

**Herausgeber:**

Prof. Dr. Thomas Hoeren, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM), Universität Münster – RA Prof. Dr. Jochen Schneider, Kanzlei SSW Schneider Schiffer Weihermüller, München – Prof. Dr. Martin Selmayr, Kabinettschef von Jean-Claude Juncker, Präsident der Europäischen Kommission, Brüssel/Direktor des Centrums für Europarecht, Universität Passau – RA Dr. Axel Spies, Morgan, Lewis & Bockius LLP, Washington, D.C./Frankfurt/M. – RA Tim Wybitul, FA Arbeitsrecht, Partner, Head of Compliance & Investigations Hogan Lovells, Frankfurt/M.

**Wissenschaftsbeirat:**

RAin Dr. Astrid Auer-Reinsdorff, FA IT-Recht, Berlin/Lissabon/Vorsitzende des Geschäftsführenden Ausschusses der Arbeitsgemeinschaft IT-Recht im DAV (davit) – Daniela Beaujean, Mitglied der Geschäftsleitung Recht und Regulierung/Justiziarin, Verband Privater Rundfunk und Telemedien e.V. (VPRT), Berlin – RAin Isabell Conrad, Kanzlei SSW Schneider Schiffer Weihermüller, München – RAin Susanne Dehmel, Mitglied der Geschäftsleitung Bitkom e.V., Berlin – Dr. Oliver Draf, LL.M., Leiter Datenschutz der Allianz Deutschland AG, München – RA Dr. Jens Eckhardt, FA IT-Recht, Düsseldorf/Vorstand (Recht) des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. – RAin Dr. Sybille Gierschmann, LL.M., Partnerin Kanzlei Taylor Wessing, München/Co-Leiterin Fachausschuss Datenschutz der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI) – RA Dr. Stefan Hanloser, München – Prof. Dr. Gerrit Hornung, LL.M., Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Umweltrecht, Universität Kassel – Prof. Dr. Jacob Joussen, Lehrstuhlinhaber für Bürgerliches Recht, Deutsches und Europäisches Arbeitsrecht und Sozialrecht, Ruhr-Universität Bochum – Thomas Kranig, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Ansbach – RA Dr. Sebastian Kraska, externer Datenschutzbeauftragter, IITR GmbH, München – Prof. Dr. Thomas Petri, Der Bayerische Landesbeauftragte für den Datenschutz, München – Prof. Dr. Andreas Popp, M.A., Inhaber des Lehrstuhls für Deutsches und Europäisches Straf- und Strafprozessrecht, FB Rechtswissenschaft, Universität Konstanz – Prof. Dr. Alexander Roßnagel, Universitätsprofessor für Öffentliches Recht, Universität Kassel/Leiter der Projektgruppe verfassungsrechtliche Technikgestaltung (provet) – RA Dr. Christian Schröder, Partner und Leiter des Fachbereichs IP/IT & Data Protection Practice Group in der Kanzlei ORRICK, HERRINGTON & SUTCLIFFE LLP, Düsseldorf – RA Dr. Jyn Schultze-Melling, LL.M., Director for Privacy Policy, Facebook Europe, Dublin – Prof. Paul M. Schwartz, Professor der Rechtswissenschaft an der University of California – Berkeley Law School/Direktor des Berkeley Center for Law & Technology, USA – RA Thorsten Sörup, Aderhold Rechtsanwaltskanzlei mbH, Frankfurt/M. – Prof. Dr. Jürgen Taeger, Lehrstuhlinhaber für Bürgerliches Recht, Handels- und Wirtschaftsrecht sowie Rechtsinformatik, Universität Oldenburg/Vorsitzender der Deutschen Stiftung für Recht und Informatik (DSRI) – RA Florian Thoma, Senior Director, Global Data Privacy, Accenture AG, stv. Leiter des AK Datenschutz des Bitkom e.V. – Prof. Dr. Marie-Theres Tinnefeld, Professorin für Datenschutz und Wirtschaftsrecht, Hochschule München

## Axel Spies USA: Neue Leitlinien für selbstfahrende Autos – Federal Automated Vehicles Policy

ZD-Aktuell 2016, 05326

In den USA gibt es eine Reihe von Projekten mit selbstfahrenden (autonomen) Kfz im Straßenverkehr, von denen das laufende Uber-Projekt in Pittsburgh mit Passagieren vielleicht das bekannteste ist. Präsident Obama hat sich in einem eigenen Zeitungseditorial in der Pittsburgh Gazette v. 19.9.2016 positiv über das Projekt geäußert, aber gleichzeitig davor gewarnt, der Sicherheit dieser Technologien nicht genügend Beachtung zu schenken. Das US-Department of Transportation (DOT) hat in diesem Sinne am 20.9.2016, wie vom Präsidenten in dem Editorial angekündigt, eine detaillierte Analyse mit Leitlinien (Federal Automated Vehicles Policy – 116 Seiten) ins Netz gestellt, damit die zuständigen Behörden den Einsatz von autonomen Fahrzeugen beurteilen und begrenzen können. Das Weiße Haus unterstützt die Initiative mit einem eigenen Fact Sheet.

Diese DOT-Leitlinien sind ein wichtiger Teil der ersten Initiative auf Bundesministerialebene in diesem Sektor. Bislang gab es in den USA nur allgemeine Richtlinien und Empfehlungen der nationalen Behörde für Straßensicherheit (NHTSA). Die DOT-Initiative ist ein erster Schritt zu detaillierteren nationalen Vorschriften. Sie beinhaltet auch konkrete Empfehlungen für die US-Bundesstaaten (Model States Policies), die u.a. in den Bereichen Verkehrsrecht und Kfz-Versicherungen erhebliche eigene Kompetenzen haben. In den nächsten 60 Tagen können über die Webseite öffentliche Kommentare zu den Leitlinien eingereicht werden. Die Leitlinien sollen dann jährlich aktualisiert und ggf. erweitert werden.

Das renommierte Brookings-Institut hat zum Thema selbstfahrende Kfz ebenfalls eine neue Studie veröffentlicht; dabei geht man von einer Marktpenetrationsrate von 25% in 10-15 Jahren aus. Das Car-Sharing und der Transport von Senioren und Behinderten werden treibende Kräfte sein.

In Deutschland haben am 27.9.2016 Audi, BMW, Daimler Benz sowie Ericsson, Huawei, Intel, Nokia und Qualcomm die Gründung der 5G Automotive Association (5GAA), die neue Kommunikationslösungen entwickeln und testen soll, bekannt gegeben.

### 1. Die 15-Punkte-Liste des DOT

Zurück zur Entwicklung in den USA: In den Leitlinien fordert das DOT die Hersteller und die involvierten Unternehmen (Zulieferer) zur Darlegung auf, dass ihre halbautonomen und autonomen Fahrzeuge eine 15-Punkte-Liste mit Sicherheitsanforderungen erfüllen, bevor die Fahrzeuge auf die Straße dürfen (vgl. für Deutschland Lutz, NJW 2015, 119). Das DOT übernimmt zur Abgrenzung die SAE International-Definitionen für die Stufen der Automatisierung des Fahrzeugs: Bei der SAE-Stufe 0 kontrolliert es der menschliche Fahrer allein, auf der SAE-Stufe 5 kann das automatisierte System alle Fahraufgaben ausführen, und zwar unter allen Bedingungen, die ein Mensch als Fahrer üblicherweise antrifft. Die Leitlinien verwenden durchweg den Begriff „hoch automatisiertes Fahrzeug“ (HAV) für die SAE-Ebenen 3-5. Die Leitlinien gelten für die Test- und die Einsatzebene der HAV. Wenn ein Fahrzeug von der Öffentlichkeit genutzt wird, also nicht bloß von Mitarbeitern des Herstellers oder autorisierten Testfahrern, gelten die Fahrten nicht als Testbetrieb. Die 15-Punkte-Liste selbst beinhaltet, kurz zusammengefasst, die folgenden Leitpunkte:

**1. Data Recording and Sharing:** Die Hersteller und Betreiber sollen die von den Fahrzeugen auf vielfältige Weise generierten Daten speichern und untereinander teilen, damit bei Fehlfunktionen oder Unfällen das Geschehen rekonstruiert werden kann. Verbesserte digitale Ereignisdatenschreiber sollen zum Einsatz kommen, um Fehlerursachen zu erkennen und zu rekonstruieren. Gerade bei Beinahe-Unfällen soll analysiert werden, ob z.B. andere Verkehrsteilnehmer vor dem Ereignis in der Nähe waren und ob das Fahrzeug andere Verkehrsteilnehmer korrekt und rechtzeitig identifiziert und somit die Geschwindigkeit oder Fahrtrichtung angepasst hat.

**2. Privacy:** Die Datensammlungen sollen mit den allgemeinen Grundsätzen über die Datensammlungen (Privacy) in Einklang stehen.

**3. System Safety:** Die Fahrzeuge müssen vom Werk aus mit Vorrichtungen ausgestattet sein, dass sie auf Fehlfunktionen (z.B. einen Software Crash) oder Beinahe-Unfälle sicher reagieren und sicher

zum Stehen kommen. Die Systemsicherheit soll mind. von einem unabhängigen Dritten (Gutachter) bestätigt werden.

**4. Vehicle Cybersecurity:** Hacking oder andere Cyberattacken sollen nach dem Stand der Technik ausgeschlossen sein. Alle sich hierauf beziehenden Unterlagen, z.B. zu Softwareentwicklung und -tests, sollen die Hersteller aufbewahren und, wenn erforderlich, anderen Marktteilnehmern zur Verfügung stellen.

**5. Human-Machine Interface:** Die Hersteller müssen eine sichere Vorrichtung einbauen, um das Fahrzeug auf Handbetrieb umzustellen. Die Fahrzeuginsassen und außenstehenden Verkehrsteilnehmer (z.B. Fußgänger) müssen wissen, wann sich das HAV im Modus „autonomes Fahren“ befindet.

**6. Crashworthiness:** Die autonomen Fahrzeuge müssen die von der *National Highway Traffic Safety Administration* allgemein vorgesehenen Standards für Aufprallsicherheit (crashworthiness) einhalten, sodass die Insassen bei einem Aufprall gleichermaßen wie in traditionellen Kfz geschützt sind. Wenn ein HAV in einen Unfall verwickelt wird, soll der Aufprallschaden nicht anders als bei einem herkömmlichen Fahrzeug der gleichen Art und Klasse ausfallen.

**7. Consumer Education:** Das Training derjenigen, die mit dem Fahrzeug in Berührung kommen (Händler, Insassen usw.), und die Betriebsanleitungen müssen die Betriebsrisiken angemessen abbilden, insbesondere müssen die Instruktionen über Notfallmaßnahmen ausreichend erklärt sein.

**8. Registration and Certification:** Darunter fasst das *DOT* diverse Pflichten zur Anzeige und Benachrichtigung der zuständigen Behörden zusammen. Die Hersteller und sonst am Projekt beteiligten Unternehmen sollten die Möglichkeiten und Grenzen der HAV-Systeme unter verschiedenen Betriebsgeschwindigkeiten, geografischen Gebieten und Wetterbedingungen in der Anzeige an die Behörden sowie in den Informationen für die Fahrzeugbesitzer vollständig darstellen.

**9. Post-Crash Behavior:** Die Hersteller müssen Lösungen für das Verhalten des Fahrzeugs bei einem leichten oder schweren Unfall aufzeigen. Wenn Sensoren oder kritische Sicherheitssteuerungen beschädigt sind, soll das Fahrzeug nicht im HAV-Modus weiterfahren können.

**10. Federal, State and Local Laws:** Die au-

tonomen Fahrzeuge müssen sich an alle Verkehrsregeln halten, die in den USA von Bundesstaat zu Bundesstaat unterschiedlich sein können.

**11. Ethical Considerations:** Die Programme der Fahrzeuge müssen auf Grenzsituationen reagieren können (z.B. durch ein Ausweichen auf die Gegenseite, um einen Unfall mit einem anderen Fahrzeug zu verhindern). Künstliche Intelligenz soll bei der Risikoabwägung und Entscheidungsfindung zum Einsatz kommen.

**12. Operational Design Domain:** Das Fahrzeug muss für die verschiedenen denkbaren Verkehrssituationen voll ausgerüstet sein (z.B. für Nachtfahrten und für unterschiedlichen Straßenbelag).

**13. Object/Event Detection and Response:** Das Fahrzeug muss auf alle möglichen anzutreffenden Verkehrssituationen angemessen reagieren.

**14. Fallback (Minimal Risk Condition):** Beim Zurückstellen des Betriebs in den vom Fahrer kontrollierten Modus muss das Programm des HAV berücksichtigen, dass der Fahrer z.B. nicht voll fahrtüchtig (z.B. alkoholisiert) ist.

**15. Validation Methods:** Angemessene Tests sind erforderlich, bevor das Fahrzeug in den öffentlichen Straßenverkehr darf.

## II. Wer haftet? Datenschutz und weitere Problemkreise

Zu diesen 15 Punkten nachfolgend noch einige ergänzende Hinweise:

### 1. Informationsaustausch

Zur Unterstützung der zuständigen Behörden werden die Betreiber und Produzenten von HAV verpflichtet, mit den anderen Herstellern und Unternehmen der Branche freiwillig Berichte auszutauschen. Dieser Reporting-Prozess (s.o. Leitpunkt 1) soll verfeinert werden. Die Hersteller und Betreiber von HAV sollten ein dokumentiertes Verfahren für die Prüfung, Validierung und Sammlung von Betriebsstörungs- und Crash-Daten sowie deren Ursachen implementieren. Diese Daten sollten sowohl bei Tests als auch beim Betrieb gesammelt werden, z.B. für die Ereignisrekonstruktion bei Fehlern. Wo die genaue Grenze zum Schutz von Betriebsgeheimnissen der Hersteller liegt, ist nicht ganz klar.

### 2. Versicherung

Das *DOT* geht auch die in Deutschland aufgeflamte Diskussion, wie die HAV

versichert werden sollen und wer bei Schäden haftet (*Jänich/Schrader/Reck, NZV 2015, 313*) an, bleibt aber mit eigenen Vorschlägen im Vagen. Im Prinzip sind die Bundesstaaten zur Regelung der Haftung für HAV berufen. Sie sollen nach Auffassung des *DOT* prüfen, wie die Haftung zwischen HAV-Eigentümer, Hersteller, Betreiber, Passagieren und Dritten zu regeln ist, wenn es zu einem schädigenden Ereignis kommt. Das *DOT* meint in diesem Zusammenhang, dass die Bestimmung, wer der „Fahrer“ eines HAV ist, nicht automatisch zur Haftung für die durch das HAV verursachten Schäden führe. Auch die Hersteller des HAV könnten in die Haftung miteinbezogen werden.

### 3. Cyber-Security

Das *DOT* nimmt den Bereich Cyber-Security sehr ernst (vgl. *Spies, ZD-Aktuell 2015, 04153* zu den Plänen für einen Spy Car Act), gibt aber nur allgemeine Leitlinien vor: Die Hersteller und Unternehmen sollten einen „robusten Produktentwicklungsprozess“ implementieren, der system-technisch so früh wie möglich die Gefahren für die Sicherheit von HAV und die Anfälligkeit für Cyber-Bedrohungen minimiert. Dieser Prozess soll das komplette HAV-System und Fahrzeugdesign abdecken, einschließlich einer systematischen und kontinuierlichen Sicherheitsrisikobewertung. Identifizierung, Schutz, Erkennung, Reaktion und Wiederherstellungsfunktionen im Fall von Cyber-Bedrohungen sollen zu den nötigen Entscheidungen für das Risikomanagement führen, um auf Bedrohungen schnell zu reagieren und aus Ereignissen die richtigen Schlüsse zu ziehen.

### 4. Training

Die richtige Instruktion und das Training sind für das *DOT* zwingend notwendig, um den sicheren Einsatz von automatisierten Fahrzeugen zu gewährleisten. Die Hersteller und andere Unternehmen müssen in diesem Bereich erhebliche Hausaufgaben für die Mitarbeiter, Händler und Nutzer erledigen. Das Ziel ist ein notwendiges Maß an Verständnis für die neuen Technologien, um sie richtig, effizient und auf die sicherste Art und Weise zu nutzen.

### 5. Datenschutz

Gerade im sensiblen Bereich des Datenschutzes (s. Leitpunkt 2 oben) bei selbst-

fahrenden Fahrzeugen sollen die Hersteller und Betreiber von HAV in ihren Datenschutzrichtlinien und Praktiken folgende Prinzipien gewährleisten:

**a) Transparenz:** Die Nutzer sollen allgemein zugängliche, klar formulierte und aussagekräftige Hinweise auf den Datenschutz und die Datensicherheit (Privacy Policies) erhalten. Die relevanten Policies sollen abdecken, welche Daten vom Fahrzeug erhoben werden, wer Zugriff auf die Daten hat, wie sie verwendet, gesichert und gelöscht werden; die Policies sollen sich an der (viel beachteten, aber nicht rechtlich verbindlichen) Consumer Bill of Rights des *Weißes Hauses* zur Privacy in den USA für Verbraucher (s. *Spies*, ZD-Aktuell 2012, 02788) orientieren.

**b) Wahlrecht:** Die Fahrzeugeigentümer (nicht die Insassen) sollen recht umfangreiche Wahlmöglichkeiten in Bezug auf die Erfassung, Verwendung, die gemeinsame Nutzung, Aufbewahrung und Kompilierung von Daten, einschließlich Geolocation, biometrische Daten und Fahrerhaltensdaten, die vernünftigerweise mit ihnen persönlich verbunden werden können (für ihre personenbezogene Daten), bekommen.

**c) Datenkontext:** Die Daten, die von HAV erzeugt werden, sollen nur in der Weise gesammelt werden, die mit den Zielen in Einklang steht, für die die Daten ursprünglich erfasst wurden (d.h. wie sie in den anwendbaren Privacy Policies/Datenschutzvereinbarungen erklärt wurden).

**d) Minimierung, De-Identifizierung und Aufbewahrung von Daten:** Das Unternehmen soll die Daten nur so lange sammeln und aufbewahren, wie dies erforderlich ist, und zwar nur die minimale Menge an personenbezogenen Daten, die erforderlich ist, um seine legitimen geschäftlichen Zwecke zu erreichen. Das Unternehmen soll die nötigen Schritte unternehmen, um sensible Daten zu anonymisieren, wo dies machbar ist – alles jeweils in Übereinstimmung mit den geltenden Privacy Policies und Vereinbarungen.

**e) Datensicherheit:** Das Unternehmen muss die Maßnahmen zum Schutz der Daten implementieren, die verglichen mit dem Schaden angemessen sind, der

durch den Verlust oder die unbefugte Offenlegung der Daten entstehen würde.

**f) Integrität und Zugang:** Das Unternehmen muss die nötigen Maßnahmen umsetzen, damit die Fahrzeugbetreiber und Eigentümer die Richtigkeit der Daten überprüfen und notfalls korrigieren können, wenn die Daten in einer Weise gesammelt werden, die auf ein einzelnes Fahrzeug oder eine Person direkte oder nachvollziehbare Rückschlüsse zulassen.

**g) Verantwortlichkeit:** Das DOT erwartet von dem Unternehmen angemessene Schritte zur praktischen Umsetzung der Prinzipien zur Wahrung der Privatsphäre und der Datenschutzmechanismen (z.B. durch internes Auditing und Training), um sicherzustellen, dass die Empfänger der Daten diese nur im Einklang mit den geltenden Datenschutzbestimmungen sammeln oder verarbeiten.

Zu den vorgeschlagenen Datenschutzbestimmungen lässt sich aus EU-Sicht einiges anmerken. Hier nur so viel: Den Fahrgästen des HAV wird z.B. kein Recht auf Datenschutz eingeräumt, obwohl diese gleichermaßen Daten produzieren (z.B. über ihren Aufenthaltsort und die Dauer der Fahrt). Vor einer strikten Zweckbindung schreckt das DOT bei der Datennutzung zurück und vermeidet diesen Begriff. Die Anonymisierung von sensiblen

Daten soll nur insoweit erfolgen, wie sie praktikabel ist. Das bedeutet, dass große Mengen von personenbezogenen Daten möglicherweise auf unbestimmte Zeit gespeichert werden. Ein klares Bekenntnis zur Verantwortlichkeit der HAV-Halter oder Betreiber bei der Weiterleitung der Daten an Dritte fehlt. Ob sich im laufenden Konsultationsverfahren hier noch Nachbesserungen zum Datenschutz erreichen lassen, wird sich zeigen.

■ Vgl. auch zum vernetzten Auto *Lüdemann*, ZD 2015, 247; *Knoke/Dahi*, ZD-Aktuell 2016, 05013 und *Ulmer*, MMR 2015, 506.

#### Dr. Axel Spies

ist Rechtsanwalt bei Morgan, Lewis & Bockius LLP in Washington DC und Mitherausgeber der ZD.

#### EGMR: Nutzung von Steuer-CD erlaubt ZD-Aktuell 2016, 05334

Der EGMR hat (U. v. 6.10.2016 – App. no. 33696/11) festgestellt, dass deutsche Finanzbehörden Durchsuchungen auf illegal beschaffte Bankdaten stützen dürfen. Die Verwendung solcher Daten habe nicht gegen das Recht auf Schutz der Privatsphäre verstoßen.

■ Vgl. auch *VerfGH Rheinland-Pfalz* ZD 2014, 596 (Ls.); zum datenschutzkonformen Steuerrecht *Heil/Greve*, ZD 2013, 481; *EuGH* ZD 2015, 577 m. Anm. *Petri* und *BFH* ZD 2015, 594.

Rezensionen · Tagungsberichte · Termine · Rezensionen · Tagungsberichte ·

## NEU AUF DER HOMEPAGE

[www.zd-beck.de](http://www.zd-beck.de)

#### Rezensionen

- **Thorsten Sörup** Peter Wedde (Hrsg.), *Handbuch Datenschutz und Mitbestimmung*, Frankfurt/M. (Bund-Verlag) 2016, ISBN 978-3-7663-6442-5, € 49,90
- **Dr. Eugen Ehmann** Niko Härting, *Datenschutz-Grundverordnung*, Köln (Dr. Otto Schmidt) 2016, ISBN 978-3-504-42059-8, € 39,80
- **Dr. Eugen Ehmann** Lorin-Johannes Wagner, *Der Datenschutz in der Europäischen Union*, Wien (Jan Sramek) 2015, ISBN 978-3-7097-0050-1, € 78,-

#### Tagungsbericht

- **Dr. Alexander Dix / Dr. Dennis-Kenji Kipker** EAID: *Datenschutzgrundverordnung – Was kommt auf die Unternehmen zu?*

Termine + Termine + Termine + Termine + Termine + Termine + Termine