TECHNISCHE HOCHSCHULE NÜRNBERG
GEORG SIMON OHM

Big Data als datenschutzrechtliche Herausforderung für eine vernetzte Automobilwelt

Masterarbeit zur Erlangung des akademischen Grads „Master of Laws (LL.M.)“

Eingereicht von: **Magdalena Nowak**

Matrikelnummer: [redacted]

Sommersemester 2017

Erstprüfer: **Prof. Dr. Roland Gegner**

Zweitprüfer: **RA Oliver Baumbach**

DANKSAGUNG

An dieser Stelle möchte ich mich bei allen Personen bedanken, ohne deren Hilfe die Anfertigung dieser Arbeit nicht möglich gewesen wäre.

„Sie müssen für Ihr Thema Feuer fangen“, war der prägendste Satz des Herrn Prof. Dr. Gegner zu Beginn der Arbeit. Gemeinsam mit RA Oliver Baumbach, stellv. Geschäftsführer der IHK Nürnberg für Mittelfranken, kristallisierte sich Big Data als datenschutzrechtliche Herausforderung für eine vernetzte Automobilwelt als ein sehr aktuelles und spannendes Thema heraus, mit welchem das Feuer gefangen wurde. Die zahlreichen konstruktiven Gespräche waren sowohl auf sachlicher, als auch persönlicher Ebene bereichernd und werden stets in guter Erinnerung behalten. Seiner kritischen Auseinandersetzung mit diesem Thema, der Durchsicht der Arbeit und seiner Unterstützung gilt mein großer Dank.

Auch Florian Wenzel möchte ich meinen tiefsten Dank aussprechen. Sein fachliches Wissen rund um das Automobilhaus stand mir jederzeit zur Verfügung. Im gemeinsamen Interview konnte ich fundierte Informationen für das Anfertigen dieser Arbeit gewinnen. Auch auf persönlicher Ebene gilt dieser Dank. Sein Engagement, eigene Motivation und Geduld, diese Arbeit vollendet zu sehen, gaben mir Halt in schweren Zeiten, neue Kraft und motivierten mich stets, auch wenn das Licht am Ende des Tunnels noch weit erschien.

Ebenso möchte ich Markus Rehm danken. Die Motivation, welche ich erhielt, war stets aufbauend und nur durch seine Unterstützung konnte der Fokus zu 100% auf der Arbeit liegen.

Für das Korrekturlesen möchte ich mich insbesondere bei RA Johannes Link und meiner Mutter Dorota Nowak bedanken – wo Zeit das wertvollste Gut ist, wurde mir ein Teil davon geschenkt. Danke dafür.

Meinen Freunden, den Kolleginnen und Kollegen am Volkswagen Zentrum Nürnberg-Marienberg gilt mein Dank, die für meine Situation stets Verständnis hatten und Geduld zeigten, als die Arbeit der Mittelpunkt der letzten Monate für mich gewesen ist.

Inhaltsverzeichnis

„Nichts ist so beständig wie der Wandel.“
Heraklit von Ephesus.

1. Einleitung

In der heutigen Gesellschaft gehört Digitalisierung zu den prägendsten Entwicklungen der Moderne. Kaum ein Lebensbereich, ob privat oder öffentlich, wird nicht von digitalen Systemen beeinflusst. Die größten Fortschritte lassen sich in der Medizintechnik, dem privaten Wohnhaus sowie in der individuellen Mobilität feststellen. Insbesondere bei Letzterem lässt sich der Fortschritt erkennen. Über 45 Millionen Fahrzeuge sind im Jahre 2016 in Deutschland angemeldet worden.[1] Während das Fahrzeug noch vor 50 Jahren einzig dem Zweck diente, seinen Halter schnell und effizient von einem an den anderen Ort zu bringen, hat sich das heutige Auto zu einem stetigen Begleiter entwickelt, welches dem Fahrer ein hohes Maß an Sicherheit und Bequemlichkeit bieten soll.

Um dieses Ziel zu erreichen, ist es unumgänglich für Automobilhersteller, einerseits elektronische Bestandteile in das Fahrzeug zu verbauen und andererseits mit elektronischen Geräten zu verknüpfen. Eine stetige technologische und mobile Weiterentwicklung führt dazu, dass das Auto bereits heute als der „ultimative mobile Computer“[2] angesehen werden darf und mit dessen Hilfe die gesammelten Informationen auch zukünftig Einfluss auf die verschiedensten Lebensbereiche nehmen kann. Eine Vernetzung von alltäglichen Gegenständen findet derzeit bereits im vollen Umfang statt und ermöglicht neue Geschäftsmodelle: So ist es für das vernetzte Automobil, anhand personalisierter Smartphones einzelner Familienmitglieder, möglich zu erkennen, wer in das Fahrzeug steigt. Anhand der Applikation des Stundenplans auf dem Handy des Schulkindes wird sogleich die Route zur Schule berechnet und angezeigt. Zeitgleich wird dem Fahrzeug durch den vernetzten Kühlschrank signalisiert, dass Lebensmittel fehlen. Eine alternative Route, welche über den gewohnten Supermarkt in der Nähe führt, wird nunmehr angezeigt. Ein weiteres Signal meldet, dass eine dritte Person in der Nähe eine

[1] Statistik gemeldete Fahrzeuge, siehe URL 1.
[2] so: Huang, Jen-Hsun, Chef des Chip-Herstellers Nvidia auf der CES Elektronikmesse, 2014.

Mitfahrgelegenheit zu einem Ziel sucht, welches sich auf der eigenen Route befindet. Der Fahrer kann nun auf dem Fahrzeugdisplay bestätigen oder ablehnen, ob er die Person mitnehmen möchte. Willigt diese ein, so werden automatisch eine Antwort, sowie eine ungefähre Ankunftszeit an den Suchenden gesendet.[3]

Diese grundlegende, weltweite Vernetzung führt unumgänglich dazu, dass Daten erhoben und gesammelt werden, weshalb der Schutz dieser immer mehr an Bedeutung gewinnt. Gleichzeitig wird hier die Frage eröffnet, wie und inwieweit sich das geltende Datenschutzrecht weiter entwickeln muss, um sich dem schnell voranschreitenden digitalen Fortschritt anzupassen, damit der Verbraucher bestmöglich geschützt ist.

1.1 Problemstellung

Jeder Mensch hinterlässt eindeutige Datenspuren[4], deren Tragweite jedoch für viele nicht absehbar ist. Das derzeit (noch) geltende Bundesdatenschutzgesetz hat sich dem Ziel verschrieben, die Daten von natürlichen Personen im Rahmen seines Persönlichkeitsrechts bestmöglich zu schützen.

Das BDSG wurde im Jahre 1977 erstmalig verabschiedet und vielfach novelliert. Ein Flickenteppich aus zahlreichen Neuerungen mit welchen der Gesetzgeber versucht, mit der rasanten Entwicklung im Bereich der Digitalisierung Stand zu halten. Nunmehr hat die Europäische Union am 27.04.2016 die Verordnung 2016/679 (Datenschutzgrund-VO) erlassen, welche einheitlich in allen Mitgliedsstaaten der EU ab Mai 2018 gelten wird. Jedoch weißt auch diese neue Verordnung bereits Regelungsdefizite auf.

Big Data ist bereits seit vielen Jahren in aller Munde und beschäftigt insbesondere Datenschützer und die freie Wirtschaft und stellt sowohl

[3] Gulde, Daten im Auto , 5/2017, S. 46.
[4] Broers/Pauls, Datenspuren, siehe URL 2.

deren Anwender als auch deren Anbieter vor neue Herausforderungen, welche sich mit einer veralteten Rechtslage auseinander setzen müssen.[5]

Wie bereits erwähnt befindet sich die Automobilbranche derzeit in einem starken Wandel und fraglich ist nunmehr, welche datenschutzrechtlichen Probleme in dieser vernetzten Automobilwelt auftreten können, ob das Datenschutzrecht diese erfolgreich beheben kann und ob weiterhin Defizite bestehen bleiben.

1.2 Aufbau der Arbeit

In der Wirtschaft ist der Begriff Big Data nicht mehr wegzudenken. Die Bedeutung von Big Data und ihre Auswirkung auf zahlreiche Bereiche soll im ersten Kapitel näher erläutert werden.

Vor allem die Automobilindustrie kann mit Hilfe von Big Data revolutioniert werden. Dieses Kapitel soll aufzeigen, wie Big Data als tragendes Element für die Vernetzung der Automobilwelt dienen kann.

Trotz aller Vorteile, die Big Data bieten kann, sollen ferner auch mögliche Risiken und negative Auswirkungen auf Marktteilnehmer erörtert werden.

Das zweite Kapitel beschäftigt sich ausführlich mit Neuerungen im Fahrzeug, welche bereits jetzt, aber auch erst in naher Zukunft verfügbar sein werden. Anhand bekannter deutscher Automobilmarken wie Volkswagen, Audi und BMW u.a. wird aufgezeigt, wie fortschrittlich die Entwicklung bereits im Bereich der Vernetzung ist.

Aufgeführte Beispiele verdeutlichen das Ausmaß der bestehenden Vernetzung. Auch Drittanbieter[6] erkennen mittlerweile das Potential der Smartifizierung des Fahrzeuges und nutzen dies für den eigenen Unternehmenserfolg.

Grundlage einer vernetzten Automobilwelt ist eine Verfügbarkeit und Analysierung von Daten. Das dritte Kapitel beschäftigt sich mit der Frage, ob eine eigentumsrechtliche Zuordnung von Daten möglich ist. Dieses

[5] Ohrtmann/Schwiering, NJW, 2014, S. 2984.
[6] In diesem Zusammenhang: Unternehmen, welche zunächst keinen direkten Bezug zur Automobilbranche vermuten lassen.

Kapitel erörtert mögliche Konflikte hinsichtlich einer rechtlichen Zuordnung und deren Konsequenzen.

Das vierte Kapitel greift die Fragestellung auf, inwieweit das derzeit geltende Datenschutzrecht Schutz bietet. In diesem Kapitel werden die wichtigsten Normen des Bundesdatenschutzgesetzes im Hinblick auf die Automobilindustrie dargestellt.

Weiterhin soll in diesem Kapitel auf bestehende datenschutzrechtliche Defizite eingegangen werden. Die rasante Entwicklung der informationellen Technologien führt unweigerlich zu der Annahme, dass das geltende Recht veraltet ist und nicht den Anforderungen entspricht, welche im Rahmen von Big Data mittlerweile erforderlich sind.

Das Ziel zahlreicher namhafter Automobilhersteller ist die Perfektionierung der Herstellung eines vollständig autonom fahrenden Fahrzeuges. Das fünfte Kapitel beschäftigt sich mit der Fragestellung, wie die Haftung im Schadensfall geregelt werden kann und wo explizite Regelungen getroffen werden müssen.

Das letzte Kapitel stellt einen Ausblick auf die Verordnung der Europäischen Kommission dar, welche im Jahr 2018 hierzulande in Kraft treten wird.

Im Hinblick auf den stetigen technologischen Fortschritt in der Automobilindustrie werden in diesem Kapitel die wichtigsten Änderungen aufgezeigt, sowie Fortschritte und Defizite im Vergleich zum Bundesdatenschutzgesetz.

2. Big Data

2.1 Begriff von Big Data

Big Data erhält zunehmend Einzug in Unternehmen verschiedenster Branchen. Eine einheitliche Definition von Big Data gibt es nicht. Zusammengefasst kann Big Data als eine Sammlung von unzähligen Datenmengen in hoher Geschwindigkeit angesehen werden. Diese werden – zumeist in Echtzeit – analysiert und ausgewertet.[7]

Die große Masse der kontinuierlich wachsenden Daten ist die Grundlage von Big Data.[8] Die Quellen der Daten sind hierbei unterschiedlichster Herkunft und Qualität. Bestandteile können sowohl Texte und Bilder sein, als auch unternehmensinterne Daten wie Verkaufszahlen und Kundenpräferenzen. Ebenso können hierzu auch Daten aus öffentlichen Netzwerken verwertet werden.[9] Die Leistungsfähigkeit von Big Data steigt je unterschiedlicher die Daten sind und miteinander vernetzt werden können.[10] Förderlich für Big Data ist somit jede digitale einzelne Handlung, durch welche neue Daten gesammelt werden.

In der Literatur wird zunehmend von Daten als Rohstoff des 21. Jahrhunderts gesprochen. Je schneller die Rechnergeschwindigkeit, größer das Datenvolumen und die Datenvielfalt sind, desto schneller und effizienter kann ein Unternehmen diese für das Erreichen seiner wirtschaftlichen Ziele und Handlungen nutzen. Allein der Stand der Technik bestimmt die Grenzen der Analysen.[11]

In Unternehmen kann die Nutzung von Big Data Analysen neue Chancen und Möglichkeiten bringen. Werden Trends frühzeitig erkannt, kann so beispielsweise der Waren- und Personalbedarf besser geplant werden. Auch werden bereits so Informationen aus Produkten gewonnen, damit frühzeitig Fehler und Qualitätsinformationen erkannt und verbessert werden können.

[7] Sarunski, Maik, DuD, 7/2016, S. 424.
[8] Grützner/Jakob, Compliance von A-Z, 2015.
[9] Ziegler, MMR, 2013, Rn. 418.
[10] Boehme-Neßler, DuD, 7/2016, S. 422.
[11] Sarunski, DuD, 7/2016, S.425.

Big Data wird in der medialen Welt als digitale Revolution bezeichnet, deren Datengröße auf mittlerweile 12 Zettabyte geschätzt wird.[12]

2.2 Big Data als Chance für Unternehmen

Die Vorteile von Big Data haben bereits zahlreiche Unternehmen erkannt, die Vorteile durch die Nutzung von Big Data sind im Allgemeinen sehr vielfältig.

Zum einen schafft es die Grundlage, fundierte Entscheidungen innerhalb eines Unternehmens zu treffen. Durch eine Erhöhung der Transparenz und der Varietät der Daten können relevante Zusammenhänge und Abhängigkeiten besser als bisher erkannt werden. Weiterhin werden anhand von Analysen der internen Daten, sowie Daten aus externen Quellen, Prozesse im Geschäftsalltag optimiert. Bisher unentdeckte Schwachstellen und Fehler sollen aufgedeckt werden, um so zukünftig Kosten zu senken und die Prozesse effizienter gestalten zu können.[13]

Ein weiterer Aspekt der positiven Nutzung von Big Data ist ein vorausschauender Umgang mit Risiken. Neu erlangte Erkenntnisse helfen Unternehmen, mögliche Risiken vorausschauend zu kalkulieren und somit zu minimieren. Eine Bewertung von Risiken mit Hilfe von Big Data kann wegweisend für Unternehmensentscheidungen sein. Wahrscheinlichkeiten und Prognosen können zunehmend exakt bewertet werden. Dies ermöglicht bei Unternehmensentscheidungen, auch risikobehaftete Optionen in Erwägung zu ziehen, welche dennoch langfristig profitabel sein können.[14]

Zum anderen unterstützt Big Data Unternehmen bei der stetigen Herausforderung, Kundenbedürfnisse zu erkennen und ihr Geschäftsmodell optimal anzupassen.[15]

Um als ein global agierendes Unternehmen im stetigen Wettbewerb bestehen zu können und die Profitabilität steigern zu können, müssen

[12] vbw (Hrsg.), Zukunft digital, 2016, S. 4.
[13] Reiner/Messerschmidt u.a., pwc (Hrsg.) Big Data, 2013, S. 19.
[14] Reiner/Messerschmidt u.a., pwc (Hrsg.) Big Data, 2013, S. 19.
[15] vbw (Hrsg.), Zukunft digital, 2016, S.58.

Maßnahmen getroffen werden, um Kunden zu binden und die Zufriedenheit zu steigern.[16]

Vor allem im Automobilsektor bietet Big Data dem Nutzer neue Chancen und Möglichkeiten hinsichtlich kundenorientierter Produkte, um so das Ziel, nachhaltig Kunden zu gewinnen, zu erreichen.

Bereits bei der Konfiguration eines Neuwagens werden gezielt Daten in Form von Kundenwünschen genutzt, um das Produkt individuell und exklusiv gestalten zu können. So haben Familien andere Erwartungen und Ausstattungsanforderungen an ein Fahrzeug als ein Unternehmer, welcher das Auto vermehrt zu Geschäftszwecken nutzt. Mit Hilfe der von Big Data erstellten Profile kann nunmehr ein preis- und leistungsorientiertes Angebot erstellt werden.[17]

Big Data ist somit eine große Chance für die Automobilbranche. Einerseits gelingt es auf diese Weise der Automobilindustrie, ein an die Kundenwünsche angepasstes Fahrzeug zu erstellen und andererseits erhält der Automobilhandel so die Möglichkeit, einen Kunden langfristig an das Autohaus zu binden und die Zufriedenheit dauerhaft zu erhöhen.

2.3 Big Data als Risiko

Die Automobilindustrie gilt als Vorreiter im Umgang mit Big Data und entscheidungsrelevanten Informationen hinsichtlich darauf folgender besserer Entscheidungen, Prozessen und Produkten.[18] Als primärer Ansprechpartner ist der Automobilhändler ein bedeutsamer Akteur hinsichtlich eines effektiven Umgangs mit Big Data und Digitalisierung. Jedoch verändert sich die Automobilwelt rasant und fraglich ist, ob sich die Branchen diesem schnellen Wandel anpassen kann, um auch in Zukunft stark im Wettbewerb zu sein.

[16] Stricker/Wegener/Anding, Big Data revolutioniert die Automobilindustrie, S.5.
[17] Stricker/Wegener/Anding, Big Data revolutioniert die Automobilindustrie, S. 9.
[18] Stricker/Wegener/Anding, Big Data revolutioniert die Automobilindustrie, S. 7.

2.3.1 Big Data im Handel

Ein wichtiger Schritt für den Handel ist die Miteinbeziehung in den Online-Markt. Große Autohäuser vertreiben jährlich bis zu 22% aller Fahrzeuge auf diese Weise, ein steigender Trend lässt sich feststellen.[19]

Das Voranschreiten der Digitalisierung auf Grundlage von Big Data kann neben den großen Chancen jedoch auch Risiken und Veränderungen für den Automobilhandel bergen und beinahe jede Handelsgruppe wird in Zukunft von den Konsequenzen aus Big Data betroffen sein.

Um den Anschluss auf dem Markt nicht zu verlieren stellen die Unmengen an Daten und derer Vielfalt neue Herausforderungen dar, zudem öffnen sich neue Möglichkeiten im Bereich Marketing und Service. Kunden können hierdurch gezielter und individueller angesprochen werden und Produkte entsprechend platziert werden. Grundsätzlich sind Automobilhändler aufgeschlossen, die Möglichkeiten von Big Data zu nutzen, ein Hemmnis stellen weiterhin rechtliche Regelungen dar. Das Risiko, ohne einer vorherigen Einwilligung auf Daten, welche einen Personenbezug aufweisen, zuzugreifen, hemmt eine aktive Nutzung dieser Daten.[20] Problematisch für den stationären Handel sind oftmals auch das fehlende Wissen und zu geringe interne Ressourcen, um die Erkenntnisse aus Big Data zu verstehen und effektiv zu nutzen.[21]

Oftmals ist der Handel mit der Geschwindigkeit, mit welcher Big Data die Digitalisierung vorantreibt, überfordert. Der Hersteller bringt neue Komplexität in laufende Prozesse, die Händler können sich jedoch nicht darauf verlassen, dass der Hersteller ausreichend Unterstützung bietet. Hier muss der Händler Investitionen tätigen, um ein abteilungsübergreifendes System zu entwickeln, um die steigende Datenflut zu bewältigen und sinnvoll zu nutzen, um einerseits die Kundenbindung zu erhöhen und andererseits den Umsatz zu steigern.[22]

[19] siehe Anhang 1.
[20] siehe Anhang 1.
[21] Gronau/Fohrholz/Weber, Wettbewerbsfaktor Analytics, , S. 54, siehe URL 3.
[22] Mauritz, kfz-betrieb, 9/2017, S. 26.

2.3.2 Risiko für die Anonymität

Durch die von jedem Menschen hinterlassenen Datenspuren[23] verhilft Big Data durch die Zusammenführung von Daten zu neuen Zusammenhängen. Die Kombination erlaubt Prognosen über das soziale Leben, politische Einstellungen und auch einen aktuellen Gemütszustand der betroffenen Person.[24] So kann auch die Möglichkeit gegeben sein, Angaben über Bonität, den privaten Konsum, die Berufstätigkeit oder finanzielle Transaktionen auszuwerten und mit diesem Wissen individuelle Angebote auf den Verbraucher zu erstellen.[25] Mit Hilfe von Big Data können Unternehmen dieses Wissen kommerziell nutzen und dem Verbraucher u.a. passgenaue Werbung einzuspielen. Diese automatisierte Beeinflussung auf das Verhalten des Konsumenten könnte somit indirekt in die freie Willensbildung des Konsumenten eingreifen.[26]

In der Automobilwelt spricht man in einem solchen Fall von einem gläsernen Fahrer.[27] Oftmals ist dem Autofahrer nicht bewusst, welche und in welcher Anzahl dessen Daten gesammelt und verarbeitet werden. Dies soll nunmehr im Folgenden erarbeitet werden.

[23] Broers/Pauls, Datenspuren, siehe URL 2.
[24] Roßnagel u.a., DSR, 2016, S. 28.
[25] Weichert, Big Data und Datenschutz, 2013, S. 1.
[26] Roßnagel u.a., DSR, 2016, S. 29.
[27] siehe URL 4.

3. Die vernetzte Automobilwelt

3.1 Smart Car

Autonome Systeme erhalten immer größere mediale Aufmerksamkeit. Sie umfassen einen weiten Bereich, deren Gemeinsamkeit es ist, computerbasierte Systeme und Algorithmen so miteinander zu verknüpfen, dass selbstständig Entscheidungen getroffen werden können. Werden solche Systeme auf ein Objekt projiziert, entsteht ein „smarter“ Gegenstand. Die Reichweite von „smarten“ Objekten kennt kaum mehr Grenzen. „Smartifizierung“ findet in beinahe allen Lebensbereichen statt.[28]

Auch in der Automobilbranche erhält die Vernetzung Einzug und eröffnet völlig neue Dimensionen bei der Verbindung von Automobil-, Informations- und Kommunikationstechniken hin zu einem Smart Car.

Grundlegende Voraussetzung für ein smartes Fahrzeug ist seine Konnektivität mit Kommunikationspartnern, welche sich zunächst in zwei Gruppen gliedern lässt.[29]

Die im Fahrzeug verbaute Sensorik und die damit verbundene Datenerfassung und -auswertung im integrierten Computer beschreibt zunächst die interne Vernetzung, das „Netz im Auto“. Das Auslesen der Daten erlaubt es so Werkstätten, Diagnosen zu erstellen und mögliche Fehler zu beheben. Fahrassistenzsysteme wie das Navigationssystem sowie die Nutzung von Telekommunikationssystemen während der Fahrt sind Bestandteil dieser internen Vernetzung.[30]

In Las Vegas kündigte der Automobilhersteller Daimler auf der Consumer Electronics Show an, zukünftig mit externen Technologiekonzernen zusammenzuarbeiten und so das Fahrzeug zu einem dritten Lebensraum machen zu wollen. Beide Konzerne planen gemeinsam, in Zukunft die Messung von Vitaldaten wie Herz- und Atemfrequenz sowie Blutdruck über speziell im Lenkrad verbaute Sensoren zu ermöglichen. Bereits

[28] Jaekel/Bronnert, Die digitale Evolution moderner Großstädte, 2013. S. 9.
[29] Auer-Reinsdorff/Conrad, Handbuch IT- und Datenschutzrecht, 2016, Rn. 582.
[30] Hansen, DuD, 6/2015, S. 367.

mögliche Wellness-Programme wie Tiefenmassagen und Aktivsitze sollen dann mit den erfassten Vitaldaten abgestimmt werden. [31]

Auf der anderen Seite wird die Vernetzung des Autos mit dem Netz beschrieben. Das Fahrzeug kommuniziert somit selbst mit der Außenwelt. Unterteilt werden die derzeit möglichen Kommunikationspartner zunächst in C2C und C2X (Car to Car und Car to Infrastructure).[32]

3.1.1 Car to Car Communication

Die C2C-Vernetzung stellt eine Kommunikation zwischen Fahrzeugen untereinander dar. Grundlegend ist hierbei die Erhöhung der Sicherheit im Straßenverkehr. Beispielhaft zu nennen ist hierbei eine Sensorik, welche rechtzeitig ein Stauende nach einer Kurve erkennt und den Fahrer rechtzeitig warnen kann, damit dieser entsprechend reagieren kann und z.B. eine alternative Route zur Zielerreichung befährt. Weitere Möglichkeiten der Kommunikation ergeben sich auch bei Unfallsituationen, in welchen das verunfallte Fahrzeug Meldungen an nahende Fahrzeuge sendet, um zu warnen und alternativ für eine Stauvermeidung neue Fahrrouten berechnet. Doch auch die automatische Betätigung des Warnblinkers kann in Zukunft ein Hinweis für andere Fahrzeuge darstellen. Nahende Fahrzeuge werden so langsam an die mögliche Unfallstelle geleitet.[33]

Diese Funktionen erfordern folglich einen ständigen Datenaustausch, damit eine sofortige Kommunikation stattfinden kann.[34]

Neben der Erhöhung der Verkehrssicherheit verfolgen Automobilhersteller das Ziel, die Umweltbelastung aufgrund von überhöhtem Verkehrsaufkommen zu verringern. Gemeinsam mit dem Technologieunternehmen Bosch erprobt Daimler derzeit im Raum Stuttgart die Möglichkeit, dass Fahrzeuge anderen Autos freie Parkplätze melden, um auf diese Weise das Verkehrsaufkommen aufgrund der Parkplatzsuche zu reduzieren. Mithilfe von Ultraschallsensoren sollen Parkplätze am Straßenrand abgetastet werden. Verfügbare Parkplätze

[31] Gerster, Automobilwoche, 1/2017, S.2.
[32] Hansen, DuD, 6/ 2015, S. 367.
[33] Hoberg, ATZ, 2/2016, S. 12.
[34] Weisser/Färber, MMR, 2015, S. 507.

werden sodann über eine Kommunikationsschnittstelle anderen Verkehrsteilnehmern mitgeteilt.[35]

3.1.2 Car to Infrastructure

Eine weitere Form der Vernetzung stellt C2X dar. C2X steht für die Kommunikation des Fahrzeuges mit seiner Umgebung, der Infrastruktur. Bislang war es Fahrzeugen auf kamerabasierten Systemen möglich, Verkehrsschilder zu lesen und den Fahrer so auf mögliche Beschränkungen hinzuweisen.[36] Der Automobilhersteller Audi entwickelte diesen Assistenten weiter zu einem prädiktiven Effizienzassistenten. Dieser weist den Fahrer auf Situationen hin, in welchen dieser sein Fahrtempo verlangsamen sollte. Erfahrungsgemäß, beruhend auf vorhandenen Streckendaten, erkennt dieser Assistent Kreisverkehre, Gefälleabschnitte oder Kreuzungen, noch bevor der Fahrer diese erkennen kann.[37] Weiterhin dienen Ultraschallsensoren an beiden Seiten eines Fahrzeuges dem Fahrer als Parkassistent, um so Hindernisse in der Umgebung anzeigen zu können.[38]

Der Automobilhersteller Audi hat nunmehr begonnen, die C2X Kommunikation auch auf Ampelsysteme auszuweiten. Zunächst soll dem Fahrer die Information weitergegeben werden, ob es ihm möglich ist, mit der erlaubten Geschwindigkeit die auf seiner Route nächste Ampel noch während der Grün-Phase zu erreichen. Sollte dies nicht der Fall sein, wird dem Fahrer ein Countdown angezeigt, wann die nächste Grünschaltung stattfindet. In Testfahrten wurde durch diese Vorrichtung erreicht, dass die Zahl der bis zum Stillstand abgebremsten Fahrzeuge um 20% gesunken ist. Dies fördere zum einen energieeffizienteres Fahren, zum anderen seien die Fahrer souveräner und entspannter im Stadtverkehr unterwegs.[39]

[35] Gerster, Automobilwoche, 2016, siehe URL 5.
[36] Hansen, DuD, 6/2015, S. 367.
[37] Audi AG (Hrsg.), Fahrerassistenzsysteme, 2016, siehe URL 6.
[38] siehe URL 7.
[39] Pillau, Audi beginnt mit C2X bei Ampelsystemen in USA, 2016, siehe URL 8.

3.2 Telematik im Straßenverkehr

3.2.1 eCall

Beinahe 3.500 Menschen wurden allein im Jahr 2015 im deutschen Straßenverkehr durch Unfälle getötet, die erfasste Anzahl der verletzten Personen betrug 325.726.[40] Europaweit wurden 26.100[41] Verkehrstote registriert. Die Mitgliedsstaaten verfolgen das Ziel, diese Zahlen bis 2020 zu halbieren, weshalb präventive Maßnahmen verstärkt werden müssen und die Fahrsicherheit erhöht werden muss. Die Zahlen führten zu der Entscheidung der Europäischen Union, dass neue Fahrzeugtypen mit einem bordeigenen eCall-System auszurüsten sind. Dieses System basiert darauf, nach einem schweren Unfall selbstständig den Notruf zu wählen.[42] Die Verordnung EU 2015/758 tritt ab dem 31.03.2018 in Kraft.[43]

Es muss gewährleistet sein, dass das System auch nach einem schweren Unfall funktionstüchtig bleibt und das Rettungsteam umgehend zum verunfallten Fahrzeug gelotst wird, auch wenn es den verletzten Insassen nicht mehr möglich ist, selbstständig mit der Notrufzentrale zu kommunizieren.[44] Je schneller es den Rettungsdiensten ermöglicht wird, vor Ort zu sein und entsprechende Hilfsmaßnahmen einzuleiten, desto höher ist die Wahrscheinlichkeit, die Schwere der Verletzungen zu verringern und die Zahl möglicher Todesopfer zu reduzieren.[45]

In Zukunft werden Automobilhersteller dafür verantwortlich sein, dass alle Fahrzeuge, welche von der Verordnung EU 2015/758 betroffen sind, mit dem eCall-System ausgestattet sind. Betroffen sind alle PKW- und leichte Nutzfahrzeug-Modelle.[46]

3.2.2 Pay as You Drive

Seit wenigen Jahren besteht auch in Deutschland die Möglichkeit, Telematik-Tarife bei Kfz-Versicherungen zu nutzen. Der Begriff Telematik setzt sich aus den beiden Begriffen „Telekommunikation“ und

[40] Statistisches Bundesamt (Hrsg.), Polizeilich erfasste Unfälle, siehe URL 9.
[41] EU-Komm., EU (Hrsg.), CARE, road accidents database, siehe URL 10.
[42] Weisser/Färber, MMR, 2015, S. 507.
[43] COM (2016) 5709, v. 12.09.2016, S. 10.
[44] COM (2016) 5709, v. 12.09.2016, S. 2.
[45] Europ. Parl., Pressemitteilung eCall, 28.04.2017.
[46] Europ. Parl., Pressemitteilung eCall, 28.04.2017.

„Informatik“ zusammen und wurde erstmals im Jahre 1978 verwendet.[47] Im Bericht von Nora und Minc, „Die Informatisierung der Gesellschaft“, wurde die These entwickelt, dass die herkömmliche Telekommunikation mit einer zunehmenden Vernetzung in der Zukunft von Computern durchdrungen wird.[48] Beinahe 40 Jahre später ist es möglich, anhand der Verschmelzung beider Technologien neue Geschäftsmodelle zu entwickeln.

So bieten seit wenigen Jahren auch in Deutschland Versicherungsunternehmen die Möglichkeit, mit Hilfe einer kleinen Box, welche im privaten Fahrzeug des Versicherungsnehmers eingebaut wird, die Versicherungsprämie des Versicherungsnehmers individuell anzupassen. In den USA ist bereits jedes siebte Auto telematisch vernetzt.[49]

Dieser Dienst wird im Allgemeinen als „Pay as You Drive“-Tarif bezeichnet.[50] Ziel dieses Tarifs ist hierbei, die Prämie des Versicherungsnehmers abhängig von dessen Fahrstil zu gestalten. Die fest verbaute Telematik-Box soll konstant Daten sammeln, welche das Fahrverhalten analysiert.[51] Der Prämienbeitrag kann so nach verschiedenen Kriterien kalkuliert werden. Hierbei wird registriert, wie häufig der Versicherungsnehmer stark beschleunigt oder abbremst und die zulässige Höchstgeschwindigkeit überschritten wird. Während diese Faktoren zu einer höheren Prämie führen, kann ein vorsichtiges Fahrverhalten zu einer Rückerstattung bzw. Vergünstigung der Versicherungsprämie führen. Auch weitere Kriterien wie die Häufigkeit von Nacht- und Stadtfahrten (gefahrrelevante Verhaltensweisen) können ausschlaggebend für die Tarifbildung sein.

Ein externes Telematikunternehmen leitet in regelmäßigen Abständen die gesammelten Daten an das Versicherungsunternehmen weiter. Verhält sich der Versicherungsnehmer konform mit den geforderten Kriterien, kann ein Teil des Versicherungsbeitrages zurückerstattet werden.

[47] Minc, Die Informatisierung der Gesellschaft, 1979.
[48] Andelfinger, 2025 – Die Versicherung der Zukunft, 2011, S. 18ff.
[49] Baum/Reiter/Methner, Rechtsgutachten Datenkontrolle, 2016, S. 20.
[50] Schwichtenberg, DuD, 6/2015, Rn.378.
[51] siehe URL 11.

Der Versicherungsgeber geht davon aus, dass vorwiegend diejenigen Fahrer Interesse an diesem Versicherungsmodell haben, welche eine vorsichtige Fahrweise haben. Auf diese Weise profitiert der Versicherungsnehmer bei vorausschauendem und vorsichtigem Fahren von Vergünstigungen bei der Versicherungsprämie.[52]

Der Versicherer profitiert auf der anderen Seite durch die Minimierung von Versicherungsfällen und des hiermit verbundenen Regulierungsaufwandes sowie der Kosteneinsparung, welche durch anhängige Gerichtsverfahren im Versicherungsfall entstünden.[53]

Die Anforderungen an eine solche Tarifbindung wurden erstmalig vom Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrheinwestfalen formuliert.[54] So sollen die gesammelten Daten in zwei Datenkreise unterteilt werden. Auf der einen Seite sammeln Telematikunternehmen die Fahrzeugdaten in Echtzeit, ohne jedoch Namen der Versicherungsnehmer zu kennen. Auf der anderen Seite stehen dem Versicherungsnehmer Namen der Fahrzeughalter zur Verfügung, sie haben jedoch nur Zugriff auf die sog. Scores[55] und die Gesamtkilometerzahl.[56]

Diese Entwicklungen werden dazu führen, dass in absehbarer Zeit nur noch diejenigen Fahrer „normale“ Tarife erhalten, die in eine Auswertung ihrer Fahrzeugdaten einwilligen. Das wirft eine Vielzahl von rechtlichen Fragen auf, welche im weiteren Verlauf dieser Arbeit erörtert werden.

3.3 Zusammenfassung

Das vorliegende Kapitel beschreibt den hohen Entwicklungsstandard der Automobilbranche hinsichtlich Smart Cars und autonomer Fahrzeuge. Die immense Zahl von erhobenen und verarbeiteten Daten birgt neue

[52] Haller, ZfV 2013, S. 782 f.
[53] Zurlutter, Datenschutzrechtliche Aspekte der Auskunfts- und Aufklärungsobliegenheit über Kfz-Daten in der Kfz-Haftpflichtversicherung, 2016, S.148.
[54] Lepper, 22. DIB LDI NRW, 2015, S. 39.
[55] Gesamtpunktebewertung, welche das Fahrverhalten als Zahl ausdrückt.
[56] Lepper, 22. DIB LDI NRW, 2015, S. 38.

Chancen und Möglichkeiten, sowohl für den Endverbraucher als auch für die Unternehmen, welche hieraus einen Nutzen ziehen können.

Zunächst können Standortdaten Aufschluss über Gewohnheiten, Regelmäßigkeiten und Reiseziele geben. Über einen längeren Zeitraum hinweg können zunehmend Rückschlüsse auf das Fahrverhalten des Einzelnen geschlossen werden. Auch können die hierdurch gewonnen Informationen verwendet werden, um bei Verkehrsunfällen mit Körperverletzung eine Schuldzumessung ermitteln zu können.

Big Data revolutioniert die Automobilwelt zunehmend. Es werden Anwendungen ermöglicht, die den Menschen in seinen körperlichen und geistigen Fähigkeiten in unterschiedlichen Bereichen unterstützen. Die gewonnenen und verarbeiteten Daten ermöglichen jedoch auch zunehmend eine Überwachung der einzelnen Person und gewähren einen umfassenden Einblick in bereits geschehene und noch folgende Ereignisse im Leben dieser Personen.[57]

Das folgende Kapitel soll nunmehr Aufschluss darüber geben, wer als wahrer Eigentümer dieser Daten angesehen werden kann um hieraus entstehende Rechte und Pflichten zuordnen zu können.

[57] Roßnagel u.a., DSR, 2016, S. 185.

4. Eigentumsverhältnisse von Daten

Wie bereits in vorangehenden Kapiteln beschrieben, zählen Daten zu einem wichtigen Wirtschaftsgut in der globalen Wirtschaft. Je qualitativ hochwertiger die Daten sind, desto höher ist deren wirtschaftlicher Wert und somit der wettbewerbliche Vorteil eines Unternehmen gegenüber einem anderen. Auch die Europäische Union hat das Geschäftsmodell der Datenwirtschaft erkannt und verfolgt das Ziel, einen vernetzten digitalen Binnenmarkt ohne technologische und rechtliche Hemmnisse zu errichten.[58]

4.1 Das rechtliche Eigentum an Daten

Fraglich ist jedoch, ob und wie Eigentumsverhältnisse an Daten definiert werden können und wem die Daten gehören. Als Eigentümer kämen zunächst all jene Personen in Frage, die ihre persönlichen Daten in diversen Systemen eingeben. Die technische Verknüpfung von unterschiedlichen Daten ermöglicht somit eine persönliche Zuordnung. Beispielsweise zu nennen ist hier die Eingabe von persönlichen Daten, um einen Zugang zu einem bestimmten Internetportal zu erlangen. Auch Unternehmen könnten als potentielle Eigentümer infrage kommen, wenn einerseits Daten auf deren physikalischen Datenträgern gespeichert sind oder andererseits die Daten über deren IT-Strukturen (Internetportale) erfasst werden.[59]

Im Folgenden soll nunmehr erörtert werden, inwieweit eine rechtliche Zuordnung des „Dateneigentums“ möglich ist.

4.1.1 Rechtsstellung nach § 903 BGB i.V.m. §§ 90 ff. BGB

Sollen Daten zu einem Rechtssubjekt zugeordnet werden, so kommt zunächst die Stellung des Eigentümers gem. § 903 BGB in Frage. Der Eigentümer einer Sache kann gem. § 903 S. 1 BGB, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen.

[58] COM (2015), 192, v. 06.05.2015, S. 2.
[59] Bachmann/Kemper/Gerzer, Big Data, 2014, S. 70.

Grundlegende Voraussetzung hierfür jedoch ist, dass es sich bei Daten um eine Sache handelt. Gemäß § 90 BGB sind Sachen jedoch nur körperliche Gegenstände. Das OLG Dresden vertritt die Meinung, dass eine Sache nur in drei Aggregatszuständen – fest, flüssig und gasförmig – als körperlicher Gegenstand angesehen werden kann, während es sich bei elektronischen Daten hingegen um eine elektrische Spannung handelt.[60]

Aus technischer Sicht werden Daten gemäß DIN 44300 Teil 2 Nr. 2.1.13 als ein Gebilde aus Zeichen oder kontinuierlichen Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Informationen darstellen, vorrangig zum Zwecke der Verarbeitung und als deren Ergebnis, definiert.[61]

Bei Daten handelt es sich somit um durch Zeichen vermittelte Informationen, welche eine eigenständige Sacheigenschaft nach § 90 BGB ausschließen.[62] Als körperlicher Gegenstand kann lediglich das Speichermedium, beispielsweise eine Festplatte, angesehen werden.[63]

Weiterhin ist fraglich, ob ein gespeichertes Datum als ein wesentlicher Bestandteil gem. § 93 BGB angesehen werden kann. Als Bestandteil einer Sache nach § 93 BGB sind Sachen, die nicht voneinander getrennt werden können, ohne dass der eine oder der andere zerstört oder in seinem Wesen verändert wird, nicht Gegenstand besonderer Rechte. Wäre eine Ableitung des Eigentums auf einen externen Datenträger möglich, so könnte davon ausgegangen werden, dass diejenige Person, bei welcher das externe Speichermedium im Eigentum steht, alsdann rechtmäßiger Eigentümer der Daten wäre, welche auf dem Gerät fixiert sind.[64]

Dieser Auffassung folgt unter anderem das OLG Karlsruhe. Ein Datenträger mit darauf gespeicherten Daten stellt eine körperliche Sache dar und kann folglich als eigentumsfähig angesehen werden.[65]

[60] OLG Dresden, Beschl. v. 05.09.2012, Az. 4 W 961/12.
[61] Dierstein, Definition DIN 44330, 2003. S.2.
[62] Markl/Löser/Hoeren u.a., Big Data Management, 2013, S. 273.
[63] Bräutigam/Klindt (Hrsg.), Gutachten Digitalisierte Wirtschaft, 2015, S. 20.
[64] Lehmann/Unseld, Die Kommerzialisierung personenbezogener Daten, 2010, S. 28.
[65] OLG Karlsruhe, Urt. v. 07.11.1995, Az. 3 U 15/95.

Die Verschmelzung von „Eigentum“ am Datum und dem Eigentum an der Sache stellt sich jedoch in der Praxis oftmals als nicht praktikabel dar. Immense Mengen an Daten werden heutzutage auf Servern (Speichermedium) oder in der „Cloud“ gespeichert und virtualisiert, weshalb eine Zuordnung zu einem individuellen Speichermedium kaum mehr möglich ist.[66] Besonders im Rahmen von Big Data und Cloud-Computing[67,68] ist eine Differenzierung zwischen dem Eigentümer am Datenträger einerseits und der Zuordnung der Daten zu einer bestimmten, natürlichen oder juristischen Person andererseits, kaum realisierbar. Im Falle einer Datenübermittlung an einen Dritten scheidet ein Eigentumseingriff aus und es kann keine Schadensersatzforderung aufgrund einer Verletzung seines Eigentums nach § 823 BGB erhoben werden.[69]

4.1.2 Rechtsstellung nach dem UrhG

Auch ein einfacher Urheberrechtsschutz an Daten scheidet aus, da es sich nicht um persönliche, geistige Schöpfungen i.S.d. § 2 Abs. 2 UrhG handelt. Um als geistige Schöpfung angesehen werden zu können, muss im Werk die Persönlichkeit des Urhebers zum Ausdruck gebracht werden, welche sich auch bei der Herstellung in freien kreativen Entscheidungen wiederspiegelt.[70] Auch ist fraglich, ob die vorausgesetzte Gestaltungshöhe vorliegt. Um dies zu bejahen, müssten Daten einen hohen Grad an Individualität aufweisen, um sich insbesondere aus der Masse an herkömmlichen Alltagswerken herausheben zu können.[71] Vor allem bei automatisch generierten Daten kann weder eine Gestaltungshöhe angenommen werden, noch kann bei Daten von einer persönlichen Schöpfung ausgegangen werden.

[66] Boesche/Rataj, Elektromobilität, 2016, S. 35.
[67] Cloud Computing definiert sich in diesem Zusammenhang als virtuelles Rechenzentrum für ein Angebot an IT-Leistungen, insbesondere Speicherplatz und Rechenleistung.
[68] Hoeren, Haftung im Internet, 2014, S. 522, Rn. 8.
[69] Bräutigam/Klindt (Hrsg.), Gutachten Digitalisierte Wirtschaft, 2015, S. 21.
[70] EuGH, Urt. v. 16.07.2009, Az.: C-5/08.
[71] Wandtke, UrhR, 2016, Rn.8.

Nachdem der Schutz durch die Eigentumsstellung und als persönliche geistige Schöpfung verneint wurde ist fraglich, ob möglicherweise ein Schutz durch das Datenbankurheberrecht gegeben sein könnte.

Es könnte ein Schutz nach § 87a UrhG vorliegen. Das Urheberrecht definiert eine Datenbank nach § 87a Abs.1 S.1 als eine Sammlung von Daten, welche systematisch oder methodisch angeordnet sind und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Diese Norm schützt also die Leistung des Datenbankherstellers.[72]

Voraussetzung für den Schutz von Datensammlungen ist zunächst, dass diese einer Anordnung unterliegen. Vom Schutz ausgeschlossen werden hiernach einzelne und unstrukturierte Daten – so wie sie bei Big Data regelmäßig vorzufinden sind.[73]

Schutz kann nur derjenige erhalten, der in den Aufbau dieser Datenbank wesentliche Investitionen getätigt hat. Dem Datenbankhersteller wird so Schutz vor einer nicht genehmigten Verbreitung, Vervielfältigung und öffentlicher Wiederhabe gewährt. Geschützt werden jedoch nicht die Daten als Inhalt dieser Datensammlung.[74]

Ein umfassendes Recht zum Ausschluss von Nutzungen durch Dritte nach § 87a UrhG liegt nicht vor.[75]

4.2 Konflikt einer rechtlichen Zuordnung

Die Tatsache, dass bislang keine eindeutige Zuordnung nach derzeit geltendem Recht möglich ist, stellt die Beteiligten vor neue Herausforderungen und vor die Frage, welche Anforderungen im Rahmen der Verwendung und Kommerzialisierung zu beachten sind. Vor allem im Umgang mit Fahrzeugdaten muss auf diese Frage näher eingegangen werden.

[72] Markl/Löser/Hoeren u.a., Big Data Management, 2013, S. 169.
[73] OLG München, Urt. v. 09.11.2000, Az.: 6 U 2812/00.
[74] Markl/Löser/Hoeren u.a., Big Data Management, 2013, S. 276.
[75] Boesche/Rataj, Elektromobilität, 2016, S. 36.

Es ist bislang ungeklärt, wem das Recht an den Daten beim vernetzten Fahrzeug zustehen soll, die Meinungen hierzu sind unterschiedlich.[76]

Die Anwendungsbereiche der Daten wurden bereits in Kapitel 2 näher beschrieben. Zusammengefasst lassen sich die Daten somit grob in drei Gruppen unterteilen. Zum einen sind dies Bewegungs- und Umgebungsdaten des Fahrzeuges wie Geschwindigkeit, die GPS-Koordinaten sowie jegliche Sensordaten welche Informationen über Straßenzustand, Witterung und Hindernisse ermitteln können. Zum anderen Daten über den Zustand des Fahrzeuges und somit die Verwendung von Assistenzsystemen, Motorrauminformationen, Kraftstoffverbrauch, Kameradaten etc. Zur dritten Gruppe zählen jegliche Komfortdaten wie die Internetnutzung, Sitzeinstellungen, bestimmte Voreinstellungen sowie auch Login-Daten für die Verwendung des bordeigenen Computers.[77]

Die Anzahl der Interessenten an diesen Daten ist sehr groß und mit hinzukommenden Innovationen im Fahrzeug steigt auch der Kreis jener, welche diese Daten wirtschaftlich nutzen wollen.

Die Interessenten lassen sich zunächst in drei Gruppen gliedern. Die erste Gruppe besteht aus dem Hersteller, den dazugehörigen Vertragshändlern sowie den Vertragswerkstätten.[78] Die Entscheidungsmacht, welche Daten im Fahrzeug verarbeitet und gespeichert werden, liegt grundsätzlich beim Hersteller. Der Hersteller nutzt jegliche Daten, um sein Produkt den Kundenwünschen anzupassen und im Hinblick auf Garantiefälle die Wartung und Entwicklung des Fahrzeuges anzupassen.[79] Auf diese Weise sind auch Ferndiagnosen möglich, indem das Fahrzeug dem Fahrer mitteilt, wann das Fahrzeug zur Inspektion muss, sich Unregelmäßigkeiten im Fahrzeugzustand offenbaren oder Reparaturen vorgenommen werden müssen. Diese Daten benötigen vor allem die Vertragswerkstätten.

[76] Schwartmann, RDVonline, Teil 1, 2015.
[77] Brossard, vbw (Hrsg.), Automatisiertes Fahren, 2016, S.3.
[78] Roßnagel, SVR, 8/2014, S.281.
[79] Brossard, vbw (Hrsg.), Automatisiertes Fahren, 2016, S.7.

Gezielte elektronische Diagnosen vereinfachen die Ersatzteilbeschaffung und punktgenaue Reparaturen.[80]

Die zweite Gruppe stellen all jene Drittanbieter dar, welche an der Entwicklung zum Connected Car teilnehmen. Schon seit längerem sind Automobilhersteller darauf angewiesen, mit der Mobilfunkbranche zu kooperieren. Während klassische Zuliefererunternehmen auf die Gunst des Herstellers angewiesen sind können IT-Unternehmen wie Apple oder Google an den Automobilhersteller kompromisslose Bedingungen stellen.[81] Bewegungsdaten werden herangezogen, um auf den Nutzer zugeschnittene Werbung, wie z.B. Restaurantvorschläge oder Sehenswürdigkeiten auf der eingegebenen Route anzuzeigen.[82] Das Angebot an neuen Geschäftsmodellen erhöht sich mit der Zahl der Innovationen, welche ein Fahrzeug hervorbringt.

Insbesondere werden die Fahrzeug- und Standortdaten auch für das gesetzlich vorgeschriebene eCall-System genutzt werden. Auch Versicherungen nutzen die Daten, um die Prämien dem Fahrverhalten des Halters entsprechend einzustufen (pay as you drive).[83]

Die dritte Gruppe sind Fahrer und Halter. Diese Gruppe produziert alle Fahrzeugdaten und ist für die beiden anderen Gruppen von großer Wichtigkeit. Das Interesse dieser Gruppe liegt in der Wahrung der informationellen Selbstbestimmung und des Vertrauens in die eigene Gewalt über die produzierten Daten.[84]

Der Interessentenkreis an Daten ist groß, jedoch bietet das deutsche Recht nur bedingt Rechtssicherheit für eine zuordenbare Rechtsstellung. Die Bundeskanzlerin Angela Merkel beschreibt Daten als den Rohstoff der Zukunft[85], weshalb davon ausgegangen werden könnte, dass eine eigentumsfähige Zuordnung möglich sei.[86]

[80] Roßnagel, SVR, 8/2014, S.282.
[81] ManagerMagazin (Hrsg.), Ausg. 11, 2014, S. 40.
[82] Adam Opel AG (Hrsg.), Pressemitteilung, 21.02.2017, siehe URL 12.
[83] siehe Kapitel 3.2.2.
[84] Roßnagel, SVR, 8/2014, S.282.
[85] CDU (Hrsg.), siehe URL 13.
[86] Plöger, GRUR, 1/2016, S. 6.

Während die Halter die Meinung vertreten, dass ihnen als Datenerzeuger ein eigentumsähnliches Recht zustünde, da sie zeitgleich auch für die Kosten der Inbetriebnahme aufkommen müssen, berufen sich die Automobilhersteller auf der anderen Seite auf die Tatsache, dass sie für die Herstellungskosten sowie Entwicklung des Produkts verantwortlich sind und im Rahmen der Weiterentwicklung diese Daten für sich beanspruchen müssen. Weiterführend könnten auch all jene Drittunternehmen, wie beispielsweise Hersteller von Navigationsgeräten ein aktives Interesse äußern, da auch diese maßgeblich zur Fertigstellung des Endproduktes beigetragen haben.[87]

4.3 Zusammenfassung

Würde eine eindeutige gesetzliche Zuordnung von Daten bejaht werden, so könnte dies zunehmend Konflikte zwischen den Beteiligten schaffen.

Der aktuelle Stand der Technik fördert zunehmend das Konfliktpotential zwischen dem Schutz von personenbezogenen Daten und der wirtschaftlichen Bedeutung der Nutzung dieser Daten.

Nur durch eindeutig und genau definierte vertragliche Regelungen zwischen den Beteiligten kann nach derzeitiger Gesetzeslage ein hinreichender Schutz der Daten erreicht werden.[88]

Fraglich ist nunmehr, ob der Rechtsunsicherheit durch das geltende Bundesdatenschutzgesetz (BDSG) weiterhin Abhilfe geschaffen werden kann.

[87] Bräutigam/Klindt (Hrsg.), Gutachten Digitalisierte Wirtschaft, 2015, S. 24.
[88] Bräutigam/Klindt (Hrsg.), Gutachten Digitalisierte Wirtschaft, 2015, S. 26.

5. Geltender Datenschutz in der Bundesrepublik

5.1 Historie

Das weltweit erste Datenschutzgesetz wurde im Jahre 1970 im Bundesland Hessen eingeführt.[89] Am 27.01.1977 trat das erste Bundesdatenschutzgesetzt in Kraft, welches nicht nur den Datenschutz der Bürger gegenüber Behörden festsetze, sondern auch den Schutz im privatrechtlichen Bereich regeln sollte.[90] Eine Novellierung sämtlicher Datenschutzgesetze führte im Jahre 1990 zu einer Neufassung des Bundesdatenschutzgesetzes.[91]

Darauffolgend trat im Jahre 1995, im Hinblick auf die weltweite Computervernetzung, die Europäische Datenschutzrichtlinie in Kraft.[92] Diese Datenschutzrichtlinie wurde zum 23.05.2001 durch eine Novellierung des BDSG in nationales Recht umgesetzt und bildet heute den geltenden Rahmen des Europäischen Datenschutzes.[93]

Trotz der fortschreitenden Vernetzung gab es bislang keine Anpassungen des Datenschutzrechts. Am 25.01.2012 reichte die Europäische Kommission den Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ein.[94]

Die neue EU-Datenschutz-Grundverordnung wird sodann am 25.05.2018 in Kraft treten.

Fraglich ist nunmehr, ob und inwieweit das derzeit geltende Datenschutzrecht geeignet ist, mit dem rasanten technologischen Fortschritt mitzuhalten und den Betroffenen ausreichend Schutz seiner informationellen Selbstbestimmung gewährleisten zu können.

In seinem Urteil zum Volkszählungsgesetz im Jahre 1983 legte das Bundesverfassungsgericht den Grundstein für das informationelle

[89] Genz, Datenschutz in Europa und den USA, 2004, S.9.
[90] Merten/Papier, Handbuch der Grundrechte, 2011, S.237.
[91] Däubler/Klebe u.a., BDSG, 2014, S. 77, Rn. 5.
[92] Däubler/Klebe u.a., BDSG, 2014, S. 77, Rn. 6.
[93] Kröger/Hanken/Moos, Datenschutzrecht schnell erfasst, 2006, S.13.
[94] Däubler/Klebe u.a., BDSG, 2014, S. 78, Rn. 6a.

Selbstbestimmungsrecht.[95] Die damalige Entscheidung des BVerfG erklärte bestimmte Regelungen des Volkszählungsgesetzes[96] aus dem Jahr 1982 für nichtig, welche den Umfang des Grundrechts auf informationelle Selbstbestimmung dahingehend verletzte, dass personenbezogene Daten von Ämtern an andere Stellen weitergeleitet wurden und dabei der Ausschluss des Personenbezuges verfahrenstechnisch nicht vorgenommen wurde.[97] Für eine freie Persönlichkeitsentfaltung zählt das Recht auf informationelle Selbstbestimmung zu den wichtigsten Voraussetzungen. Es handelt sich hierbei um das Recht des Einzelnen, frei über die Verwendung und Preisgabe seiner persönlichen Daten zu bestimmen und gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe von dessen persönlichen Daten schützen.[98]

5.2 Personenbezogene und Nichtpersonenbezogene Daten

Bei der Beziehbarkeit von Daten muss grundsätzlich zwischen personenbezogenen und nicht personenbezogenen Daten unterschieden werden. Die Relevanz der Unterscheidbarkeit ergibt sich aus der Gesetzesdefinition, wonach personenbezogene Daten durch das BDSG besonders geschützt sind. Daten, welche keinen Personenbezug aufweisen, genießen keinen gesetzlichen Schutz. Ausschlaggebend ist hierbei der Zweck, den Bürger zum einen vor Missbrauch, zum anderen vor den Gefahren für das Persönlichkeitsrecht durch die Verarbeitung und Nutzung seiner Daten zu schützen.[99]

5.2.1 Personenbezogene Daten

Personenbezogene Daten sind gem. der Legaldefinition nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Die Anwendbarkeit des BDSG wird somit nur dann garantiert, wenn einer

[95] BVerfGE, Urt. v. 15.12.1983, Az.: 1BvR 2019/83.
[96] BGBI, Nr.1 v. 05.01.1984, S. 369.
[97] Benecke, Überblick und Strukturvergleich zwischen allgemeinem und bereichsspezifischem DSR, 2010, S. 1.
[98] BVerfGE, Urt. v. 15.12.1983, Az.: 1BvR 2019/83.
[99] BGBl, Nr. 73 v. 29.12.1990, S 2954.

dieser Bereiche betroffen ist. Zu persönlichen Verhältnissen werden jegliche Angaben gezählt, welche eine Identifizierung und Charakterisierung der Person erlauben, wie beispielsweise Name, Anschrift, Familienstand und Geburtsdatum, aber auch der Beruf, Gesundheitszustand und Überzeugungen führen zu einem Personenbezug. Weiterhin werden auch Werturteile als personenbezogene Daten angesehen.[100] Kann man einen Sachverhalt auf eine Person direkt beziehen, handelt es sich um Daten über sachliche Verhältnisse.

Geschützt werden nur natürliche Personen. Das Gesetz schließt somit den Schutz juristischer Personen aus. Dies widerspricht an sich dem Leitsatz des Art. 19 Abs. 3 GG, dass auch inländische juristische Personen ein Recht auf die Wahrung der Grundrechte haben, sofern die Grundrechte dem Wesen nach auf sie Anwendung finden.[101]

5.2.2 Nicht personenbezogene Daten

Nicht personenbezogene Daten sind vom BDSG nicht geschützt. Zu dieser Kategorie gehören prinzipiell sog. Sachdaten und auch Maschinendaten sowie auch beispielsweise Wetterdaten. Jedes einzelne Datum zählt hierzu, welches keinen Bezug zu einer Person herstellen kann. Die Abgrenzung zum personenbezogenen Datum stellt das Datenschutzrecht aufgrund von fortschreitenden Technologien vor neue rechtliche Herausforderungen. Auf diese Thematik soll im weiteren Verlauf dieses Kapitels näher eingegangen werden.[102]

5.2.3 Daten im Fahrzeug

Daten, welche in Bezug auf das Automobil entstehen, können in vier Kategorien geteilt werden:[103]

Grunddaten wie das jeweilige Modell, die Fahrzeugidentifikationsnummer (FIN) sowie das Kennzeichen zählen ebenso wie der Zustand des Fahrzeuges und die aktuelle Position und dessen Veränderungen zu den

[100] Dammann, BDSG, 2014, § 3 Rn. 12.
[101] Gola/Schomerus u.a., BDSG, 2015, § 3, Rn.11.
[102] Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 144.
[103] Asaj, DuD, 2011, S. 559.

fahrzeugbezogenen Daten. Zu insassenbezogenen Daten zählen alle Daten, welche eine Identifikationsinformation, persönliche Vorlieben, das Verhalten sowie auch eine physische und psychische Verfassung über den Benutzer zu erlangen ermöglichen. Eine dritte Kategorie ergibt sich durch umweltbezogene Daten. Hierzu gezählt werden Daten über andere Verkehrsteilnehmer, die Verkehrsinfrastruktur sowie Vorfälle wie Unfälle und Staus. Auch Merkmale aus der Umgebung wie Sehenswürdigkeiten und Geschäfte sowie das Wetter zählen zur dieser Kategorie. Zuletzt entstehen Daten durch individuelle Verträge mit Kfz-Versicherungen oder Mobilfunkanbietern und Navigationsdiensten.[104]

In einem vernetzten Fahrzeug ist es jedoch kaum mehr realisierbar, dass Daten ohne einen Personenbezug entstehen. Auch rein technische Daten, welche Informationen über das System und etwaige Funktionsstörungen anzeigen, können Aufschlüsse über den Nutzer des Fahrzeuges geben. Durch den Personenbezug wird das Erheben, Speichern und Verarbeiten dieser Daten durch die Regelungen des BDSG eingeschränkt. Um dennoch personenbezogene Daten erheben, speichern und verarbeiten zu können, wurden unabdingbare Prinzipien entwickelt, welche im Folgenden näher erläutert werden.

5.3 Geltende Datenschutzprinzipien

Die primäre Funktion des Bundesdatenschutzgesetzes ist der Schutz von natürlichen Personen, weshalb es notwendig ist, die Erhebung und Verarbeitung von personenbezogenen Daten an Bedingungen zu knüpfen, damit der Mensch vor einer ihn beeinträchtigenden Verarbeitung seiner Daten, der Privatsphäre und seines Persönlichkeitsrechts geschützt werden kann.[105] Diese Bedingungen sind auch als die gängigen Datenschutzprinzipien bekannt und bilden die Grundlage für den Schutz der informationellen Selbstbestimmung.[106]

[104] Boesche/Rataj, Elektromobilität, 2016, S. 6.
[105] Däubler/Klebe u.a., BDSG, 2016, S.119, Rn. 4.
[106] Roßnagel/Geminn u.a., DSR, 2016, S. 45.

5.3.1 Zweckbindung

Der Grundsatz der Zweckbindung besagt, dass personenbezogene Daten immer nur für einen definierten Zweck verwendet werden dürfen. Dies hat zur Folge, dass die bei einem Rechtsgeschäft erhobenen Daten weder administrativ noch für andere beliebige Zwecke genutzt werden dürfen.[107] Es ist somit erforderlich, dass die Verwendung der Daten zum einen im Umfang, zum anderen in ihrer Dauer, welche zur Zweckerreichung erforderlich ist, auf ein bestimmtes Maß beschränkt wird.

Eine Ausnahme für zulässiges Speichern, Verändern oder Nutzen von personenbezogenen Daten bilden die Tatbestände des § 14 Abs. 2 Nr. 1-9 BDSG.

Das sogenannte Zweckbindungsprinzip gebietet somit, dass ohne eine erneute Einwilligung des Betroffenen Daten nur für einen vorab festgelegten Zweck verwendet werden dürfen.[108]

Eine erste Problematik ergibt sich hierbei im Zusammenhang mit Big Data. Wie bereits im vorherigen Kapitel näher beschrieben, verknüpft Big Data unzählige Daten miteinander. Die aus dem Zweckbindungsprinzip resultierende Folge für datenverarbeitende Unternehmen ist nunmehr, dass bereits vor der Verarbeitung der Daten der Verwendungszweck festgelegt sein und auf diesen beschränkt werden muss. Dies ist zunehmend hinderlich für innovative Anwendungen. Durch die Verarbeitung können zunehmend neue Erkenntnisse und Zusammenhänge gewonnen werden, welche so auch für neue Geschäftsbereiche genutzt werden könnten.[109]

Bereits jetzt werden Fahrzeugdaten generiert und genutzt, um u.a. die Verkehrsführung in Echtzeit optimieren zu können und um größere Stauphasen auf Autobahnen ermitteln zu können. Mit Einführung der E-Mobilität steigt aber auch der Bedarf an hierfür benötigten Aufladestationen. Beispielhaft könnte so durch die Generierung der Daten ausgewertet werden, welche Stadtgebiete höher von E-Fahrzeugen frequentiert sind als andere und folglich eine höhere Anzahl an E-

[107] Däubler/Klebe u.a., BDSG, 2016, S. 85, Rn. 17.
[108] Scholz/Sokol, BDSG, 2014, § 4, Rn. 42.
[109] von Grafenstein, DuD, 12/ 2015, S. 790.

Tankstellen benötigen. Weitestgehend könnte auch durch die Analyse dieser Daten festgestellt werden, in welchen Vierteln die Bewohner vermehrt dazu bereit sind, mehr Geld in Innovationen zu investieren, was wiederum die Möglichkeit bietet, Prognosen über steigende Immobilienpreise zu erstellen und so frühzeitig Handlungsstrategien zu entwickeln. Ein Interesse an diesen Daten könnten somit nicht nur die Fahrzeughersteller selbst, sondern auch die Immobilienwirtschaft und Bauunternehmen haben. Der Verwendungszweck dieser Daten ist jedoch nicht vorher bestimmbar.[110]

Unter Beachtung des Zweckbindungsprinzips gemäß § 14 Abs. 1 BDSG wären diese Anwendungen somit unzulässig.

Um diese Problematik zu umgehen, müssen Daten gänzlich anonymisiert oder pseudonymisiert werden.[111]

5.3.2 Erforderlichkeit und das berechtigte Interesse

Personenbezogene Daten dürfen erhoben, gespeichert, verändert oder übermittelt werden, wenn sie für den Zweck der Begründung, Durchführung oder Beendigung des betreffenden Schuldverhältnisses erforderlich sind. Dieses Prinzip der Erforderlichkeit wird näher in § 28 Abs. 1 S. 1 BDSG definiert. In diesem Sinne muss nach objektiven Kriterien festgestellt werden, ob diese Daten tatsächlich benötigt werden um das Vertragsverhältnis zu erfüllen.[112] Daten, welche lediglich nützlich oder geeignet sind, reichen nicht aus um eine Erforderlichkeit zu begründen.

Jedoch dürfen Daten gem. § 28 Abs. 1 S. 2 BDSG als Mittel für die Erfüllung eigener Geschäftszwecke auch dann erhoben, verarbeitet und genutzt werden, wenn keine rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisse bei der betreffenden Person vorliegen. Die Wahrung eines berechtigten Interesses an der Verarbeitung von Daten über Personen, zu denen keine vertraglichen oder

[110] von Grafenstein, DuD, 12/ 2015, S. 790.
[111] siehe S. 32.
[112] Taeger/Gabel, BDSG, S 818, Rn.47.

vertragsähnlichen Beziehungen bestehen, wenn die Verwendung der Daten zur Interessenswahrung erforderlich ist, soll als Zulassungskriterium demnach genügen.[113]

5.3.3 Datensparsamkeit und Datenvermeidung

Eine weitere Herausforderung neben der Zweckbindung ist die Datensparsamkeit. Als grundlegendes Ziel definiert § 3a BDSG, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Fallen dennoch personenbeziehbare Daten in Verfahren an, so gilt die Regel, diese Daten so gut wie möglich zu anonymisieren oder pseudonymisieren.

Gemäß der Legaldefinition in § 3 Abs. 6 BDSG bedeutet Anonymisierung, dass personenbezogene Daten derart verändert werden müssen, dass persönliche Angaben nicht mehr oder nur noch durch einen unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Das Gesetz unterscheidet demnach zwei Arten des Anonymisierens. Einerseits die sog. absolute Anonymisierung. Hierbei werden jegliche Identifikationsmerkmale unwiderruflich gelöscht und ein Wiederherstellen der Daten ist somit gänzlich ausgeschlossen.[114] Andererseits besteht die Möglichkeit des faktischen Anonymisierens, wonach eine Rekonstruierung nur noch mit einem unverhältnismäßig hohen Aufwand möglich wäre. Hiervon wird grundsätzlich ausgegangen, wenn es für das Unternehmen weniger Aufwand bedeuten würde, die Daten erneut zu erheben, als die anonymen Daten zu de-anonymisieren.[115]

Auch der Begriff der Pseudonymisierung wird im BDSG näher beschrieben. Es handelt sich hierbei um das Ersetzen eindeutiger Identifikationsmerkmale, wie beispielsweise der Name, um so eine Bestimmbarkeit der betroffenen Person auszuschließen oder wesentlich zu erschweren.

[113] Taeger/Gabel, BDSG, S 821, Rn.54.
[114] Kühling/Seidel/Sivridis, Datenschutzrecht, S. 105, Rn. 226.
[115] Paas/Wauschkuhn, Datenzugang, 1985, S. 13.

In beiden Fällen gilt jedoch das Gebot der Verhältnismäßigkeit zwischen dem erforderlichen Aufwand für die Anonymisierung und Pseudonymisierung und dem verfolgten Schutzzweck. Es soll hierbei im Interesse der verarbeitenden Stelle sichergestellt sein, dass sachgerechte Maßnahmen getroffen werden. Diese müssen nicht zwingend die besten aller Maßnahmen sein, weniger aufwendige aber auch sachgerechte Maßnahmen können auch getroffen werden.[116]

Der Gesetzgeber fordert demnach angemessene Maßnahmen, eine Verpflichtung zur Verwendung der besten oder neusten Maßnahme gibt es nicht. Als angemessen wird hierbei oftmals die Anwendung einer standardmäßig verfügbaren Software oder eines Anonymisierungs- und Pseudonymisierungsverfahrens angesehen, welches auch mit geringem Aufwand bei der verarbeitenden Stelle programmiert werden kann. Eine unangemessene (unwirtschaftliche) Verhältnismäßigkeit wird regelmäßig dann angenommen, wenn ältere Systeme noch nicht vollständig steuerlich abgeschrieben sind und dennoch ein neues System angeschafft werden müsste. Eine einzelfallbezogene Prüfung soll Aufschluss darüber geben, ob eine Neuanschaffung eine finanziell unangemessene Belastung darstellen würde oder nicht.[117]

5.3.4 Einwilligung des Betroffenen

Unabdingbar für eine zulässige Datenverarbeitung ist nach § 4 Abs. 1 BDSG, neben der Zulässigkeit durch das Gesetz oder eine andere Rechtsvorschrift, die Einwilligung des Betroffenen. Formelle und inhaltliche Anforderungen hingegen werden in § 4a BDSG geregelt. Für eine wirksame Einwilligung ist Voraussetzung, dass diese auf einer freien Entscheidung des Betroffenen beruht und der Betroffene darauf hingewiesen wurde, für welchen vorgesehenen Zweck die Daten erhoben werden, die Verarbeitung selbst und, im Falle einer Verweigerung der Einwilligung, auf die Folgen bei einer Verweigerung der Einwilligung.

Grundsätzlich soll der Einzelne bestimmen können, wem er seine Daten zugänglich machen möchte. Bei Vertragsabschlüssen ist der Betroffene

[116] BT Ds, 14/4329, S.33.
[117] Taeger/Gabel u.a., BDSG, 2010, § 3a, Rn. 54.

oftmals darauf angewiesen die Einwilligung zu erteilen, da, beispielsweise bei Arbeitsverträgen, ein Verzicht des Vertragsschlusses keine Alternative für den Betroffenen darstellt. Die Entscheidungsfreiheit ist somit meist als fiktiv anzusehen.[118] Eine Preisgabe von persönlichen Daten unter diesen Umständen ist immer dann zulässig, wenn durch den Vertragsschluss ein sachgerechter Interessensausgleich vorgenommen wird.[119]

Der Gesetzgeber erwartet vom Betroffenen, sich in Kenntnis der Sachlage zu befinden, wenn er seine Einwilligung erteilt. Er muss erkennen können, welche Wirkung seine Entscheidung auf den weiteren Umgang mit seinen Daten hat.[120] Eine pauschale Einwilligung ist immer dann unzulässig, wenn für den Betroffen nicht ersichtlich ist, zu welchem bestimmten Zweck die Datenverwendung stattfinden soll.[121] Die Art der personenbezogenen Daten sowie der Zweck der Erhebung müssen hinreichend genau offengelegt werden.[122]

Weiterhin handelt es sich bei der Einwilligung um eine in die Zukunft gerichtete Zustimmung. Wurden Daten in der Vergangenheit ohne eine vorliegende Einwilligungserklärung erhoben oder verarbeitet, so kann diese auch nicht durch eine nachträgliche Zustimmung erteilt werden.[123]

Charakteristisch für Big Data ist die Analyse von zahlreichen Daten aus unterschiedlichen Quellen. Oftmals ergeben sich hieraus Hürden in der Praxis, da zum Zeitpunkt der Datenerfassung der Zweck noch nicht bestimmt ist und eine genaue Verwendung noch nicht bekannt.[124]

5.4 Datenschutz und Big Data

Wie bereits zu Beginn erläutert, handelt es sich bei Big Data zusammengefasst um eine Verknüpfung von endlosen Datenmengen, um wirtschaftliche, soziale oder wissenschaftliche Erkenntnisse zu gewinnen

[118] Däubler/Klebe u.a., BDSG, 2014, S. 154, Rn. 2a.
[119] Taeger/Gabel, BDSG, 2013, S. 183, Rn. 54.
[120] Pollmann, DuD, 6/2016, S. 378.
[121] Taeger/Gabel, BDSG, 2013, S. 174, Rn. 30.
[122] Däubler/Klebe u.a., BDSG, 2014, S. 162, Rn. 18f.
[123] Taeger/Gabel, BDSG, 2013, S. 175, Rn. 32.
[124] vbw (Hrsg.), Zukunft digital, 2016, S. 97.

und zu nutzen. Als Rohstoff des 21. Jahrhunderts benannt[125], wirft Big Data zahlreiche datenschutzrechtliche Fragen auf.

Datenschützer befürchten, dass das informationelle Selbstbestimmungsrecht und die Privatsphäre gefährdet sind.[126]

Wie bereits zu Beginn dieses Kapitels erläutert, besteht nach § 1 Abs. 1 i.V.m. § 3 Abs. 1 BDSG ein Anspruch auf Datenschutz, wenn personenbezogene Daten vorliegen. Die Bedeutungszunahme der digitalen Vernetzung hat zur Folge, dass derzeit geltende Regelungen zum Umgang mit personenbezogenen Daten angepasst werden müssen, um einerseits für Big-Data-Anbieter Rechtssicherheit zu schaffen und andererseits die Persönlichkeitsrechte der Betroffenen weiterhin zu schützen.[127]

Für Big Data ist es grundsätzlich irrelevant, ob Analysen mit personenbezogenen Daten oder mit nicht personenbezogenen Daten durchgeführt werden. Dass nicht personenbezogene Daten keinen gesetzlichen Schutz genießen, führt zur Zulässigkeit eines uneingeschränkten Umgangs mit diesen.[128]

Das Risiko der Gefährdung der informationellen Selbstbestimmung besteht nunmehr darin, dass durch die Kombination von zahlreichen Einzeldaten dennoch Rückschlüsse auf eine einzelne Person gemacht werden können und ein Profil erstellt werden kann.[129] Hierbei handelt es sich um Daten aus verschiedenen Quellen und aus verschiedenen sozialen Zusammenhängen, welche zu unterschiedlichen Zwecken erhoben wurden.[130] Man geht davon aus, dass bereits vier Einzeldaten ausreichen können, um einen Personenbezug zu erstellen.[131]

[125] Mangold, Podcast, siehe URL 14.
[126] Marnau, DuD, 7/2016, S. 428.
[127] Marnau, DuD, 7/2016, S.428.
[128] Roßnagel u.a., DSR, 2016, Bd. IV, S.25.
[129] Bräutigam/Klindt, NJW 2015, S. 1141.
[130] Roßnagel u.a., DSR, 2016, Bd. IV, S.26.
[131] vbw (Hrsg.), Zukunft digital, 2016, S. 94

5.5 Datenschutzrechtliche Defizite

Das derzeit geltende Datenschutzrecht entstammt, wie bereits im vorangehenden Kapitel erwähnt, aus den 60/70er Jahren. Daten wurden in eigenen Rechenzentren verarbeitet und die Verarbeitung war für Betroffene kontrollierbar.[132] Die weltweite Vernetzung und Big Data erfordern Anpassungen in beide Richtungen. Einerseits, um Abwehrrechte der Betroffenen zu stärken und andererseits, um Verwertungsrechte der Beteiligten am Big Data Wertschöpfungsprozess zu bewahren.[133]

Vor allem hinsichtlich der geltenden Datenschutzprinzipien besteht Handlungsbedarf, um die Rechte der Betroffenen zu schützen. Die Prinzipien der Zweckbindung, Transparenz und Erforderlichkeit sowie Datensparsamkeit sind bei den heutigen Möglichkeiten der Speicherung, Erfassung und Auswertung nach derzeitigem Recht schlicht veraltet.[134]

Big Data schafft neue Verhältnisse, bei welchen zahlreiche Zwecke verfolgt werden können und ein Personenbezug zu Beginn noch nicht klar ist. Auch erfolgt die Datenverarbeitung oftmals unbemerkt und ist für den Betroffenen nicht zu durchschauen.[135]

Der Grundsatz der Transparenz besagt, dass die betroffene Person immer darüber informiert sein muss, welche Daten erhoben werden und zu welchem Zweck die Datenerhebung stattfindet. In der Praxis ist dies jedoch kaum zu realisieren – kaum ein Anwender von smarten Technologien, welche den Menschen im Hintergrund im Alltag unterstützen, wäre bereit, zu jeder einzelnen Datenerhebung eine Kenntnisnahme zu bestätigen oder einen Hinweis hierzu erhalten zu wollen.[136]

Vor allem bei der Datenerhebung im Fahrzeug entsteht hier ein Konflikt. Die von Unternehmen beliebteste Lösung zur Legitimierung der Datenerhebung stellen vertraglich vereinbarte datenschutzrechtliche Einwilligungserklärungen dar. Diese wird vorab schriftlich erteilt – sie erstreckt sich somit im Grunde nur auf den Käufer des Fahrzeuges. Eine

[132] Roßnagel, Modernisierung des DsR, 2012, Bd. 1190, S. 331.
[133] vbw (Hrsg.), Zukunft digital, 2016, S. 32.
[134] Roßnagel u.a., DSR, 2016, Bd. IV, S.92.
[135] Roßnagel u.a., DSR, 2016, Bd. IV, S.99.
[136] Roßnagel u.a., DSR, 2016, Bd. IV, S.100.

Einwilligung von weiteren Insassen oder anderen Fahrern im Fahrzeug ist nicht vorhanden. Auch eine solche vorab von jeder einzelnen Person unterzeichnen zu lassen, wird sich in der Praxis kaum umsetzen lassen. Weiterhin bleibt ungeklärt, inwieweit die Freiwilligkeit zur Einwilligung unberührt bleibt. Neben zahlreichen Connectivity-Diensten könnten dem Nutzer auch der Zugriff auch sicherheitsrelevante Dienste wie eCall verwehrt bleiben. Um diesen Dienst nutzen zu können, werden betroffene Personen weiterhin ihre Einwilligung geben. Mehr Transparenz könnte hier Abhilfe schaffen, wobei die betroffene Person bereits vor Abschluss des Kaufvertrages dahingehend sensibilisiert wird, in welchem Ausmaß die Datenerhebung und -verarbeitung stattfindet.[137]

Möglicherweise können mit Einführung der neuen Datenschutzverordnung diese Defizite ausgeglichen werden. Dies soll im Folgenden geklärt werden.

[137] Schwartmann, RDVonline, Teil 1, 2015.

6. Die neue Datenschutz-Grundverordnung

Das aktuell noch geltende Datenschutzrecht verfolgt das hauptsächliche Ziel, die natürliche Person vor Beeinträchtigungen im Persönlichkeitsrecht zu schützen, sodass jede Verarbeitung daran gemessen werden muss. Die neue Datenschutzgrundverordnung soll für Europa einen neuen und einheitlichen Rechtsrahmen für den Datenschutz schaffen. Bereits am 25.01.2012 wurde der erste Vorschlag einer Europäischen Datenschutz-Grundverordnung von der EU-Kommission vorgelegt.[138]

Territoriale Grenzen werden durch Art.3 DSG-VO bestimmt. Die Datenschutzverordnung soll zukünftig auch über die Grenzen der Europäischen Union Anwendung finden. Hierbei genügt es, dass sich die betroffene Person in der EU aufhält, deren personenbezogene Daten von einem Verantwortlichen verarbeitet werden, dessen Niederlassung nicht in der Union ist.[139]

Die EU-DSGVO wird die derzeit geltende EU-Datenschutzrichtlinie und somit das BDSG in seiner derzeitigen Fassung ersetzen, die Grundlagen bleiben jedoch bestehen; es wird sich weiterhin um ein Verbotsgesetz mit Erlaubnisvorbehalt handeln.[140]

6.1 Änderungen und Anpassungen in der DSG-VO

6.1.1 Personenbezug

Sowohl das BDSG in § 3 Abs. 1, als auch die DSG-VO in Art. 4 Nr. 1, 1. HS definieren den Begriff der personenbezogenen Daten[141] kurz und prägnant. Der zweite Halbsatz enthält nunmehr eine genauere Definition des Personenbezuges, wonach eine natürliche Person als identifizierbar angesehen wird, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen,

[138] COM (2012) 2012/0011 v. 25.01.2012.
[139] Baum/Reiter/Methner, Rechtsgutachten Datenkontrolle, 2016, S. 6.
[140] Albrecht/Jotzo, Das neue DsR der EU, 2017, S. 50, Rn. 2.
[141] Siehe S. 27.

genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind. Die Erweiterung zu einem Personenbezuges ergibt sich in Verbindung mit Erwägungsgrund 26 der Verordnung. Auch Daten, welche vorher zwar einer Pseudonymisierung unterzogen wurden, könnten durch Heranziehen weiterer Informationen wieder einer natürlichen Person zugeordnet werden und sollen in Zukunft als Information über eine natürliche Person angesehen werden. Weiterhin führt der Erwägungsgrund aus, dass alle Mittel zur Nutzung für eine Identifizierung des Betroffenen berücksichtigt werden müssen. Die Verordnung stellt hierbei auch auf den Aufwand ab, welcher für eine Identifizierung maßgeblich ist. Es sollen alle objektiven Faktoren beachtet werden, wie die Kosten für eine solche Identifizierung und der dafür erforderliche Zeitaufwand unter Berücksichtigung der verfügbaren Technologien und technologischen Entwicklungen.[142] Wenn die Datenverarbeitung den Personenbezug ohne unverhältnismäßigen Aufwand herstellen kann, handelt es sich um einen relativen Personenbezug.[143]

Auf der anderen Seite steht der absolute Personenbezug.[144] Bei einem absoluten Personenbezug geht man wiederum davon aus, dass alle Daten personenbezogen sind, bei welchen nicht auszuschließen ist, dass sie mit einer natürlichen Person in Verbindung gebracht werden können. Diese Annahme wird durch Erwägungsgrund 30 DSG-VO bestärkt. Hiernach können unter Umständen jeder natürlichen Person Online-Kennungen (z.B.: IP-Adressen, Cookies, etc.), die durch sein Gerät oder Software-Anwendungen geliefert werden, zugeordnet werden.

Die DSG-VO legt sich hinsichtlich einer klaren Festlegung zum Personenbezug jedoch nicht fest und verteilt die genaue Begriffsbestimmung über drei verschiedene Vorschriften.[145]

Ein Personenbezug entscheidet weiterhin über eine grundlegende Anwendung des Datenschutzrechts. Die Tendenz geht zu einer Weitung des Begriffs des Personenbezugs. Jedoch bleibt die Schwierigkeit bei der

[142] VO (EU) 2016/679 v. 27.04.2016, L 119/5 (26).
[143] Härting, Internetrecht, 2014, Rn. 187ff.
[144] Härting, DSGVO, 2016, S. 75, Rn. 285.
[145] Härting, DSGVO, AnwBl 11, 2016, S. 810.

Entscheidung, wann ein personenbezogenes Datum vorliegt und wann nicht, weiter bestehen.[146]

6.1.2 Zweckbindung und Einwilligung

Im Hinblick auf eine Kontroverse zwischen dem Schutz der Betroffenen und dem Bedürfnis nach Innovationsoffenheit hat die Europäische Union Erweiterungen hinsichtlich der weiterhin erforderlichen Zweckbindung vorgenommen. Wenn die Verarbeitung nicht zu dem nach Art. 5 Abs. 1 Buchst. b) der DSG-VO vorher bestimmten, eindeutigen und legitimen Zweck und auch nicht mit der Einwilligung der betroffenen Person erfolgt, so werden auch all jene Zwecke berücksichtigt, die eine Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung aufweisen.[147]

Diese Ausweitung der Zweckbindung könnte insoweit zur Folge haben, dass der Handlungsspielraum im Hinblick auf die Verwendung von im Fahrzeug gesammelten Daten deutlich – zu Gunsten der verarbeitenden Stellen – erweitert wird. Die nunmehr sog. Zweckvereinbarkeit nach Art. 6 Abs. 4 DSG-VO stellt eine Flexibilisierung des Grundsatzes der Zweckbindung dar. Somit wird die Erhebung für einen zunächst nicht absehbaren, aber naheliegenden Zweck, nicht mehr zwangsläufig zu einem Verarbeitungsverbot.[148]

Auch in der DSG-VO bleibt die Einwilligung des Betroffenen zur Datenverarbeitung weiterhin als eines der wichtigsten Erlaubnistatbestände für eine zulässige Datenverarbeitung bestehen. Die DSG-VO bestärkt lediglich, dass die Einwilligung freiwillig und ohne Zwang erteilt werden muss. Eine Ausführung, welche Tatbestände als freiwillig und nicht freiwillig angesehen werden könne, führt Erwägungsgrund 32 weiter aus.[149]

[146] GDD/ZAW (Hrsg.), Werbung und Kundendatenschutz nach der DSG-VO, 2016, S.25.
[147] DSG-VO Art.6 Abs. 4 v. 29.04.2016.
[148] Roßnagel, Europ. DSG-VO, S. 253, Rn. 121.
[149] VO (EU) 2016/679 v. 27.04.2016, L 119, S. 6.

6.1.3 Kopplungsverbot

In Art. 7 Abs. 4 DSGVO findet sich des Weiteren ein Kopplungsverbot. Von einer Kopplung im Datenschutz wird ausgegangen, wenn eine Leistungserbringung oder ein Vertragsabschluss von der Einwilligung des Betroffenen zur Datenverarbeitung abhängig gemacht wird und der Betroffene faktisch keine andere Wahl hat, als seine Einwilligung abzugeben, um die Dienstleistung oder das Produkt aus der vertraglichen Leistung zu erhalten.[150] Diese Regelung findet sich in § 28 Abs. 3b S.1 BDSG nur sehr schwach formuliert. Zukünftig wird sich die Einwilligung nur noch auf solche Daten beziehen dürfen, welche tatsächlich zur Erfüllung des konkreten Zweckes bei einem Vertragsabschluss benötigt werden.[151] Der Wegfall der Koppelung führt somit auch zu einem Entfall von möglichen Druck-Situationen, in welchen der Betroffene die Leistung nur erhält, wenn er seine Einwilligung erteilt, obwohl er dies unter anderen Umständen nicht getan hätte.[152]

6.2 Neuregelungen in der DSG-VO

6.2.1 Privacy by Design

Während die bestehenden Datenschutzprinzipien im BDSG noch schwächer ausgeprägt waren, erhalten sie durch die DSG-VO Stärkung und es werden zwei neue Prinzipien hinzugefügt.[153]

Auf Grundlage des Art. 25 Abs. 2 DSG-VO werden die datenverarbeitenden Stellen zunächst zu Privacy by Design verpflichtet. Dieses neu formulierte Prinzip verfolgt das Ziel, die Privatsphäre des Betroffenen bereits während der Produktentwicklung zu schützen.[154]

So soll bereits während der Programmierung von Applikationen sichergestellt werden, dass diese schon von Anfang an alle datenschutzrechtlichen Anforderungen erfüllen. So muss der Verantwortliche geeignete technische und organisatorische Maßnahmen

[150] Stemmer, DSR, DS-GVO, 2017, Art. 7, Rn. 40.
[151] Dehmel, ZD-Aktuell 2013, 03418.
[152] Kroschwalt, DuD Fachbeiträge, 2016, S. 247.
[153] Härting, DSGVO, 2016, S. 24, Rn. 81.
[154] Schneider, AnwBl, 2011, S. 233.

treffen, mit welchen sichergestellt werden kann, dass nur die personenbezogenen Daten verarbeitet werden, die auch tatsächlich für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Folglich soll der Schutz vorbeugen und eine proaktive Wirkung entfalten und nicht eine reaktive, was lediglich im Sinne einer Abhilfe wirken würde.[155]

Die zu ergreifenden Maßnahmen müssen für den Verantwortlichen dennoch zumutbar sein, um die durch Art. 5 DSG-VO vorgegebenen Ziele zu erreichen. Die Zumutbarkeit bemisst sich unter anderem am Stand der Technik, aufkommenden Implementierungskosten, sowie an der Wahrscheinlichkeit für eine Verwirklichung von Risiken und der damit verbundenen Schwere der Risiken, welche in Konsequenz darauf für die Rechte der Betroffenen entstehen würden.[156]

Im Hinblick auf Big Data muss nunmehr die Frage beantwortet werden, in welchem Verhältnis das datenschutzrechtliche Interesse und das wirtschaftliche Interesse stehen. Mit Einführung von Privacy by Design muss der Hersteller und auch die für die Datenverarbeitung Verantwortlichen entscheiden, ob diese Vorgabe bei der Entwicklung hingenommen werden kann und ab welchem Zeitpunkt die informationelle Selbstbestimmung gefährdet sein kann, sodass es wirtschaftlich nicht tragbar wäre, das Produkt weiter zu entwickeln.[157]

Privacy by Design verpflichtet den Hersteller somit zu technischen und organisatorischen Maßnahmen und zeitgleich zu Privacy by Default.[158]

6.2.2 Privacy by Default

Privacy by Default steht für datenschutzfreundliche Voreinstellungen bei den Produkten. Es soll für den Nutzer einen Grundschutz darstellen, durch welchen eine Weitergabe von personenbezogenen Daten vor einer expliziten Zustimmung des Nutzers standardmäßig nicht gestattet ist.[159] Dieser kann individuell entscheiden, welche Einstellungen er verändert haben möchte um transparenter zu sein.

[155] Schulz, CR, 2012, S. 204f.
[156] Härting, DSGVO, 2016, S. 31, Rn. 112.
[157] Markl/Löser/Hoeren u.a., Big Data Management, 2013, S. 66.
[158] Härting, DSGVO, 2016, S. 30, Rn. 112.
[159] Microsoft (Hrsg.) Privacy by Default, März 2012, siehe URL 15.

Artikel 25 Abs. 2 DSG-VO schreibt vor, dass diese Verpflichtung für die Menge der erhobenen personenbezogenen Daten gilt, für den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Derartige Maßnahmen müssen sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Zusammenfassend dient Privacy by Default dem Ziel der Datensparsamkeit, sodass eine betroffene Person davon ausgehen darf, dass die eigene Privatsphäre unberührt ist und bleibt, wenn sie nicht von sich aus Änderungen vornimmt.[160]

6.2.3 Das vernetzte Fahrzeug und die DSG-VO

Die neue Datenschutzverordnung wird alle Beteiligten der modernen Technologien vor Herausforderungen stellen. Bei zahlreichen Anwendungsmöglichkeiten im Fahrzeug fallen, wie bereits erwähnt, unabdingbar personenbezogene Daten an, weshalb es bereits jetzt nötig ist, technische Entwicklungen an die Anforderungen der DSG-VO anzupassen.

Die Hersteller versuchen stetig, ihre Systeme datenschutzrechtlich zu optimieren. So sollen beispielsweise die im Fahrzeug verbauten Kameras eine automatische Löschfunktion haben, um jegliches Bildmaterial, welches älter als 15 Sekunden ist, unwiderruflich löscht. Lediglich im Falle einer schweren Erschütterung in Folge eines Unfalls soll diese Funktion abgeschaltet werden.[161]

Vor allem beim vernetzten Fahrzeug müssen spezifische Regelungen herrschen, um Risiken bei der Verarbeitung von personenbezogenen Daten rechtzeitig zu erkennen und den Beteiligten eine rechtssichere Umgangsweise gewährleisten zu können.[162]

Auch weiterhin wird die freiwillige Einwilligung das Instrument für die Rechtmäßigkeit der Datenverarbeitung in der Automobilbranche bleiben.

[160] Rost/Bock, DuD, 2011, S. 31.
[161] Baum/Reiter/Methner, Rechtsgutachten Datenkontrolle, 2016, S. 23.
[162] 52. Deutscher Verkehrsgerichtstag (Hrsg.), Empfehlung, Januar 2014.

6.3 Fortschritt

Bislang verfügt jeder Mitgliedsstaat der EU über ein eigenes Datenschutzgesetz. Dies hat zur Folge, dass das Niveau von Land zu Land unterschiedlich ist und somit kein gleicher Schutz für die Betroffenen gewährleistet werden kann.

Durch die Verordnung wird das Datenschutzrecht innerhalb der EU harmonisiert. Folglich sind alle Bürger der EU gleichwertig geschützt. Die DSG-VO findet mithilfe Art. 3 Abs. 2 DSG-VO auch Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung unter bestimmten Voraussetzungen erfolgt. Somit müssen insbesondere auch US-Unternehmen die Vorgaben der Europäischen Union befolgen, um weiterhin ihre Dienste anbieten zu können. [163]

Das geltende Recht kennt weder den Begriff des Konzerns, noch ein damit verbundenes „Konzernprivileg“. In Art. 4 Nr. 19 DSG-VO wird der Konzern nunmehr als Unternehmensgruppe näher definiert: eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht. Ein Konzernprivileg soll im Datenschutzrecht den erleichterten Datenfluss zwischen den verbundenen Unternehmen beschreiben. Im BDSG haben Konzerne drei Möglichkeiten, um einen rechtlich abgesicherten Datenaustausch vollziehen zu können – die Einwilligung, die gesetzliche Erlaubnis sowie die Auftragsdatenverarbeitung.[164] Für Unternehmen ergibt sich nunmehr der Vorteil, dass auf die Fahrzeugdaten des Kunden europaweit zugreifen können, unabhängig davon, in welchem europäischen Land und Werkstätte dieser sich aufhält. Eine gesonderte Einwilligung müsste somit aufgrund der unternehmensübergreifenden Datenübermittlung nicht mehr erbracht werden.[165]

[163] Ackermann, EU-DS-GVO, 14.04.2017, siehe URL 16.
[164] Härting, DSGVO, 2016, S. 118 , Rn. 485.
[165] Acatech (Hrsg.), Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S. 122.

Diese Wege sind aber in der Praxis aufwendig, weshalb Unternehmen durch die DSG-VO teilweise eine Erleichterung erfahren. So wird die Verarbeitung, gestützt auf Art. 6 Abs. 1 S. 1 lit. F DSG-VO, rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Ein berechtigtes Interesse kann nach Erwägungsgrund 48 der DSG-VO immer dann bestehen, wenn personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, übermittelt werden. Dass die DSG-VO keine Differenzierung zwischen Datenverarbeitungen für eigene Zwecke und denjenigen zur Wahrung berechtigter Interessen Dritter vornimmt, erleichtert die Datenübermittlungen zwischen Konzerngesellschaften.[166]

Ein weiterer Aspekt, von Datenschützern befürwortet, ist die Neuregelung der hohen Bußgelder für Verstöße gegen die Datenschutzbestimmungen. So kann Unternehmen je nach Verstoß ein Bußgeld von bis zu 20 Millionen Euro auferlegt werden, bzw. bis zu 4% des globalen Unternehmensumsatzes.[167]

Im Allgemeinen wird eine einheitliche, europaweite Datenschutzregulierung begrüßt, jedoch weist die EU-Verordnung bereits Defizite auf, auf die im Folgenden eingegangen werden soll.

6.4 Defizite

Die neue DSG-VO erfährt jedoch auch zahlreiche Kritik und weist Defizite auf, welche im Hinblick auf reale Risiken und Gefährdungslagen nicht ausreichend geklärt sind. Kritiker befürchten, dass die Verordnung auf europäischer Ebene zwar ein Fortschritt ist, für das Niveau des deutschen Datenschutzrechtes jedoch ein Rückschritt.[168] Dies begründet sich vor allem in der Starrheit der Verordnung, welche als solche von den Mitgliedsstaaten nicht verändert werden darf. Jedoch wird das geltende

[166] Gola/Pötters/Wronka, ArbeitnehmerDS, 2016, S. 176, Rn. 547.
[167] Knierim/Rübenstahl/Tsambikakis, Internal Investigations, 2016, S. 330, Rn. 4.
[168] Becker, EU-DSGVO, siehe URL 17.

Datenschutzrecht in Deutschland nicht vollständig aufgehoben sein. Stehen nationale Vorschriften im Widerspruch zur Verordnung, so sind diese grundsätzlich aufgehoben, sie gelten allerdings weiter fort, wenn die deutsche Regelung die Vorschrift der DSGVO präziser und konkreter erarbeitet. Bereits vor diesem Hintergrund wird allein durch die Frage, welche Regelung für den Einzelfall letztendlich anwendbar ist, neue Rechtsunsicherheit entstehen.[169]

Wie bereits näher beschrieben, erlaubt das BDSG die Verwendung von personenbezogenen Daten, wenn ein im Voraus festgelegter Zweck bestimmt wurde und auch nur hierfür verwendet werden dürfen. Zukünftig wird nach Art. 6 Abs. 3a DSG-VO eine „zweckkompatible“ Verarbeitung zulässig sein. Wann eine Kompatibilität gegeben ist, wird jedoch nicht näher genannt, es werden lediglich Erwägungsaspekte genannt. So wird es beispielsweise in Zukunft ausreichend sein, wenn zwei Zwecke in einer Verbindung zueinander stehen, um eine Datenverarbeitung zu rechtfertigen.[170] Das Zweckbindungsprinzip wird durch die DSG-VO nicht schwerwiegend gelockert, das Schutzniveau des BDSG wird jedoch nicht erreicht.

Die grundlegende Problematik der DSG-VO liegt im Missverhältnis zwischen der regelungsbedürftigen Komplexität einerseits und der Unterkomplexität aufgrund ihrer Beschränktheit und Abstraktheit der Vorschriften andererseits.[171] Die DSGVO enthält 51 materiell-rechtliche Vorschriften[172], welche alle möglich aufkommenden Probleme lösen sollen, für welche im bestehenden Datenschutzrecht in Deutschland tausende Vorschriften benötigt werden und unterschätzt somit den komplexen Regelungsbedarf. Während die DSGVO sich in zahlreichen Vorschriften noch an Zielen der Datenschutzrichtlinie von 1995 orientiert[173], wird verkannt, dass Datenverarbeitung und Datenschutz zu einem allgegenwärtigen Thema der heutigen Gesellschaft geworden sind, welche nicht unterschätzt werden dürfen.

[169] Roßnagel, Alexander, Europ. DSG-VO, 2016, S. 342.
[170] Becker, EU-DSGVO, siehe URL 17.
[171] Roßnagel, DuD, 9/2016, S.564.
[172] Siehe DSGVO, Kapitel I bis V sowie Art. 82.
[173] RL 95/46/EG, ABl. L 281 vom 23.11.1995, Rn. 31.

Die DSGVO nennt keine konkreten Adressaten dieser Verordnung und verhält sich technikneutral. Dies hat zur Folge, dass auf technische Funktionen wie beispielsweise Big Data und Cloud Computing, welche bereits jetzt zu datenschutzrechtlichen Problemen führen, nicht explizit eingegangen wird und somit auch zukünftig den Datenschutz vor Probleme stellen wird, obwohl genau diese Herausforderungen eine konkrete Betrachtungsweise erfordern.[174]

Die Rechtslage des Datenschutzes verkompliziert sich insoweit, dass zahlreiche Vorschriften sehr abstrakt formuliert sind, weshalb davon auszugehen ist, dass die Regelungen von den Gerichten der einzelnen Mitgliedsstaaten weiterhin sehr unterschiedlich angewandt werden, weshalb die bereits bestehende Rechtsunsicherheit noch weiter verstärkt wird.[175]

Auf die Automobilbranche hat die DSG-VO unterschiedliche Auswirkungen. Zahlreiche Kunden befürchten bei einer Nutzung der Connected-Car-Dienste eine Weitergabe ihrer personenbezogenen Daten an Dritte und mangelnde Transparenz. Diesem kann durch Privacy by Design entgegengewirkt werden, da sich bereits in der Entwicklungsphase kritische Prozesse mit datenschutzrechtlichen Maßnahmen befasst wird. So können neue Kunden gewonnen werden, welche diese Dienste nunmehr nutzen möchten.[176]

Auf der anderen Seite jedoch können die Neuregelungen ein Hemmnis für weitere Entwicklung hin zum vollautomatisierten Fahrzeug sein. Ideen hin zu Entwicklungen, mit welchen man einen datenschutzrechtlichen Graubereich betreten würde, können so bereits zu Beginn verworfen werden, welche für das Connected Car vorteilhaft wären.

[174] Roßnagel, DuD, 9/ 2016, S.565.
[175] Roßnagel, Europ. DSG-VO, 2016, S. 342.
[176] Wirnsperger, Privacy by Design im Automobilsektor, siehe URL 18.

7. Exkurs: Haftungsregelungen

Wie bereits zu Beginn näher erläutert, ist ein grundlegendes Ziel der gänzlichen und teilweisen Automatisierung des Fahrzeugs die Steigerung der Sicherheit im Straßenverkehr. Bis zu 86% aller Unfälle beruhen auf Fehlverhalten des Fahrers.[177]

Das Einsetzen von Assistenzsystemen unterstützt den Fahrer, indem es Aufgaben ganz oder teilweise übernimmt. So stehen Autokäufern bereits jetzt Fahrzeuge mit solchen Assistenten zur Verfügung, sei es zur Lenkung, Spurhaltung und auch Bremsung. Automatisierte Fahrzeuge können den Fahrer einerseits entlasten, andererseits können sie Menschen, welchen das selbstständige Führen eines Fahrzeuges, beispielsweise aufgrund einer Behinderung oder des Alters, verwehrt bleibt, eine individuelle Mobilität ermöglichen.[178] Es verspricht dem Fahrer neben der Entlastung einen nicht unerheblichen Komfortgewinn. Jedoch ist nicht auszuschließen, dass trotz strengster Anforderungen an technische Gegebenheiten ein Unfall durch ein automatisiertes Fahrzeug verursacht wird.[179]

Im Mai 2016 erhielt der Automobilhersteller Tesla mediale Aufmerksamkeit, als ein Fahrer von Tesla tödlich verunglückte, nachdem das Auto ungebremst mit einem Lastzug kollidierte, welcher die Straße kreuzte. Hierbei sollen weder das Assistenzsystem, noch der Fahrer das andere Fahrzeug registriert haben.[180]

Jüngste Erkenntnisse haben zwar ergeben, dass es sich hierbei nicht, wie zu Beginn der Ermittlungen angenommen, um einen Software-Fehler gehandelt hat, sondern dass die Schuld beim Fahrer gelegen hat und keine Dysfunktionen am Autopiloten vorlagen.[181]

[177] Hütter, Statistisches Bundesamt, 2013, S. 38.
[178] Lutz, NJW, 2015, Rn.119.
[179] Hans, GWR, 2016, S. 393.
[180] Vetter, Die Welt, 2016, siehe URL 19.
[181] Lindner, faz, 2017, siehe URL 20.

7.1 Haftung im Schadensfall

Jedoch stellt sich nunmehr die Frage, wer in einem solchen Fall für die entstandenen Schäden haftbar gemacht werden kann, wenn ein hoch automatisiertes Fahrzeug ein „(Mit-)Verschulden“ am Unfall trägt.

Zunächst könnte eine Haftung gemäß der StVG in Frage kommen. Gemäß § 7 StVG ist der Halter eines Kraftfahrzeuges dazu verpflichtet dem Geschädigten den entstandenen Schaden zu ersetzen, wenn der Schaden durch das Fahrzeug verursacht wurde. Ist der Führer des Fahrzeuges nicht der Halter, so kann dieser gem. § 18 StVG ebenso zum Ersatz des Schadens verpflichtet werden. Ein Ausschluss der Ersatzpflicht ist immer nur dann anzunehmen, wenn er den Unfall nicht verschuldet hat.

Wird jedoch ein (technischer) Schaden durch einen Fehler des Fahrzeuges verursacht, so kommt eine Haftung gemäß der Produkt- und Produzentenhaftung des Herstellers in Frage.[182] Zahlreiche Bauteile, einschließlich der verwendeten Softwareprogramme, stammen oftmals von Automobilzulieferern. In einem Schadensfall hat der Hersteller jedoch nicht die Möglichkeit zur Exkulpation, indem er sich darauf beruft, dass es sich beim mangelhaften Teil um ein Zulieferprodukt handelt. Dessen ungeachtet kann der Hersteller später den Zulieferer des Bauteils in Regress nehmen, wenn der verschuldete Schaden dem Zulieferer zuzurechnen ist.[183]

Vor allem im Bereich der Betriebssoftware sind die Anforderungen an eine fehlerfreie Funktion enorm hoch, da eine einwandfreie Funktion die Sicherheit der Fahrzeuginsassen gewährleisten muss. Die Gefährdung von Körper und Leben durch Fehlfunktionen der Software soll stets ausgeschlossen werden können.

Fraglich ist, ob ein während einer automatisierten Fahrt erfolgter Unfall ursächlich als ein Produktfehler gewertet werden kann. Voraussetzung hierfür müsste sein, dass die Ursache des Schadens nicht dem Fehlverhalten eines anderen Verkehrsteilnehmers zuzurechnen ist oder der Fahrer des verunfallten Fahrzeugs mit einer Übersteuerungshandlung

[182] Geissl, RAW, 2013, S. 24 ff.
[183] Hans, GWR, 2016, Rn. 393.

eingegriffen hat. Handelt es sich bei einer fehlerhaften automatisierten Entscheidung des Steuergerätes um einen Produktfehler, so könnte der Automobilhersteller regelmäßig bei einer fehlerhaften Steuerung aufgrund eines Softwarefehlers zivilrechtlich haftbar gemacht werden.[184]

In Folge würde beinahe jedes Mal der Hersteller das Risiko der zivilrechtlichen Haftung für Automatisierungsrisiken tragen, welche mit maschinellem Wirken verbunden sind. In Anbetracht von zahlreichen Einflussmöglichkeiten auf das automatisierte Fahrzeug in der Steuerungssoftware würde sich hier der Anwendungsbereich hinsichtlich steuerungsrelevanter Fehler auch gegenüber dem Fahrzeugführer ausweiten.[185]

Vor diesem Hintergrund haben sowohl der Hersteller, als auch der Zulieferer die Pflicht, das Produkt zu beobachten.

Es könnte somit als sinnvoll erachtet werden, die Möglichkeit einer technischen Trennung von sicherheitsrelevanten Funktionen im Fahrzeug von den übrigen einzurichten, für den Fall, dass eine dieser Funktionen versagen sollte. Die Systemarchitektur soll somit redundant werden, um eine fehlerhafte Interpretation der erfassten Daten zu vermeiden und dem Fahrer rechtzeitig die Kontrolle über das Fahrzeug zu übergeben.[186] Der Hersteller muss zudem Sicherheitsrisiken durch den manipulativen Eingriff von Dritten auf die Betriebssoftware bedenken und vor diesen schützen. Insbesondere durch Viren und Hackerangriffe können bei fortschreitender Vernetzung Sicherheitsrisiken entstehen und damit eine Gefahr für den Fahrzeugführer darstellen.[187]

Man geht bislang davon aus, dass der Inhaber einer potentiellen Gefahrenquelle, hier der verbauten Software, für Schäden haften muss, welche durch eine durch das Produkt ausgelöste Gefahr entstanden sind.[188]

[184] Maurer, Autonomes Fahren, 2015, S.554.
[185] Maurer, Autonomes Fahren, 2015, S.554.
[186] VDA (Hrsg.), Automatisierung, 2015, S.12.
[187] Acatech (Hrsg.), Umsetzungsempfehlungen für das Zukunftsprojekt Industrie 4.0, April 2013, S.50.
[188] Spindler, NJW, 2004, S. 3145.

7.2 Gesetzliche Anpassungen

Der Fortschritt des autonomen Fahrens und die hiermit verbundene Haftungsfrage erfordert für alle Beteiligten mehr Rechtssicherheit. Vor diesem Hintergrund hat die Bundesregierung am 27.01.2017 einen Gesetzesentwurf zur Änderung des Straßenverkehrsgesetzes eingereicht.[189] Ziel dieser Gesetzesänderung ist eine rechtliche Gleichstellung des hoch- oder vollautomatisierten Fahrsystems mit dem menschlichen Fahrer.[190] Die Änderungen sollen bewirken, dass der Fahrer nur noch dann die Fahrzeugsteuerung übernehmen muss, wenn er von dem vollautomatisierten System dazu aufgefordert wird. Weiterhin soll der menschliche Fahrer die Kontrolle übernehmen, wenn eine bestimmungsgemäße Verwendung der Fahrfunktionen nicht mehr vorliegt. Dies ist insbesondere dann der Fall, wenn das System feststellt, dass sich die Sensorik wetterbedingt verschlechtern wird oder beispielsweise ein Reifen während der Fahrt platzt.[191].

Des Weiteren soll vorgeschrieben werden, dass aus Nachweiszwecken ein Datenspeicher im Fahrzeug eingesetzt wird. Aus diesem Medium soll hervorgehen, ob der Fahrer oder das System zum fraglichen Zeitpunkt die Fahraufgabe innehatte.[192]

Dieser Gesetzesentwurf jedoch wurde von der Opposition stark kritisiert.[193]

Zum einen werde die Verantwortung in Schadensfällen zu sehr auf den Autofahrer und –halter übertragen, die Produkthaftung des Herstellers ist im Entwurf nicht relevant.[194] Gemäß § 1 Abs. 2 Nr. 5 ProdHaftG haftet der Hersteller nicht, wenn der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte. Demnach entfällt die Haftung des Automobilherstellers, wenn ein Unfall auf einem Fehler des

[189] BR DS 69/17, 27.07.17
[190] BMVI (Hrsg.), Gesetzentwurf Bundeskabinett, 25.01.2017.
[191] BR DS 69/17, 27.07.17, Begründung, S.6.
[192] BMVI (Hrsg.), Gesetzentwurf Bundeskabinett, 25.01.2017.
[193] Grah, Umstrittenes Gesetz, 10.03.2017, siehe URL 21.
[194] Krempl, Stefan, Gesetzentwurf zum autonomen Fahren, 10.03.2017, siehe URL 22.

Assistenzsystems beruht, dieses jedoch auf einem aktuellen Stand der Technik ist.[195]

Zum anderen entstehen durch die einzubauende Blackbox datenschutzrechtliche Probleme. Der Entwurf enthält keine konkrete Regelung über die Art und den Inhalt der Fahrdaten, welche im Fahrzeug gespeichert werden. Problematisch ist dies vor dem Hintergrund, dass es sich bei den im Fahrzeug erhobenen Daten um personenbezogene Daten handelt.[196]

Die bislang herrschende Meinung vertritt die Ansicht, dass es hinsichtlich der Haftungsfrage eine Verschiebung weg von einer Halterhaftung hin zu einer Herstellerhaftung stattfinden wird.[197]

[195] Vzbv (Hrsg.), Stellungnahme, 04.01.2017, S. 11.
[196] Voßhoff, Automatisiertes Fahren, 09.03.17, siehe URL 23.
[197] Jänich/Schrader/Reck, NZV 2015, S. 313.

8. Fazit

Im Rahmen der informationellen Selbstbestimmung hat jeder das Recht, selbst über die Verwendung seiner persönlichen Daten zu entscheiden. Durch Fahrzeugsensoren, welche kontinuierlich personenbezogene Daten sammeln und weitergeben, stößt dieses gewährleistete Recht jedoch an Grenzen. Der Stand der Technik und regelmäßige Innovationen geben dem Nutzer zwar das Gefühl von mehr Komfort und Sicherheit, der Überblick und die Kontrollierbarkeit der gesammelten Daten fehlt jedoch zunehmend, weshalb schlussfolgernd das Recht auf informationelle Selbstbestimmung eingeschränkt wird.[198]

Das bislang geltende Bundesdatenschutzgesetz deckt zahlreiche Bereiche bereits gut ab,

Die bald in Kraft tretende Datenschutzgrundverordnung ist zwar in weiten Teilen fortschrittlich, weist jedoch klare Defizite auf. Die Rechtsunsicherheit bleibt auch bei Automobilherstellern und den Zuliefererunternehmen weiter erhalten und Unklarheiten entstehen. Ein möglicher Lösungsansatz wären hierbei bereichsspezifische Vorschriften im Datenschutzrecht, welche Bezug auf das vernetzte Fahrzeug finden.[199]

Weiterhin findet sich in der DSG-VO keine konkrete Regelung im Umgang mit Big Data. Es ist unbestritten, dass mit Hilfe von Big-Data-Anwendungen kaum mehr nicht personenbezogene Daten existieren. In einem vernetzten Fahrzeug sammeln sich geschützte und nicht-geschützte Daten, eine Trennung geschieht in der Praxis nicht hinreichend. Vor diesem Hintergrund wäre es aus datenschutzrechtlicher Sicht sinnvoll, auch nicht personenbezogenen Daten von vorn herein einem gesetzlichen Schutz zu unterstellen, wenn davon ausgegangen werden kann, dass aus diesen Daten ein Personenbezug erstellt werden kann.[200]

Es ist davon auszugehen, dass wenn die DSG-VO am 25.05.2018 in Kraft tritt, der technische Stand diese bereits überholt hat und vor neue

[198] Lüdemann, ZD, 2015, S. 247.
[199] Weichert, SVR, 2014, S. 241.
[200] Lüdemann, ZD, 2015, S. 247.

Fragestellungen stellen wird. Dass jemals ein Datenschutzrecht geschaffen wird, welches alle Fragestellungen und Unsicherheiten abdeckt, ist fraglich und bei ständigen Innovationen der Automobilindustrie kaum zu erfüllen. Der Betroffene entwickelt derzeit ein größeres Bewusstsein für den Schutz seiner persönlichen Daten, ist jedoch gerne bereit, diese preiszugeben, wenn die erhaltene Leistung wie der höhere Komfort und das Entertainmentangebot übereinstimmt.

Für Unternehmen innerhalb der Automobilbranche werden weiterhin rechtliche Risiken bestehen und datenschutzrelevante Fragestellungen zu klären und im Einzelfall zu prüfen sein. Diese Risiken bestehen sowohl für die kleine Vertragswerkstatt, als auch für milliardenschwere Konzerne, eine Differenzierung findet hier nicht statt. Um weiterhin ein hohes Niveau an Datenschutz und Datensicherheit bei vernetzten Fahrzeugen gewährleisten zu können, müssen die Hersteller sich ständig aktiv weiterentwickeln.[201]

Auch im Hinblick auf die schmerzlich hohen Bußgelder bei Verstößen gegen die DSG-VO sind Unternehmen angehalten, Risiken im Voraus zu erkennen und das Produkt vorschriftsmäßig zu entwickeln und zu vermarkten.

[201] VDA (Hrsg.), Datenschutzprinzipien für vernetzte Fahrzeuge, 2014.S.3.