Luchterhand Verlag

52.
Deutscher
Verkehrs-
gerichtstag

Veröffentlichung der auf dem
52. Deutschen Verkehrsgerichtstag
vom 29. bis 31. Januar 2014 in Goslar
gehaltenen Vorträge, Referate und
erarbeiteten Empfehlungen

52. VGT 2014

Deutscher
Verkehrsgerichtstag

Verrat durch den eigenen PKW – wie kann man sich schützen?

Dr. Daniela Mielchen
Fachanwältin für Verkehrsrecht, Hamburg

I. Einleitung

Zur Verbesserung der Sicherheit im Straßenverkehr hatte die EU-Kommission die Mitgliedsstaaten zunächst dazu angehalten, auf freiwilliger Basis bis 2009 die neue bordeigene Kommunikationstechnologie »eCall« einzuführen. Da die Umsetzung jedoch nur langsam verlief, ist nun eine verbindliche Einführung bis spätestens Oktober 2015 vorgesehen.[1] Ab diesem Zeitpunkt sollen alle neuen Modelle von Pkw und leichten Nutzfahrzeugen serienmäßig mit eCall-Einrichtungen ausgestattet werden. Das bordeigene System soll selbsttätig einen Notruf an die europäische Notrufnummer 112 absetzen, sobald fahrzeugseitige Sensoren einen schweren Zusammenstoß registrieren. Hierzu müssen die Fahrzeuge mit diversen technischen Geräten ausgestattet werden. So wird u.a. ein GPS-Empfänger zur Feststellung der Fahrzeugposition benötigt, eine GSM-Antenne zum Senden des Notrufes an die Notrufzentrale, ein Steuergerät, das den Standort im Notfall über eine Mobilfunk-Einheit an die Notrufzentrale meldet, einen Crash-Sensor zum Erkennen des Unfalls, Mikrofon und Lautsprecher, damit die Notrufzentrale mit den Fahrzeuginsassen sprechen und so die Zahl der Verletzten und die Schwere der Verletzungen in Erfahrung bringen kann.[2]

Bedenkt man, dass hierdurch jährlich 2500 Menschenleben gerettet werden sollen, ist diese Neuerung grundsätzlich begrüßenswert. Kontrovers wird allerdings diskutiert, dass dieses System auch zu einem Einfallstor für eine permanente Überwachung des Fahrzeugs und des Fahrzeugführers werden kann und hierdurch ein weiterer Schritt in Richtung »gläserner Mensch« getan wird. Denn durch die

1 Siehe Beschluss der Europäischen Kommission vom 13.06.2013 – Pressemitteilung IP/13/534.

2 Quelle: ADAC – http://www.adac.de/infotestrat/unfall-schaeden-und-panne/ecall_gps_notruf/.

neue Technologie und insbesondere durch die Vernetzung des Fahrzeuges mit dem Mobilfunk könnte es künftig nicht nur Notdiensten möglich sein, auf die erforderlichen Daten zuzugreifen, sondern auch Anbietern von Mehrwertdiensten, wie Automobilclubs, Abschleppunternehmen, Werkstätten und nicht zuletzt Versicherungen. Während die Nutzung eines derartigen Angebots durchaus vorteilhaft sein kann, drohen gleichzeitig erhebliche Gefahren für den Halter bzw. Fahrer des Fahrzeuges, wenn dieser z.B. über die Art und Menge der weitergegebenen Daten oder die Tragweite der Datenweitergabe nicht hinreichend aufgeklärt wird und seine Daten letztlich auch gegen ihn verwendet werden können. Unter den Versicherungen traut sich bereits jetzt, noch vor Einrichtung von eCall, die Sparkassen-Versicherung an ein Versicherungsmodell heran, in welchem sich die Prämie an der Fahrweise des Versicherungsnehmers orientieren soll.[3] So ist seit November 2013 eine neue Kfz-Police mit Telematik-Option auf dem Markt. Der Versicherungsnehmer muss sein Fahrzeug mit einer Telematik-Box ausstatten und kann dann durch eine vorausschauende und vorsichtige Fahrweise den Versicherungsbeitrag senken. Den gläsernen Kunden soll es nach Angaben der Verantwortlichen aber nicht geben, da nur der Fahrer selbst Einblick in seine zurückgelegten Strecken und sein Fahrverhalten bekomme. Der Kunde könne zwar auf einem Webportal überprüfen, ob und wo er zu schnell gefahren sei und wo er unangemessen gebremst oder beschleunigt habe, dem Versicherer werden hingegen nur abstrakte Scoring-Punkte übermittelt, die das Fahrverhalten benoten.[4] Registriert werden z.B. überhöhte Geschwindigkeit, hastiges Bremsen und Beschleunigen, Fahrweise, Nacht- und Stadtfahrten.[5] Datenschützer sehen diese Entwicklung kritisch, da Kunden, die sich der Datenpreisgabe verweigern, benachteiligt werden könnten. Außerdem ist zu befürchten, dass die Tragweite der Weitergabe der Daten durch den Verbraucher unterschätzt wird. Zumal die Erfassung von Risikomerkmalen im Fahrerprofil zu erheblichen Nachteilen für den Kunden führen kann und zudem ganze Bewegungsprofile erstellt werden können.

Weitgehend unbekannt ist, dass schon heute eine Vielzahl an elektronischen Daten über Fahrer und Fahrverhalten erhoben, gespeichert und ausgewertet wird.

3 In anderen europäischen Ländern und den USA bieten Versicherungen bereits seit einigen Jahren erfolgreich Telematiktarife (»pay as you drive«) an.

4 Die Datenverarbeitung wird dabei nicht von der Versicherung selbst vorgenommen, sondern von einem Sub-Unternehmer, welcher die in der Box erhobenen Daten, verarbeitet und lediglich den Score an die Versicherung schickt. Vgl. Biermann, Artikel vom 13.11.2013 bei zeit-online »Wer zu hart bremst, verliert seinen Versicherungsrabatt«, abrufbar unter http://www.zeit.de/digital/datenschutz/2013-11/versicherung-telematik-ueberwachung-kfz; siehe auch Artikel in der FAZ vom 09.11.2013 »Gute Fahrer sollen weniger Prämie zahlen«.

5 Biermann, Artikel vom 13.11.2013 bei zeit-online »Wer zu hart bremst, verliert seinen Versicherungsrabatt«, abrufbar unter http://www.zeit.de/digital/datenschutz/2013-11/versicherung-telematik-ueberwachung-kfz.

Und zwar von den Automobilherstellern selbst. Die Besitzer der Fahrzeuge werden hierüber vielfach nicht informiert[6] und erhalten häufig erst Kenntnis, wenn sie im Rahmen von Gewährleistungs- oder Haftungsprozessen die gespeicherten Daten als Beweis gegen den behaupteten Anspruch präsentiert bekommen. Dies wiederum hat eine weitere Diskussion darüber entfacht, welche Daten eigentlich erhoben und gespeichert werden, wem sie gehören und wer darauf ggf. Zugriff bzw. Anspruch hat.

II. Erhobene Daten

Je nach Erhebungsart ist zwischen verschiedenen Daten zu unterscheiden.

1. »Geheim« erhobene Daten

Unter dem Begriff der »geheimen« Daten sind solche zu verstehen, die von den Fahrzeugherstellern und Zulieferer erhoben werden, um u.a. auch nach dem Verkauf eigene Untersuchungen an ihren Produkten durchführen zu können. Da die Hersteller und Zulieferer diese durchweg sensiblen Daten durch Verschlüsselung vehement vor externem Zugriff schützen, erhalten Besitzer des Fahrzeugs regelmäßig keinen Zugriff. Obwohl es sich um eine Vielzahl von Daten handelt, die bei Gerichtsverfahren von höchster Bedeutung sein können. So werden von den in Fahrzeugen vorhandenen aktiven und passiven Sicherheitseinrichtungen, wie Antiblockiersystem, Gurtstraffer, Gurtkraftbegrenzer und den Airbags, permanent Daten erhoben. Um eine optimale wechselseitige Anpassung der unterschiedlichen Einzelsysteme aufeinander gewährleisten zu können, werden die Messwerte der verschiedenen Systeme in zentralen Steuergeräten zusammenhängend erfasst und ausgewertet.[7] Es erfolgt ein ständiger Abgleich eingehender Informationen. Sensoren melden durchgängig fahrdynamische Zustände, Steuergeräte verarbeiten diese Signale und gleichen sie untereinander und mit vorgegebenen Sollwerten ab. Da der reine Abgleich mit Sollwerten allerdings nicht ausreicht, müssen Messwerte zudem – mal länger, mal kürzer – gespeichert werden. Denn nur durch eine Speicherung ist ein Vergleich mehrerer Messwerte über einen Vergleichszeitraum möglich.[8]

6 Die Fahrzeugindustrie erhebt schon seit Jahren mittels der in Fahrzeugen eingebauten Steuergeräte diverse Daten über das Fahrverhalten. Mittlerweile gehen die Hersteller teilweise dazu über, die Kunden hierüber in der Bedienungsanleitung der Fahrzeuge oder aber beim Abschluss des Kaufvertrags darüber zu informieren. Siehe VOLVO oder BMW.

7 Michael Weyde, »Geheime Daten in Kraftfahrzeugen«, Datenspeicherung in KfZ – Fluch oder Segen? Möglichkeiten und Grenzen der Fahrdatenauswertung in der Unfallrekonstruktion: – Skript zum Vortrag bei den 33. Homburger Tagen (2013), S. 2.

8 Michael Weyde, »Geheime Daten in Kraftfahrzeugen«, Datenspeicherung in KfZ – Fluch oder Segen? Möglichkeiten und Grenzen der Fahrdatenauswertung in der Unfallrekonstruktion: – Skript zum Vortrag bei den 33. Homburger Tagen (2013), S. 2.

Um also einen Airbag im richtigen Augenblick auszulösen, müssen Werte über die Beschleunigung und die Geschwindigkeitsänderung erfasst und gespeichert werden.[9] Die Sitzbelegung im Fahrzeug wird ermittelt. Es wird geprüft, ob die Insassen angeschnallt sind und in welcher Sitzposition sie sich befinden.[10] Hierdurch kann vom Airbag-Steuergerät binnen weniger als 30 ms die Entscheidung zum Auslösen der Zündung eines Airbags getroffen werden. Eine Vielzahl von Daten wird in kurzer Zeit systematisch ausgewertet, bevor das Steuergerät das Signal zum Zünden gibt. Löst der Airbag aus, werden die Werte, die zum Auslösen geführt haben, gespeichert und können so lange ausgelesen werden, bis sie gelöscht bzw. zurückgesetzt werden.[11] Daneben sind es vor allem die Steuergeräte für das elektronische Stabilitätsprogramm (ESP) und deren Ereignisspeicher, welche eine Masse an Daten, wie z.B. die Geschwindigkeit, Motordrehzahl und Motorlast, abrufen und erfassen. Eine Vielzahl der bis zu 80 Steuerungssysteme verfügt über Speichermöglichkeiten. Welche Daten allerdings gespeichert werden, variiert von Hersteller zu Hersteller stark. Sie definieren, welche Daten »flüchtig« sind oder als »fest« oder »semifest« im Fahrzeug verbleiben.

Die Ereignisspeicher der Steuergeräte zeichnen sogenannte »Freeze Frame«-Daten auf. Dies sind u.a. Daten, die bei Eintritt eines Fehlers vorliegen und zusammen mit dem Fehler gespeichert werden. Hierbei handelt es sich um Werte, wie z.B. Öl- und Wassertemperatur, Außentemperatur, Geschwindigkeit, Bremsstellung etc. Diese Daten werden z.T. überschrieben, wenn der Fehler nicht mehr vorliegt, wofür unter Umständen ein mehrmaliges Betätigen der Zündung ausreichen kann. Die Speicherdauer ist je nach Art und Schwere des Fehlers unterschiedlich lang, die Speicherlogik legt der jeweilige Hersteller fest. Dieser sowie gesetzliche Vorgaben bestimmen auch, welche der »Freeze Frame-Daten« als Eigendiagnosedaten dem Auslesen durch Dritte zugänglich sind und welche »geheim« nur dem Hersteller oder Zulieferer zumeist zusätzlich verschlüsselt zur Verfügung stehen.

Das Wissen darum, welche Daten beim eigenen Fahrzeug der Speicherung unterliegen, ist jedoch – vorausgesetzt es stünde dem Halter oder Fahrer überhaupt zur Verfügung – nicht statisch und festgeschrieben. Es kann vielmehr bei jedem Werkstattaufenthalt durch das Aufspielen eines neuen Updates korrigiert und neu festgelegt werden. Es erfordert mithin spezialisierte sachverständige Kenntnisse und erhebliche Recherche, um zu ermitteln, welche Daten welches Fahrzeug speichert oder womöglich nach dem nächsten Werkstattaufenthalt speichern wird. Hierbei sind u.a. Länderbesonderheiten zu berücksichtigen. So verlangt das amerikanische Recht sehr viel weitreichendere Speicherungen, als das deutsche, so dass amerikanische Hersteller – auch bei in Deutschland verkauften Fahrzeugen – grundsätzlich

9 Martin Münchhausen, Innenministerium NRW, Referat 41, »Neue Methoden der Beweisführung Nutzung von Daten aus der Fahrzeugelektronik zur Verkehrsunfallrekonstruktion«, Vortrag IPOMEX am 02.04.2009, S. 17 f.

10 Wikipedia Enzyklopädie, Airbag-Sensorik.

11 Löst der Airbag nicht aus, werden die Daten überschrieben.

einen Event Data Recorder verbauen, der sehr viel weitreichendere Speicherungen vornimmt als bei deutschen Herstellen üblich.

2. Offiziell erhobene Daten

Mit »offiziell erhobene Daten« sind jene Daten gemeint, die bekanntermaßen erhoben, gespeichert und ggf. versandt werden, wie z.B. die künftigen eCall-Notruf Informationen. Dies sind in erster Linie fahrzeugspezifische Daten, wie der Zeitpunkt des Unfalls, der genaue Standort des verunfallten Fahrzeugs und die Fahrtrichtung. Eine Anonymität der Fahrzeuge ist dabei nicht vorgesehen. Vielmehr soll die Fahrzeugkennung gerade zentraler Bestandteil des Mindestdatensatzes sein.[12] Da nach Angaben des Bundesverkehrsministeriums ein Auslösen des Airbagsensors erforderlich ist, damit das eCall-System einen Notruf absetzt, werden auch Daten über die Unfallschwere mitgeteilt.[13] Diese ist aber nur durch die aufgetretene Beschleunigung und die Geschwindigkeitsänderung während des Anstoßes zu ermitteln, so dass auch fahrspezifische Daten erhoben, gespeichert und Dritten zur Verfügung gestellt werden.[14] Aus Datenschutzgründen ist allerdings ein »schlafendes System« beabsichtigt, das nur im Falle eines Unfalls aktiv wird und Daten überträgt.

3. Freiwillig erhobene Daten

Schließlich besteht für den Fahrzeughalter auch die Möglichkeit, ausgewählte Fahrdaten freiwillig zu erfassen. Dies geschieht derzeit durch sogenannte Unfalldatenspeicher (UDS), die fest in das Fahrzeug einzubauen sind und Dashcams, die auf dem Armaturenbrett oder an der Windschutzscheibe angebracht werden. Während eine Dashcam auf der Fahrt lediglich die Umgebung aufzeichnet, nimmt der Unfalldatenspeicher ständig verschiedene Fahrdaten auf. Hierzu gehören z.B. Geschwindigkeit, Beschleunigung in Längs- und Querrichtung, Bewegungsrichtung, sowie Lampen-, Blinker- und Bremstätigkeit etc.. Der Unfalldatenspeicher zeichnet diese für einige Minuten auf, bevor sie automatisch wieder überschrieben werden. Im Falle eines entsprechend heftigen Anstoßes bleiben die Daten der letzten 30 Sekunden vor und der letzten 15 Sekunden nach dem Anstoß dauerhaft gespeichert, so dass sich der Hergang eines Unfalls sehr viel präziser ermitteln lässt, als ausschließlich mithilfe der Deformationen der Fahrzeuge und der Spuren auf der Straße.[15] Als freiwillige Daten

12 vgl. Landtag NRW DS 16/4028 vom 17.09.2013.

13 Siehe Bundesverkehrsministerium – http://www.bmvbs.de/SharedDocs/DE/Artikel/LA/ecall-fuer-mehr-sicherheit-im-strassenverkehr.html, abgerufen am 20.11.2013.

14 Michael Weyde, »Geheime Daten in Kraftfahrzeugen«, Datenspeicherung in KfZ – Fluch oder Segen? Möglichkeiten und Grenzen der Fahrdatenauswertung in der Unfallrekonstruktion: – Skript zum Vortrag bei den 33. Homburger Tagen (2013), S. 8.

15 Michael Weyde, »Geheime Daten in Kraftfahrzeugen«, Datenspeicherung in KfZ – Fluch oder Segen? Möglichkeiten und Grenzen der Fahrdatenauswertung in der Unfallrekonstruktion: – Skript zum Vortrag bei den 33. Homburger Tagen (2013), S. 18–21.

sind künftig sicherlich auch solche zu verstehen, die im Rahmen einer Versicherungspolice mit Telematik-Option erhoben und gespeichert werden.

Auch wenn der Versicherer nur abstrakte Scoringpunkte übermittelt bekommt, ist hierfür zunächst einmal die Erfassung, Speicherung und Auswertung der fahrzeug- und fahrerbezogenen Daten erforderlich.

III. Zugriff auf Daten

1. Allgemeines

a) Geheim erhobene Daten

Die Bordelektronik von Fahrzeugen, mit deren Hilfe einige Fahrzeughersteller problemlos Geschwindigkeit, Lenkrichtung, Straßenlage und Bremsverhalten in den entscheidenden Sekunden vor einem Unfall auslesen können, ist sowohl für den Fahrzeughalter als auch für die Verfolgungsbehörden in der Regel nicht auslesbar. Denn eine Vielzahl dieser Daten wird verschlüsselt gespeichert und kann nur mit entsprechender Software durch die Hersteller bzw. Zulieferer ausgelesen werden. Die Automobilindustrie hat hier in der Vergangenheit extrem gemauert und selbst nach tödlichen Verkehrsunfällen den Zugang zu den Computerprogrammen verweigert, die eine Auswertung der Bordelektronik möglich machen würden.[16] Insoweit ist zu konstatieren, dass die Daten zwar vom eigenen Fahrzeug gespeichert werden, man selbst aber keinen Zugriff darauf hat. Diese Blockadehaltung ist wohl in erster Linie auf eine gewisse Sorge der Unternehmen zurückzuführen, dass der Gebrauchsmusterschutz bezüglich der Algorithmen zur Regelung der Fahrassistenzsysteme gefährdet werden könnte. Viele Hersteller klären ihre Kunden auch nicht darüber auf, dass derartige Daten erhoben, gespeichert und verwendet werden. Dies ist nicht unproblematisch, denn nach dem Bundesdatenschutzgesetz ist die Erhebung, Verarbeitung und Nutzung zumindest personenbezogener Daten nur dann erlaubt, wenn entweder eine klare Rechtsgrundlage gegeben ist (d.h., das Gesetz erlaubt die Datenverarbeitung in besonderen Fällen) oder wenn die betroffene Person ausdrücklich ihr Einverständnis hierzu gegeben hat. Zwar sind die von den Steuergeräten gespeicherten Daten gewöhnlich nicht personenbezogen, da dem Hersteller nicht bekannt ist, wer das Fahrzeug zu welchem Zeitpunkt lenkt. Spätestens bei einem Unfall wird der Fahrer jedoch meist bestimmbar. Sobald solche Daten aber einer einzelnen Person zugeordnet werden können, dürfen sie nach dem Bundesdatenschutzgesetz nur noch in Ausnahmefällen verwendet werden.[17] Es ist also zu hinterfragen, ob und wann die Erhebung, Verarbeitung und Nutzung der Daten

16 So Franz-Josef Arentz (KHK), PP Aachen Kriminalkommissariat 33 bei seinem Vortrag auf dem GdP-Verkehrsforum am 19.11.2012.

17 So auch Prof. Michael Brenner in: »Datenspeicherung in Pkw als rechtliche Grauzone« vom 24.10.2013, abrufbar unter http://www.auto.de/magazin/showArticle/article/118189/Datenspeicherung-in-Pkw-als-rechtliche-Grauzone.

überhaupt zulässig ist, wenn nicht zuvor ein Einverständnis erteilt wurde.[18] Als problematisch für Hersteller und die Schädiger bzw. Beschuldigten in Verkehrsdelikten, könnte sich die US-amerikanische Gesetzeslage erweisen, die auf deutsche Fahrzeuge ausstrahlt. In den USA sind die Steuergeräte viel weitreichender durch Polizei und spezielle Sachverständige auslesbar, sodass auf dem US-amerikanischem Markt Zusatzgeräte und Software zu beziehen sind, über die auch ein Zugriff auf die in Deutschland nur vom Hersteller auszulesenden Daten möglich ist. Da die Zulieferer ihre Systeme gleichermaßen für den europäischen wie für den US-amerikanischen Markt herstellen, kann die US-amerikanische Gesetzeslage und die hierdurch grundsätzlich geschaffenen Auslesemöglichkeiten auch für Deutschland große Bedeutung erlangen. So könnte beispielsweise die Polizei mit Hilfe derartiger Auslesegeräte zukünftig sämtliche Unfalldaten unfallbeteiligter Fahrzeuge auslesen und damit zügig die Schuldfrage klären sowie Buß- und Verwarngelder festsetzen lassen. Dies gilt zumindest bei Fahrzeugen die herstellerseitig darauf programmiert wurden, anfallende Daten weitreichend auch zu speichern.

b) Offiziell erhobene Daten

Die künftig durch eCall-Eintrichtungen erhaltenen Daten werden neben möglicherweise Dritten zumindest den Notdiensten zur Verfügung gestellt. Da hierbei aber auch Angaben über die Unfallschwere übermittelt werden sollen, stellt sich die Frage, ob die Notdienste die Polizei benachrichtigen und im Zuge dessen die vom eCall übermittelten Daten weiterleiten werden. Im Falle der Speicherung in der Notrufzentrale könnten die Daten auf der bestehenden Gesetzesgrundlage auch später von der Polizei zur Aufklärung des Unfalles beschlagnahmt werden, was in der Praxis zu einer freiwilligen oder erzwungenen Datenweitergabe bei jedem oder nahezu jedem Unfall führen könnte. Folglich würde dem Staat bei einem Unfall durch das eigene Fahrzeug auch hier ggf. nahezu automatisiert belastendes Material zur Verfügung gestellt werden können.

c) Freiwillig erhobene Daten

Daten aus einem freiwillig eingebauten Unfalldatenspeicher müssen ebenso – wie die von den Herstellern im Verborgenen erhobenen Daten – erst einmal durch einen Sachverständigen ausgelesen werden. Aufgrund der Tatsache, dass sich die Nutzung von Unfalldatenspeichern bislang bei der breiten Masse nicht durchgesetzt hat, gibt es derzeit in Deutschland nur fünf Sachverständige, die für die Auswertung

18 VOLVO z.B. informiert seine Kunden in den Betriebsanleitungen zumindest darüber, dass sich im Fahrzeug mehrere Computer befinden. Diese würden detaillierte Daten aufzeichnen, welche zu Forschungszwecken für die Verbesserung der Sicherheit und zur Diagnose verwendet werden. Die gespeicherten Daten würden in der Regel nicht ohne Genehmigung weitergeleitet werden, man könne jedoch gesetzlich zur Auslieferung der Informationen gezwungen sein.

öffentlich bestellt und vereidigt sind.[19] Die Daten gehören zunächst einmal dem Eigentümer des Fahrzeuges, welcher den Unfalldatenspeicher hat einbauen lassen. Wenn dieser nach einem Unfall Sorge hat, dass er sich durch den Unfalldatenspeicher selbst belasten könnte, kann er die gespeicherten Daten durch Betätigen eines Knopfes selbst löschen.[20] Zu bezweifeln ist demgegenüber, dass auch ein Versicherungsnehmer im Rahmen eines Telematik-Tarifs die von seiner Telematik-Box erhobenen und gespeicherten Daten löschen kann, um sie vor dem Zugriff der Verfolgungsbehörden zu schützen. Denn die Daten werden mit Einwilligung des Versicherungsnehmers erlangt und diesem lediglich auf einem Webportal zur Überprüfung bereitgestellt. Zugriff haben wird hier nur der Versicherer selbst oder eines seiner Partnerunternehmen.

2. Wem stehen die Daten tatsächlich zur Verfügung?

Mit dem Vorgesagten ist jedoch noch nicht beantwortet, wem die Daten im Ernstfall tatsächlich zur Verfügung stehen und wem sie gehören. Inwieweit kann/darf man selbst darauf zurückgreifen und entscheiden, ob sie Dritten zugänglich gemacht werden? Welche Rechte hat der Fahrzeughalter/Fahrzeugführer, welche Rechte haben Dritte und der Staat? Anhand der nachstehend beschriebenen Fallkonstruktionen soll ein Überblick über die bestehenden und kommenden Probleme gegeben werden.

a) Fall 1:

A durchfährt mit ihrem PKW eine Kreuzung ohne bei geltender Regelung »rechts vor links« den von rechts einmündenden Verkehr zu beachten. Das von rechts kommende Fahrzeug des B kollidiert auf Höhe der Beifahrertür mit dem Fahrzeug der A. Die Beifahrerin C der A wird schwer verletzt. A wendet ein, sie habe den B erst zu spät wahrgenommen, gehe daher davon aus, dass B erheblich schneller als die erlaubten 50 km/h gefahren sei.

Da zunächst feststeht, dass A die geltenden Vorfahrtregeln verletzt hat, muss sie mit Schadensersatzforderungen von B und C sowie mit einem Strafverfahren wegen fahrlässiger Körperverletzung aufgrund der sehr erheblichen Verletzungen der C rechnen. Nachdem sie einwendet, der B sei zu schnell gefahren, wird ein Unfallrekonstruktionsgutachten erstellt, bei dem sich der Gutachter anhand der Deformierung der Fahrzeuge ein Bild über die Kräfte macht. Ergänzende Fahrzeugdaten stehen ihm nicht zur Verfügung. Bremsspuren sind nicht vorhanden. Im Ergebnis wird eine Kollisionsgeschwindigkeit des B von 50-70 km/h angenommen.

19 Siehe svv.ihk.de, Stand 18.11.2013, – Sachverständige für Auswertung von Unfalldatenspeichern.

20 Wikipedia Enzyklopädie, Unfalldatenspeicher mwN.

Bei dieser Sachlage müsste A zu 100 % haften und sich mit einem Strafverfahren auseinandersetzen.

Anders sähe es aus, wenn A im Zivilprozess den Beweisantrag stellte, die dauerhaft gespeicherten Systemdaten zum Unfallzeitpunkt auszulesen. Da diese Daten im vorliegenden Fall aufgrund ihrer Verschlüsselung und fehlenden Bereitstellung unter den Eigendiagnosedaten, die wiederrum über fast jede Werkstatt auszulesen sind, nur vom Hersteller selbst ausgelesen werden können, müsste sie auf die ungewöhnliche Idee kommen, sich nicht nur auf übliche Auslesemethoden zu verlassen, sondern die Mitwirkung des Herstellers über §142 ZPO vom Gericht anordnen zu lassen.

Würde der Hersteller die Geräte nun auslesen und erkennen können, dass B unmittelbar vor der Kollision eine Geschwindigkeit von 93 km/h hatte, die durch spätes Abbremsen auf eine Kollisionsgeschwindigkeit von 73 km/h reduziert wurde, stünde zumindest eine Mithaftung, wenn nicht gar eine 100 % Haftung des B im Raum. In diesem Fall würde B durch sein eigenes Fahrzeug verraten und zwar ohne, dass er von dieser Möglichkeit und Gefahr zuvor in Kenntnis gesetzt wurde. Denn wie bereits ausgeführt, teilt bisher kaum ein Hersteller seinen Kunden mit, dass bzw. welche Daten von den Steuergeräten im Fahrzeug erhoben und gespeichert werden.[21]

Je nach Gesundheitszustand der C hätte B zudem im Strafverfahren mit einer empfindlichen Strafe zu rechnen.

Bei der Verwendung der vom Hersteller zur Verfügung gestellten Daten würde der nemo-tenetur[22] Grundsatz, wonach sich niemand selbst belasten muss, ausgehöhlt werden. Auch wenn B selbst nichts zu dem Vorfall sagen würde, wären es die Daten aus seinem Fahrzeug, die ihn vorliegend belasten und einen Nachweis für seine Schuld erbringen würden. Sein Fahrzeug würde zum Zeugen der Anklage.

Eine ähnliche Problematik würde sich ergeben, wenn die Polizei einen von B freiwillig eingebauten Unfalldatenspeicher beschlagnahmen und sich bei der Auswertung die überhöhte Geschwindigkeit ergeben würde. Die Verfolgungsbehörde könnte durch Auswertung des persönlichen, im Eigentum des Fahrzeugführers/-halters stehenden Datenspeichers sein Aussageverweigerungsrecht regelmäßig unterlaufen. Der Unterschied bestünde nur darin, dass B in diesem Fall zumindest von der Aufzeichnung der Daten wüsste.

21 Noch viel zügiger erreichbar und wahrscheinlicher wird dieses Auslesen und der damit einhergehende Aufklärungserfolg zukünftig möglicherweise durch den polizeilichen Einsatz der in den USA bereits weiträumig eingesetzten Auslesegeräte (s. Ziffer III 1b), die das Auslesen einer großen Menge von »Freeze Frame«- Daten ermöglicht. Hier ist bei manchen Fahrzeugen auch ein Zugriff auf die ansonsten nur dem Hersteller vorbehaltenen dauerhaften Airbagdaten möglich, deren Gehalt über die den Werkstätten zur Verfügung gestellten Eigendiagnosedaten hinausgeht.

22 »nemo tenetur se ipsum accusare«, §§ 136 Abs. 1 Satz 2, 163a Abs. 4 Satz 2, 243 Abs. 5 Satz 1 StPO.

Vom eigenen Fahrzeug verraten würde B künftig auch, wenn er einen Versicherungstarif mit Telematik-Option wählen und das im Fahrzeug eingebaute Telematiksystem dem Versicherer übermitteln würde, wie hoch die Geschwindigkeit seines Fahrzeuges tatsächlich war. Die Versicherer erteilen den Verfolgungsbehörden schon jetzt bereitwillig Auskunft über Angaben, die ein Geschädigter im Rahmen seiner Schadenanzeige ihnen gegenüber getätigt hat, so dass auch in Zukunft mit der Weitergabe der sodann im Telematikwege erhobenen Daten zu rechnen ist.

Bei geringfügigeren Unfällen – zumindest ohne erhebliche Personenschäden – könnte hierdurch das im Grundgesetz verankerte Recht auf informationelle Selbstbestimmung des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verletzt sein.[23] Dieses Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Zwar kann in gewissem Maße in Grundrechte eingegriffen werden, dies aber nur soweit es dem überwiegenden Interesse der Allgemeinheit dient. Ob dies bei der Aufklärung eines durchschnittlichen Unfallschadens der Fall ist, muss hinterfragt werden.

Fall 2[24]

A begibt sich in ihren am Straßenrand abgestellten PKW mit Automatikgetriebe. Sie schiebt den Schalthebel in die Position »D« und löst langsam die Bremse. Der PKW beschleunigt daraufhin mit erheblicher Geschwindigkeit und fährt gegen eine Hauswand, wobei eine Person zwischen Hauswand und PKW eingequetscht wird. Die A beteuert, dass sie das Gaspedal nicht betätigt habe und für das Fahrverhalten des PKW nicht verantwortlich sei. Da der Hersteller sich weigerte, die im vorliegenden Fall gespeicherten Daten herauszugeben, anhand derer die Elektronik des Motorsteuergerätes hätte überprüft werden können, wurde vom Gericht ein Sachverständiger beauftragt, die Einlassung der A zu überprüfen. Da

23 Siehe BVerfGE 65, 1-71, wonach eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß, mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar wäre. Wer unsicher sei, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, werde versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens sei. Hieraus folge: Freie Entfaltung der Persönlichkeit setze unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz sei daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleiste insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

24 tatsächlicher Fall, geschildert von dem Sachverständigen Michael Weyde, Berlin.

dieser nicht über die entsprechende Herstellersoftware verfügte und die hiermit auszulesenden verschlüsselten Systemdaten der Motorsteuerung sowie die erforderlichen Erkenntnisse zur vorkollisionär Drosselklappen- und Gaspedalstellung ohnehin nicht hätten entschlüsselt werden können, sich das Fahrzeug im Übrigen aber in einem mechanisch ordnungsgemäßen Zustand befand, wurde die A im Strafverfahren verurteilt.

Hier wäre der A durch die Daten aus dem eigenen Fahrzeug ggf. ein Entlastungsbeweis ermöglicht worden. Aufgrund der technischen Überlegenheit des Herstellers, der sich möglicherweise einem Produkthaftungsprozess entziehen wollte, war ihr dies jedoch nicht möglich. Erst zwei Jahre später war in der Presse zu lesen, dass PKW dieser Marke und Serie wegen »unmotivierten Hochdrehens des Motors« zurückgerufen wurden.

Dieser Fall zeigt deutlich die »Waffenungleichheit« zwischen den Parteien. Gerade vor dem Hintergrund, dass moderne Fahrzeuge mit immer mehr Fahrassistenzsystemen ausgestattet werden, sollten die Daten zumindest dem Fahrzeugführer/-halter zugänglich sein. Anderenfalls ließen sich etwaige Konstruktions- oder Fabrikationsfehler nicht nachweisen, was wiederum zu Beweisproblemen in Strafprozessen gegen einen möglicherweise unschuldigen Fahrzeugführer führen würde.

IV. Auswirkungen, Grenzen und Fiktionen

Die Probleme, die mit der Erhebung, Verarbeitung und Nutzung von fahrzeugbezogenen und fahrerbezogenen Daten einhergehen, sind vielfältig und berühren diverse Rechtsgebiete. So lässt sich auch die Frage, wem die erhobenen Daten überhaupt gehören, nicht ohne weiteres beantworten. Grundsätzlich sollte man meinen, dass die Daten, die ein Fahrzeug über den Fahrer erhebt, auch diesem bzw. dem Halter gehören und dieser über sie bestimmen kann. Selbst wenn sie ihm nicht gehörten, muss er aber zumindest darüber informiert werden, dass sie erhoben und ggf. Dritten zur Verfügung gestellt werden. Insoweit ist auch die Frage, inwieweit der Staat oder auch Dritte Zugriff auf die über den Fahrzeugführer erhobenen Daten haben, von großer Bedeutung. Darf der Staat auf alle Daten zugreifen, die er bekommen kann, oder gibt es Grenzen? Vor dem Hintergrund unserer Grundrechte und den dahinterstehenden Schutzgedanken, sind deutliche Grenzen zu fordern. So ist auf das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG zu verweisen, wonach die Befugnis des Einzelnen gewährleistet sein sollte, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Ist dieses Recht nicht erheblich eingeschränkt, wenn der Staat dem Verkehrsteilnehmern eine verbindliche Pflicht auferlegt, das eCall-System zu nutzen mit der Folge, dass Daten über ihn oder das Fahrzeug gespeichert werden? Ebenso werden strafrechtliche Schutzrechte ausgehöhlt, wenn der Staat Zugriff auf alle über seine Bürger durch deren Fahrzeuge erhobenen Daten hat. Ein Aussageverweigerungsrecht läuft faktisch leer, wenn

die Verfolgungsbehörden ohne weiteres an die über den jeweiligen Fahrzeugführer erhobenen Daten gelangten. Zwar werden seit jeher Zwangsmaßnahmen zur Erlangung und Sicherung von Beweisen in Form von Sicherstellung und Beschlagnahme gemäß §§ 94 ff. StPO durchgeführt, doch darf dies nur unter bestimmten Voraussetzungen geschehen. Denn Sicherstellungen/Beschlagnahmen stellen immer einen Eingriff in Grundrechte des Betroffenen dar. Die Anordnung hat daher, wie alle Zwangsmaßnahmen im Strafverfahren, dem Grundsatz der Verhältnismäßigkeit zu genügen. Dieser Grundsatz verlangt, dass die Maßnahme zur Erreichung des angestrebten Ziels geeignet und erforderlich sein muss und dass der mit ihr verbundene Eingriff nicht außer Verhältnis zur Bedeutung der Sache und zur Stärke des bestehenden Tatverdachts stehen darf.[25] Darüber hinaus muss er für die Ermittlungen notwendig sein.[26] Letztlich ist erforderlich, dass der Tatverdacht eine Tatsachengrundlage hat, aus der sich die Möglichkeit der Tatbegehung durch den Beschuldigten ergibt. Eine bloße Vermutung reicht grundsätzlich nicht aus.[27] So wird in der Praxis bei einem Anfangsverdacht erheblicher Straftaten der Eingriff in die Grundrechte des Beschuldigten durchaus als verhältnismäßig angesehen, so dass eine Beschlagnahme und Verwertung von Daten grundsätzlich stattfinden darf. Anders sollte es jedoch aussehen, wenn lediglich leichte Vergehen oder Ordnungswidrigkeiten im Raum stehen. Bedenkt man zum einen, dass demnächst durch eCall, Telematiksysteme, etc. eine Vielzahl an leicht abrufbaren Daten vorhanden sein wird und zum anderen bei jedem Unfall ein gewisser Anfangsverdacht besteht – zumindest einer der Beteiligten dürfte den Unfall verschuldet haben –, kann befürchtet werden, dass ein Datenabruf ggf. durch Sicherstellungen/Beschlagnahmen zukünftig möglicherweise routinemäßig und flächendeckend bei jedem Unfall durchgeführt wird. Verschärfend kommt hinzu, dass mehrheitlich nicht einmal ein Durchsuchungsbeschluss notwendig sein wird. Denn während der entsprechende Richtervorbehalt hier dem Schutz der Grundrechte dienen soll, ist dieser entbehrlich, wenn die eingreifenden Beamten von »Gefahr im Verzug« ausgehen dürfen. Diese Annahme wird bei den vielfach flüchtigen, semifesten oder löschbaren Daten regelmäßig berechtigt vorliegen, so dass die Entscheidung über die Verhältnismäßigkeit des Eingriffs überproportional häufig bei den Polizeibeamten liegen wird. Der Aufwand, der zur Erlangung der Daten investiert werden müsste, wäre zudem deutlich geringer als bei bisherigen Ermittlungsmethoden, wenn es zentrale Anlaufstellen gibt, an denen die Daten verfügbar sind, was diese Ermittlungsmöglichkeit für die Verfolgungsbehörden zusätzlich attraktiv macht. Gerade Personen, die sich künftig für eine Versicherungspolice mit Telematik-Option entscheiden, droht ein permanenter Verrat durch das eigene Fahrzeug bzw. die eigene Versicherung. Auch Versicherungen gewinnen erhebliche Vorteile im Kampf

25 vgl. BVerfG NStZ 1992, 91, 92.
26 vgl. BVerfGE 20, 162, 186.
27 BVerfG NStZ-RR 2004. 143.

gegen ihre Versicherungsnehmer. Durch deren der Versicherung freimütig zur Verfügung gestellte Daten, könnten die Versicherungen begangene Obliegenheitsverletzungen oder versehentliche Falschangaben, die als Täuschungsversuche ausgelegt werden können und ggf. zur Leistungsfreiheit des Versicherers führen, wesentlich leichter nachweisen. Meldet ein Versicherungsnehmer z.B. den Diebstahl seines Fahrzeuges bei der Versicherung und gibt im Rahmen der Schadenanzeige versehentlich einen falschen Zeitpunkt für den Diebstahl an, kann es zu Problemen mit der Versicherung kommen. Denn diese kann die Angaben des Versicherungsnehmers mit den durch das Telematiksystem erhobenen und gespeicherten Daten vergleichen und etwaige Falschangaben feststellen. Unter Berücksichtigung dieser Entwicklungen scheinen wir nicht mehr weit vom »gläsernen Menschen« entfernt zu sein, wobei sich weitere Fiktionen aufdrängen. Was passiert, wenn das vom Haftpflichtversicherer erstellte »Telematik-Fahr-Brems-Verkehrsregeleinhalte-Profil« im Vergleich mit massenweise gesammelten Vergleichsdaten von Vergleichspersonen ergibt, dass der Versicherungsnehmer zu 80 % in den nächsten Monaten einen schweren Unfall an einem Zebrastreifen oder einer Fußgängerampel – dort war er bislang besonders auffällig -verursachen wird? Angenommen, diese Telematikprognosen treffen mit 99 % iger Wahrscheinlichkeit zu: Soll die Gesellschaft in derartigen Fällen noch deutlich weitgehender als bislang zum Schutz der Allgemeinheit Repressalien – z.B. Anordnung einer MPU, Fahrerlaubnisentzug – verhängen können, bevor überhaupt eine Gefahrensituation eingetreten ist? Bereits jetzt kann die Fahrerlaubnisbehörde nach § 13 FeV zur Klärung von Eignungszweifeln bei Alkoholproblematik die Beibringung einer MPU anordnen, wenn sie Kenntnis von Tatsachen erhält, die die Annahme von Alkoholmissbrauch begründen, etwa durch Mitteilung von Angehörigen oder der Polizei. Die Alkoholauffälligkeit muss dabei nicht im Zusammenhang mit einer Teilnahme am Straßenverkehr stehen; es reicht, wenn die Gesamtumstände Zweifel rechtfertigen, ob der Betroffene Trinken und Fahren sicher trennen kann.[28] Angenommen, das vom Versicherer zukünftig erstellte Fahrerprofil begründet die Befürchtung erheblicher zukünftiger Verstöße, ggf. mit Personenschaden. Kann in diesem Fall demnächst nach – auf welcher Grundlage auch immer beruhender – Datenweitergabe ähnlich verfahren werden?

V. Fazit

Um den Risiken der vorgeschilderten Entwicklungen frühzeitig entgegenzuwirken, müssen ausreichende Schutzgesetze geschaffen und die Beteiligten ausführlich

28 vgl. VGH Mannheim NZV 2002, 580, 582; OVG Koblenz ZfS 2006, 713; ZfS 2007, 656; OVG Lüneburg, DAR 2007, 227; VG Oldenburg DAR 2010, 42; Hentschel, Straßenverkehrsrecht, 42. Aufl., §13 FeV Rn. 20 ff., mwN.

aufgeklärt werden. Jeder muss darüber informiert werden, welche Daten erhoben, gespeichert und weitergeleitet werden. Derzeit besteht eine große Unübersichtlichkeit, wobei die Gründe dafür unterschiedlicher Natur sind. So ist die Erhebung der Daten teilweise nicht bekannt, häufig liegen die Gründe aber auch darin, dass der Verbraucher gar nicht bzw. nicht mehr weiß, bei welcher Vertragsunterzeichnung er welcher Datenerhebung zugestimmt hat oder in welche Regelung z.B. der Vorbesitzer eines Fahrzeuges eingewilligt hat. Klauseln über die Erhebung, Verarbeitung und Nutzung von Daten finden sich oft nur im Kleingedruckten. Durch die Unterzeichnung eines Vertrages wird z.T. in die Datenerhebung und –verarbeitung eingewilligt, ohne dass dies dem Verbraucher bewusst ist. Vor dem Hintergrund wachsender Datensammlungen und davon ausgehender Gefahren, sollte zukünftig deutlicher und übersichtlicher, ggf. durch zusätzliche Einverständniserklärungen, darauf hingewiesen werden, welche Daten erhoben, wo sie gespeichert und an wen sie möglicherweise weitergeleitet werden. Darüber hinaus muss es möglich sein, die vom eigenen Fahrzeug erhobenen und gespeicherten Daten frühzeitig und ggf. als Erster einsehen zu können. Daten, die von den bis zu 80 Steuergeräten des Fahrzeuges gespeichert werden und aufgrund der Verschlüsselung derzeit z.T. ausschließlich durch die Hersteller bzw. Zulieferer ausgelesen werden können, müssen dem Fahrzeughalter bzw. Fahrzeugführer auf Anfrage auch außergerichtlich zugänglich gemacht werden. Zugang zu den Daten ist zwar bereits jetzt auf Anordnung des Gerichts nach §§ 142 ff. ZPO möglich. In einem solchen Fall gelangt aber regelmäßig gleichzeitig die Gegenpartei an die Daten, ohne dass man den Gehalt zuvor prüfen konnte. Eine ähnliche Problematik weisen die Produkthaftungsfälle auf. Die »technische Waffenungleichheit«, die derzeit zwischen Herstellern und Fahrzeughaltern besteht, sollte im Hinblick auf die weitere Zunahme von Fahrassistenzsystemen dringend und zügig ausgeglichen werden.

Abschließend scheint eine engere Auslegung strafrechtlicher Schutzgesetze im Hinblick auf künftige Entwicklungen wünschenswert.

VI. Empfehlungen

Welche Auswirkungen die allerorts anzutreffenden anwachsenden Datensammlungen haben werden, ist vielfach noch im Bereich der Fiktion angesiedelt, so dass zum jetzigen Zeitpunkt nicht jeder Eventualität durch eine Empfehlung vorgebeugt werden kann. Als Minimalbasis ist folgendes zu empfehlen.

Der Fahrer eines mit eCall-Einrichtung ausgestatteten Fahrzeugs muss selbst darüber entscheiden dürfen, ob er die Funktion aktivieren möchte oder nicht. Dementsprechend sollte eine Ausschaltmöglichkeit in Erwägung gezogen werden. Zudem ist sicherzustellen, dass nach dem Hilfeeinsatz eine sofortige Löschung der Daten erfolgt.

Nutzer von eCall – Systemen müssen darüber informiert werden, welcher Mindestdatensatz an die Notdienststellen übermittelt wird. Es ist festzulegen,

welche Daten an wen weitergegeben werden dürfen. (z.B. Weitergabe der Daten an die Polizei).

Die derzeit bestehende Unübersichtlichkeit über die Erhebung, Speicherung und Weiterleitung von Daten muss aufgehoben werden. Fahrzeughalter/Fahrzeugführer müssen einfach und verständlich darüber informiert werden, wann, wo und über welchen Zeitraum welche Daten im Fahrzeug gespeichert werden. Sie müssen darüber aufgeklärt werden, dass diese Daten bei berechtigtem Interesse möglicherweise Dritten zur Verfügung gestellt werden können, was weitergehend als bisher von Einverständniserklärungen abhängig gemacht werden sollte.

Hohe Anforderungen an eine wirksame Einverständniserklärung in diesem Bereich müssen sichergestellt werden. Mindestanforderungen sind hierbei die Freiwilligkeit (keine Koppelung mit etwaigen Versprechen/Vorteilen) und die Möglichkeit eines jederzeitigen Widerrufs.