Gerrit Hornung

Verfügungsrechte an fahrzeugbezogenen Daten

Das vernetzte Automobil zwischen innovativer Wertschöpfung und Persönlichkeitsschutz

Moderne Kraftfahrzeuge sind schon heute rollende Computer. Die verbaute IT und der Zugang zum Internet dienen zunehmend nicht nur der Fahrsicherheit und dem Fahrkomfort, sondern allen möglichen weiteren Zwecken. Viele der durch die heute schon über 100 Sensoren erhobenen Daten haben einen wirtschaftlichen Wert. Eine der drängendsten Fragen für Automobilhersteller, Internetanbieter und Fahrzeuginsassen ist deshalb, wer über die fahrzeugbezogenen Daten verfügen und diese ökonomisch ausbeuten darf.

1 Einleitung

Dass Daten einen wirtschaftlichen Wert haben und die Grundlage vieler innovativer Dienste und Geschäftsmodelle sind, ist inzwischen ein Allgemeinplatz. Wenn IT einen neuen, bisher nicht oder wenig technisierten Lebensbereich durchdringt, so ist dies typischerweise mit der Erhebung und Verwendung neuer (personenbezogener oder anonymer) Daten verbunden. Diese dienen der Verbesserung der angebotenen Dienste, der Übermittlung zielgruppenspezifischer Werbung, der Kontrolle der Betroffenen, dem schlichten Verkauf an Dritte und anderen wirtschaftlichen Zwecken.

Der Einsatz von IT in Kraftfahrzeugen erfolgt schon seit Jahrzehnten, hat sich in den letzten Jahren aber massiv ausgeweitet.[1] Er geht längst über die Verarbeitung von Standortdaten im Rahmen von Navigationsdiensten und anderen LBS oder die automatische Anbindung von Mobilfunkgeräten an die Freisprechanlage hinaus. In einer nicht allzu fernen Zukunft werden alle Fahrzeuginsassen (auch der durch autonome Fahrsysteme „befreite" Fahrer)[2] die Möglichkeit haben, allgemeine und automobilspezifische Internetdienste während der Fahrt zu nutzen und so mehr über ihre Umgebung zu erfahren, zu arbeiten oder freizeitorientierten Entertainment-Aktivitäten nachzugehen. Das weltweite Umsatzwachstum für derartige Dienste wird von 31 Mrd. Euro (2015) auf 113 Mrd. Euro (2020) geschätzt.[3]

Wer auch immer diese Dienste anbieten wird, wird ein erhebliches Interesse an den personenbezogenen Daten der Insassen haben. Aber auch die unmittelbar durch das Fahrzeug produzierten Informationen über seinen Zustand, die Umgebung (Geschäfte, andere Verkehrsteilnehmer, Wetter etc.) oder die Aktivitäten in seinem Inneren sind für jeden Anbieter attraktiv. Dasselbe gilt für staatliche Stellen, die zu Zwecken der Verkehrslenkung, der Straßenverkehrssicherheit, der Milderung von Unfallfolgen oder der allgemeinen Kriminalitätsbekämpfung tätig sind. Im Spannungsverhältnis der vielen interessierten Parteien ist es deshalb von großer Bedeutung zu klären, wer über welche Daten verfügen und diese nutzen darf.[4]

2 Hintergründe

Im vernetzten Automobil der Zukunft werden verschiedene Datentypen erhoben und verwendet werden, an denen verschiedene Akteure Interesse haben.

1 Zu den technischen Grundlagen s. z.B. die Beiträge in *Reif* (Hrsg.), Sensoren im Kraftfahrzeug, 2. A. 2012; *Bönninger*, in: 52. VGT, 2014; *ders.*, zfs 2014, 184.

2 Die Rechtsfragen dieser Systeme bleiben hier ausgeklammert; s. z.B. *Lutz/Tang/Lienkamp*, NZV 2013, 57; *Lutz*, NZV 2014, 67; *ders.*, NJW 2015, 119; allgemeiner schon *Bewersdorf*, Zulassung und Haftung bei Fahrerassistenzsystemen im Straßenverkehr, 2005.

3 http://www.wiwo.de/9647526.html.

4 S. zu dieser Frage und zum Datenschutz im Kraftfahrzeug *Roßnagel*, NZV 2006, 281; *ders.*, SVR 2014, 281; *Asaj*, DuD 2011, 558; *Schulz/Roßnagel/David*, ZD 2012, 510; *Mielchen*, SVR 2014, 81; *Weichert*, SVR 2014, 201 und 241; *Kremer*, RDV 2014, 240; *Kinast/Kühnl*, NJW 2014, 3057; *Pohle/Zoch*, CR 2014, 409; zu den Besonderheiten der Elektromobilität *Lüdemann/Jürgens/Ortmann*, RDV 2014, 3; erste Überlegungen z.B. schon bei *Hassemer/Topp*, NZV 1995, 169; *dies.*, DAR 1996, 85; *Weichert*, DuD 1996, 77.

Prof. Dr. Gerrit Hornung, LL.M.

Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau und Sprecher des dortigen Institute of IT-Security and Security Law (ISL).
E-Mail: Gerrit.Hornung@uni-passau.de

2.1 Datenkategorien

Die anfallenden Daten können nach verschiedenen Gesichtspunkten kategorisiert werden.[5] Eine Unterscheidung nach dem hauptsächlichen Bezug legt die folgende Gruppierung nahe:

- fahrzeugbezogene Daten, z.B. Grunddaten (Modell, Fahrzeug-Identifizierungsnummer, Kennzeichen) aktuelle Position und Positionsveränderungen (Geschwindigkeit, Beschleunigung- und Bremsvorgänge), Zustand des Fahrzeugs (Batterie, Bremsen und andere Komponenten),
- direkt insassenbezogene Daten, etwa Identifizierungsinformationen (PIN oder Passwort, biometrische Daten, Hardware-Token, Kreditkarteninformationen), persönliche Vorlieben (wie Sitzeinstellungen, Temperatur oder Radiosender), Angaben über das Verhalten (Fahrerverhalten, Interessen der Mitfahrer, Ton- oder Videoaufzeichnungen aus dem Innenraum) oder die körperlich-geistige Verfassung (etwa Reaktionszeiten, Müdigkeit, Alkohol- oder Drogenkonsum),
- umweltbezogene Daten, z.B. über andere Verkehrsteilnehmer (Fahrzeuge, Fahrradfahrer, Fußgänger), die Verkehrsinfrastruktur (Verkehrsschilder, Straßenzustand), Verkehrsvorfälle (Unfälle, Staus), sonstige Umgebungsmerkmale (Geschäfte, Sehenswürdigkeiten, Veranstaltungen) oder das Wetter,
- drittanbieterbezogene Daten, die in Verträgen anfallen, welche mit anderen als den Kfz-Herstellern geschlossen werden (Anbietern von Navigationsdiensten, Mobilfunk, Internet-Apps oder Kfz-Versicherungen).

Mit dieser Typologie ist noch keine rechtliche Einordnung verbunden. Insbesondere können alle vorgenannten Daten personenbezogen im Sinne von § 3 Abs. 1 BDSG sein; bei vielen wird dies sogar regelmäßig zutreffen.[6]

Unterscheiden lassen sich die Daten auch nach ihrer Komplexität. Dies legt eine Differenzierung nach Basismerkmalen des Fahrzeugs (Modell, Fahrzeug-Identifizierungsnummer, Größe, Farbe, Sonderausstattungen, Kennzeichen etc.), Verbindungsdaten (etwa zu einem Mobilfunknetzwerk oder ad-hoc Netzwerken in der Car2Car- oder Car2Infrastructure-Kommunikation), Sensor-Basisdaten (Temperatur, Geschwindigkeit, Helligkeit, Abstand etc.), deren Verknüpfung und Aufbereitung für den Fahrer oder andere Insassen (etwa für Navigations- oder Fahrassistenzsysteme) sowie schließlich Daten über Multimedia-Infotainmentangebote nahe.

Eine wesentliche Frage ist, ob die jeweiligen Daten freiwillig erhoben und verwendet werden. In vielen Bereichen neuer Angebote der Kfz-Hersteller und anderer Provider wird dies der Fall sein. Demgegenüber gibt es aber auch eine zunehmende Zahl gesetzlich vorgeschriebener Anwendungen und Datensammlungen. Dazu gehören etwa das künftig europaweit vorgeschriebene Notfallassistenzsystem eCall oder der in den USA durch die U.S. Department of Transportation's National Highway Traffic Safety Administration vorgeschlagene verbindliche Standard zum Einbau von Event Data Recordern (EDRs oder „Black Boxes").[7]

Mit zunehmender Verbreitung der Datennutzung könnten auch viele AGB einen nicht-freiwilligen Charakter annehmen, wenn z.B. essentielle Garantien von der Einwilligung in die Erhebung technischer Daten abhängig gemacht werden oder erschwingliche Kfz-Versicherungen nur noch um den Preis der kontinuierlichen Übermittlung von Informationen über das Fahrverhalten zu haben sein sollten.[8]

2.2 Anwendungsfälle und interessierte Parteien

Mit den Daten lassen sich sehr unterschiedliche Zwecke verfolgen.[9] Inzwischen schon fast konventionell anmutende Anwendungsfälle sind die Produktentwicklung und -verbesserung (Betriebs- und Verschleißinformationen werden zur Steigerung von Leistung, Effizienz und Umweltverträglichkeit der Komponenten verwendet), die Geolokalisation (für Navigationsdienste und alle Arten von LBS)[10] und die Telekommunikation (Anbindung von Mobilfunkgeräten für die Sprachtelefonie, künftig überdies für jede Form der Internetnutzung).

Wirtschaftlich und rechtlich interessanter sind demgegenüber innovative Dienste, die man wie folgt unterscheiden kann:

- die Verbesserung der Fahr- und Straßenverkehrssicherheit („safety"), z.B. durch die Diagnose von Statusdaten und Fehlfunktionen des Fahrzeugs, Fahrerassistenzsysteme zur Verbesserung des Verkehrsflusses und zur Warnung bzw. Vorhersage unvorhergesehener Ereignisse oder nachlassender Reaktionsfähigkeit des Fahrers (automatisches Spurhalten und Bremsen, Unfallwarnungen, perspektivisch das autonome Fahren) oder Notfallassistenzsysteme (eCall),
- die Straßenverkehrsüberwachung im weiteren Sinne („security"), also die staatlich organisierte Verkehrskontrolle (Mauterhebung, Eingriffe bei Verkehrsstörungen etc.), die Aufdeckung und Verfolgung von Verkehrsstraftaten und -ordnungswidrigkeiten (etwa durch „Section Control"),[11] die Prävention und Aufklärung von Fahrzeugdiebstählen, die allgemeine Personenfahndung (etwa durch elektronische „Nachfolger" der Kfz-Kennzeichenerfassung),[12] aber auch die Feststellung zivilrechtlicher Verantwortlichkeit durch den verbindlichen Einsatz von EDR,[13]
- die Dokumentation und Überwachung von Verträgen, etwa Kfz-Versicherung,[14] Leasing- oder Mietverträge (Beschränkung auf bestimmte Maximalgeschwindigkeiten, zulässige Fahrziele, Fahrer, maximale Ladung o.ä.) oder Arbeitsverträge von Außendienstmitarbeitern.[15]

5 S. z.B. *Asaj*, DuD 2011, 558, 559 f.; *Hornung/Goeble*, CR 2015, 265, 266 f.

6 S.u. 3.1, 5.1.

7 Zur Entwicklung in den USA s. insoweit https://epic.org/privacy/edrs/; Übersicht zu einzelstaatlichen Regelungen unter http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx; zu den Rechtsfragen aus deutscher Sicht *Schmidt-Cotta*, ZRP 2000, 518; *Graeger*, NZV 2004, 16; *Brenner/Schmidt-Cotta*, SVR 2008, 41; *Schlanstein*, VD 2014, 15.

8 Zum ersten Telematik-Tarif „S-Drive" der S-Direkt s. *Borsetzky*, VW 2014, 24 ff.; *Weichert*, SVR 2014, 241, 245 f.; *Kremer*, RDV 2014, 240, 250; näher *Lüdemann/Sengstacken/Vogelpohl*, RDV 2014, 203.

9 Zu den interessierten Parteien s. *Weichert*, SVR 2014, 201, 202 f.; *Roßnagel*, SVR 2014, 281 f.; *Hornung/Goeble*, CR 2015, 265, 266 f.

10 S. allgemein *Schnabel*, Datenschutz bei profilbasierten Location Based Services, 2009; für Automobile *Weichert*, SVR 2014, 201, 206 f.

11 Dazu *Albrecht*, SVR 2009, 161; *Arzt/Eier*, NZV 2010, 113; für Österreich *Hofer*, DAR 2009, 23.

12 Dazu BVerfGE 120, 378; s. zuletzt BVerwG, DuD 2015, 196 (kein Grundrechtseingriff, wenn im Trefferfall eine manuelle Kontrolle einen Fehler ergibt und das Kennzeichen sofort gelöscht wird, ohne dass die Anonymität des Inhabers aufgehoben wird).

13 Zu den Rechtsfragen s. Fn. 7.

14 S. Fn. 8.

15 Zum Arbeitnehmerdatenschutz beim Flottenmanagement s. *Schröder*, ZD 2013, 13.

Schon aus der Fülle der Anwendungen ist ablesbar, dass die traditionellen Automobilhersteller diese nicht alle und nicht ausschließlich anbieten werden. Wer sich in den neuen Märkten durchsetzen wird und ob die teilweise geäußerten Warnungen vor dem Beispiel der Marginalisierung ehemaliger Marktführer wie Nokia[16] berechtigt sind, ist derzeit nicht absehbar. Völlig von der Hand zu weisen sind die Parallelen jedenfalls nicht.

3 Grundrechtliche Zuordnung

Als Ausgangspunkt für die Verfügungsbefugnisse kann die grundrechtliche Zuordnung der durch das vernetzte Automobil erzeugten Daten dienen. Diese bildet den unmittelbaren Maßstab, wenn der Staat selbst – etwa durch Sicherheitsbehörden – die fahrzeugbezogenen Daten nutzen möchte oder wenn er Verfügungsrechte anderer verbindlich vorgibt. Daneben spielen die Grundrechte im Rahmen der mittelbaren Drittwirkung[17] auch für die Zuordnung im Verhältnis zwischen Privaten (Eigentümer, Halter, Fahrer, Beifahrer, Dritte in der Umgebung, Hersteller, Zulieferer, Diensteanbieter) eine Rolle. Hier können sich auch Pflichten des Staates ergeben, sich „schützend und fördernd“[18] vor die Grundrechte der Betroffenen zu stellen.

3.1 Recht auf informationelle Selbstbestimmung

Wenn und soweit die erzeugten Automobildaten personenbezogen oder personenbeziehbar sind, ist der Schutzbereich des Rechts auf informationelle Selbstbestimmung eröffnet. Diese Grundrechtsinnovation des BVerfG von 1983[19] ist nach wie vor die verfassungsrechtliche „Grundregulierung“ des Persönlichkeitsschutzes gegen den Umgang mit entsprechenden Daten. Eingriffe sind im überwiegenden Allgemeininteresse zulässig, erfordern aber eine normenklare gesetzliche Grundlage, die dem Grundsatz der Verhältnismäßigkeit entsprechen muss. Dies hat das BVerfG im Bereich staatlicher Überwachung immer wieder im Detail kontrolliert; dies betrifft mit der Kfz-Kennzeichenüberwachung[20] auch den Automobilbereich.

Der erforderliche Personenbezug kann sich zum Fahrer, Eigentümer, Halter oder zu sonstigen Insassen, aber auch zu Personen außerhalb des Fahrzeugs ergeben. Es ist demzufolge falsch, aus der Tatsache, dass der konkrete Fahrer nicht identifiziert werden kann, einen fehlenden Personenbezug abzuleiten.[21] Dasselbe gilt für den in der Diskussion bisweilen unter dem Schlagwort einer „data ownership“[22] zu findenden Versuch, „technische Daten“ per se den Herstellern zuzuordnen.[23] Ist einem Datenverarbeiter der Eigentümer oder Halter bekannt, so sind vielmehr alle fahrzeugbezogenen Daten personenbezogen, auch wenn der konkrete Fahrer nicht identifiziert werden kann. Der Anwendungsbereich des Rechts auf informationelle Selbstbestimmung ist dementsprechend etwa bei staatlichen Stellen eröffnet, die sich mittels einer Halterabfrage ein entsprechendes Zusatzwissen verschaffen können. Im nicht-öffentlichen Bereich können Kfz-Händler, Werkstätten oder Pannenhilfen die Daten ohne weiteres zuordnen.[24]

Weder der verfassungsrechtliche noch der einfachgesetzliche Datenschutz kennen einen Bagatellvorbehalt. Folglich sind restlos alle Daten erfasst, z.B. die Information, in welchem Verschleiß- oder Wartungszustand sich einzelne Komponenten befinden. Eine Ausnahme für solche – ohnehin nur vordergründig „belanglo-

16 Auf die Parallele weißt z.B. *Lobo* hin, s. http://www.spiegel.de/netzwelt/web/sascha-lobo-ueber-vernetzte-autos-google-und-apple-a-1020417.html.

17 St. Rspr., seit BVerfGE 7, 198 diese „grundsätzliche Frage“ (ebd., 204) beantwortet hat.

18 So die ständige Formulierung, s. BVerfGE 35, 79 (113); 39, 1 (1. Leitsatz und 42); 46, 160 (164); 53, 30 (57); 56, 54 (73); 85, 360 (384); 88, 203 (232); 90, 145 (149); 115, 25 (45); 115, 118 (153); 121, 317 (356).

19 BVerfGE 65, 1; zur Innovationsgeschichte s. *Hornung*, Grundrechtsinnovationen, 2015, 266 ff.

20 S. Fn. 12.

21 Mit Fokus allein auf den Fahrer z.B. *Brenner*, DAR 2014, 619, 623; *Kinast/Kühnl*, NJW 2014, 3057, 3058; umgekehrt zu weit *Lüdemann/Sengstacken*, RDV 2014, 177, 180: Erhebung von Anschnallinformationen bei Beifahrern nur mit Einwilligung, ohne die Identifizierbarkeit zu problematisieren.

22 Dazu für das vernetzte Automobil *Hornung/Goeble*, CR 2015, 265 m.w.N. zu eigentumsähnlichen Konstruktionen des Datenschutzes.

23 Z.B. *Zetsche*, http://www.welt.de/wirtschaft/article136402513.html; noch deutlicher VW-Chef *Winterkorn*: „Die Daten gehören uns!“, s. http://www.tagesschau.de/wirtschaft/auto212.html.

24 S.a. *Weichert*, SVR 2014, 201, 204; *Kremer*, RDV 2014, 240, 243 f.

se“[25] – Daten gibt es nicht. Der Anwendungsbereich des Rechts auf informationelle Selbstbestimmung ist nur zu verneinen, sofern Daten technisch sicher anonymisiert werden, also weder Fahrer noch Eigentümer, Halter, Insassen oder sonstigen Personen zugeordnet werden können.

3.2 Neue Grundrechte für den Straßenverkehr

Verstärkt wird die allgemeine grundrechtliche Datenschutzposition durch eine Reihe weiterer Grundrechte, die bisher im Straßenverkehr keine oder nur eine untergeordnete Rolle gespielt haben. Wenn Fahrzeuge im Rahmen der allgemeinen Sprachtelefonie, der verschiedenen Formen der Internetnutzung oder künftig durch Zwangsanwendungen wie Notrufsysteme TK-Verbindungen aufbauen, so schützt Art. 10 GG sowohl den Inhalt als auch die Umstände dieser Kommunikation.[26]

Drei weitere Verstärkungen knüpfen unmittelbar an das Fahrzeug an:

- In bestimmten Fällen genießt dieses erstens den Schutzbereich von Art. 13 GG, nämlich bei Wohnmobilen, Wohnwagen und Wohnbooten.[27] Dies erfasst insbesondere so genannte Lausch- und Spähangriffe auf den Innenraum, die mit dem Einbau von Freisprechanlagen und Innenkameras mit Internetanschluss erheblich leichter werden.
- Zweitens werden viele Systeme der Fahrzeuge oder sogar diese als Ganzes die Tatbestandsvoraussetzungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfüllen, auch wenn unklar ist, ob dieses über die bislang singuläre Entscheidung des BVerfG zur Online-Durchsuchung[28] hinaus in Zukunft verfassungspraktische Wirkung erlangen wird.[29]
- Drittens kann die Schranken-Schranke des Kernbereichs der privaten Lebensgestaltung betroffen sein, wenn z.B. Selbstgespräche aufgezeichnet werden. Dies betrifft auch PKWs und führt nach der Rechtsprechung des BGH zu einem Beweisverwertungsverbot.[30] Dies könnte perspektivisch auch ähnlich sensible Daten erfassen, die in Bordsystemen gespeichert werden.

Auch die Hersteller und sonstige Anbieter innovativer Dienste können sich auf Grundrechte stützen. Dies gilt insbesondere für die Berufsfreiheit des Art. 12 GG, die neben der konkreten Art der Berufsausübung auch Betriebs- und Geschäftsgeheimnisse schützt;[31] hierfür greifen manche ergänzend auf Art. 14 GG zurück.[32] Allerdings fallen nicht alle fahrzeugbezogenen Daten in diesen Bereich. Neben dem Bezug zum Unternehmen und dem Geheimnischarakter ist auch erforderlich, dass der Unternehmer ein berechtigtes wirtschaftliches Interesse an der Geheimhaltung hat.[33] Dies trifft sicher auf viele Informationen zur Funktionsweise des Fahrzeugs oder seiner Komponenten zu, nicht aber auf Daten zu Position, Tankfüllstand, Wetter, Radiosender, Wartungsintervalle, Präferenzen der Insassen etc.[34] Grenzfälle ergeben sich, wenn etwa aus Verschleißinformationen Details über Aufbau oder Funktionsweise von Komponenten erkennbar sind.

4 Gesetzliche Vorgaben für die Verwendung

Wie in anderen Bereichen hat der Gesetzgeber auch beim vernetzten Automobil die Möglichkeit, den Datenumgang gesetzlich zu regeln.[35] Ein Beispiel für den Einsatz zur Gefahrenabwehr ist das eCall-System. Umgekehrt sind auch gesetzliche Verwendungsverbote denkbar. Ein solches wird derzeit vielfach für den Einsatz so genannter Dash-Cams angenommen.

4.1 Verwendung zur Gefahrenabwehr: das Beispiel eCall

Das in seiner Einführung mehrfach verschobene System eCall (für „emergency call“) soll nunmehr zum 31. März 2018 starten. Nach diesem Datum zugelassene Fahrzeuge müssen über ein nicht abschaltbares Notrufsystem verfügen, dass im Notfall zumindest einen Minimaldatensatz (nach DIN EN 15722) an eine Notrufzentrale[36] übermittelt. Wird mittels eines Unfall-Sensors Alarm ausgelöst, so werden insbesondere Zeitpunkt, Unfallort, Fahrtrichtung und Fahrzeugkennung weitergegeben.[37] Optional sind weitere Informationen wie Treibstoffart, Zahl der angelegten Sicherheitsgurte oder Schwere des Unfalls (z.B. Überschlagen). Vorgegeben ist der automatische Aufbau einer Sprechverbindung, über die die Insassen weitere Informationen übermitteln, aber auch Entwarnung bei Fehlalarmen geben können. Handelt es sich um einen so leichten Unfall, dass das System nicht automatisch auslöst, wird auch eine manuelle Kontaktaufnahme möglich sein.

Die gesetzlichen Grundlagen dieses Systems müssen grundrechtlichen Anforderungen genügen, wobei in diesem Fall die Vorgaben aus Art. 7 und Art. 8 GRC einschlägig sind. Das hauptsächliche rechtliche Problem ist der verpflichtende Charakter des Gesamtsystems. Dieses erscheint auf den ersten Blick nicht nur wegen des Eingriffs in das Recht auf Schutz personenbezogener Daten (Art. 8 GRC), sondern auch wegen eines inhärenten Pa-

25 Dass es unter den Bedingungen der automatischen Datenverarbeitung kein „belangloses“ Datum mehr gibt (BVerfGE 65, 1 (45)), trifft heute noch mehr als zur Zeit des Volkszählungsurteils zu.

26 Zur Reichweite s. z.B. BVerfGE 130, 151 (179 ff.) m.w.N.

27 S. *Papier*, in: Maunz/Dürig, Art. 13 Rn. 10; nicht erfasst sind dagegen PKW, s. BGH NStZ 1998, 157.

28 BVerfGE 120, 274; dazu z.B. *Hoffmann-Riem*, JZ 2008, 1009; *Hornung*, CR 2008, 299; *Bäcker*, in: LfDI NRW (Hrsg.), Privatsphäre mit System, 2010, 4; *Drallé*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, 2010; *Gudermann*, Online-Durchsuchungen im Lichte des Verfassungsrechts, 2010.

29 Zur Innovationsgeschichte und der bislang sehr eingeschränkten Diffusion s. *Hornung* (Fn. 19), 277 ff.; zur Anwendbarkeit auf das vernetzte Fahrzeug *Roßnagel*, SVR 2014, 281, 283.

30 S. BGHSt 57, 71; zum Kernbereichsschutz s. *Dammann*, Der Kernbereich privater Lebensgestaltung, 2011; *Barrot*, Der Kernbereich privater Lebensgestaltung, 2012; zur Genese *Hornung* (Fn. 19), 319 ff.

31 BVerfGE 115, 205 (229 ff.).

32 Offengelassen von BVerfGE 115, 205 (248); abl. z.B. *Wolff*, NJW 1997, 98; s.a. *Beyerbach*, Die geheime Unternehmensinformation, 2012, 210 f.

33 BVerfGE 115, 205 (230); BGH, GRUR 2003, 356, 358; 2006, 1044, 1046; 2009, 603, 604.

34 Zum Schutz der Unternehmensinformationen in „intelligenten“ Netzwerken s. *Hofmann*, InTeR 2013, 210.

35 Das gilt außer für die Beispiele im Folgenden z.B. für die OBD-Daten auf der Basis von Art. 5 Abs. 3 VO (EG) 715/2007 und Art. 4 VO (EG) 692/2008 (bestätigt durch VO (EU) 566/2011 und VO (EU) 459/2012), s. *Roßnagel*, SVR 2014, 281, 284.

36 Die Mitgliedstaaten müssen bis zum 1.10.2017 die Infrastruktur für „eCall-Notrufabfragestellen“ errichten, s. Beschluss Nr. 585/2014/EU des Parlaments und des Rates v. 15.5.2014 über die Einführung des interoperablen EU-weiten eCall-Dienstes, ABl. EU L 164 v. 3.6.2014, 6; s.a. *Pohle/Zoch*, CR 2014, 409, 412.

37 S. z.B. *Bönninger*, zfs 2014, 184, 186; *Kinast/Kühnl*, NJW 2014, 3057; *Lüdemann/Sengstacken*, RDV 2014, 177, 178; *Pohle/Zoch*, CR 2014, 409, 412 f.

ternalismus bedenklich. Bei näherer Betrachtung lässt sich der zweite Einwand allerdings entkräften. Der Gesetzgeber bezweckt nicht (nur) den Schutz des Fahrers vor sich selbst, sondern auch den von Beifahrern und anderen Unfallbeteiligten, die ebenfalls schneller Hilfe erhalten. Ähnlich wie die Gurtanlege- und Helmpflicht[38] lässt sich mit diesem Zweck auch das verpflichtende eCall-System im Grundsatz rechtfertigen.[39]

Dies setzt allerdings zweierlei voraus, nämlich eine tatsächliche signifikante Reduzierung der Unfallfolgen und die datenschutzfreundliche Gestaltung des nicht optionalen Systemteils. Sofern sich die Erwartung der Kommission bewahrheitet, das System könne die Zeit bis zur Ankunft der Helfer um durchschnittlich 50 % reduzieren und so hunderte von Menschenleben pro Jahr in der Union retten,[40] ist das erste Kriterium erfüllt.

Auf der Gestaltungsebene ist wesentlich, dass zu dem angestrebten Zweck keine kontinuierliche Ortung des Fahrzeugs oder gar die Anlegung eines Bewegungsprofils erforderlich sind.[41] Vielmehr handelt es sich um ein geradezu prototypisches Beispiel für einen Dienst, der nur im Bedarfsfall Daten übermitteln muss. Dementsprechend ist diese Beschränkung technisch sicherzustellen und auf die tatsächlich erforderlichen Informationen zu begrenzen. Diese unterliegen einer Beschränkung auf den Zweck der Notfallrettung. Eine spätere Erweiterung des Minimaldatensatzes bedarf einer gesetzgeberischen Entscheidung; schleichende Veränderungen durch eine Modifizierung technischer Standards sind bedenklich.[42] Solange der Alarm nicht ausgelöst wird, dürfen die Daten das Fahrzeug nicht verlassen, sind kurzfristig zu überschreiben und von sonstigen Bordsystemen zu trennen. Vorgaben sind auch für die Datensicherheit erforderlich.

Die auf Initiative des Europäischen Parlaments aufgenommenen Vorgaben zu vielen dieser Punkte sind eine klare Verbesserung. Auf dieser Basis erscheint die technische Umsetzung eines derart beschränkten verpflichtenden Systems als lösbar. Die eigentlichen datenschutzrechtlichen Probleme werden deshalb dadurch erzeugt, dass die im Fahrzeug verpflichtend verbaute Schnittstelle nicht nur dazu dienen wird, die Wahl zwischen eCall-Angeboten der Hersteller und Dritter zu ermöglichen. Ziel der Kommission war es von Anfang an auch, eine Infrastruktur für das Angebot von Zusatzdiensten aufzubauen.[43]

Hierfür kommt eine Vielzahl der schon erwähnten Dienstleistungen in Betracht. Dementsprechend haben freie Anbieter ein erhebliches Interesse daran, dass die Hersteller die eCall-Schnittstelle nicht monopolisieren und etwa Vertragswerkstätten bevorzugen.[44] Die Versicherungswirtschaft sieht offenbar gerade in einer Verbindung aus eCall und EDR ein erhebliches Potenzial. Genannt werden eine schnellere Pannenhilfe, die vereinfachte Beweisführung zur Unfallursache, neue Wege zur Erkennung von Betrugsfällen, Möglichkeiten der Prozessautomation sowie die Diebstahlsbekämpfung.[45]

Der europäische Gesetzgeber hat für den Einsatz der verbindlichen Schnittstelle keine weiteren rechtlichen Vorgaben gemacht. Folglich gilt das allgemeine Datenschutzrecht, soweit personenbezogene Daten vorliegen.[46]

4.2 Gesetzliche Erhebungsverbote: Dash-Cams

In anderen Bereichen geht es nicht um neue gesetzliche Befugnisse, sondern um die Frage, ob bestehende gesetzliche Bestimmungen die Datenerhebung und -verwendung im vernetzten Automobil nicht bereits regeln. Instruktiv ist das Beispiel der permanenten, anlasslosen Überwachung des Straßenverkehrs durch eine in einem PKW installierte Autokamera („Dash-Cam"). Hier stellt sich zum einen die Frage der datenschutzrechtlichen Zulässigkeit, zum anderen das Problem eines etwaigen Beweisverwertungsverbots im Gerichtsverfahren.

Die Zulässigkeit der Außenbeobachtung ist inzwischen durch mehrere Gerichte wegen eines Verstoßes gegen §§ 6b, 28 BDSG verneint worden.[47] Eine ausschließlich persönliche oder familiäre Tätigkeit sei bei einer Aufnahme des öffentlichen Raums zu verneinen; dies entspricht auch der zwischenzeitlich ergangenen Rechtsprechung des EuGH.[48] Über die nach den datenschutzrechtlichen Normen erforderliche Interessenabwägung mag man streiten können.[49] Mit Blick auf die weitere technische Entwicklung ist allerdings zu begrüßen, dass der anlasslosen umfassenden Bilderhebung Grenzen gesetzt werden. Im März 2015 wurde z.B. eine App vorgestellt, mit der Dash-Cam Videos live ins Internet gestreamt werden können.[50]

Mit der datenschutzrechtlichen Unzulässigkeit ist die Frage der prozessualen Verwertungsbefugnis allerdings noch nicht entschieden. Diese steht im größeren Kontext der Verwendung der fahrzeugbezogenen Daten als Mittel der prozessualen Wahrheitsfindung.[51] Die Annahme eines relativ strikten Beweisverwertungsverbots[52] ist sehr weitgehend und bedarf insbesondere dort der Relativierung, wo Halter und Fahrer besondere Gefähr-

38 S. BVerfG, NJW 1987, 180 (Sicherheitsgurt); BVerfGE 59, 275 (Motorradhelm).

39 Ebenso *Kremer*, RDV 2014, 240, 249; *Lüdemann/Sengstacken*, RDV 2014, 177, 179; wohl auch *Pohle/Zoch*, CR 2014, 409, 416; a.A. (Freiwilligkeit „in jeder Hinsicht") *Bönninger*, zfs 2014, 184, 188 f.

40 S. http://ec.europa.eu/digital-agenda/ecall-time-saved-lives-saved; nach anderen Angaben bis zu 2.500 (*Lüdemann/Sengstacken*, RDV 2014, 177).

41 Zu den datenschutzrechtlichen Anforderungen s. *Art. 29-Gruppe*, Eingriffe in den Datenschutz im Rahmen der Initiative eCall, WP 125, 2006; *Kremer*, RDV 2014, 240, 249 f.; *Lüdemann/Sengstacken*, RDV 2014, 177, 178 ff.; *Pohle/Zoch*, CR 2014, 409, 413 ff.

42 Zum Problem s. *Pohle/Zoch*, CR 2014, 409, 414 f.

43 *Weichert*, SVR 2014, 241, 245; zu den Datenschutzfragen *Art. 29-Gruppe* (Fn. 41), 7 ff.; *Kremer*, RDV 2014, 240, 250; *Lüdemann/Sengstacken*, RDV 2014, 177.

44 S. *Müller*, VW 2012, 783.

45 Näher *Epple*, VW 2012, 734.

46 S.u. 5 zu den einzelnen anwendbaren Befugnissen. Wieso etwa § 28 Abs. 1 BDSG „nicht einschlägig" sein soll (so *Lüdemann/Sengstacken*, RDV 2014, 177, 180), ist nicht ersichtlich.

47 VG Ansbach, DuD 2015, 49 (die Anordnung des BayLDA wurde dennoch wegen Ermessensfehlern aufgehoben); AG München, ZD 2014, 530 (zusätzlich § 22 S. 1 KUG); LG Heilbronn, DuD 2015, 333; nach *Atzert/Franck*, RDV 2014, 136, 137 soll kein „Beobachten" i.S.v. § 6b BDSG vorliegen.

48 EuGH, DuD 2015, 195; a.A. *Klann*, DAR 2013, 188; insofern kommt es nicht erst auf die geplante Verwendung vor Gericht an, auf die z.B. *Atzert/Franck*, RDV 2014, 136, 137; *Balzer/Nugel*, NJW 2014, 1622, 1625 abstellen.

49 Für die Unzulässigkeit *Weichert*, SVR 2014, 241, 246; *Lachenmann/Schwiering*, NZV 2014, 291, 294 ff.; ebenso die Aufsichtsbehörden in Deutschland (Beschluss des Düsseldorfer Kreises v. 25.2.2014), Österreich (http://www.dsb.gv.at/site/8105/default.aspx; s.a. *Knyrim/Trieb*, ZD 2014, 547, 549 ff.) und der Schweiz (http://www.edoeb.admin.ch/datenschutz/00625/00729/01075); a.A. *Klann*, DAR 2013, 188 f.; *ders.*, DAR 2014, 667 f.; *Diehl*, zfs 2014, 150 f.; *Atzert/Franck*, RDV 2014, 136, 137 ff.; differenzierende Kriterien bei *Balzer/Nugel*, NJW 2014, 1622 ff.

50 S. http://www.heise.de/-2576437.html; auf derartige Gefahren insbesondere in Verbindung mit biometrische Gesichtserkennung weist AG München, ZD 2014, 530, 531 hin.

51 Dazu schon *Roßnagel*, NZV 2006, 281, 285.

52 AG München, ZD 2014, 530; LG Heilbronn, DuD 2015, 333; a.A. (Interessenabwägung) AG München, ZD 2014, 39 mit Anm. *Schröder* (allerdings für eine manuelle Aufnahme von einem Fahrrad); zust. *Diehl*, zfs 2014, 150; für ein Verwertungsverbot mit Ausnahme von notwehrähnlichen Situationen *Bachmeier*, DAR 2014, 15, 19 ff.; für eine regelmäßige Zulässigkeit *Klann*, DAR 2013, 188, 190 f.

dungslagen plausibel machen können.[53] Immerhin wird so aber verhindert, dass der permanente Verstoß gegen §§ 6b, 28 BDSG durch das abstrakte Risiko, sich in einem Schadensprozess verteidigen zu müssen, legitimiert wird. Ob sich die gerichtliche Bewertung bei einer anderen technischen Ausgestaltung (insbesondere der kurzfristigen Überschreibung der Videodaten, die nur bei einem Unfall unterbrochen wird) anders darstellen wird,[54] bleibt abzuwarten.

Am Beispiel der Dash-Cams lässt sich schließlich demonstrieren, dass die fehlende datenschutzrechtliche Harmonisierung im europäischen Binnenmarkt zu Schwierigkeiten führt. So existieren etwa in Großbritannien Kfz-Versicherungsmodelle, die die Versicherten zum ständigen Betrieb einer Kamera verpflichten.[55] Damit sind Konflikte beim Grenzübertritt in Staaten wie Deutschland oder Österreich vorprogrammiert, in denen die Aufsichtsbehörden von der Rechtswidrigkeit der Aufzeichnung ausgehen.

5 Allgemeine rechtliche Zuordnung unter Privaten

Soweit der Staat nicht seine eigenen Verwendungsbefugnisse oder die von Privaten spezifisch normiert, ist auf allgemeine rechtliche Regeln zurückzugreifen.

5.1 Datenschutzrecht

Entsprechend dem Anwendungsbereich des Rechts auf informationelle Selbstbestimmung gilt nach § 1 Abs. 1 i.V.m. § 3 Abs. 1 BDSG das einfachgesetzliche Datenschutzrecht immer dann, wenn personenbezogene Daten vorliegen.[56] Die Zuordnung zu einem Halter oder Eigentümer wird vielfach leicht möglich sein oder sich über die Zeit ergeben, weil dieses Merkmal selten wechselt. Die Ermittlung des konkreten Fahrers ist bei Anmeldemodellen (Car Sharing)[57] ebenfalls vielfach unkompliziert; im Übrigen ist auf den konkreten Fall abzustellen. Wird das Fahrzeug verliehen, kann sich auch ein Risiko der Überwachung des Fahrers durch den Halter oder Eigentümer ergeben, wenn dieser z.B. laufend den Standort erfahren kann.[58] Ein zunehmendes Problem dürften die Daten werden, die sich auf Beifahrer und Dritte außerhalb des Fahrzeugs beziehen, weil diese regelmäßig weder in die Erhebung oder Verwendung eingewilligt noch einen Vertrag mit der verantwortlichen Stelle haben. Schließlich können sich Daten auch auf mehrere Personen beziehen. Bei bestimmten Informationen wird dies sogar regelmäßig der Fall sein, wenn etwa der Standort eines vom Halter verschiedenen Fahrers ermittelt wird.

Wenn es sich um personenbezogene Daten handelt, greift das Verbotsprinzip (§ 4 Abs. 1 BDSG, § 12 Abs. 1 TMG). Je nach Art der Daten und Dienste kommen spezialgesetzliche Regelungen in Betracht. Für Mobilfunkanbindungen wie eCall und andere Dienste von TK-Anbietern gelten die §§ 88 ff. TKG, insbesondere das einfachgesetzliche Fernmeldegeheimnis (§ 88 TKG) sowie die stark durchregulierten Vorgaben für Standortdaten (§ 98 TKG). Die im Automobil angebotenen neuen Multimediaangebote werden regelmäßig Telemedien sein, sodass vorrangig die Regelungen der § 11 ff. TMG anwendbar sind;[59] für Inhaltsdaten bleibt es bei der Anwendbarkeit des BDSG.

Dementsprechend können im Fahrzeug verbaute IT-Systeme mobile personenbezogene Speicher- und Verarbeitungsmedien (§ 3 Abs. 10 BDSG) sein und damit die Transparenzpflichten des § 6c BDSG auslösen.[60] Verhaltensbasierte Versicherungstarife sind nach geltendem Recht zulässig, wenn die Erhebung und Verwendung der Daten auf die (je nach Modell sehr vielen) Daten beschränkt wird, die nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erforderlich sind sowie die Anforderungen an das Verbot der automatisierten Einzelentscheidung (§ 6a BDSG) und das Scoring (§ 28b BDSG) eingehalten werden.[61] Solange alternative Modelle ohne Erfassung des Fahrverhaltens noch erschwinglich sind, dürfte es sich vor allem um Probleme der Transparenz und der Freiwilligkeit (Kopplungsverbote bei Verträgen, freiwillige Einwilligungen) handeln. Dass derartige risikobasierte Vertragsmodelle in ihrer Konsequenz den Versicherungsgedanken ad absurdum führen, ist eine andere Diskussion.

Da das Automobil Teil des Internets der Dinge wird, treten alle datenschutzrechtliche Probleme des Internets in neuem Gewand auf: massenhafte Datenerhebung, Intransparenz, unklare Verantwortlichkeiten, Übermittlung in unsichere Drittstaaten, fehlende Möglichkeiten der Datenlöschung und des technischen Selbstschutzes. Es spricht alles dafür, dass auch im vernetzten Fahrzeug weitreichende und für die Betroffenen nicht oder wenig gestaltbare Verträge und Einwilligungen die Basis für den Datenumgang bilden werden – mit allen bekannten Folgen. § 28 Abs. 1 Satz 1 Nr. 1 BDSG enthält lediglich das Kriterium der Erforderlichkeit, das sich nach dem Vertragsgegenstand richtet und je nach dessen Ausrichtung im Falle des halbautonomen Fahrens oder stark profilabhängiger Dienstleistungen sehr leicht umfassende Datensammlungen rechtfertigt, auch ohne dass Anbieter auf die zusätzliche Möglichkeit „berechtigter Interessen" (Nr. 2) zurückgreifen müssen.

Ein Instrument zur Kontrolle von Vertragsklauseln und Einwilligungserklärungen könnte das Verbraucherschutzrecht sein. Dieses bietet einen Ansatzpunkt sowohl für die Einschränkung zu weiter Erhebungs- und Verwendungsbefugnisse als auch für die Frage, ob die Betroffenen an einem etwaigen ökonomischen Wert der durch sie und ihre Fahrzeuge produzierten Daten partizipieren müssen.[62] Dies bedürfte allerdings einer näheren Analyse der einzelnen, gerade erst entstehenden Vertragstypen, um

53 Zum Parallelproblem der heimlichen Videoüberwachung am Arbeitsplatz s. zuletzt BAG, DuD 2012, 841.

54 In diese Richtung *Werkmeister*, ZD 2014, 532 ff.; *Knyrim/Trieb*, ZD 2014, 547 ff.; differenzierend auch *Bachmeier*, DAR 2014, 15, 17 ff.; *Balzer/Nugel*, NJW 2014, 1622, 1623 ff.; im Fall von LG Heilbronn, DuD 2015, 333, waren solche technischen Sicherungen nicht vorhanden. Ein Parallelproblem stellt sich bei der Gestaltung von EDR; näher *Brenner/Schmidt-Cotta*, SVR 2008, 41.

55 S. http://www.swiftcover.com/carinsurance/dashcams/: „To be eligible for a dashcam discount, your car must have a dashcam that records video of the road ahead on every journey".

56 Zum Personenbezug schon oben 3.1.

57 S. aus rechtlicher Sicht *Schulze*, BB 2013, 195.

58 S. für Telematik-Versicherungstarife *Lüdemann/Sengstacken/Vogelpohl*, RDV 2014, 203, 204.

59 *Weichert*, SVR 2014, 201, 203.

60 Dazu *Hornung*, DuD 2004, 15 ff.; *ders.*, Die digitale Identität, 2005, 253 ff.

61 Zu den Herausforderungen *Lüdemann/Sengstacken/Vogelpohl*, RDV 2014, 203 ff.; s.a. Fn. 8. § 28b BDSG greift bei Prognosen für künftiges Verhalten. Dass die Vorschrift Tarifierungen von Versicherungen nicht erfassen soll (s. die Begründung, BT-Drs. 16/10529, 16), dürfte den hiesigen Fall nicht betreffen, weil es um eine kontinuierliche Verhaltenserfassung geht.

62 Dazu *Hornung/Goeble*, CR 2015, 265, 271 f.; das Ziel einer Beteiligung an der Wertschöpfung liegt auch einigen eigentumsorientierten Ansätzen zugrunde, s. z.B. *Rees*, CLSR 2014, 75, 77 f. (der allerdings mittels dieses Ansatzes expli-

zu bestimmen, von welcher „gesetzlichen Regelung" abgewichen werden soll (§ 307 Abs. 2 Nr. 1 BGB), was wesentliche Rechte oder Pflichten sind, die sich aus der „Natur des Vertrags" ergeben (Nr. 2) und was dessen „äußeres Erscheinungsbild" ist, von dem in ungewöhnlicher Art und Weise abgewichen werden soll (§ 305c Abs. 1 BGB). Diese Untersuchung kann hier nicht geleistet werden.[63] Es spricht aber einiges dafür, dass zumindest bei wirtschaftlich sehr wertvollen Daten nicht von einem unentgeltlichen Vertragstyp ausgegangen werden sollte. Dementsprechend wäre bei solchen Verträgen genau zu prüfen, ob ein Entgelt oder eine geldwerte Vergünstigung an die Betroffenen zurückfließt.

5.2 Aufbrechen der faktischen Zugriffsmöglichkeiten?

Eine Besonderheit gegenüber den allgemeinen Datenschutzfragen des Internets ergibt sich, wenn die Betroffenen selbst oder andere Anbieter auf Daten zugreifen wollen, die in den Fahrzeugsystemen gespeichert sind. Diese Fälle sind problematischer als die Befugnisse von Behörden und Gerichten, die nach allgemeinen Sachaufklärungsregeln weithin die Möglichkeit haben, Hersteller, Drittanbieter oder Unfallbeteiligte zur Herausgabe oder Entschlüsselung der fahrzeugbezogenen Daten zu zwingen.[64]

Dem Betroffenen steht der Auskunftsanspruch nach § 34 Abs. 1 BDSG zur Verfügung. Zumindest im Falle von Eigentümer und Halter erfasst dieser sämtliche im Fahrzeug gespeicherte Daten. Ergänzend kommt eine vertragliche Nebenpflicht des Herstellers in Betracht, wenn die Daten aus nachvollziehbaren Gründen (Werkstattbesuch, Pannenhilfe etc.) benötigt werden. Diese Nebenpflicht ist bedeutsam, weil der Anspruch nach § 34 Abs. 1 BDSG keinen eigenen Zugriff auf die Daten umfasst[65] und kein Recht auf eine Bereitstellung in einem elektronischen, zur Weiterverarbeitung geeigneten Format.[66] Überdies wird nicht geregelt, ob die anschließende Verwendung durch die Betroffenen vertraglich einschränkbar ist. Demgegenüber kann mittels einer Nebenpflicht und/oder der AGB-Kontrolle begründet werden, dass die Daten in einem für freie Werkstätten oder andere Wartungsunternehmen geeigneten Format bereitgestellt werden müssen und auch hierfür verwendet werden dürfen.

Relevant wird ein solcher Anspruch auch, wenn ein Halter oder Fahrer sich berechtigte Hoffnungen macht, seine prozessuale Situation durch die Verwendung der im eigenen Automobil gespeicherten Daten verbessern zu können. Soweit keine eigene technische Zugriffsmöglichkeit besteht, stellt sich die Frage eines Anspruchs gegen die Hersteller. Anscheinend sperren sich diese selbst bei Ermittlungen wegen tödlicher Verkehrsunfälle massiv gegen die Herausgabe und Entschlüsselung der Daten.[67] Offenbar muss sich insoweit erst die Erkenntnis durchsetzen, dass die allgemeinen Zeugen- und Herausgabepflichten auch diese Fälle betreffen.

Aus der Perspektive der Drittanbieter stellt sich die Frage eines Anspruchs auf Fahrzeugdaten entweder direkt im Verhältnis zum Hersteller, oder über „Umweg" des Betroffenen. Im direkten Verhältnis kommen das Lauterkeits- und Kartellrecht in Betracht, das freien Werkstätten, Pannenhilfen und Internetanbietern allerdings nur in relativ engen Grenzen hilft. Wenn die Hersteller selbst oder in Verbindung mit Vertragswerkstätten Exklusivität anstreben oder die Daten willkürlich vorenthalten, kommen eine gezielte Behinderung von Mitbewerbern (§ 4 Nr. 10 UWG) und ein Verstoß gegen kartellrechtliche Missbrauchsverbote zumindest in Reichweite.[68] In der Praxis dürfte es vor allem darum gehen, welches Entgelt für den Datenzugang angemessen ist.

Der Weg über den Eigentümer oder Halter wird sich für Drittanbieter insbesondere deshalb anbieten, weil schon aus datenschutzrechtlichen Gründen regelmäßig ein Vertrag oder eine Einwilligung erforderlich sein wird. Allerdings lässt sich bei neuen Infotainment-Diensten viel schwieriger als bei Reparaturdienstleistungen begründen, dass die Betroffenen so essentiell auf die Daten angewiesen sind, dass die Hersteller diese quasi auf Anforderung an Drittanbieter weitergeben müssen. Insofern ist die Situation eher der eines Smartphones vergleichbar, bei dem die Hersteller eine gewisse Kontrolle über proprietäre App-Stores und ähnliche Mechanismen ausüben.

Ebensowenig wie die Hersteller können folglich die Betroffenen durch ein simples „meine Daten gehören mir" oder eine nach geltendem Recht kaum greifbare „data ownership"[69] begründen, dass etwa die Sensordaten an Internetanbieter übermittelt werden müssen, nur weil ein Vertrag zwischen dem Halter und einem solchen Anbieter dies vorsieht. Vielmehr sind die legitimen Interessen der Hersteller im Rahmen der Vertragsbeziehungen zu würden. Dies schließt insbesondere auch die Hoheit über die sicherheitstechnisch relevanten Komponenten ein, weil sich ansonsten ein erhebliches Haftungsrisiko ergeben kann.[70]

Zurückhaltung ist demgegenüber geboten, wenn die Kfz-Hersteller mit einer Art Prinzipal-Agent-Verhältnis argumentieren, in dem sie die Betroffenen vor dem Datenmissbrauch durch Dritte schützen wollen oder sogar müssen. Verlautbarungen wie die, „alle personenbezogenen Informationen über den Nutzer" müssten „von uns als Hersteller vor Dritten geschützt werden"[71] sollten nicht darüber hinwegtäuschen, dass die Hersteller selbst ein natürliches Interesse an der Kontrolle der Informationsflüsse haben und diese zumindest auch nach eigennützigen, ökonomischen Kriterien ausüben werden. Auch der zutreffende Verweis auf eine Produktbeobachtungspflicht der Hersteller rechtfertigt als solche nicht den Ausschluss Dritter. Dasselbe gilt für die IT-Sicherheit: Aus der Gesamtverantwortung des Herstellers für das ausgelieferte Automobil hinsichtlich der Sicherheit von Schnittstellen[72] lässt sich kein Recht ableiten, einen – technisch abgesicherten – Datenfluss aus dem Fahrzeug an Dritte zu unterbinden.

zit zur Überwindung eines angeblich überholten Datenschutzkonzepts beitragen will).

63 Zur vertragstypologischen Einordnung von Datenüberlassungsverträgen s. *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2011, 119 ff. (ohne Fokus auf die Entgeltlichkeit).

64 Offenbar geschieht dies bislang allerdings so gut wie nicht; näher *Mielchen*, SVR 2014, 81, 83 ff.

65 S. im hiesigen Kontext *Roßnagel*, SVR 2014, 281, 286.

66 Anders das derzeit im Rahmen der europäischen Reform diskutierte Recht auf Datenportabilität; dazu *Hornung*, in: Hill/Schliesky, E-Volution IV, 2014, 141 ff.; näher *Bräutigam/Schmidt-Wudy*, CR 2015, 56.

67 *Mielchen*, SVR 2014, 81, 83; s.a. *Schlanstein*, VD 2014, 15, 20 f.

68 Näher *Roßnagel*, in: 52. VGT, 2014, 272 ff.

69 S. Fn. 22.

70 Insbesondere bei zunehmender Autonomie der Fahrzeuge; s. näher *Schulz*, Verantwortlichkeit bei autonom agierenden Systemen, 2015, 128 ff.

71 S. *Zetsche*, http://www.welt.de/wirtschaft/article136402513.html.

72 *Weichert*, SVR 2014, 201, 205.

6 Technische Gestaltung

Insgesamt ergibt sich so ein komplexes System aus Ansprüchen und berechtigten Interessen sehr vieler Beteiligter. Für die technische Gestaltung folgt daraus, dass sie einerseits entsprechend dem Grundsatz des privacy by design zur Datenvermeidung und Datensparsamkeit beitragen, andererseits aber die rechtlich zulässigen und von den Beteiligten gewünschten Datenflüsse rechtssicher abbilden können muss. Auch Standardisierung und Portabilität können also technische Gestaltungsziele sein.

Im Bereich des Datenschutzes können Verfahren der Anonymisierung und Pseudonymisierung den Personenbezug und damit die Anwendbarkeit des Datenschutzrechts entfallen lassen.[73] Wenn anonyme Daten für bestimmte Geschäftsmodelle ausreichen, wird auch im Interesse der Anbieter die ökonomische Nutzung rechtlich erleichtert oder erst ermöglicht. Pseudonymisierung unter Einbindung verschiedener Stellen kann z.B. bei Telematik-Versicherungstarifen eine direkte Beobachtung der Kunden durch die Versicherer verhindern.[74]

Das Prinzip des privacy by design wird inzwischen auch in der Wirtschaft als wesentlich anerkannt, etwa in den Datenschutz-Prinzipien des VDA von 2014.[75] Bestimmte Daten werden schon aus technischen Gründen nur in flüchtigen Speichern erfasst werden können. Dies gilt insbesondere für Videodaten, die bei hoher Auflösung schnell einen Umfang erreichen, der eine unmittelbare sensornahe Reduktion erfordert, weil andernfalls die Weiterleitung und Verarbeitung im Automobil unmöglich sind. Als weitere Maßnahmen kommen technisch gestützte Transparenzmechanismen, definierte Löschungsereignisse (Abstellen des Motors, Öffnen der Fahrertür), die Verwendung von Einmalpseudonymen für jede Fahrt, die Verarbeitung innerhalb des Fahrzeugs, datenschutzfreundliche Voreinstellungen (privacy by default),[76] oder Mechanismen zur Einhaltung des Zweckbindungsgebots in Betracht.[77]

Privacy enhancing technologies effektiv einzusetzen, kann dabei durchaus eine Herausforderung sein. Wenn z.B. die Ortung des Fahrzeugs abschaltbar ist, so werden möglicherweise gerade hierdurch sensible Informationen generiert („Fahrer X möchte jeden Donnerstagabend zwischen 18 und 22 Uhr nicht geortet werden"). Einschränkungen können sich auch in funktionaler Hinsicht ergeben. So lassen anonyme Daten zwar Produktverbesserungen zu, nicht aber individuelle Wartungs- und Servicehinweise.

Die Gewährleistung der IT-Sicherheit wird schließlich umso bedeutsamer, je sensibler die im Fahrzeug gespeicherten Daten sind und je autonomer sich dieses bewegt. Das jüngste Beispiel der Sicherheitsmängel im BMW-System ConnectedDrive[78] mag nicht symptomatisch sein, es zeigt aber, dass diese Probleme gelöst werden müssen, wenn die neuen vernetzten Systeme durch die Verbraucher akzeptiert werden sollen. Dies führt zu neuen Wartungspflichten der Hersteller, aber auch zur Frage einer unabhängigen Produktzertifizierung, die im Automobilbereich bisher wenig verbreitet ist.

7 Ausblick

Die faszinierende Entwicklung des vernetzten Automobils steht erst am Anfang. Es ist deshalb nicht verwunderlich, dass sich für die komplexen Interessen und Ansprüche noch keine festen rechtlichen Regeln herausgebildet haben. Letztlich wird es maßgeblich darauf ankommen, durch eine angemessene vertragliche Gestaltung und eine entsprechende technische Umsetzung sinnvolle innovative Technologien, Dienste und Geschäftsmodelle zu ermöglichen, ohne die Persönlichkeitsrechte der Verbraucher zu gefährden. Zu hoffen bleibt, dass sich der damit verbundene Aufwand nicht nur im Premiumsegment wirtschaftlich darstellen lässt; eine Zweiklassengesellschaft des Datenschutzes in der mobilen Gesellschaft kann niemand wollen.

Die Automobilindustrie hat diese Herausforderung offenbar erkannt und ist dabei, im Rahmen von Selbstregulierungsmechanismen Regeln für einen effektiveren Daten- und Verbraucherschutz aufzustellen.[79] Sinnvoll wäre es auch, entsprechende Vorgaben in internationale Übereinkommen und technische Normen für Fahrzeuge sowie in das europäische und deutsche Zulassungsrecht aufzunehmen.[80] Für die konkreten Geschäftsmodelle und Datenflüsse sollte der nationale Gesetzgeber demgegenüber die weitere Entwicklung ebenso wie die europäische Datenschutzreform abwarten, bevor er über die Notwendigkeit (und kompetentiell Möglichkeit) sektorspezifischer Vorgaben für die vernetzte Mobilität entscheidet.

73 S. im hiesigen Kontext *Roßnagel*, SVR 2014, 281, 284.

74 S. *Borsetzky*, VW 2014, 24: monatliche Übermittlung von Scores für Geschwindigkeitsübertretungen, Fahrstil, Nacht- und Stadtfahrten sowie eines Gesamt-Score; s.a. *Pohle/Zoch*, CR 2014, 409, 411; *Lüdemann/Sengstacken/Vogelpohl*, RDV 2014, 203 f.

75 S. https://www.vda.de/dam/vda/media/DE/Themen/Innovation-und-Technik/Vernetzte-Mobilitaet/VDA-Datenschutz-Prinzipien-2014/VDA%20Datenschutz-Prinzipien%202014.pdf.

76 S. *Pohle/Zoch*, CR 2014, 409, 411.

77 S. z.B. *Weichert*, SVR 2014, 201, 205 f. sowie 242 f.; *Roßnagel*, NZV 2006, 281, 285 ff.

78 S. www.heise.de/-2540786.html.

79 S. außer Fn. 75 z.B. die „Consumer Privacy Protection Principles" der US-Automobilindustrie, http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163.

80 Diese enthalten derzeit so gut wie keine Regelungen zum Datenschutz, s. *Bönninger*, zfs 2014, 184 (Plädoyer für „no spy"-Regeln in diesen Bestimmungen ebd., 189).