CReport

Gerrit Hornung/Thilo Goeble

„Data Ownership" im vernetzten Automobil

Die rechtliche Analyse des wirtschaftlichen Werts von Automobildaten und ihr Beitrag zum besseren Verständnis der Informationsordnung

Rechtliche Analyse des wirtschaftlichen Werts der Automobildaten zum besseren Verständnis der Informationsordnung

Moderne Autos verfügen über immer mehr Informationstechnologie, die immer stärker im Auto und mit externen Systemen vernetzt wird („car-to-x-communication"). Die Vielzahl der Sensoren (z.B. Positions-, Raddrehzahl-, Regen- Video- und Ultraschallsensoren) führt zur Sammlung von immer mehr Daten. Diese wecken – als personenbezogene, aber auch als aggregierte, anonymisierte Daten – Begehrlichkeiten nicht nur seitens der Automobilhersteller und Werkstätten, sondern auch bei Anbietern von Mobilfunk, Location Based Services, Information- und Unterhaltungsdiensten. Es ist deshalb von essentieller Bedeutung zu klären, wem diese Daten „gehören". Der Beitrag geht dieser Frage nach, die in der Praxis derzeit häufig unter dem Schlagwort einer „data ownership" diskutiert wird.

I. Hintergrund

Menschen haben – oftmals hört man: gerade in Deutschland – ein besonderes Verhältnis zum Automobil. Es ist Ausdruck persönlicher Wertentscheidungen und von Freiheit, Mobilitätsinstrument zu beruflichen und privaten Zwecken, Statussymbol und anderes mehr. Als Käufer oder Leasingnehmer entscheidet man sich bewusst für eine bestimmte Marke, einen bestimmten Fahrzeugtyp und bestimmte Ausstattungsmerkmale. Schon in der Vergangenheit gab es hierfür eine erhebliche Vielfalt von Angeboten.

Mit dem zunehmenden Einzug von IT ins Auto erweitern sich die Möglichkeitsräume nochmals. Das Fahrzeug verbessert seine Grundfunktionalitäten und hilft dem Fahrer, sich sicher fortzubewegen. Vor allem aber wird es zum Smartphone, zum internetfähigen „ultimativen mobilen Computer",[1] zum Multimedia-Entertainmentraum – und zum Instrument massenhafter Datensammlungen. Dieser „Datenschatz" bietet im Interesse von Wirtschaft und Konsumenten die Chance zu neuen Diensten, Geschäftsmodellen und Wertschöpfungen. Er bringt aber auch das Risiko der unkontrollierten Datennutzung durch Dritte und der Komplettüberwachung der Fahrzeuginsassen mit sich, wie es *Jim Farley*, US-Marketingchef von Ford auf einer Podiumsdiskussion der CES in Las Vegas zum Ausdruck brachte: „We know everyone who breaks the law, we know when you're doing it. We have GPS in your car, so we know what you're doing".[2]

II. Das vernetzte Automobil

1. Technische Hintergründe

In modernen Fahrzeugen befinden sich schon heute bis zu 80 Steuergeräte und eine Vielzahl von Sensoren. Während hochkomplexe technische Innovationen wie das vollautonome Fahren[3] noch ein gutes Stück von der Serienreife entfernt sind, haben insbesondere im hochpreisigen Fahrzeugsegment viele neue Technologien und Anwendungen bereits Einzug gehalten.[4] Grundlage ist ein massiver Ausbau der Konnektivität innerhalb des Autos und mit anderen Systemen. Normiert sind bisher nur der CAN-Bus (Controller Area Network) und als Datensammelstelle die ODB-2-Schnittstelle (On-Board-Diagnose), die z.B. für Unfallsachverständige interessant ist und Daten teilweise länger vorhält. Für Sensordaten und deren Fusion in Steuergeräten gibt es bislang keine herstellerübergreifenden Standards.

a) Vernetzung

Neben dieser internen gibt es zunehmend auch externe Konnektivität über stabile oder ad hoc-Netzwerke.[5] Das Auto kommuniziert so mit seiner Umgebung: Car2Car, Car2Pedestrian, Car2Infrastructure, Car2Manufacturer, Car2Service Provider – letztlich also „Car2X". Bislang häufig passiv operierende Navigationsgeräte übermitteln immer öfter Positionsdaten an Dritte (andere Fahrzeuge, Hersteller, Werkstätten etc.);[6] eine Lokalisie-

▷ Prof. Dr. Gerrit Hornung, LL.M. (Edinburgh), ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau und Sprecher des dortigen Instituts für IT-Sicherheit und Sicherheitsrecht (ISL). Thilo Goeble ist Wissenschaftlicher Mitarbeiter am genannten Lehrstuhl. Der Text geht auf einen Vortrag des Erstautors auf der EY-Conference „Connected Car and Data Privacy" am 27.11.2014 in Berlin zurück.

1 So *Jen-Hsun Huang*, Vorstand des Chip-Herstellers Nvidia, s. *Fromm*, *http://www.sueddeutsche.de/auto/-1.1857553*.

2 S. *http://www.businessinsider.com/ford-exec-gps-2014-1?IR=T*. Weder der folgende Satz („By the way, we don't supply that data to anyone") noch der anschließende Widerruf der kompletten Aussage sind in dieser Hinsicht eine wirkliche Beruhigung.

3 Dieses bleibt im Folgenden außer Betracht; s. aus rechtlicher Sicht z.B. *Lutz/Tang/Lienkamp*, NZV 2013, 57; *Lutz*, NZV 2014, 67; *Lutz*, NJW 2015, 119; allgemeiner schon *Bewersdorf*, Zulassung und Haftung bei Fahrerassistenzsystemen im Straßenverkehr, 2005.

4 Zu den technischen Grundlagen s. z.B. die Beiträge in *Reif (Hrsg)*, Sensoren im Kraftfahrzeug, 2. Aufl. 2012; *Bönninger* in 52. Deutscher Verkehrsgerichtstag, 2014; *Bönninger*, zfs 2014, 184 ff.; Sensoren erfassen z.B. Achslast, Motorleistung, Drehzahl, Reifendruck, Temperatur, Querbeschleunigung, Geschwindigkeit, Glasbruch, Verformung, Bremsvorgänge, Beleuchtung, Leistung von Kleinmotoren, Sitzbelegung und Gewicht, Gebrauch des Sicherheitsgurts, Spurwechsel, Fahrtdauer und Pausen sowie die Umgebung (Kamera- und Radarsysteme), s. *Kremer*, RDV 2014, 240, 241 ff.; zu den Steuerungsdaten z.B. *Mielchen*, SVR 2014, 81 (82 ff.).

5 Zur Datenübermittlung aus dem Auto z.B. *Bönninger*, zfs 2014, 184, 186 f.

6 Teilweise erfolgt die Übermittlung offenbar ohne Transparenz gegenüber dem Eigentümer (s. für den Nissan Leaf *Rees/Wettach*, *http://www.wiwo.de/9647526.html*). In Deutschland enthalten die AGBs der

rung ist auch über Smartphone-Apps möglich, um das Fahrzeug auf Parkplätzen o.Ä. wiederzufinden. Mit den angelegten Bewegungsprofilen können Fahrer ihre Nutzungshistorie verfolgen, Aufsichtsbehörden die ordnungsgemäße Abrechnung von Taxifahrten kontrollieren,[7] aber auch staatliche Stellen die Alibis von Verdächtigen überprüfen.[8]

b) Generierte Daten

Viele Sensoren erheben Daten zur unmittelbaren Unterstützung des Fahrers (Abstandsmessung mittels Video- oder Radaraufnahmen, Spurhaltesysteme, Warngeräte für tote Winkel oder zum Erkennen anderer Verkehrsteilnehmer). Im Rahmen einer Car-to-Car Kommunikation können diese Daten im Verkehr weitergegeben werden, um z.B. folgende Fahrzeuge vor Glatteis zu warnen, so dass eine schnellere und präzisere Abbremsung als durch Menschen erfolgen kann.[9] Diese vielfältigen Umgebungsdaten können regelmäßig schon aus Kapazitätsgründen nicht dauerhaft gespeichert werden.[10] So genannte Event Data Recorder (EDR, Unfalldatenspeicher oder „Black Box")[11] können die Daten aber für den jeweils letzten Zeitraum aufzeichnen und im Anschluss Werkstätten, Behörden oder Parteien eines Regressprozesses zur Verfügung stellen.[12] Ein Hersteller könnte etwa Garantieansprüche ablehnen, wenn der Besitzer das Fahrzeug überladen hat.[13]

Je mehr die Autos über standardisierte Schnittstellen oder ad-hoc Kommunikation mit anderen Systemen vernetzt sind, desto mehr können derartige Daten auch in Echtzeit übermittelt werden. Ein Beispiel sind Notfallsysteme (eCall), die bereits privat angeboten werden und in der EU bei Neufahrzeugen ab 31.3.2018 verpflichtend werden sollen.[14] Zugleich werden mit umfassenden Schnittstellen Eingriffe von außen möglich, etwa die Stilllegung von Fahrzeugen, wenn Leasingraten nicht bezahlt wurden oder Mietwagen unzulässigerweise eine Ländergrenze überschreiten.[15]

Andere Sensoren richten sich direkt auf den Fahrer, seine Eigenschaften und Verhaltensweisen. Bestimmte abrupte Steuerungsvorgänge deuten auf Müdigkeit hin und können entsprechende Warnungen auslösen oder auf das Kaffeeangebot der nächsten Raststätte hinweisen. *Ford* hat in einem neuartigen Sitz sechs Sensoren eingebaut, die den Herzschlag überwachen und ein EKG anfertigen; bei Auffälligkeiten könnte ein Krankenhaus alarmiert und im Fall der Ohnmacht der Wagen am Straßenrand zum Stehen gebracht werden. Das *Volvo*-System Alcolock kann die Atemluft kontrollieren und so vor einer Erkältung warnen oder den Alkoholpegel messen.[16] Auch der psychische Zustand des Fahrers ist feststellbar, etwa durch eine Sprachanalyse.[17] Erste Spekulationen gehen dahin, auf Basis individueller Risikoprofile präventive Maßnahmen gegen Fahrer zu erlassen.[18]

Völlig neue Möglichkeiten ergeben sich durch die Einbindung internetbasierter Dienste. Vergleichbar der automatischen Anbindung von Mobilfunkgeräten über Bluetooth-Schnittstellen an Freisprechanlagen wird es in Zukunft möglich sein, mehr oder weniger jede Internetanwendung – einschließlich mobiler Bezahldienste[19] – ins Auto zu bringen. Während die traditionellen Hersteller versuchen, über eigene App-Stores die Kontrolle über diese Dienste zu behalten, drängen inzwischen die großen Provider auch ins Auto. Sowohl *Apple* (Carplay) als auch *Google* (Android Auto mit seiner „Open Automotive Alliance") haben Kooperationen mit wichtigen Autobauern geschlossen, die vielfach beide Systeme bedienen. Dies ermöglicht die Nutzung von Apps im Auto z.B. zur Suche von Restaurants oder freien Parkplätzen, aber auch zum Download des gerade laufenden Radiohits. Durch eine intensive Nutzung kann dann wiederum ein noch umfassenderes Profil erstellt werden, das noch stärker personalisierte Werbung ermöglicht.[20]

2. Beteiligte und ihre Interessen

Die neuen Anwendungen und Szenarien bringen es mit sich, dass eine Vielzahl von Personen mit ihren jeweiligen Interessen beteiligt sind.[21] Eigentümer, Halter, Fahrer und Mitfahrer haben (zum Teil unterschiedliche) Interessen an der Fahrzeugsicherheit, dem Fahrkomfort, vor allem aber an der Nutzung vieler Internet- und Multimedia-Anwendungen. Dies bezieht sich insbesondere auf Location Based Services oder andere Informations- und Serviceprogramme (z.B. zur Routenführung, aber auch im gesamten Infotainment-Bereich).

a) Klassische Dritte

Neben dem Fahrzeugeigentümer und -nutzer haben vor allem Fahrzeughersteller und Zulieferer (Produktverbesserungen) und Werkstätten (Reparaturen und Serviceangebote) ein Interesse an den Daten. Hinzu kommen unabhängige Anbieter von Navigations- oder Telekommunikationsdiensten, die ihre Dienste anbieten oder verbessern wollen. Informationen über das Fahrverhalten ermöglichen überdies völlig neuartige Anwendungen, etwa in der Kfz-Versicherung *(„pay as you drive")*.[22]

Hersteller typischerweise detaillierte Beschreibungen, s. z.B. *http://www.bmw.de/dam/brandBM/marketDE/countryDE/topics/fascination-bmw/connecteddrive-2013/AGB/BMW_i3_Infos.pdf.download.1402476095056.pdf*.

7 Ab 2016 sind Fiskaltaxameter in Taxis verpflichtend, s. RL 2004/22/EG, ABl. EU Nr. L 135 v. 30.4.2004, 1.

8 In den USA offenbar mittlerweile weit verbreitete Praxis, s. *Rees/Wettach* (Fn. 6).

9 Zu den technischen Möglichkeiten s. *Harding/Powell/Yoon/Fikentscher/Doyle/Sade/Lukuc/Simons/Wang*, Vehicle-to-vehicle communications: Readiness of V2V technology for application, 2014.

10 Zu den einzelnen Speichermöglichkeiten *Bönninger*, zfs 2014, 184 (187).

11 Dazu *Schmidt-Cotta*, ZRP 2000, 518; *Graeger*, NZV 2004, 16; *Brenner/Schmidt-Cotta*, SVR 2008, 41; *Schlanstein*, VD 2014, 15.

12 Zur weiter fortgeschrittenen US-Entwicklung s. *Electronic Privacy Information Center, https://epic.org/privacy/edrs; zum* Vorschlag einer verpflichtenden Einführung s. *https://www.federalregister.gov/articles/2012/12/13/2012-30082/federal-motor-vehicle-safety-standards-event-data-recorders*. Aus Deutschland sind bisher keine Fälle bekannt, in denen staatliche Stellen (z.B. in einem Haftungsprozess) auf diese Daten zugegriffen hätten; zur abwehrenden Haltung der Hersteller s. *Mielchen*, SVR 2014, 81 (83 f.).

13 So im Fall eines Lkws offenbar MAN, s. *Schneider, http://auto-presse.de/autonews.php?newsid=200501*.

14 Nach der grundsätzlichen Einigung zwischen dem Europäischen Parlament und dem Rat steht die abschließende Abstimmung im Parlament derzeit noch aus; s. aus rechtlicher Sicht z.B. *Pohle/Zoch*, CR 2014, 409; *Scherer*, MMR 2014, 353; *Art. 29 Datenschutzgruppe*, Eingriffe in den Datenschutz im Rahmen der Initiative eCall, WP 125, 2006.

15 Beispiele bei *Brenner*, DAR 2014, 619 (623); *Rees/Wettach* (Fn. 6); s.a. ebd. für denkbare weitere Anwendungen bis hin zur automatischen Geschwindigkeitsdrosselung in Wohngebieten.

16 *Kremer*, RDV 2014, 240 (241).

17 *Kremer*, RDV 2014, 240 (241).

18 Die von *Rees/Wettach* (Fn. 6) genannten Beispiele des vorläufigen Entzugs der Fahrerlaubnis oder der Anordnung einer MPU sind vorläufig nicht realistisch – allerdings werden derartige Maßnahmen auch heute schon auf Basis allgemeiner Risikoprognosen (z.B. bei Alkohol- und Drogenkonsum) angeordnet.

19 S. z.B. *http://www.spiegel.de/netzwelt/web/visa-bietet-mobiles-bezahlen-mit-dem-auto-an-a-1021513.html*.

20 *Rees/Wettach* (Fn. 6).

21 S. z.B. *Weichert*, SVR 2014, 201 (202 f.); *Roßnagel*, SVR 2014, 281 f.

22 S. *Weichert*, SVR 2014, 241 (245 f.) zum Versicherungstarif der Spar-

b) Neue Dritte: ISPs

Werden Automobile mit dem Internet verbunden, so kommen schließlich alle großen und kleinen Internet Service Provider ins Spiel. Diese möchten einerseits ihre Angebote ins Auto bringen und die dort verbauten Benutzerschnittstellen ihren sonstigen Internet-Vertriebswegen hinzufügen. Andererseits haben sie ein erhebliches Interesse an den Informationen über das Fahrzeug und seine Insassen, um beispielsweise auf der Basis der Fahrzeugposition, des gewählten Radiosenders oder durch Verknüpfung mit anderweitig erhobenen Präferenzen gezielt Werbung schalten zu können. Beides ist von erheblicher wirtschaftlicher Relevanz: Es wird mit einem weltweiten Umsatzwachstum im Bereich des vernetzten Autos von 31 Mrd. Euro (2015) auf 113 Mrd. Euro (2020) gerechnet.[23]

c) Zu wessen Bedingungen?

Eine entscheidende Frage wird sein, zu wessen Bedingungen sich das Auto der Zukunft mit derartigen Angeboten technisch vernetzt. Man kann dies auf die Frage zuspitzen, ob man in diesem Auto ein Gesamtprodukt der traditionellen Hersteller sieht, dass sich „nur" (und unter deren Kontrolle) mit dem Internet verbindet, oder eine zwar elaborierte, funktional aber weniger wichtige Benutzerschnittstelle für die überlegenen und weitreichenden Angebote der großen Informationsdienstleister. Angesichts der beträchtlichen weltweiten Marktmacht gerade der großen Smartphone-Hersteller sollten sich die traditionellen Automobilanbieter jedenfalls nicht zu sicher fühlen. Nach Umfragen würde beispielsweise ein substantieller Teil der Kunden für ein Auto mit Internetzugang dessen Marke wechseln.[24] Das Beispiel *Nokia*[25] sollte hinreichend deutlich machen, dass weder eine beträchtliche Marktmacht noch überlegenes Know-how in einem traditionellen Produktsegmente davor schützen, auch in kürzester Zeit *de facto* vom Markt zu verschwinden. Die Autohersteller müssen sich folglich durch gut durchdachte Partnerschaften entlang der Wertschöpfungskette ansiedeln, wenn sie die Kontrolle über die Gesamtlösung „vernetztes Auto" nicht verlieren wollen. Eine wesentliche Herausforderung sind insoweit die stark unterschiedlichen Innovationszyklen, die bei Internetdiensten erheblich kürzer sind.

d) Staatliche Stellen

Schlussendlich haben auch staatliche Stellen in verschiedenen Situationen ein erhebliches Interesse an den Automobildaten. Im Bereich der Car2Infrastructure Kommunikation ergeben sich perspektivisch erhebliche Chancen für intelligente Verkehrsleitsysteme oder automatisierte Mautverfahren. Umgebungssensoren dienen der Unfallverhütung.[26] Geschieht ein Unfall, so können durch automatisierte Notrufsysteme (eCall) die Folgen abgemildert und mittels EDR-Daten genauer als bisher die Verursachungsbeiträge bestimmt werden – mit der Folge, dass sehr viele Beteiligte Interesse an den Daten haben können.[27] Lokalisierungstechnologien können bei der Aufklärung von Diebstählen oder allgemein bei der Aufenthaltsbestimmung verdächtiger Personen helfen. Auch ansonsten werden Sicherheitsbehörden ein umso größeres Interesse an den Automobildaten haben, je mehr über die entsprechenden Systeme kommuniziert wird und je mehr Daten sie speichern. Auch ansonsten werden Sicherheitsbehörden ein umso größeres Interesse an den Automobildaten haben, je mehr über die entsprechenden Systeme kommuniziert wird und je mehr Daten sie speichern.

Angesichts dieser Möglichkeiten verwundert es nicht, dass das Thema inzwischen auch die Politik erreicht hat. Ein Beispiel ist die europäische eCall-Verordnung,[28] die ein wichtiges Projekt der europäischen „eSafety-Initiative" ist. Ziel der *Europäischen Kommission* ist, die Straßensicherheit durch intelligente Sicherungssysteme zu erhöhen. Dabei spielen Geschwindigkeitsregulierungssysteme und weitere Kontrollsysteme genauso eine Rolle wie Stabilitätsprogramme und EDR. Neben der Straßensicherheit sollen durch neuartige Effizienzsysteme auch die Auswirkungen auf die Umwelt reduziert werden, indem z.B. intelligente Navigationssysteme Staus reduzieren.[29]

3. Rechtliche Herausforderungen

Der Einsatz von IT wirft – vor allem im Bereich semi- oder vollautomatisierter Fahrassistenzsysteme – eine Fülle zulassungs-, verkehrs- und (produkt-)haftungsrechtlicher Fragestellungen auf, die im weiteren außer Betracht bleiben.[30] Neuartige Fragestellungen des IT-Sicherheitsrechts entstehen, wenn beispielsweise Systeme unzureichend geschützt werden und so für Kriminelle offen stehen.[31] *„Pay as you drive"*-Modelle werfen nicht nur versicherungsrechtliche, sondern auch Probleme mit § 28b BDSG auf.[32] Die umfassende Beobachtung Straßenverkehrs mit sog. Dashcams ist nach den ersten deutschen Gerichtsentscheidungen nicht nur rechtswidrig,[33] sondern führt auch zu einem prozessualen Beweisverwertungsverbot.[34]

Viele andere Probleme lassen sich auf die – umgangssprachlich formulierte – Frage zurückführen: Wem „gehören" die Daten? Diese stellt sich in vielen Konstellation: Hat der Eigentümer, Halter oder Fahrer das Recht, die Datenerhebung aus dem Auto durch den Hersteller

kassen-Direktversicherung (S-Direkt); dazu auch *Kremer*, RDV 2014, 240, 250; näher *Lüdemann/Sengstacken/Vogelpohl*, RDV 2014, 203.

23 *Rees/Wettach* (Fn. 6).

24 Umfragen zufolge 20 %, bei Vielfahrern sogar 40 %, s. *http://www.mckinsey.de/internet-im-auto-wird-marktgewichte-der-industrie-massiv-veraendern.*

25 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.*

26 Zu den Rechtsfragen von Assistenzsystemen zum Fußgängerschutz s. *Schulz/Roßnagel/David*, ZD 2012, 510.

27 So möchte ein Halter oder Fahrer die Daten des eigenen Fahrzeugs ggf. selbst nutzen, um gegen den Unfallgegner oder (bei Fehlfunktionen) den Hersteller vorgehen zu können. Dieser könnte dann seinerseits mit Hilfe der Daten bei Zulieferern Regress nehmen. Dem Unfallgegner können die Daten wichtige Informationen gegen den Fahrer, den Hersteller oder Zulieferer liefern. S. zu den Rechtsfragen der EDR oben Fn. 11.

28 S. Fn. 14.

29 *http://ec.europa.eu/transport/road_safety/specialist/knowledge/esave/; zur* Regelungskompetenz der Union im Bereich von EDR s. schon *Brenner/Schmidt-Cotta*, SVR 2008, 41 (44 ff.).

30 S. außer den Nachweisen in Fn. 3 z.B. *Vogt*, NZV 2003, 153 (155 ff.); *Albrecht*, SVR 2005, 373 (374 f.); *Frenz/Casimir-van den Broek*, NZV 2009, 529; *Lutz*, NJW 2015, 119.

31 Das IT-System ConnectedDrive von BMW ließ es z.B. zu, dass über Jahre hinweg 2,2 Mio. Fahrzeuge elektronisch per Mobilfunk geöffnet werden konnten, s. *http://www.spiegel.de/auto/aktuell/adac-entdeckt-it-sicherheitsluecke-bei-bmw-connected-drive-a-1015819.html.*

32 S. *Weichert*, SVR 2014, 241 (245 f.); *Lüdemann/Sengstacken/Vogelpohl*, RDV 2014, 302 ff.

33 VG Ansbach v. 12.8.2014 – AN 4 K 13.01634, CR 2014, 746; differenzierend *Knyrim/Trieb*, ZD 2014, 547; s.a. *Atzert/Franck*, RDV 2014, 136.

34 AG München, ZD 2014, 530 mit abl. Anm. *Werkmeister*; ZD 2014, 539; näher *Bachmeier*, DAR 2014, 15.

zu verbieten oder sonst zu beeinflussen? Kann er umgekehrt beliebigen Drittanbietern den Zugriff auf Komponenten auch dann gestatten, wenn der Hersteller dies (beispielsweise im Bremsbereich aus Sicherheitsgründen) nicht möchte? Dürfen Hersteller oder sonstige Anbieter die mit Einwilligung der Fahrzeuginsassen erhobenen Daten für beliebige Zwecke verwenden und an interessierte Dritte weitergeben? Ändert sich etwas an der Bewertung, wenn die Daten aggregiert oder anonymisiert werden?[35]

Besondere Herausforderungen stellen sich in Unfallkonstellationen: Können EDR oder andere Systeme auf Basis allgemeiner Vorschriften (§§ 94 ff. StPO) sichergestellt und ausgelesen werden, bzw. ergibt sich eine Pflicht zur Herausgabe der Daten gem. § 142 ZPO? Besteht die Gefahr einer Aushöhlung von Aussageverweigerungsrechten oder sogar ein Konflikt mit dem *Nemo-tenetur*-Grundsatz (§§ 55 Abs. 1, 136 Abs. 1 S. 2, 163a Abs. 4 S. 2, 243 Abs. 5 S. 1 StPO), weil das eigene Auto den Fahrer „belastet"? Wie ist mit dem Informationsungleichgewicht umzugehen, wenn gemutmaßt wird, dass ein Unfall nicht aufgrund eines Fahrerverschuldens entstanden, sondern Folge eines Konstruktions- bzw. Fabrikationsfehlers ist, der Hersteller aber aus Sorge vor einem Produkthaftungsprozess die Herausgabe der Fahrzeugdaten verweigert?[36]

III. Die Idee einer „Data Ownership"

Es erscheint verführerisch, diese Fragen aus der Perspektive des Fahrzeugeigentümers oder Fahrers mit einem schlichten „Meine Daten gehören mir!" zu beantworten. Aber auch einige Fahrzeughersteller versuchen, mit dem aus dem Englischen importierten Begriff einer „Data Ownership" Nutzung- und Verfügungsrechte an den Kraftfahrzeugdaten zu begründen. Ganz offensichtlich ist der Eigentumsbegriff so assoziativ-kraftvoll, dass er auch in der (rechts-) politischen Diskussion in dieser Weise Verwendung finden kann.

1. Rechte und Pflichten

Materiell-rechtlich ist unmittelbar eindeutig, dass es nach deutschem Recht kein zivilrechtliches Eigentum an Daten geben kann. Mangels Körperlichkeit sind sie keine Sachen (§ 90 BGB), so dass die §§ 903 ff. BGB keine Anwendung finden.[37] Die bestehenden Immaterialgüterrechte erfassen zumindest nicht *per se* personenbezogene Daten.[38] Konzeptionell und zur Beantwortung der aufgeworfenen Zuordnungsfragen lohnt es dennoch, über die Möglichkeiten und Grenzen einer eigentumsähnlichen Konstruktion der Datennutzungsbefugnisse der einzelnen Beteiligten nachzudenken.[39]

„Eigentum" bezieht sich herkömmlich auf bestimmte Objekte, nämlich Mobilien, Immobilien oder Immaterialgüter. Das Eigentum an diesen kann auf verschiedenen Wegen erworben, übertragen und verloren werden. Es begründet bestimmte Rechte, aber auch eine Reihe von Pflichten. Beide sind abhängig vom Eigentumsobjekt, von der Art des Erwerbs und insbesondere von Rechten Dritter.

Für die weitere Analyse – insbesondere aber für die inflationäre Verwendung des Begriffs in der öffentlichen Diskussion – ist es wichtig festzuhalten, dass mit dem Eigentum zwar praktisch immer bestimmte Rechte verbunden sind, diese jedoch keineswegs zwingend exklusiver Natur sein müssen.[40] Dies gilt schon wegen der *Sozialbindung des Eigentums* (Art. 14 Abs. 2 GG). Überdies gibt es im Wirtschaftsleben nicht nur Alleineigentum, sondern auch Miteigentum und öffentliche Güter. Von einigen Vordenkern des Internets wird vertreten, niemand solle in diesem Sinne Daten „besitzen" und der Handel mit ihnen verboten werden.[41]

2. Konzeptionelle Möglichkeiten und Grenzen

Aus einer bestimmten Perspektive ergibt es durchaus Sinn, von einem „Eigentum" an Daten zu sprechen. Immerhin werden Daten häufig von privaten Dingen (wie dem eigenen Auto) produziert oder entstammen privaten Räumen (wie dem eigenen Auto oder der eigenen Wohnung). *Prima facie* spricht also einiges für eine Zuordnung der Verfügungsbefugnis zum Eigentümer des jeweiligen Objekts.[42] Diese Zuordnung könnte dann als Ausgangspunkt für zwei wichtige Funktionen des Eigentumsrechts dienen, nämlich zum einen die Begründung von Abwehransprüchen (gegen Diebstahl, Zerstörung oder unberechtigte Nutzung) zum anderen die Basis für vertragliche Verhandlungen mit anderen (Verkauf, Tausch oder Miete) – beides ließe sich auch bei Daten fruchtbar machen.

Aus einer anderen, *kommunikationswissenschaftlichen Perspektive* ist diese Beschreibung jedoch fundamental unterkomplex. Personenbezogene Daten entstehen typischerweise nicht in der Eremitage, sondern in sozialen Beziehungen. Die Kommunikation in derartigen Beziehungen „gehört" aber weder ausschließlich dem Kommunikator noch ausschließlich dem Rezipienten.[43] Dies hat das *Bundesverfassungsgericht (BVerfG)* schon im Volkszählungsurteil erkannt, wenn es dort feststellt, dass

35 Auch solche Daten können zum Nachteil der Fahrer wirken. So verkauft der Navigationsanbieter TomTom Daten seiner Nutzer an die niederländische Polizei, so dass diese besonders „lohnende" Punkte für Geschwindigkeitskontrollen identifizieren kann, s. *Weichert*, SVR 2014, 201 (206). Dadurch wird zwar nicht der einzelne Fahrer direkt verraten (so dass das Datenschutzrecht keine Anwendung findet), aber durch die Weitergabe besteht eine größere Wahrscheinlichkeit, dass er belangt wird.

36 *Mielchen*, SVR 2014, 81 (84 f.).

37 *Buchner* in Redeker/Hoppen, DGRI Jahrbuch 2011, 53 f.; *Hoeren/Völkel* in Hoeren, Big Data und Recht, 2014, 17; aus österreichischer Perspektive *Staudegger*, ÖJZ 2014, 107 ff.

38 Zu den Möglichkeiten und Grenzen des Schutzes s. z.B. *Dorner*, CR 2014, 617 (619 ff.).

39 Grundsätzliche Überlegungen hierzu bei *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 202 ff.; *Buchner* in Redeker/Hoppen, DGRI Jahrbuch 2011, 53 ff.; *Kilian*, CRi 2012, 169; *Kilian* in GS Steinmüller, 2014, v.a. 204 ff.; *Zech*, Information als Schutzgegenstand, 2012. Ansätze zu einer eigentumsorientierten Strukturierung des Umgangs mit (personenbezogenen und anderen) Daten sind immer wieder vorgeschlagen und diskutiert worden, s. z.B. *Ladeur*, DuD 2000, 12, 18; aus jüngerer Zeit *Hoeren/Völkel* in Hoeren, Big Data und Recht, 2014, 11 ff.; *Dorner*, CR 2014, 617; *Rees*, CLSR 2014, 75 ff.; *Zech*, CR 2015, 137; zur Diskussion auch *Staudegger*, ÖJZ 2014, 107. zur vertraglichen Ausgestaltung des „Datenhandels" *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, v.a. 75 ff.; 113 ff. Vorschläge aus den USA (z.B. *Samuelson*, 52 Stanford Law Review 1125 (2000); *Schwarz*, 117 Harvard Law Review 2056 (2004), 2094 ff.) sind nur sehr eingeschränkt übertragbar, da sie dort angesichts des Fehlens grundrechtlicher Standards und allgemeiner Datenschutzgesetze klar auf die Stärkung des Datenschutzes zielen.

40 S. zur Frage der „Monopolisierung" eines Verfügungsrechts an Daten *Buchner* in Redeker/Hoppen, DGRI Jahrbuch 2011, 56 ff.

41 S. das Interview mit *Evgeny Morozow*, taz v. 31.1.2015: „Niemand sollte Daten besitzen. Luft gehört auch keinem. [...] Daher müssen wir die Daten vergemeinschaften, sie sozialisieren. [...Es sollte Menschen verboten werden, mit ihnen zu handeln,] das würde die Daten aus diesem Kreislauf nehmen.".

42 Für eine Analogie zu § 903 BGB z.B. *Hoeren/Völkel* in Hoeren, Big Data und Recht, 2014, 11 ff.

43 S. allgemein z.B. *Steinmüller*, Informationstechnologie und Gesellschaft, 1993, 216 ff.; am konkreten Beispiel *Roßnagel*, SVR 2014, 281 (283 f.).

Daten „ein Abbild sozialer Realität" sind.[44] In der grundrechtlichen Konzeption des Rechts auf informationelle Selbstbestimmung haben Daten dann auch eine gesellschaftliche und demokratische Bedeutung.[45] Aus dieser Perspektive gibt es folglich keinen absoluten Herrschaftsanspruch über „eigenen" Daten.

Dies gilt auch für kommerzielle Daten wie die des vernetzten Automobils. Ohnehin ist die Anknüpfung an die Eigentümerschaft des Fahrzeugs nur auf den ersten Blick weiterführend.[46] Erwirbt man im Zuge des Kaufs eines Autos das Eigentum an diesem, so mag nicht nur intuitiv, sondern auch rechtlich einiges für eine analoge Zuordnung der durch dieses produzierten Daten sprechen. Bei modernen Autos wird dies bereits in dem Moment kompliziert, in dem diese regelmäßige Software-Updates benötigen und bei Wartungen Daten anfallen. Wird ein Auto gemietet oder geleast, so müsste man zwischen fahrzeug- und fahrerbezogenen Daten und den entsprechenden Eigentümerstellungen unterscheiden. Modelle des Car-Sharing, in denen Hersteller zunehmend als Anbieter auftreten, würden den Ansatz weiter verkomplizieren.[47] Schließlich wäre es kaum haltbar, die durch Taxikunden oder private Beifahrer produzierten personenbezogenen Daten rechtlich exklusiv dem Eigentümer des Autos zuzuweisen.

IV. Rechtliche Zuordnungen

De lege lata kommt man zumindest für personenbezogene Daten nicht umhin, die Frage eines „Dateneigentums" als datenschutzrechtliches Problem zu rekonstruieren. Denn nach geltendem Recht stellt das Datenschutzrecht als Querschnittsmaterie eine Grundordnung sowie in vielen spezifischen Gesellschafts- und Wirtschaftsbereichen besondere Regeln für den Umgang mit personenbezogenen Daten auf.[48] Erst im zweiten Schritt lässt sich – innerhalb dieses Regelungsrahmens oder in Überlegungen zu seiner Erweiterung – darüber spekulieren, ob die Vorstellung eines Dateneigentums oder von Daten als Handelsware Vorteile gegenüber der selbstbestimmungsorientierten Konzeption des *BVerfG* und des hergebrachten Datenschutzrechts bietet.

1. Datenschutzrechtliche Konzeption

Privatheit und Datenschutz sind – das haben *Warren* und *Brandeis* schon in ihrem berühmten Artikel aus dem Jahre 1890 erkannt – zeitabhängige Konzepte.[49] Ihre Anwendung auf technische Innovationen wie das vernetzte Automobil kann also auch zur Notwendigkeit führen, die entsprechenden Konstrukte zu hinterfragen oder fortzuentwickeln.

a) Grundrechtliche Ausgangspunkte

Der deutsche Referenzpunkt des grundrechtlichen Datenschutzes ist nach wie vor das Volkszählungsurteil von 1983[50] – das Jahr, in dem u.a. der „VW Golf II" auf den Markt kam. Der konkrete Anlass der verfassungsgerichtlichen Entscheidung mag aus heutiger Sicht sowohl technologisch als auch gesellschaftspolitisch aus einer anderen Zeit erscheinen; die normativen Aussagen sind nach wie vor gültig. In bestimmten Bereichen sind ergänzend andere Ausprägungen des verfassungsrechtlichen Persönlichkeitsschutzes heranzuziehen. Dies gilt insbesondere für das Telekommunikationsgeheimnis (Art. 10 GG), das bei der Anbindung des Autos über SIM-Karten und die damit verbundene Telekommunikation eine Rolle spielt. Überdies werden viele informationstechnische 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[51] hinaus in Zukunft verfassungspraktische Wirkung erlangen wird.[52]

Das Recht auf informationelle Selbstbestimmung konzipiert das *BVerfG* gerade nicht wie *Warren* und *Brandeis* als „right to be let alone", sondern als auf individuelle Selbstentfaltung bezogenes Verfügungs- und Kontrollrecht: Es gewährleistet „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[53] Auf den ersten Blick ist dies durchaus mit einem eigentumsähnlichen Kontroll- und Ausschließungsrecht kompatibel.

Zugleich finden sich in der Entscheidung jedoch auch grundlegende Passagen, die starke Argumente gegen jede Form von Dateneigentum oder Datenhandel bilden. In den berühmten Ausführungen, dass „[m]it dem Recht auf informationelle Selbstbestimmung [...] eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar [wäre], in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß" und dass „[d]ies [...] nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen [würde], sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines [...] freiheitlichen demokratischen Gemeinwesens ist,"[54] verknüpft das Gericht Datenschutz mit der Menschenwürde und dem demokratischen Prozess. Beide sind ganz offensichtlich keine handelbaren Güter.

b) Einfachgesetzliche Zuordnungsregeln

Auf einfachgesetzlicher Ebene enthält das Datenschutzrecht relative klare Vorgaben dafür, um „wessen" Daten es sich handelt. Der Anwendungsbereich erfasst nach Art. 2 lit. a DSRL, § 3 Abs. 1 BDSG alle Arten personen-

44 BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (44).

45 Näher zur Genese der Schutzbereichsinnovation *Hornung*, Grundrechtsinnovationen, 2015, 266 ff.

46 Zu den Möglichkeiten und Grenzen einer Anknüpfung an das Sacheigentum s. z.B. *Roßnagel*, SVR 2014, 281 (282 f.).; zu einzelnen Analogien noch unten IV.2.a).

47 S. zu den rechtlichen Herausforderungen des Car Sharing *Schulze*, BB 2013, 195.

48 Für unternehmensbezogene Daten ist auf die spezifischen Schutzinstrumente v.a. des Geheimnisschutzes abzustellen; dazu z.B. *Hofmann*, InTeR 2013, 210; *Zech*, CR 2015, 137 (139 ff.); aus verfassungsrechtlicher Perspektive *Beyerbach*, Die geheime Unternehmensinformation, 2012.

49 S. *Warren/Brandeis*, 4 Harvard Law Review 193 (1890): „That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extend of such protection".

50 BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1.

51 BVerfG v. 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274; dazu z.B. *Hoffmann-Riem*, JZ 2008, 1009 ff.; *Hornung*, CR 2008, 299 ff.; *Bäcker* in LfDI NRW, Privatsphäre mit System, 2010, 4 ff.; *Drallé*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, 2010; *Gudermann*, Online-Durchsuchungen im Lichte des Verfassungsrechts, 2010.

52 Zur Innovationsgeschichte und der bislang sehr eingeschränkten Diffusion s. *Hornung* (Fn. 45), 277 ff.

53 BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (42).

54 BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (43).

bezogener Daten.[55] Es besteht keine Beschränkung auf bestimmte Verarbeitungsformen, Branchen, berechtigte Vertraulichkeitserwartungen oder sensible Daten – schon das *BVerfG* hat im Volkszählungsurteil formuliert, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr" gibt.[56] Mit anderen Worten ist der Zustand einer Bremse ein personenbezogenes Datum, wenn die Bremse einem Eigentümer, Halter oder Fahrer zugeordnet werden kann.[57]

Nach dem datenschutzrechtlichen *Verbotsprinzip* (Art. 7 DSRL, § 4 Abs. 1 BDSG, § 12 Abs. 1 TMG) erfordert jede Erhebung, Verarbeitung und Nutzung der Daten eine Rechtsgrundlage, nämlich Gesetz oder Einwilligung. Ohne eine solche Ermächtigung ist der Umgang mit den Daten rechtswidrig – in diesem Sinne ist es durchaus möglich, von „eigenen" Daten zu sprechen, weil ohne Einwilligung oder sonstige Ermächtigung niemand über diese verfügen darf. Da sich die jeweilige Ermächtigung auf eine bestimmte verantwortliche Stelle beziehen muss, ist diese im Einzelfall ebenso zu bestimmen[58] wie etwaige Übermittlungsbefugnisse. Willigt der Eigentümer des Autos z.B. beim Kauf darin ein, dass seine Daten durch den Hersteller verwendet werden, heißt das nicht, dass der Hersteller sie anschließend an Zulieferer oder Betreiber von Komponenten (etwa Navigationsgeräte) weitergeben darf.

Auch in den Betroffenenrechten lassen sich Anknüpfungspunkte für eine eigentumsähnliche Zuordnung finden. So lässt sich gut vertreten, dass dem Eigentümer des Wagens ein datenschutzrechtlicher Auskunftsanspruch (§ 34 BDSG) in Bezug auf jedes in seinem Auto gespeicherte Bit zusteht – weil es das eigene Auto ist und diese Daten deshalb *per se* personenbezogene Daten sind. Damit ist nicht zwingend eine eigene technische Zugriffsmöglichkeit erforderlich,[59] wohl aber werden intransparente Verarbeitungsvorgänge und Speichermedien unmöglich.[60] Nach deutschem Recht sind die Betroffenenrechte überdies gem. § 6 Abs. 1 BDSG nicht im Rahmen von Austauschgeschäften oder sonst abdingbar. Zumindest unter diesem Gesichtspunkt „gehören" die Daten also niemandem außer dem jeweiligen Betroffenen.

c) Verträge und Einwilligung als ökonomische Verfügungen

Für die Hersteller besteht die große Herausforderung darin, die relativ abstrakten datenschutzrechtlichen Vorgaben und Anforderungen in eine möglichst *datensparsame* (§ 3a BDSG), die *Betroffenenrechte ermöglichende* technisch-organisatorische Gestaltung zu überführen.[61] Dies betrifft insbesondere den Umgang mit den Daten der über 100 Sensoren, die Informationen über das Fahrzeug, zunehmend aber auch über die im Innenraum befindlichen Personen aufzeichnen.

aa) Betriebswirtschaftlich-pragmatische Perspektive

Durch die Anbindung an das Internet werden dabei prinzipiell alle datenschutzrechtlichen Probleme relevant, die im Internet ohnehin bestehen. Aus einer betriebswirtschaftlich-pragmatischen Perspektive könnten die Anbieter freilich versucht sein, diese Probleme genauso zu lösen wie die bisherigen Informationsdienstleister im Internet- nämlich durch Einwilligungen und Verträge, die nach §§ 4 Abs. 1, 4a BDSG, §§ 12 Abs. 1, 13 Abs. 2 TMG bzw. § 28 Abs. 1 S. 1 Nr. 1 BDSG, §§ 14, 15 TMG eine Rechtsgrundlage für die Erhebung und Verwendung der jeweiligen Daten darstellen. Die Erfahrung insbesondere mit attraktiven neuen Internetdiensten zeigt, dass die Betroffenen in der typischen Situation des „take it or leave it" in praktisch alles einwilligen, wenn der erwartete Nutzen nur groß genug ist oder zu sein scheint. Es besteht kein Anlass anzunehmen, dass dies im vernetzten Auto der Zukunft anders sein wird. Die bestehenden rechtlichen Anforderungen an die datenschutzrechtliche Einwilligung (Einsichtsfähigkeit, Informiertheit, Freiwilligkeit, Formvorschriften) bieten bisher gegen umfassende Einwilligungserklärungen mit weit formulierten Zweckbestimmungen und Befugnissen zu Datenübermittlungen kaum einen effektiven Schutz.[62]

In diesem Sinne „gehören" dem Betroffenen die Daten – da nur er wirksam Einwilligungen und Verträge abschließen kann – und er „handelt" mit ihnen durch diese Instrumente. Mit Blick auf die Verankerung des Rechts auf informationelle Selbstbestimmung in der Autonomie des Einzelnen ist dagegen auch prinzipiell nichts einzuwenden. Problematisch ist allerdings, dass der Nutzer in der realen Praxis für seine Daten entweder gar keine oder eine viel *zu geringe Gegenleistung* erhält. Mit Blick auf die exorbitanten Gewinne, die in der Internetwirtschaft entweder aktuell oder (ablesbar an den hohen Börsennotierungen innovativer Unternehmen) in der Hoffnung der Anleger künftig erzielt werden, ist eben auch die kostenlose Nutzung sinnvoller Dienste keine wirtschaftlich adäquate Gegenleistung; die zur Verfügung gestellten Daten sind ganz offensichtlich ein Vielfaches wert.

Darüber hinaus sind die *Marktplätze* (im Endkundenbereich z.B. App-Stores, vor allem aber die nachgelagerten Datenmärkte, auf denen die eigentliche Wertschöpfung stattfindet) für den Einzelnen teilweise völlig intransparent. Es ist häufig nicht absehbar, welche Daten überhaupt betroffen sind, an wen diese weitergegeben werden, wie sie wirtschaftlich genutzt werden können und was ihr eigentlicher ökonomischer Wert ist.

bb) Keine Verhandlung auf Augenhöhe

Dies führt zu dem eigentlich Problem, nämlich den fehlenden Verhandlungsmöglichkeiten auf Augenhöhe. Diese sind zum einen durch die beschriebene Informationsasymmetrie bedingt, deretwegen die Betroffenen den Wert der von ihnen „angebotenen" Leistung nicht kennen. Hinzu treten ökonomische Ungleichgewichte zwischen Privatpersonen einerseits, weltweit operierenden Oligopolen andererseits. Wenn letztere in einer Art

55 Die Ausnahme der ausschließlich persönlichen oder familiären Tätigkeit (§ 1 Abs. 2 Nr. 3 BDSG) wird im vernetzten Auto typischerweise nur für einige Verarbeitungen durch die Insassen eingreifen.

56 BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (45).

57 S. z.B. *Roßnagel*, SVR 2014, 281 (283 f.); *Weichert*, SVR 2014, 201 (203).

58 S. z.B. *Weichert*, SVR 2014, 201 (205).

59 S. *Roßnagel*, SVR 2014, 281 (286).

60 Allgemein zu den Transparenzanforderungen *Weichert*, SVR 2014, 241 (241 f.); zur Problematik der durch Hersteller „geheim" erhobenen Daten *Mielchen*, SVR 2014, 81 ff.

61 S. zu den Anforderungen im vernetzten Automobil und den Umsetzungsfragen z.B. *Asaj*, DuD 2011, 558; *Schulz/Roßnagel/David*, ZD 2012, 510; *Mielchen*, SVR 2014, 81; *Roßnagel*, NZV 2006, 281; *Roßnagel*, SVR 2014, 281; *Weichert*, SVR 2014, 201; *Weichert*, SVR 2014, 241; *Kremer*, RDV 2014, 240; *Kinast/Kühnl*, NJW 2014, 3057; zu den Besonderheiten der Elektromobilität *Lüdemann/Jürgens/Ortmann*, RDV 2014, 3.

62 Zur Einwilligung s. näher *Liedke*, Die Einwilligung im Datenschutzrecht, 2012; zu den Anforderungen im Automobil s. *Weichert*, SVR 2014, 241 (243 f.); *Kinast/Kühnl*, NJW 2014, 3057 (3059 f.).

lex mercatoria digitalis[63] ein binäres Modell des „take it or leave it" ohne Verhandlungsspielräume der Einzelnen etablieren und sich wie vielfach auch noch ein Recht zur nachträglichen Änderung der Vertragsbedingungen herausnehmen,[64] so spielt es keine Rolle mehr, ob man die Beziehungen des Einzelnen zu seinen Daten eher *persönlichkeitsrechtlich* oder eher *eigentumsrechtlich* konstruiert – weder die eine noch die andere Perspektive führen zu einem angemessenen Schutz.

2. Wege zu einer marktadäquaten Regulierung eines „Dateneigentums"?

Wie ließe sich diese unbefriedigende Situation verändern? Wenn personenbezogene Daten rein faktisch ein weltweit gehandeltes Wirtschaftsgut sind und ihr Wert auch gemessen werden kann, so ist es jedenfalls nicht hinreichend, unter Verweis auf die deutsche menschenwürde- und demokratieorientierte Konzeption des Rechts auf informationelle Selbstbestimmung Kämpfe gegen Windmühlen zu führen.[65]

a) Ansatzpunkte

Ein erster Ansatzpunkt für die Rechtsfortbildung könnte dabei die Klarstellung der „Eigentumsverhältnisse" sein. Insoweit ist zwischen *personenbezogenen* und *sonstigen Daten* zu unterscheiden. Erstere sind rechtlich über Art. 2 lit. a DSRL, § 3 Abs. 1 BDSG dem Betroffenen zugeordnet. Hieran könnte allenfalls der europäische Gesetzgeber etwas ändern, wofür es im Zuge der aktuellen Reform[66] jedoch (zu Recht) keine Anhaltspunkte gibt. Die Zuordnung anonymisierter, Kfz-produzierter Daten ist – insbesondere im Verhältnis zwischen Fahrzeugherstellern und anderen Unternehmen – jedoch viel weniger klar. Aus der *datenschutzrechtlichen Perspektive* „gehören" diese Daten niemand, so dass der Hersteller sie nutzen oder auch an Dritte veräußern kann. Aus einer *wirtschaftlichen Sichtweise* besteht jedoch ein klares Interesse daran, dass der Fahrzeughalter bzw. Fahrzeugführer auch von den Daten profitiert, die er selbst erzeugt. Dies ist im Moment nicht der Fall.

Auch für den Hersteller kann die Situation rechtlich unbefriedigend sein, weil er typischerweise nicht gegen eine Verwendung durch Dritte geschützt ist.[67] *De lege ferenda* ließe sich deshalb auch der Entstehungsvorgang eines „Dateneigentums" klarstellen. Dabei weisen denkbare Analogien freilich in unterschiedliche Richtungen. Eine Anlehnung an die Regeln zur Fruchtziehung (§ 953 BGB) würde für eine Zuordnung zum Eigentümer des Automobils sprechen. Allerdings bestehen auch hier Ausnahmen (Nießbrauch), und die Eigentümerstellung kann wie gesehen sehr unterschiedlich ausfallen.[68] Die Regelungen zu Verbindung, Vermischung und Verarbeitung (§§ 946-952 BGB) könnten für eine Unterscheidung zwischen den Grunddaten des Fahrzeugs (Eigentümer) und den Fahrdaten, standortbezogenen Informationen und Vorgängen im Fahrzeug (Fahrer und gegebenenfalls andere Fahrzeuginsassen) sprechen; eine Übertragung strafrechtlicher Schutzkonzepte v.a. zu §§ 202a, 303a StGB würde zu einer stärkeren Berücksichtigung der „Verfügungsbefugnis" an Daten und den sie erzeugenden Skripturakten sprechen.[69] Zumindest für anonyme Daten wäre auch eine Analogie zu den Regeln über herrenlose Sache oder den Fund denkbar (§ 958 bzw. § 973 BGB). Dies würde dazu führen, dass jeder, der Zugang zu den Daten hat, diese auch nutzen dürfte.

Insgesamt dürften die Datenverarbeitungsstrukturen in der Praxis jedenfalls zu komplex sein, um durch schlichte Analogien zum Sacheigentum oder durch die Anknüpfung an rein faktische, oftmals zufällige Zugriffs- und Verarbeitungsmöglichkeiten allgemeine Regeln für Exklusivrechte zu etablieren.

b) Vertragskontrolle

Schließlich besteht die Möglichkeit, Regeln für die Möglichkeiten und Grenzen von Verträgen über die wirtschaftliche Nutzung personenbezogener und/oder anonymer Daten zu definieren. Anders als die vorgenannten Ansätze lässt dies Raum für Aushandlungen der Beteiligten. Dabei müssen allerdings Lösungen für die genannten Probleme der fehlenden Verhandlungsparität zwischen den Verbrauchern (Käufer, Halter, Fahrer und Beifahrer) und den Fahrzeugherstellern und anderen involvierten Unternehmen gefunden werden. Insoweit sind verschiedene Fallgruppen zu unterscheiden:

aa) Fallgruppe Verbraucher

Für die Verbraucher, die unmittelbare Vertragspartner sind, bietet das geltende *Verbraucherschutz- und Wettbewerbsrecht* Ansatzpunkte. Beide bieten Möglichkeiten zur Einschränkung der Vertragsautonomie, um Abhängigkeitsverhältnisse oder Machtungleichgewichte auszugleichen. Hier hat sich in den letzten Jahren die Erkenntnis verbreitet, dass zumindest viele Normen des geltenden Datenschutzrechts auch verbraucherschützenden und marktregulierenden Charakter haben.[70] Dies könnte im Zuge der europäischen Datenschutzreform klargestellt und weiter ausgebaut werden. Problematischer sind die Kontrollmöglichkeiten für die Nutzung etwaiger anonymisierter Kfz-Daten, weil hier das Datenschutzrecht nicht eingreift und deshalb die Inhaltskontrolle nach § 307 Abs. 2 Nr. 1 BGB keine Hilfe bietet. Im Rahmen der allgemeinen Angemessenheitskontrolle (§ 307 Abs. 1 S. 1 BGB) spricht dennoch viel dafür, dass die Erzeuger der Daten an der nachgelagerten wirtschaftlichen Wertschöpfung partizipieren sollten.

63 S. *Hornung*, Regelungsinstrumente im virtuellen Raum, *https://www.datenschutzzentrum.de/sommerakademie/2010/sak10-hornung-regelungsinstrumente-im-virtuellen-raum%20.pdf*.

64 S. am Beispiel von Facebook KG, Urt. v. 24.1.2014 – 5 U 42/12 (insoweit in CR 2014, 319 nicht abgedruckt); zu den strukturellen Ungleichgewichten auch *Weichert*, NJW 2001, 1463 (1468 f.); *Kilian* in GS Steinmüller, 2014, 212 ff.

65 S. *Buchner* in Redeker/Hoppen, DGRI Jahrbuch 2011, 58 f.; zur Tendenz der Ökonomisierung des Rechts auf informationelle Selbstbestimmung schon *Weichert*, NJW 2001, 1463.

66 Dazu statt vieler *Hornung* in Scholz/Funk, DGRI Jahrbuch 2012, 2013, 1 ff.

67 Zu weitergehenden Überlegungen eines Schutzes des Datenerzeugers s. *Zech*, CR 2015, 137 ff.

68 S.o. III.2. a.E.; speziell zur Fruchtziehung *Grosskopf*, ITRB 2011, 259 (260); *Specht* (Fn. 39), 161 ff.; *Zech*, CR 2015, 137 (142) m.w.N.

69 Zu diesen und anderen Ansätzen für eine Analogie s. *Kilian* in GS Steinmüller, 2014, 208 ff.; *Hoeren/Völkel* in Hoeren, Big Data und Recht, 2014, 11 ff.; *Specht* (Fn. 39), 136 ff., 215 ff.; *Dorner*, CR 2014, 617 (618 ff.) (s.a. ebd., 619 zu den Problemen der Einordnung von Cloud-Diensten im Rahmen eigentumsorientierter Anknüpfungen, z.B. bei § 823 BGB sowie ebd., 625 im Ergebnis allgemein abl. zur Analogie); *Zech*, CR 2015, 137 (140 ff.) (grds. positiv zur Rechtsentwicklung, s. ebd., 144 ff.); *Hoeren*, MMR 2013, 486, insbesondere zur Analogie zu § 303a StGB (486) und zu § 950 BGB (490).

70 S. z.B. *Huppertz/Ohrmann*, CR 2011, 449; *Schröder*, ZD 2012, 330; für die Anwendung von § 4 Nr. 11 UWG zumindest in manchen Fällen z.B. OLG Köln v. 14.8.2009 – 6 U 70/09, NJW 2010, 90; v. 19.11.2010 – 6 U 73/10, CR 2011, 680; v. 17.1.2014 – 6 U 167/13, NJW 2014, 1820; OLG Karlsruhe v. 9.5.2012 – 6 U 38/11, NJW 2012, 3312; zurückhaltend KG v. 29.4.2011 – 5 W 88/11, CR 2011, 468; OLG München, ZD 2012, 330; zur Frage der Verbandsklage s. *Köpernik*, VuR 2014, 240.

bb) Fallgruppe Dritter und Beifahrer

Problematischer ist der Umgang mit den personenbezogenen Daten derjenigen, die bisher typischerweise keine vertragliche Beziehung zu Herstellern, Zulieferern oder Drittanbietern haben. Wird das Fahrzeug leihweise einem Dritten überlassen, so mag man im Rahmen der ersten Inbetriebnahme noch an eine fahrerbezogene Einwilligung beispielsweise in die Identifizierung mittels eines verbundenen Smartphones oder in die kontinuierlichen Ortung denken. Bei spontanen Beifahrern ist es dagegen kaum vorstellbar, dass in jedem Einzelfall die Einwilligung zur Erhebung von Innenraumdaten eingeholt oder darüber abgestimmt wird, ob eine mitgeführte Blackbox ein- oder ausgeschaltet wird. Für die Erhebung und Verwendung der Daten bestimmbarer Beifahrer (dies wird künftig schon aufgrund der Verbindung des Fahrzeugs mit Smartphones immer häufiger der Fall sein) sind deshalb Lösungen zu entwickeln, die insbesondere die datenschutzrechtlichen Verbots- und Transparenzprinzipien umsetzen.

cc) Fallgruppe dritte Unternehmen

Von diesen verbraucher- und datenschutzrechtlichen Verträgen sind die Verträge zu unterscheiden, die Hersteller mit Zulieferern, Anbietern von Navigationsdiensten, Plattformbetreibern wie *Google* oder *Apple*[71] und schließlich den Anbietern von Apps schließen, die über diese Plattformen vertrieben werden. Insoweit dürfte es typischerweise an einer Verhandlungsdisparität fehlen, die ein staatliches Eingreifen legitimieren könnte. Im geltenden Recht finden sich Bestimmungen zum Schutz von Betriebs- und Geschäftsgeheimnissen (§§ 4 Nr. 9 c), 17, 18 UWG), die aber regelmäßig nicht einschlägig sein werden, wenn fahrzeugbezogene Daten durch Dritte genutzt werden; jedenfalls können sich die Unternehmen durch entsprechende Vertragsklauseln schützen. Das allgemeine Kartell- und Lauterkeitsrecht dürfte zumindest solange keine Anhaltspunkte bieten, wie die einzelnen Beteiligten nicht nach exklusiver Nutzung der Daten streben. Dies könnte sich allerdings anders darstellen, sobald die Hersteller beispielsweise nur ihren Vertragswerkstätten Zugriff auf die OBD-Daten gewähren (und freie Werkstätten oder Anbieter von Pannenhilfen ausschließen) oder bestimmte Mobilfunk- oder App-Anbieter gezielt benachteiligen.[72]

3. Die Grenzen rechtlicher Schutzinstrumente

Am Ende stellt sich – insbesondere in der Beziehung zwischen den Herstellern und den großen Internetanbietern – die Frage nach dem Verhältnis zwischen rechtlichem Schutz und der Kraft des Marktes. Wenn in der politischen Diskussion bisweilen vorgeschlagen wird, die „Eigentümerschaft" (oder Nutzungs- oder Verfügungsrechte) an den produzierten Daten klarzustellen, so sollte nämlich nicht übersehen werden, dass damit nicht zwingend eine faktische Besserstellung der solcherart rechtlich Begünstigten verbunden ist.

So könnte der Gesetzgeber beispielsweise versucht sein, die traditionellen (deutschen) Kfz-Hersteller dadurch vor einem drohenden Bedeutungsverlust zu schützen, dass er ihnen die *exklusive Nutzungsbefugnis* an anonymisierten fahrzeugbezogenen Daten und das Recht zuweist, diese auf den entstehenden Datenmarktplätzen an Dritte zu veräußern. Auf den ersten Blick würde eine solche exklusive Zuweisung die Position der Hersteller stärken und ihnen eine gute Verhandlungsposition für die Preisbildung geben.

Bei näherem Hinsehen ist dies jedoch weniger sicher, wenn es um Verhandlungen mit weltweit operierenden Interessenten geht. Dies lehrt insbesondere das – strukturell vergleichbare – Beispiel des *Leistungsschutzrechts für Presseverleger.* Mit der Einführung von §§ 87f–87h UrhG räumte der Gesetzgeber den Presseverlagen das ausschließliche Recht ein, Presseerzeugnisse zu gewerblichen Zwecken öffentlich zugänglich zu machen, es sei denn, es handelt sich um einzelne Wörter oder kleinste Textausschnitte. Unabhängig von der Frage, ob dies inhaltlich angemessen ist,[73] ist der Versuch bisher gescheitert, durch diese Zuweisung die Verleger effektiv zu schützen. Diese erhielten innerhalb des Marktes der Verwertung von Presseerzeugnissen eine neue, wirtschaftlich relevante Rechtsposition und die Befugnis, diese am Markt anzubieten. Im Zusammenspiel zwischen Angebot und Nachfrage bildete sich ein Preis, aufgrund der massiv überwiegenden Marktmacht der Nachfrageseite (*Google*) ist dieser jedoch – exakt null. *Google* stellt die Verlage vor die Wahl, entweder eine kostenlose Lizenz zu erteilen oder nicht mehr gelistet zu werden; bislang ist der Konzern damit erfolgreich.[74] Ein ähnliches Szenario könnte sich auch bei Verhandlungen zwischen Automobilherstellern und den großen Internetanbietern ergeben.

4. Open Innovation

Ohnehin spricht wertungsmäßig zwar alles dafür, die Verbraucher sowohl im Verhältnis zu den hergebrachten Automobilanbietern als auch gegenüber den neuen Playern wie *Apple, Google* oder *Microsoft* effektiv zu schützen – viel weniger jedoch dafür, in die Marktprozesse zwischen letzteren einzugreifen. Dies gilt nicht nur, weil es sich insoweit auf beiden Seiten um große Wirtschaftsunternehmen handelt, sondern auch aus einer *innovationsorientierten Perspektive.*

Insoweit ist das vernetzte Auto nämlich ein neuer Markt, in dem sich Elemente des traditionellen Produkts Auto und des Internets treffen. Wie in anderen konvergierenden Märkten sollte dabei keine Seite einen Startvorteil oder exklusive Nutzungsbefugnis haben. Will man innovative Dienste am vernetzten Automobil fördern, so spricht vielmehr einiges dafür, entsprechend der Leitideen von *open data*[75] und *open innovation*[76] die durch das Kfz produzierten Daten in ihrer Rohform möglichst allgemein zur Verfügung zu stellen, so dass auf ihrer Basis neue und individuelle Ideen für neue Wertschöpfungsmodelle entstehen können. Ziel muss es sein, auf diesem Weg Anreize für nützliche Innovationen zu setzen. Dies erfordert eine angemessen Gewinnallokation, bei der Monopole auf die Nutzung bestimmter Daten oder Datenkategorien wenig hilfreich sind.[77]

71 Mittels der Plattformen Open Automotive Alliance und Carplay, s.o. II.1.

72 S. *Roßnagel* in 52. Deutscher Verkehrsgerichtstag, 2014, 272 ff.

73 Zur Diskussion s. *Frey*, MMR 2010, 291; *Ensthaler/Blanz*, GRUR 2012, 1104; *Wandtke*, ZUM 2014, 847; *Kreutzer*, CR 2014, 542, jew. m.w.N.

74 Zur Frage einer etwaigen Missbrauchskontrolle nach §§ 19, 20 GWB s. den (auf ein Gutachten für die VG Media zurückgehenden) Beitrag von *Koenig/Meyer*, K&R 2014, 765.

75 Dazu *Schulz*, VerwArch 2013, 327; umfassend *Lederer*, Open Data. Informationsöffentlichkeit unter dem Grundgesetz, 2014.

76 Der Begriff geht zurück auf *Chesbrough*, Open Innovation, 2003; zu aktuellen Perspektiven der Vernetzung internen und externen Wissens z.B. *Blohm*, Open Innovation Communities, 2013; *Weiers*, Innovation through Cooperation, 2014.

77 S.a. *Dorner*, CR 2014, 617 (625 f.); zum Parallelproblem der angemessenen wirtschaftlichen Nutzung staatlicher Informationen *Hornung* in

V. Ausblick

Im Ergebnis kann der Fokus auf die *wirtschaftlichen Aspekte* und den *wirtschaftlichen Wert* der durch vernetzte Automobile erzeugten Daten auch ohne ein rechtlich fixiertes Konzept eines Dateneigentums zum besseren Verständnis der Informationsordnung beitragen – und zwar nicht nur in Bezug auf die vernetzte Mobilität, sondern für den gesamten Handel mit Daten und die damit in Verbindung stehenden Dienstleistungen. Wenn der Begriff der „data ownership" in der Diskussion als Kampfbegriff gegen eine selbstbestimmungsorientierte Konzeption des Datenschutzes eingesetzt wird,[78] so ist dem entschieden entgegenzutreten. Wenn der Vergleich mit eigentumsrechtlichen Konzepten jedoch als Instrument dient, um den Blick auf die wirtschaftlichen Zusammenhänge der Datenflüsse zu schärfen und im Idealfall die Betroffenen an der Wertschöpfung mit ihren Daten zu beteiligen,[79] so wäre für den Daten- und Verbraucherschutz viel gewonnen.

In keinem Fall darf die wirtschaftliche Sichtweise dazu dienen, *Persönlichkeitsrechte der Betroffenen* zu ignorieren. Insoweit ist vielmehr eine Spezifizierung allgemeiner datenschutzrechtlicher Prinzipien erforderlich, für die es inzwischen einige Ansätze gibt.[80] Das vernetzte Automobil könnte überdies von der Anwendung moderner Datenschutzinstrumente (*privacy by design* und *privacy enhancing technologies, privacy by default*, Datenschutzaudit und -siegel, etc.) profitieren, die im Rahmen der europäischen Reform ausgebaut werden sollen.[81]

Während diese Instrumente auf einer allgemeinen Gestaltungsebene wirken, werden die konkreten Rechtsbeziehungen und Informationsflüsse vertraglich geregelt werden. Dies gilt sowohl für Eigentümer, Halter, Fahrer und Beifahrer als auch für das Verhältnis zwischen den beteiligten Unternehmen. Insofern wird es entscheidend darauf ankommen, auch den einzelnen Betroffenen eine echte Verhandlungsposition zu verschaffen.

Schließlich geht es maßgeblich um Innovationen, Innovationssteuerung und Innovationsfolgenmanagement. Wie bei anderen Prozessen der „schöpferischen Zerstörung"[82] wird es dabei Gewinner und Verlierer geben. Aus den 130 Jahren Produktionsgeschichte der traditionellen Automobilhersteller folgt weder ein Anspruch noch eine Garantie für die Zukunft. Das Beispiel *Nokia* sollte insofern allen Beteiligten eine Warnung sein. Der Gesetzgeber steht in der Verantwortung, schwächere Parteien (insbesondere die datenschutzrechtlich Betroffenen) in ihren persönlichen und wirtschaftlichen Rechten zu schützen. Die Herausforderungen des Wettbewerbs mit US-dominierter Internet-Marktmacht wird die deutsche Industrie selbst annehmen müssen.

Towfigh et al., Recht und Markt, Beiträge zur 49. Assistententagung Öffentliches Recht, 2009, 75 ff.; *Wiebe/Ahnefeld*, CR 2015, 127 ff.; *Wiebe/Ahnefeld*, CR 2015, 199 ff.; eher positiv zu Ausschließlichkeitsrechten unter wirtschaftlichen Gesichtspunkten *Zech*, CR 2015, 137 (144 ff.).

78 Explizite Verwendung eines eigentumsorientierten Ansatzes zur Überwindung eines angeblich überholten Datenschutzkonzepts z.B. bei *Rees*, CLSR 2014, 75 (76 ff.). Dem Eigentumsbegriff wird auch in anderen Diskussionen vorgehalten, als Kampfbegriff verwendet zu werden; s. zum „geistigen Eigentum" *Hilty, www.faz.net/aktuell/wirtschaft/-11778608.html*.

79 In diese Richtung z.B. *Buchner* in Redeker/Hoppen, DGRI Jahrbuch 2011, 53 ff. (mit Überlegungen zu Treuhändermodellen, ebd., 59 ff.); *Kilian* in GS Steinmüller, 2014, 211 f.; ähnliches Ziel letztlich auch bei *Rees*, CLSR 2014, 75 (77 f.).

80 S. z.B. die Empfehlungen des 52. Deutschen Verkehrsgerichtstages, 2014; *Janker*, SVR 2014, 77; Entschließungspapier der 88. Konferenz der Datenschutzbeauftragten zum Datenschutz in Kraftfahrzeugen, 2014. In den USA findet sich mit den „Consumer Privacy Protection Principles" der US-Industrie *(http://www.autoalliance.org/index.cfm?objectid=CC629950-6A96-11E4-866D000C296BA163)* ein Ansatz zur Selbstregulierung. In dieselbe Richtung geht eine Mustervereinbarung des Verbands der deutschen Automobilindustrie und der Datenschutzaufsichtsbehörden, *http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Muster-Information_Fahrzeugdatenspeicher.pdf*.

81 Zum Datenschutz durch Technik (vorgesehen in Art. 23 DS-GVO-E) s. insoweit *Hornung* in Friedewald/Pohoryles, Privacy and Security in the Digital Age, 2014, 181 ff.; zum Datenschutzaudit *Hornung/Hartl*, ZD 2014, 219.

82 *Schumpeter*, Kapitalismus, Sozialismus und Demokratie, 7. Aufl. 1993, 134 ff.

Robert Selk/Sibylle Gierschmann

Stellungnahme der DGRI zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Die Bundesregierung hat den Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vorgelegt (Drucks. 18/4096). Der „Fachausschuss Datenschutz" der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI) hat sich mit dessen Art. 4 (Änderung des TMG-Gesetzes) und Art. 5 (TKG-Änderung) aus datenschutzrechtlicher Perspektive befasst. Die DGRI hat die daraus gewonnenen Erkenntnisse im Rahmen der Verbändeanhörung zum Entwurf eines IT-Sicherheitsgesetzes in einer Stellungnahme vom 17.3.2015 dem Bundesministerium des Innern zugeleitet.

▷ Dr. Robert Selk, LL.M. und Dr. Sibylle Gierschmann, LL.M., beide Leitende des Fachausschusses Datenschutz der DGRI. Stand: 17.3.2015.

A. Stellungnahme zu Art. 4 des IT-SiG: Änderungen des TMG (Einfügung eines neuen Absatz 7 bei § 13 TMG)

Bei dem im Rahmen des IT-SiG geplanten neuen Absatz 7 zu § 13 TMG fallen eine Reihe von Unstimmigkeiten und Begriffsungenauigkeiten auf, die zu einem Widerspruch zu den bestehenden Regelungen sowohl im TMG wie auch BDSG führen. Zudem beinhaltet die Regelung keinen Mehrwert im Verhältnis zur bestehenden Rechtslage, diese wird vielmehr durch die entstehenden Widersprüche verschlechtert, welche zu Rechtsunsicherheit führen.

1. Vorab

Folgt man der herrschenden Meinung, gilt das TMG für die Bestands- und Nutzungsdaten, das BDSG für die In-