung nicht geglückt.

Letztendlich spielen die Daten auch für die Versicherungen eine große Rolle, eine Versicherungsverschiebung von Fahrzeughalter und Versicherung auf den Hersteller könnte durch die Nutzungen von automatisierten Steuerungen erfolgen. Kfz-Haftpflicht würde dann praktisch zur Produkthaftpflicht werden.

Für Versicherungen könnten Datenauswertungen dabei von großem Nutzen sein. Versicherungen können dann die Leistungen verweigern, wenn eine Obliegenheitsverletzung des Versicherungsnehmers

vorliegt. Danach könnte möglicherweise ein Versicherungsanspruch erlöschen, wenn der Fahrer bei angezeigter Übermüdung dennoch weiterfährt und einen Unfall verursacht. Auch werden bereits besondere Versicherungspakete mit verbesserten Prämien für diejenigen angeboten werden, die sich mit einer laufend Datenübermittlung zum Fahrverhalten (Bremsen, Beschleunigen) an ein Rechenzentrum einverstanden erklären. Hersteller könnten eigene Versicherungen anbieten, dabei würden sich beispielsweise gewonnene technische Erkenntnisse für die Gestaltung der Tarife nutzen lassen.

Der Deutsche Anwaltsverein plädierte schon 2015 bereits für Klarheit im Umgang mit Daten (Erhebung, Speicherung, Dokumentation, Weitergabe). Der Verbraucherzentrale-Bundesverband hat 2016 ein Gutachten zum Datenschutz erstellen lassen. Danach müsse technisch sichergestellt sein, dass personenbezogene Daten nicht aufgezeichnet werden. Erhobene Daten dürften nur in Ausnahmefällen Unternehmen oder Behörden zur Verfügung gestellt werden. In der vom VDA und der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder veröffentlichen gemeinsamen Erklärung ist auch der Aspekt der Datenhoheit und des Auskunftsrechts angesprochen worden. Gegenüber dem Hersteller besteht ein unentgeltliches Auskunftsrecht des Halters über seine durch den Hersteller erhobenen oder gespeicherten personenbezogenen Daten gemäß § 34 BDSG. In Bezug auf Datenhoheit sollen die Fahrzeugnutzer durch verschiedene Optionen über die Verarbeitung und Nutzung personenbezogener Daten selbst bestimmen können.

Fazit

Das Thema Datensicherheit ist eine der großen Herausforderungen bei der zunehmenden Automatisierung der Fahrzeuge. Manipulationen von außen sind über die zahlreichen Schnittstellen möglich und müssen daher bestmöglich ausgeschlossen werden. Aber auch beim Thema Datenschutz sind die Regelungen des Gesetzesentwurfs noch weiter zu präzisieren. Viele Institutionen haben aus den unterschiedlichsten Aspekten Interesse an den Daten, die ein automatisiertes Kraftfahrzeug hervorbringt. Die Daten werden zu einem wichtigen Wirtschaftsfaktor.

IMPRESSUM

HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH
Luisenstr. 5, D-30159 Hannover
Fon 0511-30756-0 Fax 0511-30756-10
Mail info@herfurth.de, Web www.herfurth.de
Hannover · Göttingen · Brüssel
Member of the ALLIURIS GROUP, Brussels

REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.)

Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Marc-André Delp, M.L.E., Rechtsanwalt; Martin Heitmüller, Rechtsanwalt, Maître en Droit (FR); Günter Stuff, Steuerberater; Xiaomei Zhang, Juristin (CN), Mag. iur. (D); Dennis Jlussi, Rechtsanwalt; Sabine Reimann, Rechtsanwältin (D); Araceli Rojo Corral, Abogada (ES); Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia); Cord Meyer, Jurist und Bankkaufmann; Dr. jur. Reinhard Pohl, Rechtsanwalt (D); Elena Duwensee, Juristin (RU), Master of Law (RU).

KORRESPONDENTEN

u.a. Amsterdam, Athen, Barcelona, Brüssel, Budapest, Bukarest, Helsinki, Istanbul, Kiew, Kopenhagen, Lissabon, London, Luxemburg, Lyon, Mailand, Madrid, Moskau, Oslo, Paris, Prag, Sofia, Stockholm, Warschau, Wien, Salzburg, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, Dubai, Kairo, New Delhi, Bangkok, Singapur, Peking, Shanghai, Tokio, Sydney, Johannesburg

VERLAG

CASTON GmbH, Law & Business Information
Luisenstr. 5, D-30159 Hannover,
Fon 0511 - 30756-50 Fax 0511 - 30756-60
Mail info@caston.info Web www.caston.info