www.jusletter-it.eu

Max von Schönfeld

Daten — das neue Öl?!

Kampf um die Datenhoheit in Fahrzeugen

The car is developing in increasingly speed from a solely use as a means of transportation to a mostly unexplored source for information and data procurement. This source has huge potential both in quantity and quality of the data. The question of the legal evaluation of the topic, which inevitably raises against the background of the conflict of interest between economical use and privacy, is still unclear. (ah)

Category: Articles
Field of law: Big Data, Open Data & Open Government; Data Protection; Road Traffic
Region: Germany

Citation: Max von Schönfeld, Daten — das neue Öl?!, in: Jusletter IT 21 May 2015

Inhaltsübersicht

1 Einleitung

[Rz 1] Das Auto von heute ist nicht mehr nur Fahrzeug, das den Fahrgast von A nach B bringt, sondern auch Datenspeicher, Messgerät und Steuergerät.[1]

[Rz 2] Mittlerweile drängen die führenden IT-Unternehmen Apple, Google und Co. massiv in den Markt der Bordfahrelektronik. Stichwort: Digitalisierung, Vernetzung, Unterhaltungselektronik und selbstfahrende Autos. Der Chef des Grafikchipherstellers NVIDIA bestätigt dies durch seine Aussage: «Das Auto ist der ultimative mobile Computer».[2] Bezüglich Apple kursieren sogar Gerüchte, sie würden ein eigenes Elektrofahrzeug entwickeln; Google hat bereits ein autonom fahrendes Kfz vorgestellt. Das Thema ist derart von Bedeutung, dass die Chefs der «alten Autoindustrie» sich genötigt sehen Stellung zu beziehen. *Didier Leroy*, Europa-Chef des aktuellen Marktführers Toyota, führt beispielsweise im Rahmen des Genfer Autosalon 2015 aus: «Wir wollen nicht nur Lieferant einer leeren Kiste sein». *Dieter Zetsche*, aktueller Daimler-Chef, bekräftigt: «Wir haben momentan die gesamte Wertschöpfungskette in unserer Hand».[3]Fraglich ist allerdings wie lange noch. Apple könnte mit seinem riesigen Kapital derzeit wohl die meisten Autobauer weltweit übernehmen. Warum? Daten, Daten, Daten. Nachdem mittels Smartphones bereits Profile von Einzelnen angelegt werden können, könnten diese durch die Daten aus Fahrzeugen vielversprechend ergänzt werden.

[Rz 3] Die Informationstechnologie-Industrie wird in Zukunft für die althergebrachte Automobilindustrie also Partner und Konkurrent zugleich. Tesla Industries hat vorgemacht wie es geht und gezeigt wie schnell man die «big player» technisch überholen kann, indem das Unternehmen die Reichweite in Elektrofahrzeugen revolutionierte.

[Rz 4] Das Gremium der Datenschutzbeauftragten hat in seiner 88. Konferenz reagiert und in einer EntschlieSSung die Automobilindustrie, aber auch Zulieferer konkret aufgefordert die informationelle Selbstbestimmung in und um das Kraftfahrzeug zu gewährleisten.[4]

[Rz 5] Gefordert wird insbesondere das Befolgen der Ansätze «privacy by design» und «privacy by default».

---

1 Jürgen Bönninger, ZfSch 2014, 184—189 (185).

2 Thiemo Heeg/Christoph Ruhkamp, Das Auto als ultimativer mobiler Computer, FAZ 7. Januar 2014, http://www.faz.net/-hog-7l23g (alle Internetquellen zuletzt besucht am 11. Mai 2015).

3 Newsticker Heise.de, http://heise.de/-2566336.

4 EntschlieSSung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Datenschutz im Kraftfahrzeug, https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9632.de.

[Rz 6] Dabei handelt es sich um grundlegende Herangehensweisen zum Thema Datenschutzrecht im 21. Jahrhundert.

[Rz 7] Einige der Fragestellungen lassen sich mit denen der Nutzung von modernen Smartphones vergleichen. Auf der einen Seite kann es auch hier immense Datenverarbeitung geben. Auf der anderen Seite bestehen jedoch entscheidende Unterscheide: Das Auto stellt schlieSSlich allein durch die Möglichkeit des AbschlieSSens der Türen eine besondere Art von Rückzugsort dar. Diesen Nimbus könnte es bei ständiger Konnektivität verlieren. Bei einem Smartphone rechnet der Nutzer dagegen eher mit einer aktiven Netzverbindung und Datenübertragung.

[Rz 8] Dieser Artikel versucht sich mit einigen grundlegenden Fragen auseinanderzusetzen und Lösungsansätze zu präsentieren, wobei insbesondere die Vielschichtigkeit der Thematik aufgezeigt werden soll.

2 Anwendbares Recht

[Rz 9] Beim Datenschutzrecht ist nicht nur das Bundesdatenschutzgesetz (BDSG) einschlägig, sondern insbesondere auch Grundrechte und spezifisches Datenschutzrecht.

[Rz 10] Entscheidend ist das vom Bundesverfassungsgericht im Rahmen des Volkszählungsurteils entwickelte Grundrecht der informationellen Selbstbestimmung. Dogmatischer Ausgangspunkt ist das allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 des Grundgesetzes (GG) in Verbindung mit Art. 1 Abs. 1 GG. Der Schutzbereich umfasst dabei das Recht des Einzelnen, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[5] Das Volkszählungsurteil ist im Übrigen auch die maSSgebliche Grundlage für das bestehende BDSG mit seinen Grundsätzen der Datensparsamkeit und beeinflusste zudem auch die Entwicklung der europäischen Datenschutzrichtlinie 95/46/EG. Datenschutz kann als Begriff auch irreführend sein, sollen schlieSSlich nicht die Daten an sich geschützt werden, sondern die informationelle Selbstbestimmung des Dateninhabers.[6]

[Rz 11] Grundrechte gelten zwar zunächst nur zwischen Bürger und Staat in ihrer Hauptfunktion als Abwehrrechte, allerdings geht das Bundesverfassungsgericht in ständiger Rechtsprechung seit dem Lüth-Urteil auch von einer mittelbaren Wirkung der Grundrechte inter privatos aus.[7]

[Rz 12] Von Bedeutung ist ferner Art. 10 GG hinsichtlich des Telekommunikationsgeheimnisses.

[Rz 13] Auch das noch recht neue Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme, das als Ergänzung des Schutzes des allgemeinen Persönlichkeitsrechts verstanden wird, kann zur Disposition stehen.[8]

[Rz 14] Spezialgesetzliche Vorschriften finden sich ferner in den §§11 ff. des Telemediengesetzes (TMG), welche über den §1 Abs. 1 TMG dann Anwendung finden, wenn kein Telekommunikationsdienst im Sinne des §3 Nr. 24 des Telekommunikationsgesetzes (TKG) vorliegt. Ein solcher liegt dann vor, wenn der Dienst ausschlieSSlich oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht. Demnach sind wohl die meisten angebotenen

5 Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983, NJW 1984, 419 f.

6 RoSSnagel, NZV 2006, 281 (282).

7 Urteil des Bundesverfassungsgerichts vom 15. Januar 1958, BVerfGE 7, 198 (205).

8 Urteil des Bundesverfassungsgerichts vom 17. Februar 2008, BVerfGE 120, 274 (302 f.); Gersdorf/Paal, Beck'scher Online-Kommentar Informations- und Medienrecht, Art. 2GG, Rn. 22.

Dienste in Fahrzeugen als Telemediendienste anzuerkennen.[9]Wann ist also das BDSG oder eben andere sogenannte bereichsspezifische Regelungen einschlägig? Nach §1 Abs. 4 BDSG besteht der Grundsatz der Subsidiarität, sodass dieses nur dann gilt, wenn keine spezielleren Regelungen wie eben das TMG vorliegen.[10]

[Rz 15] Das BDSG ist für den Schutz der informationellen Selbstbestimmung bei den sensiblen Inhaltsdaten verantwortlich; das TMG für den Schutz der sogenannten Metadaten bzw. Verkehrsdaten, also solcher Daten, die Auskünfte über die Merkmale anderer Daten beinhalten, aber nicht die Inhaltsdaten selbst.[11]

[Rz 16] Auf supranationaler Ebene besteht zurzeit noch ein mehrgliedriger Aufbau. Die EU hat allerdings mit dem Ziel der Harmonisierung des Binnenmarktes die Entwicklung vorangetrieben: Auf der einen Seite besteht seit 1995 die EG-Datenschutzrichtlinie 95/46/EG hinsichtlich der Inhaltsdaten. Auf der anderen wurde im Jahr 2002 die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation verabschiedet. Sie befasst sich mit den Meta- bzw. Verkehrsdaten.[12]

[Rz 17] Die sich in Arbeit befindende europäische Datenschutz-Grundverordnung (DS-GVO) soll die Richtlinie von 1995 ersetzen. Am 12. und 13. März 2015 verhandelten die Justizminister der Mitgliedsstaaten über eine Einigung zum zweiten Kapitel der Verordnung. Es ist daher davon auszugehen, dass bis zum Inkrafttreten der DS-GVO noch einige Zeit vergehen wird.

3 Technische Infrastruktur und erhobene Daten

[Rz 18] Technologie in Fahrzeugen kann und wird in Zukunft viel bieten können. Dazu seien einige Beispiele exemplarisch erwähnt: Erhöhte Sicherheit durch Notfallhilfe, Fahrassistenzsysteme, Unfalldokumentation, automatisierte Warnungen oder sogar autonomes Fahren. Dazu kommt gesteigerter Komfort durch die Analyse von Verkehrsfluss und darauf basierte dynamische Navigation in Echtzeit, Information und Unterhaltung oder Telefonie und sonstige digitale Kommunikation. Ferner bietet sich die Möglichkeit, den Zustand des Fahrzeugs selber besser hinsichtlich VerschleiSS und Reparaturbedürftigkeit zu kontrollieren.[13]

[Rz 19] Heutzutage werden allerdings viele verschiedene technische Standards im Rahmen der Informationstechnologie in modernen Fahrzeugen eingesetzt. Gerade die Entwicklung der volldigitalen Mobilfunknetze überholt sich teilweise selbst, was zu einer gewissen Unübersichtlichkeit führen kann: GSM (Global System for Mobile Communications) als weltweit am meisten verbreiteter Standard und als erster Vertreter der sogenannten zweiten Generation («2G») wird zunehmend durch UMTS (Universal Mobile Telecommunications System), der dritten Generation («3G») ersetzt. Dazu kommen mit LTE (Long Term Evolution) bzw. LTE-Advanced bereits

9 Weichert, SVR 2014, 201 (203).

10 Helfrich, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, Teil 16.1 Einführung und Grundbegriffe des Datenschutzes, 40. Ergänzungslieferung 2014, Rn. 97.

11 Weichert, SVR 2014, 201 (203).

12 Helfrich, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, Teil 16.1 Einführung und Grundbegriffe des Datenschutzes, 40. Ergänzungslieferung 2014, Rn. 95.

13 Weichert, SVR 2014, 201 (202).

die Vertreter des 3,9G bzw. 4G Standards.[14] Ferner die klassische WLAN-Technik, bei der das Fahrzeug teilweise sogar als Hotspot fungieren kann und den Insassen einen Zugang zum Netz bietet. Noch wird bei den verschiedenen Fahrzeugherstellern hinsichtlich Netzzugang allerdings nicht standardisiert vorgegangen: Beispielhaft erwähnt seien Audi und BMW, die auf einen eigenen Internetzugang und dazugehörige Apps setzen. Andere Hersteller wie Citroën oder Toyota nutzen teilweise noch die sogenannte Tetheringtechnik bei der ein Mobiltelefon per Bluetooth mit dem Fahrzeugcomputer verbunden wird und als Router dient.[15] Die einzigen Daten aus dem Kfz selber, die einen herstellerübergreifenden gemeinsamen Standard verwenden sind solche aus der sogenannten On-Board-Diagnose (OBD). Diese beinhaltet Daten hinsichtlich Schadstoffemissionen aber auch solche über das Beschleunigungs-, Geschwindigkeits- und Bremsverhalten des Fahrers. Alle anderen Daten werden, Stand heute, noch in hersteller-spezifischen Formaten und Standards gesichert.[16]

[Rz 20] Nun drängen dazu die ganz GroSSen wie etwa Apple mit eigenen Autoentwicklungen auf den Markt.[17]Aufgrund der Vielzahl verschiedener Systeme und Technologien ist noch nicht abzusehen, welche Technologie sich letztlich durchsetzt. Aus Erfahrung kann jedoch davon ausgegangen werden, dass Apple, Google und Co auch hier in den nächsten Jahren ihren Marktanteil und ihre Marktmacht signifikant ausweiten werden wollen.[18]

[Rz 21] Es gilt also festzuhalten welche Daten in modernen Fahrzeugen erfasst werden können. Zunächst natürlich Bewegungsdaten mittels GPS-Technik über das Navigationsgerät, welches heutzutage standardmäSSig verbaut wird. Erfasst werden Ort und Zeitpunkt, Geschwindigkeit, Haltepunkte, Fahrstrecken und Dauer. Ferner, wie bereits erwähnt, Verhaltensdaten des Fahrers hinsichtlich Beschleunigen, Bremsen, Steuern, Blinken etc.. Dazu kommen Daten über den Zustand des Kfz. Exemplarisch genannt seien Temperatur des Motors und des Innenraums, Reifendruck, Airbag, Klimaanlage und Licht. Daneben sind vor allem Angaben über die Telekommunikationsnutzung zu nennen wie Telefon, Internet und sonstige Informationsabrufe. Von Bedeutung sind ferner Daten zur äuSSeren Umgebung wie AuSSentemperatur, Wetterinformationen, Lichtverhältnisse und Abstandssensorik. Diesbezüglich gesondert zu erwähnen sind Daten zu Personen in der Umgebung des Fahrzeugs, die durch Videokameras erfasst werden könnten. SchlieSSlich können auch Daten zu Mitfahrern beispielsweise über deren Sitzsensorik oder Telekommunikationsnutzung anfallen.[19]

[Rz 22] Nicht zuletzt lassen Videokameras, die in der Fahrerkabine installiert sind, und der Unfalldatenspeicher (UDS) es zu, dass der Fahrzeughalter Umgebungsinformationen und bestimmte Fahrzeugdaten für eigene Zwecke erfasst. Bei einem Unfall speichert der UDS beispielsweise Daten wie Geschwindigkeit, Beschleunigung in Längs- und Querrichtung, Bewegungsrichtung und Bremstätigkeit, die sonst nach wenigen Sekunden überschrieben werden, zwecks Beweissicherung dauerhaft.[20]

---

14 Ebd.

15 Axel Kossel, Auto trifft Handy, 11. Januar 2014, http://heise.de/-2085369.

16 RoSSnagel, SVR 2014, 281 (282).

17 Varinia Bernau, Apple plant angeblich iCar, 16. Februar 2015, http://sz.de/1.2352053.

18 Newsticker Heise, http://heise.de/-2582270.

19 ULD, Zusammenfassung des Arbeitskreis VII vom 52. VGT in Goslar, 30. Januar 2014, https://www.datenschutzzentrum.de/artikel/627-Datenschutz-im-Auto-Kfz-IT-elektronische-Intelligenz-und-praktizierter-Datenschutz.html.

20 Mielchen, SVR 2014, 81 (83).

[Rz 23] Diese Aufzählung hat derweil allenfalls exemplarischen Charakter und wird zukünftig fortlaufend ergänzt werden müssen. Selbst das Smartphone muss wohl eingestehen im Vergleich weniger Daten zu bearbeiten.

4 Beteiligte mit Interesse an Fahrzeugdaten

[Rz 24] Besonders komplex wird die datenschutzrechtliche Situation im Rahmen der Datenverarbeitung in Kfz aufgrund der vielschichtigen Interessen verschiedener Parteien. Folgende Parteien und Stellen sind an der Datenverarbeitung in Kfz direkt oder mittelbar beteiligt:

[Rz 25] Zunächst ist natürlich der Halter selbst zu nennen. Halter ist derjenige, der ein Fahrzeug in eigenem Namen nicht nur vorübergehend auf eigene Rechnung betreibt und die Verfügungsgewalt besitzt, er muss nicht zwangsläufig auch Eigentümer sein.[21] Hinzu kommt der Fahrer, gegebenenfalls samt Insassen wie Familienangehörigen oder Freunden. Fahrer ist der, der das Kfz lenkt und die tatsächliche *Gewalt* über das Steuer hat.[22] Beide haben ein Interesse an der Wahrung ihrer informationellen Selbstbestimmung, dem Grundgedanken des Datenschutzrechtes. Sie wollen wissen, wer was mit «ihren Daten» zu welchen Zwecken beabsichtigt.[23] Ferner der Hersteller des Kfz selbst, er ist Entwickler und leitet den Vertrieb. Für diesen hat er ein Netz aus Vertragshändlern und Vertragswerkstätten aufgebaut. Während der Herstellung ist er es, der die IT in das Fahrzeug einbaut und kann damit auch gröSStenteils entscheidet, welche Daten verarbeitet werden können und sollen.

[Rz 26] Sein Interesse liegt natürlich bei den Daten, die ihm helfen können Fehler bei der Entwicklung zukünftig zu vermeiden, bei solchen, die ihm bei der Wartung der Fahrzeuge helfen und bei denjenigen, die ihm in Gewährleistungsfällen von Nutzen sein können.[24] Ferner zu nennen sind die Hersteller der IT und die der zugehörigen Software und oder Applikationen. Hier kommen natürlich Apple, Google, Facebook und Co. ins Spiel. Sie haben ein Interesse an genauer Analyse, um den Kunden personalisierte Werbung und dergleichen zukommen zu lassen.

[Rz 27] Der Händler selber ist ebenfalls an gewissen Daten interessiert: Er übereignet dem Käufer das Fahrzeug, hat also ebenfalls ein natürliches Interesse an Daten im Rahmen seiner gewährleistungsrechtlichen Haftung oder der Überprüfung des Fahrzeugzustandes. Letzteres kann gerade dann von Bedeutung sein, wenn der Händler im Rahmen eines Kreditkaufes o.Ä. als Eigentümer des Fahrzeuges verbleibt. Auch Daten hinsichtlich einer effektiven Fernüberwachung samt rechtzeitigen Hinweisen auf Inspektion, UnregelmäSSigkeiten, VerschleiSSerscheinungen oder dergleichen können von Belang sein.[25]

[Rz 28] Des Weiteren zu nennen ist der Mobilfunkanbieter, über dessen Netz die Daten übermittelt werden. Andere Verkehrsteilnehmer, unter Umständen auch FuSSgänger, können ebenfalls betroffen sein, speziell hinsichtlich kommunizierender Assistenzsysteme wie Car-2-Car oder Car-2-Pedestrian.[26] Hinzu kommen mögliche sonstige private Parteien wie die Werbewirtschaft und

---

21 BGHZ 116, 200

22 Burmann/HeSS/Jahnke/Janker, StraSSenverkehrsrecht, 23. Auflage 2014, Rn. 3.

23 RoSSnagel, SVR 2014, 281 (282).

24 RoSSnagel, SVR 2014, 281 (281).

25 Ebd.

26 Schulz/RoSSnagel/David, ZD 2012 , 510 (511).

eigene oder fremde Versicherungen.[27] Auch Reiseroutendaten können gerade für Tourismusanbieter sehr wertvoll sein.

[Rz 29] Letztlich zu nennen sind staatliche Behörden wie beispielsweise Polizei, Staatsanwaltschaft oder Finanzamt, aber auch Feuerwehr oder Rettungsleitstellen.[28] Diese Liste lieSSe sich beliebig in allen Bereichen, in denen ein Auto genutzt wird, fortführen.

[Rz 30] Interessant ist dabei aber insbesondere, dass gerade jüngere Fahrer augenscheinlich weniger Probleme mit der Weitergabe ihrer Daten haben, sofern sie davon selber profitieren können. Dies könnte beispielsweise durch Rabatte bei der Kfz-Versicherung geschehen:[29] Die Direktversicherung der Sparkasse hat einen Versicherungstarif getestet, der auf einer Telematiktechnik namens S-Drive basiert; der defensivste Fahrer des Monats erhält eine Prämie.[30]Es ist offensichtlich, dass diese Aufzählung von interessierten Parteien nicht vollständig sein kann; ihrem Zweck wird sie aber gerecht: Es wird deutlich, dass der Wust von Beteiligten mit konträr laufenden Interessen und Belangen höchstes Konfliktpotenzial bietet. Diesen zu entwirren und allen Interessen fair und angemessen gerecht zu werden, ist die elementare Herausforderung.

5 Personenbezogene Daten

[Rz 31] Entscheidend ist die Frage, inwiefern es sich bei den in modernen Fahrzeugen erhobenen technischen Datensätzen um personenbezogene gemäSS §3 Abs. 1 BDSG handelt. SchlieSSlich greift nur dann der Schutz durch das Datenschutzrecht. Die Wirtschaft hat natürlich ein erhebliches Interesse daran möglichst wenigen in einem Fahrzeug produzierten Daten einen Personenbezug zuzugestehen, um nicht an den Datenschutz gebunden zu sein und die Daten umfänglich verarbeiten und verwerten zu können. Personenbezogene Daten sind nach der Legaldefinition des §3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Bestimmt ist die Person, wenn die Daten selbst einen unmittelbaren Rückschluss auf die Identität des Nutzers zulassen. Bestimmbar ist eine Person dann, wenn der Nutzer nicht durch die Daten allein, aber durch zusätzliche Kenntnisse identifiziert werden kann. Dabei kommt es auf das Wissen, die Mittel und die Möglichkeiten der verantwortlichen Stelle im Einzelfall an. Sie muss den Bezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäSSigen Aufwand durchführen können.[31] Persönliche Einzelangaben sind solche, welche sich auf eine bestimmte oder eben bestimmbare natürliche Person beziehen und ihrer Identifikation dienen. Dazu gehören etwa der Name, die Adresse, eine E-Mail-Adresse, Konfession oder der Familienstand. Sachliche Verhältnisse sind dagegen Angaben über einen auf den Betroffenen beziehbaren Sachverhalt.[32]

[Rz 32] Daten, die Verhältnisse betreffen, die keinen Bezug zu einer einzelnen Person haben, sind also keine personenbezogenen Daten. Im Kontext der IT in modernen Fahrzeugen wären das beispielsweise Daten über Verhältnisse oder Zustände wie Entwicklungen von Wetterfronten,

---

27 RoSSnagel, NZV 2006, 281 (281).

28 Mielchen, SVR 2014, 81 (82).

29 ZD-Aktuell 2015, 04541.

30 Kinast/Kühnl, NJW 2014, 3057 (3057); https://www.sparkassen-direkt.de/telematik.

31 Gola/Klug/Körffer, in: Gola/Schomerus BDSG 12. Auflage 2015, §3 Rn. 10.

32 Gola/Klug/Körffer, in: Gola/Schomerus BDSG 12. Auflage 2015, §3 Rn. 2.

Verkehrszeichen oder Hindernisse im StraSSenverkehr. Sogar menschliche Verhältnisse könnten von Daten betroffen sein, aber genügend aggregiert sein, so dass die Identifikation des Einzelnen nicht mehr möglich ist, beispielsweise Informationen über Staus und Verkehrsfluss.[33]

[Rz 33] Andererseits wurde vom VG Ansbach in Bayern der Einsatz von sogenannten Dashcams für unzulässig erklärt.[34] Diese zeichnen das Verkehrsgeschehen rund um die Uhr auf, erfassen also andere Fahrzeuge samt Kennzeichen und auch FuSSgänger. Der Einsatz von solchen Überwachungskameras muss sich an den Grenzen von §6 b BDSG messen lassen, wonach Beobachtung, die öffentlich zugänglicher Räume nur zulässig ist, wenn dies für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Betroffeneninteressen überwiegen. Ferner müssen die Beobachteten über den Umstand der Aufzeichnung und die entsprechende Verantwortlichkeit benachrichtigt werden, was letztlich logischerweise regelmäSSig nicht erfüllt werden kann.[35]

[Rz 34] Darüberhinaus könnte das Kfz-Kennzeichen oder die Fahrzeug-Identifizierungsnummer gegebenenfalls zu einem identifizierbaren Faktor im Sinne des §39 Absatz 1 StVG werden.[36]

[Rz 35] Als nicht personenbezogen gelten anonymisierte bzw. pseudonymisierte Daten nach §3 Abs. 6 BDSG bzw. nach §3 Abs. 6a BDSG. Von anonymisierten Daten kann dann gesprochen werden, wenn personenbezogene Daten derart verändert werden, dass ein unverhältnismäSSiger zeitlicher und oder technischer Aufwand von Nöten ist, um den Bezug zu einer natürlichen Person herstellen zu können.

[Rz 36] Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschlieSSen oder wesentlich zu erschweren. Daten werden dabei mittels einer Zuordnungsvorschrift dahingehend verändert, dass die Einzelangaben ohne Kenntnis eben jener Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können.[37] Pseudonyme Daten werden also für den Kenner der Zuordnungsregel unter Umständen zu personenbeziehbaren Daten, für alle anderen bleiben sie nicht personenbeziehbare, also anonyme Daten.[38] Die Bewertung eben dieses Kriteriums wird in Zukunft von entscheidender Relevanz sein: Eine Kfz-Werkstatt kann mit der entsprechenden Diagnose- und Messtechnik auf die IT im Fahrzeug eines Kunden zugreifen, der bereits in der Kundenkartei hinterlegt ist; ein Autohersteller, der sich mit seinem Kunden neben dem Kaufvertrag über das Fahrzeug auch über den Abschluss eines sogenannten Assistancevertrag geeinigt hat und dadurch die Person identifizieren kann.[39] Bei der Pseudonymisierung besteht zwar regelmäSSig ein gewisses Re-Identifizierungsrisiko, einem solchen kann jedoch effektiv entgegengewirkt werden, wenn die Identifikatoren zügig gelöscht werden und faktisch eine Anonymisierung eintritt, sodass die spätere Zuordnung nicht mehr möglich ist.[40] Hierin können wichtige Lösungsansätze gesehen werden, um einen Interessensausgleich herstellen zu können.

---

33 RoSSnagel, NZV 2006, 281 (282).

34 VG Ansbach, Urteil vom 12. August 2014 — Az. 4K1301634.

35 Weichert, SVR 2014, 241 (246).

36 Weichert, SVR 2014, 201 (204).

37 Gola/Klug/Körffer, in: Gola/Schomerus BDSG 12. Auflage 2015, §3 Rn. 45.

38 RoSSnagel/Scholz, MMR 2000, 721 (724); RoSSnagel, NZV 2006, 281 (281).

39 Michael Kamps, Das vernetzte Auto als Herausforderung für den Datenschutz, http://www.cms-hs.com/NewsMedia/Press_Coverage/Documents/IV_201402_Datenschutz.pdf.

40 Weichert, SVR 2014, 201 (205, 206).

6 Zuordnung von Daten

[Rz 37] Schon jetzt entsteht erster Streit, wem die Daten «gehören» sollen bzw. wer den Zugriff darauf für sich beanspruchen darf.[41] Zu klären gilt es also, inwiefern unsere Rechtsordnung eine Zuordnung von Daten vornimmt.

[Rz 38] In Betracht kommen vor allem sachenrechtliche Überlegungen und eine datenschutzrechtliche Zuordnung.

[Rz 39] Das Sachenrecht regelt die dinglichen Rechte an Sachen.

[Rz 40] Daten als solche sind als immaterielle Informationen zunächst de lege lata nicht eigentumsfähig im Sinne des §903 des Bürgerlichen Gesetzbuches (BGB).[42] Es fehlt ihnen an der Sacheigenschaft nach §90 BGB hinsichtlich der Körperlichkeit. Es gibt mögliche Ansätze, eine Eigentumsfähigkeit von Daten zu konstruieren, etwa über eine Analogie zu §303a des Strafgesetzbuches (StGB).[43] Allerdings haben sich solche Gedanken bezüglich eines Datenschutzes auch über das klassische Zivilrecht noch nicht durchgesetzt und bleiben umstritten.[44]

[Rz 41] Dingliche Rechte können also nur an den Datenträgern selber als körperliche Gegenstände bestehen, etwa am Bordcomputer. Zöge man in Betracht, dass der Verkäufer bei der VeräuSSerung eines Fahrzeugs versuchen würde, sich Besitzrechte im Sinne des §868 BGB als mittelbarer Besitzer oder gar als Eigentümer im Sinne des §903 BGB an der IT an Bord vorzubehalten, was beispielsweise theoretisch bei Datenträgern als nicht wesentliche Bestandteile eines Kfz im Sinne des §93 BGB möglich wäre, würde dies jedoch nicht das Recht begründen in dieser personenbezogene Daten zu speichern und / oder zu verarbeiten. Dies ist eben allein aufgrund eines Erlaubnistatbestands des Datenschutzrechts zulässig. Das Eigentum oder der Besitz an Datenträgern im Fahrzeug selber kann also letztlich nicht dazu führen, dass der Eigentümer diese Daten verwenden, verarbeiten oder nutzen darf.[45]

[Rz 42] Das Datenschutzrecht besitzt also eine eigene Struktur auf einer anderen Ebene als das Sachenrecht, zwecks Würdigung des immateriellen Charakters. Es richtet sich an die verantwortliche Stelle im Sinne des §3 Abs. 7 BDSG und soll den Betroffenen im Sinne des §3 Abs. 1 BDSG schützen. Verantwortliche Stelle ist nach der Legaldefinition jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Betroffener sind nach dem Gesetz die natürlichen Personen, die für die verantwortliche Stelle durch die Informationen aus den Daten zuordenbar werden. Aufgrund der verschiedenen Interessen der einzelnen beteiligten Parteien verändert sich das klassische Gegenüberstellen von einer verantwortlichen Stelle und einem Betroffenen: Durch die diversen Kommunikationspartner erhöht sich schlieSSlich die Komplexität der Rechtsbeziehungen zwischen den einzelnen Beteiligten in jeweils veränderter Funktion, was einen der wesentlichen Problemfaktoren darstellt.[46]

---

41 Newsticker Heise.de, http://heise.de/-2576824.

42 Fritzsche, Beckscher Onlinekommentar, §903 Rn. 10.

43 Hoeren, MMR 2013, 486 f.

44 Dorner, CR 2014, 617 f.

45 RoSSnagel, SVR 2014, 281 (283).

46 Weichert, SVR 2014 201 (202).

7 Datensparsamkeit und Transparenz

[Rz 43] Unabhängig von der Frage welche Datennutzung im Einzelfall materiell-rechtlich zulässig ist oder nicht ergibt sich aus §3 a BDSG ein entscheidender Grundsatz: Alle Arten der Datenverarbeitung, welcher Art auch immer, müssen sich dem Ziel der Datenvermeidung und der Datensparsamkeit andienen. Es sind also so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.[47] Der Grundsatz der Datensparsamkeit ist nicht nur im deutschen Datenschutzrecht verankert, sondern ergibt sich auch aus Art. 8 der Charta der Grundreche der Europäischen Union und hat damit immenses Gewicht. Für Verkehrsteilnehmer als potenziell Betroffene sollte also die Möglichkeit bestehen bleiben durch technische Neuheiten im Bereich von modernen Fahrzeugen, wie durch verbesserte Navigation, gesteigerte Sicherheit und mehr Unterhaltungsangebote, erhöhten Komfort und Flexibilität nutzen zu können, ohne zu wissen, dass sie auch mit den durch ihr Verhalten erzeugten Daten bezahlen. Technischer Fortschritt darf also nicht zu einer Selbsteinschränkung führen, es muss möglich sein auch mit neuer IT möglichst anonym unterwegs zu sein. Im Sinne dieses Grundsatzes soll und muss durch technische Mittel von den Möglichkeiten der bereits angesprochenen Anonymisierung und Pseudonymisierung Gebrauch gemacht werden. Im Übrigen genügen diesen Anforderungen auch Techniken bei denen die Daten zeitig oder sofort gelöscht werden und nicht langfristig gespeichert werden.[48]

[Rz 44] Daneben ist der Grundsatz der Transparenz als eine weitere tragende Säule des Datenschutzrechts, gerade aufgrund der Vielschichtigkeit von datenschutzrechtlichen Fragen im Kontext von IT in Fahrzeugen entscheidend. Das Prinzip Transparenz umschreibt den Anspruch, dass jeder von Datenverarbeitung Betroffene wissen soll, dass Daten über ihn erhoben werden. Er soll wissen, welche Daten zu welchem Zweck bei welcher Stelle für wie lange und aus welchem Grund gespeichert werden. Beim Kauf eines neuen Fahrzeugs mit moderner IT sollte der zukünftige Halter beispielsweise rundum aufgeklärt werden. Allein auf diese Art und Weise kann das informationelle Selbstbestimmungsrecht und damit letztlich die Wahlfreiheit eines jeden Einzelnen gesichert werden. Zu einem solchen Ergebnis kommt auch der 52. Verkehrsgerichtstag in Goslar in seinen Empfehlungen, wenn er höchste Aufklärungspflichten auf Seiten der Fahrzeughersteller und der Dienstleister beim Vertragsabschluss fordert.[49]

8 Profilbildung und eCall

[Rz 45] Eine der gröSSten Sorgen von Nutzern, Kunden und Datenschützern ist die vor einer Profilbildung mit der für jeden Einzelnen individuell Raster und Muster hinsichtlich Bewegungs-, Nutzungs- oder Kommunikationsdaten anzulegen, auch wenn es sich dabei im Rahmen von modernen Kfz noch um eine verhältnismäSSig frische Praxis handelt.[50] Auch der Thüringer Landesdatenschutzbeauftragte *Hasse* warnt in diesem Kontext vor einer sogenannten Profilbildung.[51]

[Rz 46] Werden alle verschiedenen in einem Fahrzeug erhobenen Daten effektiv zusammenge-

47 Weichert, DuD 1996, 79 f.

48 Weichert, SVR 2014, 201 (206).

49 Empfehlungen des 52. VGT in Goslar 2014, http://www.deutscher-verkehrsgerichtstag.de/images/empfehlungen_pdf/Gesamt_Empfehlungen_52._VGT_2014.pdf.

50 Weichert, SVR 2014, 241 (241).

51 Becklink 1030799.

führt und kombiniert, ist es möglich, einen überaus umfangreichen und detailgetreuen Überblick über Fahrverhalten und auch Lebensroutine entstehen zu lassen, besonders unterstützt durch den Umstand, dass IT heutzutage ständig mit dem Telekommunikationsnetz verbunden ist.[52] Eine Vorstellung die doch recht beängstigend sein kann, gerade weil man sich das eigene Auto eben noch als privaten Rückzugsort vorstellt. Dazu kommt der Umstand, dass ab 2018 neue Autos in Europa mit der sogenannten eCall-Technik ausgerüstet werden müssen. Eine Technik, die im Falle eines Unfalls erste Daten an Rettungskräfte übermittelt und diese gleichzeitig alarmiert.[53] Ein System, das sicher zu einem verbesserten und effizienteren Umgang mit gefährlichen Unfallsituationen seitens der Rettungskräfte führen wird und im wahrsten Sinne des Wortes Leben retten kann: Mit eCall soll es möglich sein die Zeit bis zum Eintreffen der Rettungskräfte zu verkürzen.[54]

[Rz 47] Trotz dieser Vorteile gilt es nicht zu vergessen, dass die Technik zur Überwachung mit eCall ins Fahrzeug verbaut wird: Spätestens mit eCall beginnt technisch das Zusammenwachsen von Kfz und Internet.[55] Es ist schlieSSlich technisch möglich aus der vorhandenen eCall-Technik eine bCall-Technik, also eine Businesstechnik, werden zu lassen. Bedenklich ist zudem der Umstand, dass im Rahmen des Art. 20 der geplanten DS-GVO das Profiling ausdrücklich unter den Einwilligungsvorbehalt des Betroffenen gestellt wird. Ein Umstand, der zumindest nicht mit der Ansicht des Bundesverfassungsgerichts einhergeht, das schon vor einiger Zeit eine Gefährdung von Persönlichkeitsrechten durch die Bildung von Persönlichkeitsbildern erkannt hat und ein sogenanntes Verbot von Totalbildern ausgegeben hat.[56] Auch wenn dieses Urteil eine Verobjektivierung des Einzelnen durch den Staat verhindern soll, kann und muss eine gewisse Wertigkeit dieser Aussage auch für das Verhältnis zwischen Privaten verstanden werden.

[Rz 48] Festhalten lässt sich also, dass eCall als Rettungstechnik wünschenswert ist, aber nicht vergessen werden sollte, dass damit der «gläserne Fahrer» ein Stück näher kommt und auch Missbrauchsmöglichkeiten mit erheblichen wirtschaftlichen Potenzial bestehen.[57] Immerhin erläutert die europäische Kommission in Erwägungsgrund 8 des Vorschlages zur Regelung der neuen eCall-Systeme, dass «das Recht aller Interessenträger, zum Beispiel von Fahrzeugherstellern und unabhängigen Anbietern, unberührt (bleibt), zusätzliche Notfalldienste und/oder *Dienste mit Zusatznutzen* parallel oder aufbauend auf dem bordseitigen 112-eCall-System anzubieten».[58] Es ist keine fadenscheinige Interpretation, wenn man davon ausgeht, dass die Kommission durch die Einführung von eCall zumindest auch eine technologische Infrastruktur aufbauen möchte, auf der in Zukunft auch andere Anwendungen oder Dienste aufbauen könnten.[59]

---

52 RoSSnagel, NZV 2006, 281(284).

53 Haupt, Vom Auto verraten, Zeit 6. Dezember 2013, http://www.zeit.de/mobilitaet/2013-12/auto-datenschutz-elektronik.

54 Kinast/Kühnl, NJW 2014, 3057 (3057).

55 Weichert, Kfz-Notfallsystem eCall — Möglichkeiten und Versuchungen, https://netzpolitik.org/2014/thilo-weichert-kfz-notfallsystem-ecall-moeglichkeiten-und-versuchungen/.

56 Beschluss des Bundesverfassungsgerichts vom 16. Juli 1969, BVerfGE 27, 1 (3).

57 Mielchen, SVR 2014, 81 (81).

58 EU-Kommission, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282013%290316_/com_com%282013%290316_de.pdf.

59 Weichert, SVR 2014, 241 (245).

9 Spannungsverhältnis

[Rz 49] Vorläufig muss man zu dem Zwischenergebnis kommen, dass das «big data»-Zeitalter im Kontext des Autos angekommen ist und damit auch alle seine Chancen und Risiken. Der Grundsatz der Datensparsamkeit steht in einem diametralen Widerspruch zur unternehmerischen Wirklichkeit.

[Rz 50] Unternehmen müssen allein aus rein wirtschaftlichen Gesichtspunkten im Zeitalter der Industrie 4.0 versuchen, ihr Kundenpotenzial voll auszuschöpfen. Dazu brauchen Sie Daten und sind nicht bereit zu teilen.[60] Gerade hier wird der Unterschied im Umgang mit Daten zwischen Deutschland bzw. Europa auf der einen und den USA — wo dem Speichern von Daten rechtlich kaum Schranken entgegenstehen — auf der anderen Seite deutlich. Auch Versuche der Europäischen Union, einen Datenaustausch zwischen deutschen und nordamerikanischen Unternehmen zu ermöglichen und trotzdem datenschutzrechtliche Mindeststandards einzuhalten, sind mit der Safe Harbour Entscheidung der europäische Kommission aus datenschutzrechtlichen Gesichtspunkten mehr oder minder gescheitert, weil sich vor allem amerikanische Nachrichtendienste de facto nicht um so etwas kümmern.[61] Dadurch können europäische Fahrzeugunternehmen am globalen Markt einen Wettbewerbsnachteil bei der modernen Datenanalyse erleiden. Der Widerspruch wird dann klar, wenn Bundesjustizminister *Maas* mahnt, dass die Hersteller sich an die Grundsätze des Datenschutzes halten sollen, aber auf der anderen Seite *Dieter Kempf*, Präsident des Branchenverbandes BITKOM, leicht ironisch festhält, man könne nicht bei allem Neuen einen verlässlichen Rahmen haben, sonst würde man einen Teil der Zukunft verpassen.[62]

[Rz 51] Auf der anderen Seite kann effektiver Datenschutz auch eine Chance für die hochangesehene deutsche Automobilindustrie bieten. Gerade bezüglich der in den letzten Jahren gestiegenen öffentlichen Sensibilität für Datenschutz von Politik und Verbraucherseite müssen Hersteller von Fahrzeugen und Anbieter von IT-Anwendungen rund ums moderne Fahrzeug allein aus Eigeninteresse für eine direkte Kommunikation mit dem Kunden einstehen, versuchen, nur nötige Daten zu erheben und Wahlmöglichkeiten hinsichtlich der Intensität der Datenerfassung anzubieten.[63]

10 Lösungsansätze

[Rz 52] Ziel von Ansätzen muss es sein, das Recht der informationellen Selbstbestimmung der Betroffen weit möglichst zu schützen und sich gleichzeitig nicht systematisch gegen neue Systeme zu stellen und damit etwa technologisch ins Hintertreffen zu geraten. Von effizienter Datenauswertung kann der Kunde mittelfristig schlieSSlich wieder selber profitieren etwa durch besser abgestimmte IT-Systeme und Produkte. Nichtdestotrotz besteht natürlich ein faktisches Übergewicht zugunsten der Unternehmensseite, seien es die Autohersteller oder eben Apple, Google und Co. Diesem muss die Politik angemessen entgegenwirken.

---

60 Newsticker Heise.de, http://heise.de/-2576824.

61 Wendt/Beuth, Angriff auf Safe Harbour, Zeit 24. März 2015, http://www.zeit.de/digital/datenschutz/2015-03/eugh-facebook-safe-harbor-max-schrems.

62 Newsticker Welt.de, http://www.welt.de/newsticker/dpa_nt/infoline_nt/computer_nt/article137298432/Maas-mahnt-Datenschutz-bei-vernetzten-Autos-an.html.

63 Michael Kamps, Das vernetzte Auto als Herausforderung für den Datenschutz, http://www.cms-hs.com/NewsMedia/Press_Coverage/Documents/IV_201402_Datenschutz.pdf.

[Rz 53] Vielversprechende Möglichkeiten werden in den Ansätzen «privacy by design» und «privacy by default» gesehen. Mit ersterem ist ein Ansatz gemeint, bei dem bereits bei der Grundkonzeption neuer Entwicklungen von Hard- und Software mögliche Probleme im datenschutzrechtlichen Kontext herausgearbeitet, beachtet und in die Konzeption eingearbeitet werden sollen. Dadurch kann vermieden werden, dass Datenschutzprobleme erst im Nachhinein aufwendig analysiert und behoben werden müssen. «Privacy by design» verfolgt ebenfalls das Ziel, dass der Umfang der personenbezogenen Daten im Sinne des Grundsatzes der Datensparsamkeit möglichst reduziert wird.

[Rz 54] Trotzdem können Unternehmen durch das Anonymisieren und Pseudonomysieren Daten in groSSem Umfang erheben. Diese können anschlieSSend zwar nicht individuell für jeden Einzelnen ausgewertet werden, dennoch kann das Verhalten der Kunden im eigenen Interesse analysiert werden. «Privacy by default» beschreibt den verbundenen Ansatz, dass Voreinstellungen bei Hard- und Software so eingestellt sind, dass zunächst ein datenschutzrechtlicher Grundschutz besteht. Vereinfacht gesprochen kann man «privacy by design» als «Datenschutz durch Technik» und «privacy by default» als «datenschutzfreundlichen Voreinstellungen» verstehen.

[Rz 55] Diese beiden Ansätze werden insbesondere dem Umstand gerecht, dass die meisten Internetnutzer, sei es auf dem Laptop, dem Smartphone oder eben im Auto, keine IT-Spezialisten sind und sich für Technik, solange sie ordnungsgemäSS funktioniert, nicht sonderlich interessieren. Gesetzt den Fall «privacy by design und «privacy by default» würden sich auf breiter Ebene durchsetzen, würden eben diese Nutzer erstmal einem gewissen Grundschutz unterworfen. Sie könnten nach umfassender Aufklärung seitens der jeweiligen Anbieter gegebenenfalls in eine weitere Verarbeitung und Nutzung einwilligen, was wiederum einem hohen MaSS von notwendiger Transparenz gerecht werden. Die European Union Agency for Network and Information Security (ENISA) hat in diesem Zusammenhang Mitte Januar einen höchstinteressanten Bericht veröffentlicht: Darin will sie eine Brücke zwischen dem rechtlichen Rahmen des Datenschutzes auf der einen Seite und den technischen Möglichkeiten auf der anderen Seite schlagen. Laut ENISA gibt es die technische Möglichkeit, die interessanten Daten mit Rauschdaten ohne inhaltlichen Wert zu ergänzen, bestimmte Eigenschaften zu unterdrücken oder Datengruppen zu erstellen. Ferner kann mittels kryptografischer Technik, die die inhaltlich interessante Werteverteilung der Daten erhält, ein Rückschluss auf bestimmbare Personen allerdings unmöglich gemacht werden.[64] Diese hochkomplizierten Techniken sind bis jetzt nur bestimmten Expertengruppen bekannt, nicht aber Politik und breiter Öffentlichkeit.[65] Ein Aufnehmen dieser Ansätze unter den Stichwörtern «privacy by design» und «privacy by default» in die breite Diskussion und auch in die Ausarbeitung der aktuell geplanten und verhandelten DS-GVO kann groSSes Lösungspotenzial bieten und das nicht nur im Kontext von vernetzten Fahrzeugen. Die Autobranche könnte sich auch im Sinne des §38 a BDSG auf gemeinsame Verhaltensregeln in dieser Hinsicht — unter angemessener Berücksichtigung des Datenschutzes — einigen und so der legislativen Entwicklung sinnvoll vorgreifen.[66] Es ist also zu konstatieren, dass die Lage nicht hoffnungslos ist und Lösungsansätze durchaus bestehen; sie müssten also nur aufgegriffen werden, um einen

64 ENISA, Privacy and Data Protection by Design, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.

65 Schulzki-Haddouti, Die EU wurschtelt sich zur GroSSreform, Zeit 12. März 2015 http://www.zeit.de/digital/datenschutz/2015-03/datenschutzverordnung-zweckbindung-datensparsamkeit.

66 Weichert, SVR 2014, 241 (247).

angemessen Ausgleich herstellen zu können.

11 Fazit und Ausblick

[Rz 56] Der Widerspruch zwischen den beteiligten Interessen ist offensichtlich, aber wie wird in Zukunft damit umgegangen? Das BDSG hilft nicht immer: Wie geht man mit diesen neuen vielschichtigen Zusammenhängen bei modernen vernetzten Autos um? Braucht man ein neues bereichsspezifisches Datenschutzrecht für moderne Fahrzeuge? Abzuwarten bleibt die Entwicklung hinsichtlich der dogmatisch komplexen Frage nach der Eigentumsfähigkeit von Daten. Die wissenschaftliche Diskussion zu diesem Thema steht noch am Anfang, eine Tendenz ist noch nicht absehbar.

[Rz 57] Das Eigentum an körperlichen Gegenständen, wie etwa den datenverarbeitenden technischen Komponenten in einem modernen Fahrzeug, kann allein keine Nutzungsrechte nach §903 BGB bezüglich Daten begründen. Dafür ist, Stand heute, eben das Datenschutzrecht auf einer anderen Ebene zuständig.

[Rz 58] Seit 2014 wird im Ministerrat von den Mitgliedsstaaten über die DS-GVO verhandelt, eine Einigung soll im kommenden Sommer in Zusammenarbeit mit der Kommission und dem Parlament folgen.[67] Als Verordnung wird dieses Gesetz in der ganzen EU gemäSS Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unmittelbar geltendes Recht, besitzt also eine immense Bedeutung.

[Rz 59] BegrüSSenswert ist es, dass unter dem voraussichtlichen Art. 23 DS-GVO die Ansätze zu «privacy by design» und «privacy by default» aufgenommen werden sollen, obwohl die Formulierungen doch recht schwammig sind und zumindest noch nicht über einen Programmsatz hinausgehen.

[Rz 60] Durchaus kritisieren kann man allerdings, dass laut einem von statewatch.org geleakten Positionspapier die Grundsätze von Zweckbindung und Datensparsamkeit geschwächt werden sollen.[68] Dieser Umstand kann auf das möglicherweise massive Lobbying von Seiten der führenden IT-Unternehmen aus den USA zurückzuführen sein.[69] Die Frage ist schlieSSlich die Folgende: Muss im Zeitalter von «big data» zwangsläufig eine Entscheidung zwischen bürgerfreundlichem, starken Datenschutz oder wirtschaftsfreundlichem, einfachen Datensammeln ohne Zweckbindung stattfinden? Gibt es nicht die Möglichkeit eines Kompromisses?

[Rz 61] Ansätze wie eben «privacy by design» oder «privacy by default», sofern von Anfang der Entwicklung bis zur Produktion beachtet, können und sollten als datenschutzrechtliche Infrastrukturverbesserung die vielversprechendsten Lösungsmöglichkeiten sein, um den Fahrern und Haltern die möglichst gröSSte Sicherheit anbieten zu können und den an den Fahrzeugdaten interessierten Stellen trotzdem Daten zu Analysezwecken zuzugestehen. Entscheidend ist dennoch, dass der Grundsatz der informationellen Selbstbestimmung, wonach der Einzelne selbständig entscheidet innerhalb welcher Grenzen er persönliche Sachverhalte offenbart, nicht untergraben

[67] Schulzki-Haddouti, Die EU wurschtelt sich zur GroSSreform, Zeit 12. März 2015 http://www.zeit.de/digital/datenschutz/2015-03/datenschutzverordnung-zweckbindung-datensparsamkeit.

[68] Statewatch.org, http://statewatch.org/news/2015/feb/eu-council-dp-reg-chapII-17072-rev3-14.pdf.

[69] Dazu: Jan Philipp Albrecht, http://www.janalbrecht.eu/themen/datenschutz-und-netzpolitik/lobbyismus-zur-eu-datenschutzreform.html.

werden darf.[70]

Max von Schönfeld, ITM/Münster, Wissenschaftlicher Mitarbeiter im ABIDA-Forschungsprojekt.

[70] Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983, BVerfGE 65, 1 (42 f.).