Bachelorarbeit

Zur Erlangung des akademischen Grades LL.B.

Titel: *Der rechtliche Schutz von Fahrzeugdaten*

bei

Prof. Dr. Sebastian Kubis, LL.M. (Illinois)

Wilhelm Peter Radt Stiftungslehrstuhl für Bürgerliches Recht, Gewerblichen Rechtsschutz, Internationales Privat- und Zivilprozessrecht

im Studiengang

Bachelor of Laws

Fernuniversität Hagen, Fakultät für Rechtswissenschaften

vorgelegt von

Dipl.-Ing. Christoph Diemberger, Ayrenhoffgasse 1/26, A-1090 Wien, email: christoph@diemberger.com, Tel: +436801152237, Mat.Nr 9086749

Wien, Dezember 2017

Gliederung

A. Einführung 1
I. Problemaufriss 1
II. Gegenstand und inhaltlicher Aufbau der Arbeit 4
B. Grundlagen 5
I. Begriffsdefinitionen 5
II. Beteiligte Rechtssubjekte 7
III. Schutzziele, Datennutzung und Datenverfügung 8
C. Mögliches Schutzkonzept über eigentumsähnliche Konstruktion 11
I. Direkte Anwendung von § 903 BGB 12
II. Analoge Anwendung von § 903 BGB über § 303a StGB 13
III. Analoge Anwendung von § 903 BGB als *Früchte* über § 99 I BGB bzw. als *Nutzungen* gem. § 100 BGB 15
IV. Rückgriff auf Eigentum am Datenträger 16
V. Zwischenergebnis 17
D. Schutzkonzepte an Fahrzeugdaten ohne eigentumsähnliche Konstruktion 19
I. Schutz von Fahrzeugdaten über das Urheberrecht 19
1. Fahrzeugdaten als Werk gem. § 2 UrhG 19
2. Mögliche Anwendung eines verwandten Schutzrechts des UrhG 22
3. Zwischenergebnis Urheberrecht 23
II. Schutz von Fahrzeugdaten über datenschutzrechtliche Konstruktion 24
1. Datensätze mit Personenbezug über Fahrzeug-Identifikationsnummer 25
a) Datenverarbeitung durch die Werkstatt 25
b) Datenweitergabe durch den Werkstattsbetrieb an den Fahrzeughersteller 26
2. Anonymisierung der Fahrzeug-Identifikationsnummer 28
3. Ergebnisse der datenschutzrechtlichen Analyse 29
III. Schutz von Fahrzeugdaten durch Lauterkeitsrecht 30
1. Fahrzeugdaten als Unternehmensgeheimnis aus Sicht des Fahrzeughalters 31
2. Fahrzeugdaten als Unternehmensgeheimnis des Fahrzeugherstellers 33
3. Nachahmungsschutz gem. § 4 UWG 36
4. Zusammenfassung des lauterkeitsrechtlichen Schutzes 37
IV. Deliktrechtliche Schutzkonzepte aus dem allg. Zivilrecht 38
1. Deliktsrechtliche Schutzkonzepte an Daten gem. § 823 I BGB 39
a) Vertraulichkeitsschutz gem. § 823 I BGB auf „Systemebene“ 39

b) Schutzkonzept § 823 I BGB auf „Datenebene“ 41
2. Deliktsrechtliche Schutzkonzepte an Daten gem. § 823 II BGB i.V.m dem Strafrecht 43
3. Ergebnis der deliktsrechtlichen Analyse 45
V. Bereicherungsrechtliche Schutzkonzepte 47
E. Schlussbetrachtung 49
I. Syntaktische Ebene – Zusammenfassung der Ergebnisse 49
II. Semantische Ebene – Zusammenfassung der Ergebnisse 51
III. Bewertung der Ergebnisse 52
Anhang 54
Literaturverzeichnis 55

A. Einführung

„Wir brauchen ein Datengesetz in Deutschland!“ [1]

Der Überschrift des „Strategiepapiers Digitale Souveränität“, veröffentlicht durch BM Alexander DOBRINDT auf der Webseite seines Ministeriums, mangelt es nicht an Klarheit. Die seit Jahren laufende angeregte rechtswissenschaftliche Debatte über die derzeitige und mögliche zukünftige juristische Behandlung von Daten trat im Jahr 2017 ins politische Rampenlicht. Während andere Spitzenpolitiker der Bundesregierung sich weitgehend darüber einig waren, dass über zusätzliche gesetzliche Regelungen auf nationaler bzw. auf europäischer Ebene zumindest nachgedacht werden müsse, erstaunte BM DOBRINDT bereits mit einem konkreten juristischen Lösungsvorschlag: „*Wir wollen Daten im Ergebnis mit Sachen gleichstellen und damit die Voraussetzung schaffen, dass diese eindeutig natürlichen oder juristischen Personen als ‚Eigentum‘ zugewiesen werden können“.* Passenderweise nimmt der Minister, zwar exemplarisch aber dennoch klar hervorgehoben, Bezug auf die im Automobil erzeugten Daten und begründet damit die Notwendigkeit einer gesetzlichen Initiative. Unter dem Titel „Der rechtliche Schutz von Fahrzeugdaten“ soll die vorliegende Arbeit vorwiegend einen Beitrag auf der Analyseebene und weniger auf der Lösungsebene liefern.

I. Problemaufriss

Ein Automobil besteht heute aus einer Vielzahl von Steuerrechnern[2]. Elektronische Eingangssignale werden von Sensoren und Schaltern aufgenommen, von dem Steuergerät verarbeitet und verknüpft, sowie in weiterer Folge als Steuersignale an Aktoren wieder ausgegeben. Beispielsweise entscheidet ein Steuergerät darüber, ob der mittels Radar (Sensor) gemessene Abstand zum vorausfahrenden Fahrzeug zu gering ist woraufhin eine Notbremsung (Aktor) eingeleitet wird. Auf diese Weise entstehen bis zu 25 GB[3] pro Fahrstunde an Daten. Darunter fallen sogenannte *Sensordaten*, z.B.: Videobilder, Messwerte und logische Zustände von Schaltern. Dazu kommen die Ergebnisse der Datenanalyse in Form von diversen Zwischenverarbeitungszuständen bzw. daraus letztlich die Steuerdaten für die Aktoren. Zum Zwecke der Dokumentation von Betriebszuständen erfolgt die Generierung von Fehler- und Analyseprotokollen. Da die Kosten für Speicherplatz sinken, werden immer größere Anteile des oben genannten Datenvolumens auch dauerhaft im Fahrzeug gespeichert. U.a. für die folgenden Zwecke:

[1] http://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html [abgerufen am 11.10.2017].
[2] sogenannte *Steuergeräte.* Im englischen Sprachgebrauch: *Electronic Control Units (ECU)* .
[3] siehe Fußnote 1.

- Nachträgliche Analyse in der Werkstatt zum Zweck der technischen Diagnose von Defekten
- Nachträgliche Analyse durch den Hersteller zum Zweck der Verbesserung seines Produkts (z.B: Training von Algorithmen, Auswertung von Anomalien im Verhalten der Software bzw. Hardware)
- Zwischenspeicherung von Zuständen um den Bedienkomfort des Fahrers zu erhöhen (z.B: Autositz-Einstellung abspeichern)
- Dokumentation von Zuständen bzw. kompletten Fahrsituationen, die aus gesetzlichen Gründen notwendig[4] oder sich für einen oder mehrere Beteiligte im Nachhinein als nützlich erweisen kann (z.B: Bremsverhalten des Fahrers unmittelbar vor einem Unfall).
- Statistische Auswertungen die durch längerfristige Beobachtung von verschiedenen Datenquellen erhoben werden und Rückschlüsse auf die persönlichen Vorlieben und Eigenschaften des Fahrers erlauben (z.B: Schaltverhalten im Verhältnis zur Motordrehzahl, Fahrziele und Strecken via GPS, Fahrstilbewertung über Beschleunigungssensoren, Nutzungsintensität von im Auto vorhandenen Komfortfunktionen etc.). Diese Informationen können nicht nur vom Hersteller für eine rein technische Produktverbesserung bzw. zur Planung von präventiven Wartungsaktivitäten verwendet werden, sondern können von ihm selbst oder gar durch Weitergabe an andere für produktstrategische Entscheidungen bis zu zielgruppenspezifischen Marketingaktivitäten Einsatz finden.

Mit diesem Wissen stellt sich für den Fahrzeughalter die Frage, ob das Auslesen und Analysieren dieser gespeicherten Daten durch eine andere Person, bspw. den Fahrzeughersteller oder die Werkstatt, für eben diese Person einen Nutzen darstellt. An diesem Nutzen kann der Fahrzeughalter i.A. nicht partizipieren bzw. es könnte sich daraus in speziellen Fällen sogar ein Nachteil für ihn selbst ergeben. Als Beispiel sei der Nachweis einer Fehlbedienung genannt. Der Nachteil muss dabei aber nicht notwendigerweise monetär bezifferbar sein - eine Zuordnung von Verhaltensprofilen, die ohne konkrete Gegenleistung erhoben werden, wird allgemein als zumindest potentiell nachteilig angesehen. Der Fahrzeughalter geht richtigerweise davon aus, dass sein Fahrzeug auf Seiten des Herstellers eindeutig identifiziert ist und daher „seine“ Daten letztlich auch ihm als Person, z.B: über den abgeschlossenen Kaufvertrag, zugeordnet sind.

[4] Verordnung (EG) Nr. 715/2007 i.V.m Nr. 692/2008 sowie diverse US amerikanische Vorschriften zum „Event Data Recorder“ .

Aufgrund der Informationsasymmetrie zwischen Fahrzeughalter und Hersteller in Bezug auf die Art und Menge der abgespeicherten Daten ergibt sich für den Fahrzeughalter daher unmittelbar die Frage, ob er für „seine“ Daten im Fahrzeug eine rechtliche Schutzposition in Form eines Abwehrrechts (z.B: gegen Auslesen oder gegen Löschen) oder gar ein originäres Selbstnutzungs- oder Verfügungsrecht hat. Durch die Anbindung des Fahrzeugs an das Internet, teilweise bereits mit dauerhaft aktivierter Datenverbindung, erfährt diese Fragestellung einen stark gesteigerten Stellenwert.

Als eindringliches Beispiel, welche Möglichkeiten sich alleine auf technischer Ebene ergeben, sei folgendes angeführt: Im Frühjahr dieses Jahres[5] hat *die Tesla Motors Corporation* auf dem Fahrzeugbildschirm ihrer Kunden eine Textmeldung eingeblendet, mit welcher das Unternehmen die Zustimmung zur regelmäßigen Übermittlung von kompletten Videosequenzen, aufgenommen durch die Außenkameras des Fahrzeugs, abgefragt hat. Nach der Zustimmung durch die Benutzer wurden die Videosequenzen über die Internetanbindung des Fahrzeugs direkt an *Tesla* übermittelt und in deren Datencenter für die Weiterentwicklung der Videodetektionsalgorithmen zum autonomen Fahren verwendet. Dass Fahrzeughersteller nicht so transparent vorgehen wenn die datenschutzrechtliche Relevanz der zu übermittelnden Daten nicht so offenkundig und eindeutig ist, stellt der ADAC regelmäßig fest[6]. Die Fahrzeuge übermitteln mehr Daten, als der Hersteller in Eigenwerbung seiner i.A. kostenpflichtigen Telematik-Dienste[7] offenlegt. Auch ohne den Telematik-Zusatzvertrag und ohne weitere Information an den Kunden werden laut ADAC und anderen Quellen[8] bei Werkstattbesuchen regelmäßig Daten ausgelesen und an die Fahrzeughersteller übermittelt. Diese Daten gehen nach ihrem Bedeutungsgehalt deutlich über die technischen Notwendigkeiten für die Erfüllung der eingegangenen Garantieverpflichtung, Produktsicherheit, Ersatzteilbevorratung u.ä. hinaus.

[5] http://www.teslarati.com/tesla-autopilot-fleet-data-sharing-policy/ [abgefragt am 12.10.2017].
[6] https://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/datenkrake_auto.aspx [abgefragt am 12.10.2017].
[7] Bei Telematik-Diensten handelt es sich um Online-Services die der Fahrzeughalter mit dem Fahrzeughersteller per zusätzlichen Vertrag vereinbart. Dabei stellt der Hersteller gegen eine monatliche Gebühr eine GSM Datenkarte für die Internetzugangsverbindung mit dem Fahrzeug bereit. Dem Benutzer werden u.a. Notruf-Services, Remote-Diagnose sowie Fernzugriff auf sein Auto (z.B: Heizung einschalten) angeboten. Auf einem Webportalen kann der Benutzer dann auf aus dem Fahrzeug übermittelte Daten wie z.B: Batterieladestand, Reifendruckanzeige, Kilometerstand etc. zugreifen. Optional werden auch GPS Standortdaten an die zentrale Stelle übermittelt und im Webportal angezeigt.
[8] c’t Magazin für Computertechnik 2016/9 170, 171; *Markey* Report „Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk“ - https://www.markey.senate.gov//imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf [abgefragt am 05.12.2017].

II. Gegenstand und inhaltlicher Aufbau der Arbeit

Gegenstand der Arbeit ist eine Beurteilung, ob es an den genannten Fahrzeugdaten bereits eine Güterzuordnung im rechtlichen Sinne gibt und ob bereichsspezifische Nutzungs-, Abwehr- oder Ausschließlichkeitsrechte der Rechtsordnung de lege lata entnommen werden können und welche Rechtssubjekte davon gegebenenfalls profitieren.

Zunächst wird grundlegend auf die verwendeten Begriffe eingegangen, sowie eine Klassifizierung in unterschiedliche Datentypen vorgenommen. Nach einer Darstellung der beteiligten Rechtssubjekte werden deren Interessen in Form von Schutzzielen angesprochen.

In Kapitel C wird anhand einer rechtsdogmatischen, strukturierten Analyse verschiedener Rechtsmaterien erhoben, ob es ein „Eigentum an Daten“ bereits heute gibt oder dieses durch Rechtsfortbildung hergeleitet werden könnte. Diese Analyse nimmt keinen direkten Bezug auf Fahrzeugdaten und die im Automobilumfeld einschlägigen Benutzungsmodalitäten. Abhängig von der Entscheidung pro- oder contra Dateneigentum werden in Kapitel D die konkreten rechtlichen Probleme im Umgang mit den fahrzeugseitig gespeicherten Daten untersucht. Im Mittelpunkt steht dabei der Fahrzeughalter als Verfügungsbefugter über das Fahrzeug im sachenrechtlichen Sinn.

B. Grundlagen

I. Begriffsdefinitionen

Daten: Das Datenschutzrecht[9] spricht zwar ebenfalls von „Daten“, jedoch liegt dem Begriff dort ein *semantisches* Verständnis zugrunde[10]. Klarer ist hier der Wortlaut von § 202a StGB, wo von „als Daten dargestellte Information“ die Rede ist. Auf der semantischen Ebene spricht man i.A. von Information, denn diese beinhaltet bereits eine Bedeutung, einen Informationsgehalt, und ist somit eine Interpretation des rein technischen Datums[11]. Letzteres wird in der Informationstechnik als eine *maschinenlesbare, codierte Information* verstanden und als *Zeichen* bzw. als *Zeichenkette* dargestellt – Hierfür sei in weiterer Folge der Begriff *syntaktische Information* verwendet[12]. Im Problembereich „Fahrzeugdaten“ wollen wir in weiterer Folge auf der Zeichenebene bleiben um die kleinstmögliche Einheit, den „Rohstoff“, zu erfassen. Ein wichtiges Merkmal von Daten ist die Länge der Zeichenkette die notwendig ist um die jeweilige Information darzustellen. So wird beispielsweise der aktuelle Wert eines Temperatursensors in 2-3 Byte dargestellt, während ein Bild oftmals mehrere MByte Datenlänge verursacht.

Fahrzeugdaten: Als Fahrzeugdaten gelten zunächst alle im Fahrzeug *existierenden* Daten. Existieren können Daten in flüchtigen sowie in nicht-flüchtigen Speichern (Datenträgern). Aber auch Daten, die ohne komplette Speicherung innerhalb eines Fahrzeugs von A nach B übertragen werden, sind Fahrzeugdaten im Sinne dieser Definition, da sie zumindest in Teilen zwischengespeichert werden und außerdem nach Außen übertragen werden können. Von *dauerhaft gespeicherten Fahrzeugdaten* ist dann zu sprechen, wenn die Daten auch bei Außerbetriebnahme des Fahrzeugs weiterhin gespeichert bleiben.

Software: Unter dem Begriff *dauerhaft gespeicherte Fahrzeugdaten* wie zuvor definiert, ist Software streng genommen ebenfalls umfasst, da es sich ebenfalls um maschinenlesbar codierte Information handelt, die im Fahrzeug dauerhaft gespeichert ist. In der Diskussion um das Dateneigentum und auch im allgemeinen Sprachgebrauch wird Software aber nicht als Teil der „Daten im Fahrzeug“ verstanden. Diese Abgrenzung ist insofern wichtig, weil Software als Computerprogramm durch das Urheberrecht geschützt ist und zwar unabhängig von der konkreten Speicherung auf einem Datenträger. Software wird nicht durch

[9] Das dt. Datenschutzrecht definiert Daten als „Einzelangaben über Verhältnisse“ und nimmt somit auf eine konkrete Bedeutung Bezug. DSG-VO Art. 4 I verwendet bereits den Begriff *Information*.
[10] *Zech* S.33.
[11] *Specht* CR 2016, 288, 290.
[12] *Zech* S.32;*Schulze-Heiming* S.25; *Welp* S.444; DIN 44300 Nr.19.

die Computer im Fahrzeug generiert, sondern sie stellt überhaupt erst die Funktionalität der Steuergeräte in Verbindung mit deren Hardware dar und soll in weiterer Folge als Teil der Steuergeräte wahrgenommen werden.

Statische Fahrzeugdaten: Das sind Daten die beim Fahrbetrieb des Fahrzeugs nicht automatisch verändert werden. Eine Datenänderung findet durch manuelle Eingriffe statt. Dies können z.B: Konfigurationsdaten der Software sein, die im Zuge einer Wartungsleistung modifiziert werden (z.B: Alarmschwellwerte) aber auch Identifikationsmerkmale wie die Fahrzeug-Identifikationsnummer (VIN[13]) – ferner auch das Hinterlegen von digitalem Kartenmaterial. Zu den statischen Daten gehören auch die *statischen Nutzerdaten.* Das sind gespeicherte Daten, die der Nutzer durch manuelles und bewusstes Zutun im Fahrzeug speichert, z.B: indem er eine Radiofrequenz im Autoradio speichert oder eine Kontaktliste seines Telefons in den Fahrzeugspeicher überträgt.

Dynamische Fahrzeugdaten: Unter diesen Begriff fallen die eigentlichen maschinengenerierten Daten. Beispiel dafür sind *Sensorrohdaten* die durch Aufnahme der Wirklichkeit entstehen und zumeist irgendeine Art von Umwandlung erfahren, z.B.: in Form eines gespeicherten Bildes oder eines anderen strukturierten Datenelements wie z.B.: einem weiterverarbeitbaren Temperaturwert der bereits auf einen konkreten Messbereich bezogen ist oder durch Kombination von mehreren einzelnen Rohdaten zustande kommt. Nach dieser Umwandlung heißen diese Daten allgemeiner *Sensordaten*. Dynamische Fahrzeugdaten sind auch sogenannte *Protokolldaten* die nach bestimmten Kriterien gezielt abgespeichert werden. Zu nennen sind hier bspw. das Abspeichern eines Fehlerzustandes oder ein aussagekräftiges Ergebnis einer durchgeführten Datenanalyse – Dieses Ergebnis kann wiederum mittels statistischer Methoden von den *Sensordaten* abgeleitet sein oder repräsentiert softwarespezifische Zustandsdaten. Ähnlich zu Protokolldaten sind reine *Steuerdaten*, deren vordergründiger Zweck nicht die Dokumentation von Zuständen, sondern die Beeinflussung von Aktoren im Fahrbetrieb ist. Ein wahlweise dauerhaftes Abspeichern dieser Steuerdaten führt dann wiederum zu Protokolldaten.

Personenbezogene Daten: Aus einer datenschutzrechtlichen Perspektive ist eine Unterklassifikation notwendig, welche gem. § 3 BDSG lautet: „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“. Nach dieser Definition können statische und dynamische Fahrzeugdaten personenbezogene Daten sein. Prägendes Element ist die

[13] *Vehicle Identification Number,* auch bekannt als *Fahrgestellnummer,* in weiterer Folge *Fahrzeug-Identifikationsnummer* genannt.

Bestimmbarkeit, also die Möglichkeit die Identität einer real existierenden natürlichen Person festzustellen[14]. Hier werden zwei Theorien vertreten, die absolute und die relative Theorie. Bei der relativen Theorie kommt es auf die Mittel und Möglichkeiten alleine der datenerhebenden Stelle an[15], den Personenbezug durch Verknüpfung von mehreren Datenquellen, z.B: unter Zuhilfenahme öffentlich verfügbarer Verzeichnisse oder anderer veröffentlichter Informationen, herzustellen. Als datenerhebende Stelle kann hier beispielhaft eine KFZ Werkstatt genannt werden, welche Fahrzeugdaten im Umfang ihres Reparaturauftrags zu Diagnosezwecken ausliest. Die strengere, absolute Theorie klassifiziert ein Datum unabhängig von den existierenden Möglichkeiten der datenerhebenden Stelle bereits dann als personenbezogen, wenn der Bezug mithilfe des Zusatzwissens eines beliebigen Dritten, auch nur theoretisch, hergestellt werden kann[16]. In Bezug auf die gespeicherten Daten im Fahrzeug kommen beide Theorien vorerst zum selben Ergebnis, denn es gibt mit der gesetzlich normierten Registerauskunft beim Kraftfahrt-Bundesamt gem. § 39 I,II STVG eine niedrige Hürde, Name und Anschrift eines Fahrzeughalters alleine durch Übermittlung der Fahrzeug-Identifizierungsnummer abzufragen - das Glaubhaftmachen eines Rechtsverfolgungsinteresses genügt. § 45 S.2 STVG statuiert klarstellend, dass die Fahrzeug-Identifizierungsnummer ein Datum ist, das einen Bezug zu einer bestimmten oder bestimmbaren Person ermöglicht. Im Ergebnis ist demnach jedes im Fahrzeug gespeicherte Datum als ein personenbezogenes Datum anzunehmen, denn die Fahrzeug-Identifizierungsnummer ist fix im Fahrzeug gespeichert. Sie ist elektronisch lesbar und wird außerdem, sofern keine zusätzlichen Mechanismen angewendet werden wie (z.B. Anonymisierung), beim Auslesen der Fahrzeugdaten regelmäßig als Identifikationsmerkmal des Fahrzeugs zur allgemeinen Kennzeichnung der ausgelesenen Datensätze mitübertragen. Auch der VDA (Verband der Automobilindustrie) erkennt die Fahrzeug-Identifikationsnummer als personenbezogenes Datum an[17].

II. Beteiligte Rechtssubjekte

Fahrzeughalter: Der Fahrzeughalter ist der Zulassungsinhaber des Fahrzeugs, wie im Fahrzeugschein mit Name und Anschrift angeführt. Das Kraftfahrt-Bundesamt speichert den Fahrzeughalter mit seinen persönlichen Daten (Name, Adresse) und

[14] BeckOKDatenschutzrecht/*Schild* §3 Rn. 17.
[15] Boecken-Düwell-Diller-Hanau/*Gola-Brink* §3 Rn. 27.
[16] Simitis/*Dammann* §3 Rn. 24.
[17] Gemeinsame Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) - https://www.vda.de/de/themen/innovation-und-technik/vernetzung/gemeinsame-erklaerung-vda-und-datenschutzbehoerden-2016.html [abgerufen 23.10.2017]

weist ihm die Fahrzeug-Identifikationsnummer und das aktuelle KFZ Kennzeichen zu. Im Zuge der vorliegenden Arbeit wird der Fahrzeughalter mit dem sachenrechtlichen Eigentümer des Fahrzeugs gleichgesetzt.

Fahrer: Der Fahrer ist derjenige, der das Fahrzeug für eine bestimmte Wegstrecke führt. Er muss nicht mit dem Fahrzeughalter identisch sein.

Werkstatt: Die Werkstatt ist ein Fachbetrieb, der Reparatur und Wartungsleistungen am Fahrzeug des Fahrzeughalters auf dessen Beauftragung hin vornimmt. Eine Vertragswerkstatt ist eine Werkstatt, die in einem besonderen Vertragsverhältnis mit einem Fahrzeughersteller steht und gegenüber diesem verschiedene Rechte und Pflichten hat. Diese wirken sich regelmäßig auf die faktische Abwicklung und oftmals auch auf die rechtliche Ausgestaltung des Reparaturauftrags mit dem Fahrzeughalter aus.

Fahrzeughersteller: Der Hersteller ist jenes Unternehmen, in dessen Namen das Auto produziert wird - im allgemeinen Sprachgebrauch auch als „Automarke“ bekannt. Annahmegemäß gibt es eine juristische Person in einem EU Mitgliedsstaat, welche als Rechtssubjekt des Herstellers gegenüber dem Fahrzeughalter und der Werkstatt als Vertragspartner auftritt. Dieses Rechtssubjekt soll in weiterer Folge als Fahrzeughersteller bezeichnet werden.

III. Schutzziele, Datennutzung und Datenverfügung

Wie in Kapitel A.1 erwähnt stellt sich für den Fahrzeughalter in Bezug auf die gespeicherten Daten in *seinem* Fahrzeug die Frage nach rechtlichem Schutz, Eigennutzungsbefugnissen und möglicher rechtsgeschäftlicher Verfügung über diese Befugnisse.

Aus dem Fachgebiet der Informationssicherheit sind die folgenden Schutzziele[18] übernommen:

- *Integrität*: Daten sollen über einen bestimmten Zeitraum vollständig und unverändert vorhanden sein
- *Vertraulichkeit*: Nur autorisierte Benutzer haben Zugriff auf die Daten
- *Verfügbarkeit*: Der Zugriff auf die Daten ist zu jedem Zeitpunkt möglich

Aus einer juristischen Perspektive ist es aber notwendig zu diesen Schutzzielen ebenfalls einen Berechtigten zu identifizieren, sodass dieser bei einer Einschränkung bzw. Verletzung eines Schutzzieles eventuell einen Rechtsanspruch geltend machen kann. Der Schutz soll dabei unabhängig von

[18] ISO/IEC 27001:2013.

einem bestehenden Vertragsverhältnis existieren, also als subjektives, absolutes Recht gegenüber jedermann wirken.

Dieser Schutz könnte über Ausschließlichkeitsrechte gestaltet sein. Nach dem Vorbild § 903 BGB werden damit positive Befugnisse an einem Gut einer Person, dem Eigentümer, zugewiesen[19] während andere Personen von jeder Einwirkung auf das Gut ausgeschlossen werden *können*. Die Befugnisse und die Ausschlüsse stehen einander gegenüber – der Eigentümer kann alle Einwirkungen Dritter ausschließen, die ihm selbst gestattet sind[20]. Ausschließlichkeitsrechte an immateriellen Gütern sind z.B. im UrhG kodifiziert.

Die rechtliche Realisierung der oben genannten Schutzziele erfordert aber nicht unbedingt Ausschließlichkeitsrechte. Subjektive Abwehrrechte, z.B. gesetzliche Handlungsverbote, erfüllen ebenfalls diese Funktion. Das Abwehrrecht determiniert aber gerade nicht einen positiven Zuweisungsgehalt im Sinne der Befugnisse an einem Gut. Im Gegensatz zu den Ausschließlichkeitsrechten, welche auch im unverletzten Zustand *gedachterweise* existieren, entsteht aus einem Abwehrrecht ein gesetzliches Schuldverhältnis erst im Moment der Erfüllung des statuierten Tatbestandes gegen den jeweiligen Handelnden[21].

Zunächst noch unabhängig von der Klassifizierung als körperliche oder unkörperliche Sachen, sind in Bezug auf Daten die folgenden Nutzungsformen zu nennen:

- *Kenntnisnahme*: Unter der Voraussetzung der Verfügbarkeit sowie der positiven Zugangsberechtigung (vgl. Schutzziel Vertraulichkeit) soll ein manuelles oder maschinelles *Lesen* der Daten erfolgen können. Manuelles Lesen ist nur auf Bildschirmen möglich, während maschinelles Lesen über Datenschnittstellen zu Stande kommt. Durch die Kenntnisnahme alleine erfolgt annahmegemäß noch keine dauerhafte Speicherung der Daten außerhalb des informationsverarbeitenden Systems (z.B: dem Auto).
- *Vervielfältigung*: Abgesehen von technisch notwendigen Abläufen innerhalb des informationsverarbeitenden Systems soll eine Vervielfältigung an dieser Stelle nur dann angenommen werden, wenn es zu einer dauerhaften Speicherung der gelesenen Daten außerhalb des Systems (z.B: Auto) kommt, z.B. zum Zwecke der nachträglichen Datenanalyse. Die Nutzungsform der Kenntnisnahme ist somit Voraussetzung für die Nutzungsform Vervielfältigung.

[19] *Peukert* S. 59.
[20] Staudinger/*Althammer* § 903 Rn. 11.
[21] *Peukert* S. 858.

Aus den oben erwähnten Gründen (Kapitel B.I) sollen die Nutzungsmöglichkeiten von Software hier nicht weiter erläutert werden.

Für die Verkehrsfähigkeit von Daten wird außerdem zu erläutern sein, ob der Berechtigte über die ihm zugewiesenen Schutzziele und Nutzungsbefugnisse auch rechtsgeschäftlich verfügen kann, z.B. durch Übertragung an eine andere Rechtspersönlichkeit. Dabei ist nicht nur an eine vollständige Verfügung des gesamten Rechtebündels zu denken, sondern auch an die spezifische Einräumung einzelner Nutzungs- bzw. Schutzrechte.

C. Mögliches Schutzkonzept über eigentumsähnliche Konstruktion

Bevor die existierenden spezialgesetzlichen Regelungen zum Schutz von Daten im Allgemeinen und deren Anwendung im Bereich von Fahrzeugdaten im Speziellen näher analysiert werden, erfolgt eine Erörterung, ob nicht eine umfassende eigentumsrechtliche Zuweisung von Daten unabhängig von den konkreten Inhalten und unabhängig vom Speicherort konstruierbar ist.

Das Eigentum nach § 903 BGB ist das umfassendste dingliche Recht. Wären Daten als Gut unter § 903 BGB subsumierbar, würde dem zugewiesenen *Dateneigentümer* über die existierenden sachenrechtlichen Vorschriften mit einem Schlag die meisten der im vorangegangenen Kapitel angeführten Befugnisse und Schutzkonzepte zuteilwerden. Während dies für die Nutzungen und die Verfügungsbefugnis unmittelbar einleuchtet, soll dies für die Schutzziele wie folgt erläutert werden:

Eine Verletzung der Datenintegrität wäre zivilrechtlich als Eigentumsverletzung über § 823 I BGB unmittelbar geschützt.

Das Schutzziel der uneingeschränkten Verfügbarkeit für den Berechtigten kann über den Besitz und die entsprechenden Ansprüche gem. 858 ff. BGB bzw. den Besitz als sonstiges Recht i.S.v. § 823 I BGB gelöst werden. Dazu wörtlich der BGH: „Soll der berechtigte Besitz an einer Sache dazu dienen, eine bestimmte Nutzung der Sache zu ermöglichen, so stellt es eine Rechtsgutsverletzung im Sinne des § 823 I BGB dar, wenn der Besitzer an eben dieser Nutzung durch einen rechtswidrigen Eingriff in relevanter Weise gehindert wird“[22]. Aber auch eine Verletzung des Rechtsguts *Eigentum* wurde bei einem vollständigen Ausschluss der Nutzungsmöglichkeiten gem. § 823 I BGB bereits mehrfach zugestanden[23].

Das Schutzziel der Vertraulichkeit könnte erreicht werden, indem der Eigentümer faktisch allen Nichtberechtigten physisch den Zugang zu den Daten verweigert – Dieser Nutzungsausschluss ist Teil seiner Befugnisse. Etwaige Ansprüche gegenüber einer unberechtigten Kenntnisnahme von Daten gegen den Willen des Dateneigentümers sollen an dieser Stelle noch nicht vertieft werden.

Eine mögliche Subsumption von Daten unter § 903 BGB erfordert eine passende Interpretation des Tatbestandsmerkmals „Sache“ oder, falls keine direkte Anwendung möglich ist, eine Rechtsfortbildung i.S einer Analogie.

[22] BGH, Urt. vom 09.12.2014, Az. VI ZR 155/14 – NJW 2015, 1174; BGH, Urt. vom 04.11.1997, VI ZR 348/96 – NJW 1998, 377.
[23] BGH, Urt. vom 21. 12.1970, II ZR 133/68 – NJW 1971, 886; LG Aachen, Urt. vom 16.03.2006, 1 O 126/05 - NJW-RR 2007, 89.

I. Direkte Anwendung von § 903 BGB

Die direkte Anwendung von § 903 BGB setzt voraus, dass Daten als Sache gem. § 90 BGB eingeordnet werden können. Der Begriff der „Sache“ ist in § 90 BGB legal definiert als „körperlicher Gegenstand“. Ein Gegenstand ist dann körperlich, wenn er sinnlich wahrnehmbar ist und im Raum abgegrenzt ist[24]. Während beide Merkmale unbestritten für den Datenträger zutreffen, stößt man bei einer Trennung von Daten und Datenträger notwendigerweise auf ein Problem.

Gegen eine Einordnung von Daten als körperlicher Gegenstand spricht bereits ein erster Blick auf eine der wenigen spezialgesetzlichen Regelungen, die wörtlich auf Daten referenziert: § 202a II StGB bezeichnet elektronisch gespeicherte Daten als „nicht unmittelbar wahrnehmbar“ – Eine Vergleichslage mit den Objekten *Elektrizität* und *Luft* bietet sich an und spricht gegen die Körperlichkeit von Daten.

Es wird im Hinblick auf Software zutreffend argumentiert, dass Software nur in ihrer verkörperten Form, nämlich in irgendeiner Art von physikalischer Verfestigung nutzbar ist und daher die Kombination aus Datenträger und Software sehr wohl als *eine* Sache qualifiziert werden kann[25]. Dazu auch der BGH wörtlich: „Der Bundesgerichtshof hat wiederholt entschieden, dass eine auf einem Datenträger verkörperte Standardsoftware als bewegliche Sache anzusehen ist“[26].

Fraglich ist, ob die Übertragung dieses Gedankens auf Daten zum selben Ergebnis führt. Man könnte argumentieren, dass man „verkörperte Daten“ als Erweiterung der Rechtsprechung des BGH als Sache i.S.v. § 90 BGB einordnet und daran sämtliche eigentumsrechtlichen Schutzkonzepte anheftet. Dagegen gibt es keine Einwände, jedoch wird dadurch die Frage nicht beantwortet, ob bei einer Trennung von Datenträger und Daten letztere diese Schutzkonzepte „mitnehmen“ können. Auch wenn man Daten und Software auf der rein speichertechnischen Ebene als gleichwertig einstufen muss, darf man die spezifischen Aspekte der Software, nämlich deren immaterialgüterrechtlichen Schutz, ihre bereits existierende Handelbarkeit über das Kaufrecht und die gut passende Anwendung des Sachmangelrechts nicht außer Acht lassen. Heute wird in überwiegender Ansicht Software aufgrund ihrer fehlenden Abgrenzbarkeit als unkörperlicher Gegenstand und somit nicht als Sache eingeordnet[27]. Im Ergebnis ist die Abgrenzbarkeit von Daten, welche nicht auf einem Datenträger verkörpert sind, aus den oben genannten Gründen noch einmal schwieriger als bei Software. Im

[24] Staudinger/*Stieper* § 90 Rn. 2.
[25] BGH, Urt. vom 18.10.1989, VIII ZR 325/88 – NJW 1989, 320; *Zech* S. 334;BeckOKBGB §90 Rn. 25.
[26] BGH, Urt. vom 15. 11.2006, XII ZR 120/04 - NJW 2007, 2394.
[27] *Zech* S. 334; *Hoeren-Sieber-Holznagel* Teil 18.4 Rn. 51; BeckOKBGB §90 Rn. 25; Staudinger/*Stieper* § 90 Rn. 12; *Härting* CR 2016, 646, 647

Sinne eines Erst-recht-Schlusses sind Daten daher übereinstimmend mit der Literatur[28] keine Sachen gem. § 90 BGB, und eine direkte Anwendung von § 903 BGB scheitert an der klaren Definition der „Sache".

II. Analoge Anwendung von § 903 BGB über § 303a StGB

Nach der Verneinung der Direktanwendung ist fraglich, ob eine planwidrige Regelungslücke besteht und diese aufgrund einer vergleichbaren Interessenslage durch Analogieschluss über den klaren Wortlaut von § 903 BGB hinaus geschlossen werden könnte. Eine vielversprechende Argumentation ergibt sich über das Strafrecht. Dort existiert mit § 303a StGB eine Vorschrift die auf den ersten Blick eine umfassende Güterzuordnung an Daten vollzieht – Dies wäre eine wichtige Voraussetzung für die fragliche Analogie. In verschiedenen Kommentaren zu dieser Strafrechtsnorm wird hier teilweise der Begriff *eigentumsähnliches Verfügungsrecht über die Daten* verwendet[29].

§ 303a StGB ordnet die Strafbarkeit der Schutzziele Integrität und Verfügbarkeit an. Die Vorschrift ist systematisch direkt hinter der Sachbeschädigung eingeordnet und deutet somit eine Nähe zum Sacheigentum an[30]. Um dem strafrechtlichen Bestimmtheitsgebot Genüge zu tun und das Tatbestandsmerkmal der Rechtswidrigkeit auszufüllen, ist ein *Berechtigter* von einem *Unberechtigtem* abzugrenzen[31]. Dabei herrscht Klarheit, dass Datenträger und Daten auf dieser Ebene zwei unterschiedliche Rechtsobjekte darstellen. Aus strafrechtlicher Sicht hat sich daraus eine Diskussion entwickelt, wie der Berechtigte – also der durch den Täter Geschädigte - abseits von schuldrechtlich zugewiesenen Befugnissen zu ermitteln ist[32]. Dafür gibt es einen interessanten Ansatz von *Welp*[33] - dieser wurde unter der Bezeichnung „Skripturakt" bekannt und bezeichnet die Zuordnung des Berechtigten i.S.v § 303a StGB auf denjenigen, der als *technischer Urheber*[34] der Daten anzusehen ist. Diese Suche nach dem Berechtigten hat Parallelen mit dem Versuch einer zivilrechtlichen Güterzuordnung an Daten.

Aus dieser Parallele heraus versucht *Hoeren* eine analoge Anwendung von § 903 BGB auf Daten zu konstruieren. Er argumentiert dies vorwiegend über das Prinzip der Einheit der Rechtsordnung zwischen Zivilrecht und Strafrecht[35]. Überträgt man diese strenge, von der konkreten Art der gespeicherten Information unabhängige,

[28] *Zech* S. 337; *Härting* CR 2016, 646, 647; *Hornung-Goeble* CR 2015, 265, 268.
[29] Lackner-Kühl*/Heger* § 303a Rn. 4*;* MüKoStGB*/Wieck-Noodt* § 303a Rn. 9*;* Schönke-Schröder*/Stree* § 303a Rn. 3.
[30] *Haft* NStZ 1987, 6, 10.
[31] Lackner-Kühl*/Heger* § 303a Rn. 4; *Hoeren* MMR 2013, 486, 487.
[32] *a.a.O.*
[33] *Welp* IuR 443, 447.
[34] *Hoeren* MMR 2013, 486, 487.
[35] *Hoeren* MMR 2013, 486, 488.

Zuordnung von Daten zu einem „Berechtigten“ hinüber in das Zivilrecht, steht mangels spezialgesetzlicher Regelungen dafür nur eine Subsumption unter § 903 BGB zur Verfügung.

Eine Rechtfertigung für die vorgeschlagene Analogie konstruiert *Hoeren* über eine Regelungslücke in § 453 BGB: Als *sonstige Gegenstände,* die nach dieser Vorschrift dem Kaufrecht unterliegen, wurden bereits unkörperliche Gegenstände wie Know-How, Erfindungen, Ideen und Informationen als „verkaufbare“ Vermögenswerte anerkannt[36]. Diesen sonstigen Gegenständen ist gemein, dass in kaufrechtlicher Hinsicht keine Verfügung eines subjektiven Rechts stattfindet, sondern lediglich die Übergabe geschuldet ist. Bei den genannten Gegenständen sind Ausschließlichkeitsrechte auch bewusst nicht von der Rechtsordnung vorgesehen – Informationen, Know-How und so weiter sollen abseits von spezialgesetzlichen Schutzmechanismen, z.B: Geheimnisschutz, eben gerade nicht der Allgemeinheit vorenthalten werden. Gegen eine Subsumption von Daten unter der Vorschrift § 453 als „sonstiger Gegenstand“ gibt es zunächst keinerlei Bedenken. Aufgrund des klaren Wortlauts von § 303a StGB sieht die Rechtsordnung bei Daten aber sehr wohl einen Schutz des Berechtigten gegen jedermann vor. Dieser Schutzmechanismus kann, so *Hoeren*, nur dann in das Zivilrecht „hinübergerettet“ werden, wenn man im Zuge des Kaufs von Daten über § 433, 453 BGB eine Verfügung über das subjektive Recht „Berechtigung an den Daten“ annimmt[37]. Letztlich, so *Hoeren*, muss die *Verfügung* daher auch eine eigentumsähnliche Position beim Käufer bewirken.

Der Argumentation von *Hoeren* kann letztlich nicht zugestimmt werden, weil der strafrechtliche Schutz von Daten nicht gegen *jedermann* im Sinne einer gedachten Verletzungshandlung schützt, sondern sich erst als rechtliches Sanktionsinstrument manifestiert, wenn ein Täter tatsächlich den Tatbestand einer Verletzungshandlung erfüllt. Daraus ergibt sich gerade kein zivilrechtlicher Zuweisungsgehalt, sondern allenfalls ein Abwehrrecht und daraus ein gesetzliches Schuldverhältnis. § 903 BGB spricht wörtlich von: „*Beliebig* verfahren und andere ausschließen“ – diese *Beliebigkeit* liegt nicht vor, denn § 303a StGB stellt an die Verletzungshandlung ganz konkrete Anforderungen - die umfassten Verletzungshandlungen sind explizit genannt. Dem Grundsatz *nullum crimen, nulla poena sine lege* folgend, besteht für den Berechtigten daher überhaupt kein Gestaltungsspielraum, wann der Schutz greifen soll und wann nicht. Dazu kommt, dass § 303a StGB nur bei vorsätzlichem Handeln greift – ein eigentumsrechtliches Schutzkonzept müsste aber gerade auch eine fahrlässige Verletzungshandlung

[36] MüKoBGB/*Westermann § 453 Rn. 6.*
[37] *Hoeren* MMR 2013, 486, 489

umfassen. Der Schutz gegen fahrlässiges Handeln darf aber nicht einfach durch die Übertragung auf das Zivilrecht zusätzlich entstehen, denn er ist teleologisch-strafrechtlich ausdrücklich ausgeschlossen (§§ 15 i.V.m § 303a StGB).

Als weiteres Gegenargument sei an dieser Stelle angeführt, dass die strafrechtliche Literatur die schuldrechtliche Zuweisung an den Berechtigten genügen lässt, um zwischen berechtigter und nicht-berechtigter Datenveränderung zu unterscheiden[38]. Der (neue) Berechtigte benötigt somit kein subjektives, absolutes Recht, um eine Datenveränderung vorzunehmen – Es genügt das relative Recht, ausgestellt durch den ursprünglich Berechtigten.

Gegen die Argumentation von *Hoeren* sei hier außerdem darauf hingewiesen, dass die von ihm aufgegriffenen Referenzen aus der Strafrechtsliteratur den Eigentumsbegriff überwiegend in einem erläuternden und versinnbildlichten Kontext verwenden. Konsequenterweise hinterfragt er die Zulässigkeit der Analogie im Hinblick auf die Planwidrigkeit der gesetzlichen Regelungslücke auch kritisch, verwirft die Argumentation letztlich aber nicht[39] . Andere Autoren sprechen sich jedoch mit Hinblick auf die mittlerweile zahlreich vorhandenen immaterialgüterrechtlichen Spezialvorschriften[40] klar gegen die Planwidrigkeit der Lücke aus[41] bzw. verneinen die vergleichbare Interessenslage mit dem klassischen Sachenrecht aufgrund der „Flüchtigkeit“ und dem raschen Wertverlust von Daten[42].

Als Zwischenergebnis kann demnach festgehalten werden, dass eine analoge Anwendung von § 903 BGB i.V.m § 303a StGB auf Daten abgelehnt werden muss.

III. Analoge Anwendung von § 903 BGB als *Früchte* über § 99 I BGB bzw. als *Nutzungen* gem. § 100 BGB

Im Umfeld von automatisiert generierten Daten kann man die Frage stellen, ob sich über das Eigentum an der Maschine nicht auch die generierten Daten in einem eigentumsähnlichen Verhältnis zum Eigentümer der Maschine darstellen lassen. Hier vertritt *Grosskopf*[43], dass Daten die Früchte einer Muttersache (des Fahrzeugs) sind und diese daher nach der Trennung von der Muttersache gem. §§ 99 I, 953 BGB dem Eigentümer der Muttersache als neues Eigentum zuzuordnen

[38] Lackner-Kühl/*Heger* § 303a Rn.4; MüKoStGB/*Wieck-Noodt* § 303a Rn. 9;Schönke-Schröder/*Stree* § 303a Rn. 3.
[39] *Hoeren* MMR 2013, 486, 488.
[40] Diese beziehen sich allerdings überwiegend auf den Schutz der gespeicherten Information und nicht der Daten selbst.
[41] *Zech* CR 2015, 137, 144; *Dorner* CR 2014, 617, 626.
[42] *Boesche/Rataj*, Zivil- und datenschutzrechtliche Zuordnung von Daten vernetzter Elektrokraftfahrzeuge, S. 34. - http://schaufenster-elektromobilitaet.org/media/media/documents/dokumente_der_begleit__und_wirkungsforschung/EP21_Zivil-_und_datenschutzrechtliche_Zuordnung.pdf [abgerufen 09.12.2017].
[43] *Grosskopf* IPRB 2011,259,260.

sind. Dagegen wird ausgeführt, dass Maschinen nach ihrer Bestimmung nicht ausbeutbar sind und keine Erzeugnisse abwerfen[44]. Als dogmatisches Gegenargument kommt hinzu, dass § 99 BGB die Sacheigenschaft der Frucht implizit annimmt und diese nicht über §§ 99, 953 I BGB begründet werden kann[45] - Daten sind aber keine Sachen und daher auch keine Früchte i.S.v. § 99 BGB.
Eine analoge Anwendung von § 99 BGB auf Früchte, die keine Sachen sind, stößt ebenfalls auf Bedenken: Charakteristisch für die Frucht, wie für jede Sache, ist ihre Einmaligkeit und rivale Nutzbarkeit unter der Bedingung des Besitzes. Daten können hingegen beliebig vervielfacht werden und schaffen daher potentiell einen nicht-rivalen Nutzen – Für eine analoge Anwendung von § 99 BGB auf Daten fehlt es somit an der vergleichbaren Interessenslage[46].

Nach der Ablehnung von „Früchten als Sache“ könnten Daten aber immer noch *Nutzungen* gem. § 100 BGB sein. Nutzungen sind *Vorteile*, welche der Gebrauch der Sache gewährt. Der Begriff des Gebrauchsvorteils setzt keine Sacheigenschaft voraus[47], schafft aber im Gegenzug auch keine güterrechtliche Zuordnung im Sinne eines eigentumsähnlichen Ausschließungsrechts[48].

Im Ergebnis ergibt sich daher weder über die Konstruktion als Frucht i.S.v. § 99 BGB noch über die Konstruktion des Gebrauchsvorteils ein „Dateneigentum“ i.S.v § 903 BGB in möglicher analoger Anwendung.

IV. Rückgriff auf Eigentum am Datenträger

Fraglich ist, ob eine eigentumsrechtliche Zuordnung an Daten überhaupt erforderlich ist, oder ob nicht über den Umweg der Speicherung auf dem Datenträger alle eigentumsrechtlichen Befugnisse und Ausschließlichkeitsrechte an den gespeicherten Daten mitumfasst sind. In diesem Fall wäre die Herleitung eines Dateneigentums i.S.v. § 903 BGB hinfällig.
Wie oben bereits erwähnt, existieren Daten zutreffend nur in ihrer verkörperten Form, nämlich in irgendeiner Art von physikalischer Verfestigung. Die Kombination aus Datenträger und Daten ist als Sache einzuordnen, und die Kombination unterliegt uneingeschränkt den sachenrechtlichen Schutzkonzepten mit dem Sacheigentümer als Begünstigtem[49].

[44] BeckOKBGB/*Fritzsche* § 99 Rn.4; *Specht* CR 2016, 288, 292.
[45] *Zech* CR 2015, 137,142.
[46] a.a.O.
[47] Den Vergleich mit „gewonnener Energie“ ziehend: BeckOKBGB/*Fritzsche* § 100 Rn. 6.
[48] *Zech* CR 2015, 137, 142; *Härting* CR 2016, 646, 647; Studie BMVI „Eigentumsordnung für Mobilitätsdaten“ S.88.
[49] OLG Karlsruhe, Urt. vom 7.11.1995, 3U 15/95 – NJW 1996, 200; BGH, Urt. vom 15.11.2006, Az.: XII ZR 120/04 - NJW 2007, 2370; *Bartsch* CR 2010, 553, 554.

Daher kann problemlos zugestimmt werden, dass das Löschen oder Überschreiben von Daten auf dem Datenträger als Eigentumsverletzung am Datenträger gem. § 823 I BGB anerkannt ist[50]. In ähnlicher Weise hat der Eigentümer des Datenträgers über das Besitzrecht auch jederzeit das Nutzungsrecht der *Kenntnisnahme* an den gespeicherten Daten[51].

Das Schutzkonzept über den Rückgriff auf den Datenträger gem. § 823 I BGB versagt jedoch, wenn die Daten von diesem Datenträger unbefugt ausgelesen oder durch Vervielfältigung auf einem anderen Datenträger gespeichert werden. Das Sacheigentum schützt die Integrität der Sache – diese wird durch ein (annahmegemäß) unberechtigtes Auslesen jedoch nicht beeinträchtigt. Folgerichtig hat der Sacheigentümer des Datenträgers dagegen keine Handhabe[52]. Dazu kommt, dass mangels Sacheigenschaft der ausgelesenen Daten diese auf einem fremden Zieldatenträger gespeichert werden können und dort wiederum, nach der hier vorgebrachten vereinfachten Sichtweise, in den Integritätsschutz des neuen Datenträgers übergehen. Die ursprüngliche eigentumsrechtliche Zuordnung an der Kombination aus Datenträger und Daten erstreckt sich mangels Sacheigenschaft gerade nicht auf die unkörperlichen Daten[53], und daher behält nach dieser Betrachtungsweise der Eigentümer des ursprünglichen Datenträgers keinerlei güterrechtliche Berechtigung an den gespeicherten Daten auf dem fremden Zieldatenträger.

V. Zwischenergebnis

Die prinzipielle sachenrechtliche Einordnung von Daten als „Dateneigentum“ ist wie angeführt de lege lata nicht herleitbar. Aufgrund des sachenrechtlichen Numerus clausus und der fehlenden expliziten Berücksichtigung durch den Gesetzgeber ist bei einer möglichen Rechtsfortbildung Zurückhaltung geboten. Das Sachenrecht wurde aus seiner Historie heraus für Güter entwickelt, an welchen nur rivale Nutzungen stattfinden können – es knüpft an den Besitz an[54]. Verlustlos vervielfältigbare Daten passen nicht in dieses Konzept.

Solange die Daten auf einem Datenträger verfestigt sind und dieser Datenträger eigentumsrechtlich einer Person zugewiesen ist, kann diese Person Schutzkonzepte und Befugnisse für die Kombination aus Datenträger und Daten verwirklichen[55]. Wie im vorangegangen Kapitel gezeigt, führt eine alleinige Betrachtung des Sacheigentums am Datenträgers aber bereits zu einer

[50] *Zech* S.272.
[51] *Zech* CR 2015, 137, 142.
[52] *Härting* CR 2016, 646, 647.
[53] *Zech* S.273; *Härting* CR 2016, 646, 647; *Hoeren* MMR 2013, 486, 490.
[54] *Zech* CR 2015,137,142.
[55] siehe Kapitel C.IV.

Schutzlücke in Bezug auf das Schutzziel der Vertraulichkeit. Und weiter: Beim Auslesen und Abspeichern auf fremden Datenträgern fehlt die güterrechtliche Zuordnung verloren - sofern keine anderen Schutzkonzepte gefunden werden gibt es für den ursprünglichen Eigentümer keine sachenrechtlichen Ansatzpunkte mehr, Rechte an der Kopie „seiner“ Daten einzufordern.
Im Hinblick auf die Verfügungsbefugnis ergibt sich soweit auch keine neue Erkenntnis – die Daten sind auf dem Datenträger verfestigt und eine Verfügung über den Datenträger setzt den Käufer des Datenträgers in die identische Rechtsposition, die der Verkäufer innehatte. Dem Verkäufer steht nach der Übergabe des Datenträgers keine Rechtsposition an den gespeicherten Daten mehr zu.

Da nach der hier in Kapitel C erfolgten Analyse mehrere praxisrelevante Fragestellungen im Umgang mit Daten nicht beantwortet werden konnten, soll nun folgend die Suche nach Schutzkonzepten außerhalb einer eigentumsrechtlichen Zuweisung erfolgen.

D. Schutzkonzepte an Fahrzeugdaten ohne eigentumsähnliche Konstruktion

Bei der Suche nach anwendbaren Schutzkonzepten von Daten anhand der bestehenden Gesetzeslage beschränkt sich die nachfolgende Analyse auf Fahrzeugdaten und damit verbundene Schutzziele und Interessen. Zu diesem Zweck sollen die folgende **Fallstudie** definiert werden:

Fallstudie „Werkstatt“: Das Fahrzeug wird einer Vertragswerkstatt des Fahrzeugherstellers für die Dienstleistung „Service“ übergeben. Im Vertrag mit der Werkstatt über die zu erbringende Dienstleistung finden sich keine spezifischen Vereinbarungen über den Umgang mit den im Fahrzeug gespeicherten Daten. Ein vertragliches Verhältnis über zusätzliche Telematik-Dienstleistungen zwischen Fahrzeughersteller und Fahrzeughalter gibt es nicht. Das Auto verfügt auch nicht über eine drahtlose Datenanbindung. Während der Servicearbeiten werden routinemäßig Fahrzeugdaten über die OBD[56] Schnittstelle ausgelesen.

I. Schutz von Fahrzeugdaten über das Urheberrecht

Wegen der technischen Nähe zu Software bzw. dem urheberrechtlichen Schutz von Immaterialgütern generell liegt es nahe, die Suche nach anwendbaren Schutzkonzepten im Urheberrecht zu beginnen. Könnte man an Fahrzeugdaten ein urheberrechtliches Schutzkonzept herleiten, so ergebe sich dadurch für den Fahrzeughalter die Möglichkeit, Rechte an Kopien „seiner“ Daten auch für außerhalb seines Fahrzeugs gespeicherte Fahrzeugdaten zu beanspruchen.

Die Abgrenzung zwischen Daten und Software wurde bereits erläutert – Fahrzeugdaten sind generell keine Computerprogramme. Es gibt keinen Ansatzpunkt für eine Direktanwendung und keine Rechtfertigung für eine Analogie der hochgradig spezialisierten Regelungen § 69a ff. UrhG. Dennoch kann in weiterer Folge auf die dort normierten Wertungsmaßstäbe u.U. zurückgegriffen werden.

1. Fahrzeugdaten als Werk gem. § 2 UrhG

Das Urheberrecht schützt gem. § 2 II UrhG persönliche geistige Schöpfungen und benennt diese als „Werk“. Etwas, das aus Zufall oder durch eine rein mechanische Tätigkeit entstanden ist, ist somit kein Werk im Sinne des Gesetzes – Notwendig ist ein Beitrag eines Menschen, der einen durch seinen Geist oder seine Persönlichkeit geprägten Gestaltungsspielraum in das Werk einfließen lässt[57].

[56] Die OBD (On-Board Diagnose) Schnittstelle ist eine digitale Datenschnittstelle und erlaubt das Auslesen von Diagnosedaten und das Schreiben von Konfigurationsdaten von/auf die untereinander vernetzten Steuergeräte. Die Schnittstelle ist bezüglich des Steckersystems und des Datenformats standardisiert (ISO 15031-x) und für alle in der EU zugelassenen PKW seit 2004 vorgeschrieben.

[57] Spindler-Schuster/*Wiebe* UrhG § 2 Rn. 1.

Dynamische Fahrzeugdaten werden von den Sensoren bzw. den Steuergeräten im Fahrzeug erzeugt. Es gilt daher: Unter den exakt selben Bedingungen und Eingangsdaten der Sensoren würden zwei Fahrzeuge identischer Bauart identische Datensätze erzeugen. Somit kann man argumentieren, dass die Vorschriften zum Erzeugen der Datensätze, die sogenannten Algorithmen, bereits in der Software des Steuergerätes vorliegen und durch das Ablaufen dieser Algorithmen im Sinne einer mechanischen Tätigkeit kein Werk i.S.d UrhG entstehen kann. Der Algorithmus ist als Teil des Computerprogrammes geschützt. Die persönliche Schöpfung ist auf das *Design* der Maschine begrenzt und kann nicht im Sinne einer Kausalkette auf die Erzeugnisse der Maschine ausgedehnt werden.

Allerdings nimmt die Sensorik die Umwelt durch Abtastung wahr und man könnte daher bei diesem Vorgang mit Bezug auf die am Fahrzeug montierten Videokameras, Infrarotkameras und Radarsensoren an einen Werksschutz als Filmwerk bzw. als Lichtbildwerk gem. § 2 I UrhG denken*. Werke die ähnlich wie Lichtbildwerkwerke geschaffen werden* (§ 2 I Nr. 5 UrhG), sind alle Verfahren mit denen ein Bild unter Benutzung strahlender Energie erzeugt wird[58]. Der Fahrer nimmt zumindest über die gewählte Fahrtroute Einfluss auf die Motivauswahl. Die Fahrzeugelektronik kann sowohl Standbilder als auch bewegte Bilder in Echtzeit analysieren und, je nach Speicherbedarf, auch dauerhaft aufzeichnen. Durch die Abgrenzung zwischen Lichtbildwerken und Lichtbildern (Leistungsschutzrecht § 72 UrhG) ist für ersteres eine individuelle, schöpferische Leistung in Form einer gezielten Aufnahme des Fotographen notwendig[59]. Diese notwendige Gestaltungshöhe ist bei automatisierten Aufnahmen von Standbildern durch fahrzeugseitig montierte Kameras nicht zu erreichen.
Ähnlich ist die Lage bei der Abgrenzung von Lichtbildwerken und Laufbildern (Leistungsschutzrecht § 95 UrhG). Das bloße Abfilmen eines tatsächlichen Geschehens ohne eigene gestalterische Überlegungen zur Bildkomposition, ohne Einflussnahme auf die Abfolge der einzelnen Sequenzen, z.B über den Schnitt, und ohne planerisch-technische Leistung zur besonderen Positionierung der Kamera ist kein Filmwerk i.S.d § 2 I UrhG[60].

Für andere Sensordaten im Fahrzeug, z.B: Temperaturdaten, gilt: Mögliche Konstruktionen über Schriftwerke (§ 2 I Nr. 1 UrhG) oder Darstellungen technischer Art (§ 2 I Nr. 7 UrhG) scheitern ebenfalls an der mangelnden

[58] BGH, Urt. vom 27.02.1962, I ZR 118/60 – NJW 1962, 636, 639.
[59] Dreier-Schulze/*Schulze* § 2 Rn. 195.
[60] KG Berlin, Urt. vom 28.03.2012, 24 U 81/11 - GRUR-Prax 2012,237; Spindler-Schuster/*Wiebe* UrhG § 2 Rn. 22; Wandtke-Bullinger/*Bullinger* § 2 Rn. 121.

persönlichen geistigen Schöpfung. Abzulehnen ist auch das Werk der Datensammlung gem. § 4 I UrhG, denn hier müsste bei der Auswahl und Anordnung der Sensordaten eine entsprechende Gestaltungshöhe vorliegen. Die mittelbare Einflussnahme auf die einzelnen Datensätze durch Fahrstil und Fahrverhalten des Fahrers hat zwar eine individuelle Komponente, aber diese Individualität ist nicht auf die konkrete Ausgestaltung, Anordnung oder Auswahl der jeweils gespeicherten Datensätze ausgerichtet.

Als Datenbankwerk gem. § 4 II UrhG ist die Ansammlung von unabhängigen, systematisch und methodisch strukturierten Datenelementen geschützt. Auswahl und Anordnung müssen wiederum einer persönlich, geistigen Schöpfung entspringen. Der Schutz erstreckt sich aber nicht auf die einzelnen Datenelemente selbst[61], was die Wirksamkeit mit Bezug auf Fahrzeugdaten bereits stark relativiert. Die Rechtsprechung fordert für eine Rechtsverletzung zusätzlich eine *wesentliche* Entnahme, und setzt diese quantitativ bei ca. 10% des Datenbestandes an[62]. Mit Bezug auf die Sensorrohdaten fehlt es bereits an der notwendigen systematischen und methodischen Anordnung, die eine Datenbank ausmacht – vgl. „Datenhaufen“[63]. Allerdings folgt die Speicherung von im Fahrzeug erzeugten Protokolldaten einer systematisch und methodischen Anordnung, z.B: in einer sogenannten Datenbankstruktur. Das Design solch einer Datenbankstruktur, welche zur Laufzeit mit Daten befüllt wird, ist Teil des Softwareentwicklungsprozesses. Dieses Design ist gem. § 69a I UrhG als „Entwurfsmaterial“ Teil des urheberrechtlichen Softwareschutzes. Die geistige Leistung ist damit abgedeckt und für einen parallelen Schutz unter § 4 II UrhG bleibt kein Raum. Beim automatischen „Befüllen“ dieser Datenbankstruktur mit Laufzeitdaten fehlt es wiederum an einer persönlich, geistigen Schöpfung, welche sich auf die konkrete Auswahl und Anordnung von *einzelnen* Datenelementen beziehen muss – diese Auswahl wird von einem Algorithmus getroffen, welcher für sich selbst geschützt ist aber nichts urheberrechtlich Schützenswertes erzeugen kann.

Eine Einordnung von Farzeugdaten als Werk i.S.d Urheberrechts scheidet demnach für alle Werkarten aus - es ergibt sich kein Schutzkonzept nach diesem Rechtsinstitut.

[61] *Zech* S.360.
[62] BGH, Urt. v. 1.12.2010, I ZR 196/08 – CR 2011, 498; BGH, Urt. v. 13.8.2009, I ZR 130/04 – CR 2010, 190.
[63] Dreier-Schulze/*Dreier* § 4 Rn. 17.

2. Mögliche Anwendung eines verwandten Schutzrechts des UrhG

   Scheitert der urheberpersönlichkeitsgeprägte Werkschutz, so stehen im Urheberrecht immer noch die Leistungsschutzrechte zur Verfügung.

   § 95 UrhG begründet ein Leistungsschutzrecht für den Filmhersteller, welches unabhängig von einer Einordnung als „Filmwerk“ gem. § 2 UrhG die erbrachte Leistung der Laufbildaufnahme im Sinne der getätigten wirtschaftlichen Aufwendungen schützt[64]. Zentral ist hier die Einordnung als „Filmhersteller“, denn nur er ist gem. §§ 94, 95 UrhG anspruchsberechtigt für dieses Schutzkonzept. Der Filmhersteller ist derjenige, der die organisatorische und wirtschaftliche Leistung der Filmherstellung tatsächlich erbringt[65] - der Filmhersteller muss Unternehmer sein, denn der Leistungsschutz soll die Abgeltung des unternehmerischen Risikos der Filmherstellung schützen[66]. Für die Einordnung als Laufbilder soll es keine Relevanzschwelle geben, sodass vollautomatisierte Aufnahmen, wie z.B: von Überwachungskameras, in den Schutzbereich der Vorschrift fallen können[67]. Umgelegt auf die automatischen Kameras am Fahrzeug ergeben sich hier allerdings Zweifel, und zwar mit dem Tatbestandsmerkmal des „Filmherstellers“ gem. § 94 UrhG. Selbst wenn man den Fahrzeughalter als Unternehmer annimmt, können die erstellten Video-Aufnahmen durch die Fahrzeugkameras i.A. nicht seiner unternehmerischen Tätigkeit zugeordnet werden. Es gibt kein schützenswertes unternehmerisches Risiko, das der Unternehmer bewusst trägt um diese Video-Aufnahmen anzufertigen. Seine Investitionen in das Auto tätigt er zum Zweck der Fortbewegung und nicht zum Zweck der Erstellung eines Filmes im Sinne von §§ 94,95 UrhG.

   Für den Lichtbildschutz gem. § 72 UrhG gilt zunächst, dass Einzelbilder die aus Filmaufnahmen entnommen werden unabhängig vom Schutz des Filmwerks einen Schutz gem. § 72 UrhG entfalten können[68]. Einzelne Bilder, die von den fahrzeugseitig montierten (Video)-Kameras abgespeichert werden, kommen daher prinzipiell dafür in Frage. Der Schutz gem. § 72 UrhG wurde bereits für Standbilder bejaht, die durch einen computergesteuerten Auslöser-Mechanismus erzeugt werden[69]. Erforderlich ist eine fotografisch-technische Leistung eines Menschen, der das Aufnahmegerät so einstellen, programmieren oder ausrichten muss, dass

[64] BeckOKUrhR/*Diesbach* § 95 Rn. 1.
[65] BGH, Urt. 14.10.1992, VIII ZR 91/91 – NJW 1993,259; OLG Köln, Urt. v. 10.12.2010, I-6 U 92/10 - GRUR-RR 2011,161; OLG Düsseldorf, Urt. v. 23.10.2001, 20 U 19/01 – GRUR-RR 2002, 121.
[66] Fromm-Nordemann/*Nordemann* § 94 Rn. 12.
[67] Fromm-Nordemann/*Nordemann* § 94 Rn. 15; a.A. Wandtke/*Czernik* S. 376 Rn. 18.
[68] BGH, Urt. vom 6.2.2014, I ZR 86/12 – GRUR 2014, 363.
[69] OGH, Urt. vom 1.2.2000, 4 Ob 15/00k - ÖBl 2000, 276; LG Berlin, Urt. vom 30.05.1989, 16 O 33/89 - GRUR 1990, 270.

eine technisch einwandfreie Aufnahme bzw. Abbildung entsteht[70]. Für die Zuerkennung des Lichtbildschutzes ist demnach zu fordern, dass die Aufnahme auf ein konkretes Zielobjekt optimiert ist, denn nur diese Optimierung kann als Leistung angesehen werden und rechtfertig einen Schutz des Ergebnisses. Diese Optimierung im Sinne einer handwerklichen Leistung gibt es aber nicht, wenn fahrzeugseitig montierte Kameras durchgängig aufzeichnen und dabei jedes einzelne Bild abspeichern. Dasselbe gilt, wenn ein Algorithmus aufgrund von anderen Eingangsparametern (z.B: drohende Unfallsituation) gezielt ein Bild aus dem Videostream auswählt und nur dieses abspeichert. Es fehlt an der fotografisch-technische Leistung eines Menschen die unmittelbar zur Bildaufnahme geführt hat[71].

Im Ergebnis entstehen daher keine durch das UrhG geschützte Lauf- oder Standbilder durch das unspezifische, ständige Aufnehmen der Umgebung mittels fahrzeugseitig montierten Kameras. Für andere Sensorquellen kann nichts anderes gelten, denn hier fehlt es schon an einem passenden Leistungsschutzrecht für die aufgenommene Information.

Als weiteres verwandtes Schutzrecht kommt der Leistungsschutz des Datenbankherstellers gem. § 87 ff UrhG in Betracht. In Abgrenzung zum Datenbankwerk ist keine persönliche geistige Schöpfung bei Auswahl und Anordnung der Datenelemente verlangt, allerdings ist eine Investition in die Beschaffung, Sammlung, Überprüfung, Aufbereitung und Darbietung des Inhalts erforderlich[72]. Das automatische Befüllen einer vorgegebenen Datenbankstruktur mit Sensorrohdaten oder Protokolldaten ist nicht schützenswert, da keinerlei Leistung für die selektive Beschaffung und Zusammenstellung der Daten erbracht wird – Investitionen in die Datenerzeugung sind nicht geschützt[73]. Die einzelnen Datenelemente sind wie bei § 4 UrhG ebenfalls nicht Teil des Schutzes.

3. Zwischenergebnis Urheberrecht

Es bleibt festzuhalten, dass an Fahrzeugdaten nach obiger Analyse kein urheberrechtliches Schutzkonzept greift. Im Vergleich zu den Erkenntnissen aus Kapitel C.V eröffnet das Urheberrecht daher keine weiteren Schutzmöglichkeiten aus Sicht des Fahrzeughalters.

[70] Fromm-Nordemann/*Nordemann* § 72 Rn. 10.
[71] *Jlussi* S.3.
[72] Dreier-Schulze/*Dreier* § 87a Rn. 1.
[73] EuGH, Urt. v. 9.11.2004 Rs. C-444/02 - CR 2005, 412; *Grosskopf* IPRB 2011, 259, 260.

II. Schutz von Fahrzeugdaten über datenschutzrechtliche[74] Konstruktion

Wie in Kapitel B.I dargestellt, ist jeder gespeicherte Datensatz im Fahrzeug bereits deshalb ein personenbezogenes Datum, weil die Verknüpfung zur Fahrzeug-Identifikationsnummer dauerhaft besteht und diese Nummer bei einer einfachen Datenabfrage i.A. innerhalb der ausgelesenen Datensätze mitgeliefert wird.

Das BDSG untersagt die Erhebung, Verarbeitung und Nutzung (in Folge: Datenverwendung) personenbezogener Daten generell. Sofern demnach keine im BDSG zutreffenden Erlaubnistatbestände vorliegen oder die betroffene Person vertragsrechtlich eingewilligt hat, ist sie durch Abwehrrechte gegenüber einer Datenverwendung der „verantwortlichen Stelle“ (§ 3 VII BDSG) geschützt. Darüberhinausgehende, eigentumsähnliche Ausschließlichkeitsrechte an den personenbezogenen Daten stehen der Person nach h.M. nicht zu[75].

Die Speicherung von Fahrzeugdaten im Fahrzeug ist bereits ein *Verarbeiten* gem. § 1 II BDSG. Die „verantwortliche Stelle“ i.S.d § 3 VII BDSG ist eine Person oder Stelle, die für sich Daten verarbeitet oder im Auftrag eines anderen diese Verarbeitung vornehmen lässt[76]. In der Literatur wird angemerkt, dass der Fahrzeughalter oder Fahrer auf die Datengenerierung kaum Einfluss nehmen kann und daher der Fahrzeughersteller durchgehend als verantwortliche Stelle für die im Fahrzeug erzeugten Daten anzusehen sein könnte[77]. Allerdings kann man aus der oben dargestellten Ansicht (Kapitel C.IV) folgern, dass die Speicherung der Fahrzeugdaten auf einem Datenträger stattfindet, der im Eigentum des Fahrzeughalters steht und dieser im normalen Fahrbetrieb faktisch jedermann vom Zugriff auf diese Daten ausschließen kann. Der Betroffene der nur Daten über sich selbst verarbeitet ist nicht *verantwortliche Stelle* i.S.d BDSG[78]. Ein datenschutzrechtlicher Ansatzpunkt ergibt sich daher erst, wenn die Daten, wie in der Fallstudie angenommen, im Sinne einer Fremdverarbeitung *ausgelesen* werden[79] - das A*uslesen* ist eine zielgerichtete Kenntnisnahme und damit ein *Erheben* gem. § 1 II BDSG[80]. Die tw. in der Literatur[81] vertretene Ansicht, dass mithilfe des Auskunftsanspruch gem. § 34 BDSG der Fahrzeughalter quasi Bit-für-Bit über jedes im Fahrzeug gespeicherte Datum (inklusive dem aktuellen

[74] Die datenschutzrechtliche Analyse wird anhand des BDSG ["Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist"] bewertet. Bezüge auf die ab 25.05.2018 geltende Gesetzeslage (DSGVO, DSAnpUG-EU) werden nur in eingeschränktem Maße hergestellt.

[75] *Zech* S.219 ; *Jlussi* S. 4; *Härting* CR 2016, 646, 648; *Dorner* CR 2014 617, 625; im Ergebnis wohl auch: *Hornung-Goeble* CR2015 265,270; a.A. *Kilian* S. 195, 207.

[76] Erbs-Kohlhaas/*Ambs* § 3 Rn. 33.

[77] *Roßnagl* S. 284.

[78] Erbs-Kohlhaas/*Ambs* § 3 Rn. 33.

[79] Studie BMVI „Eigentumsordnung für Mobilitätsdaten“ S.142.

[80] *Zech* S.216.

[81] *Hornung-Goeble* CR 2015, 265, 270.

Datenwert!) Kenntnis erlangen könnte, ist abzulehnen. Der Auskunftsanspruch kann erst an einer Kopie des Datums greifen, welche außerhalb des Fahrzeug auf einem Computer der verantwortlichen Stelle (z.B: die Werkstatt) erstellt wird.

1. Datensätze mit Personenbezug über Fahrzeug-Identifikationsnummer

a) Datenverarbeitung durch die Werkstatt

Das Standardverfahren zum Auslesen der Diagnosedaten des Fahrzeugs ist der Zugriff auf den sogenannten *Fehlerspeicher*. In diesem Speicher sind Protokolldaten in einem standardisierten Speicherformat hinterlegt. Diese entstehen aufgrund von Grenzwertüberschreitungen von Sensoren oder sonstigen detektierten Fehlerzuständen, welche während des normalen Betriebs des Fahrzeugs auftreten.

Wie im Anhang dieser Arbeit exemplarisch gezeigt, ist der Auslesevorgang auch immer mit dem Auslesen der Fahrzeug-Identifikationsnummer verbunden. Während der gesamten Verarbeitung und Analyse der Protokolldaten auf den Computersystemen der Werkstatt wird die Fahrzeug-Identifikationsnummer als Zuordnungselement der angezeigten bzw. gespeicherten Fehlerspeicher-Datensätze zu dem jeweiligen Fahrzeug verwendet. Aus den oben genannten Gründen wird die Werkstatt durch das Auslesen des Fehlerspeichers somit eine verantwortliche Stelle i.S.d BDSG.

Annahmegemäß liegt keine Einwilligung zur Datenverwendung von personenbezogenen Daten vor die den Voraussetzungen von § 4a BDSG genügt[82]. Gemäß den datenschutzrechtlichen Grundprinzipien nach Zweckbindung und Datensparsamkeit wird man in der Fallstudie für das Auslesen des Fehlerspeichers den Erlaubnistatbestand § 28 I Nr.1 BDSG bejahen können, da es für die Erfüllung des Service-Auftrags notwendig und geboten ist, diese Informationen verfügbar zu haben. Ein tieferes Einsteigen in die Diagnosedaten, z.B: aktuelle Sensorwerte oder gespeicherte Protokolldaten außerhalb des Fehlerspeichers wird man der Werkstatt anlassbezogen ebenfalls zubilligen, um notwendige Informationen zur Erfüllung des Routineeingriffs zu erheben. Eine Berechtigung zum Speichern aller ausgelesenen Daten über den Kundenauftrag hinaus kann aus dem Erlaubnistatbestand aber nicht abgeleitet werden. Der Kunde könnte somit bei der Übernahme des Fahrzeugs gem. § 20 II Nr.2 BDSG die Löschung aller ausgelesenen Daten verlangen. Dagegen könnte die Werkstatt geltend machen, sie müsse zur Wahrung ihrer berechtigten Interessen (§ 28 I Nr.

[82] Beispielhaft wurden im Zuge dieser Arbeit mehrere Kauf-, Reparatur und Garantieverträge von VW, Audi und KIA sowie von unabhängigen Werkstattunternehmen untersucht. Eine Überlassung von Daten generell bzw. personenbezogenen Daten im Speziellen ist in den untersuchten Verträgen Stand Oktober 2017 nicht geregelt.

2 BDSG) diese Daten weiterhin vorhalten. Berechtigte Interessen sind alle tatsächlichen, wirtschaftlichen und ideellen Interessen, die von der Rechtsordnung gebilligt werden[83]. Als berechtigtes Interesse der Werkstatt kann jedenfalls nicht unproblematisch angenommen werden, dass die Fahrzeughistorie und die Fahrzeugdaten gespeichert werden um beim nächsten Service Termin das Fahrzeug „wiederzuerkennen" und damit gegebenenfalls effizienter und effektiver den nächsten Service- oder Reparaturauftrag abzuarbeiten. Das könnte zwar im Interesse des Kunden liegen, müsste diesem aber zur Auswahl gestellt werden - schließlich kann der Kunde auch eine andere Werkstatt für den Folgeauftrag auswählen. Eine dauerhafte Speicherung der ausgelesen Fahrzeugdaten kann der Werkstatt demnach nicht zugestanden werden.

b) Datenweitergabe durch den Werkstattsbetrieb an den Fahrzeughersteller

Zur vertraglichen Situation zwischen Fahrzeughalter und Fahrzeughersteller sei einhergehend mit der Literaturmeinung[84] angenommen, dass der Garantievertrag ein direktes Vertragsverhältnis mit dem Fahrzeughersteller darstellt, welcher durch den Vertragshändler vermittelt wird und durch den Garantieschein und die schriftlich beiliegenden Garantiebedingungen verbrieft ist.

Teil dieses Garantievertrags ist bei neueren Fahrzeugen auch das sogenannte „elektronische Serviceheft". Hierbei wird in einer durch den Hersteller betriebenen, weltweit verfügbaren Datenbank jedes am Fahrzeug durchgeführte Service zentral gespeichert. Nach dem durchgeführten Service erzeugt die Werkstatt in dieser Datenbank via Internet einen neuen Eintrag (Datensatz) und übermittelt zumindest die folgenden Attribute: Fahrzeug-Identifikationsnummer, Kilometerleistung zum Service-Termin sowie Informationen über die jeweils durchgeführten Wartungsarbeiten. Der Primärschlüssel[85] für den Datensatz ist die Fahrzeug-Identifikationsnummer und somit ist der komplette Datensatz als personenbezogenes Datum zu klassifizieren. Annahmegemäß gibt es keine freiwillige Einwilligung von Seiten des Fahrzeughalters für die Verarbeitung bzw. Übermittlung dieser Daten. Eine Erlaubnis zur Übermittlung dieser Daten an den Fahrzeughersteller und einer dortigen Speicherung könnte sich wiederum aus § 28 I Nr. 1 BDSG ergeben, nämlich mit Bezug auf die Erfüllung des Garantievertrages. Der Volkswagen Konzern veröffentlicht zu diesem Thema auch

[83] Spindler-Schuster/*Nink* BDSG § 28 Rn. 7.

[84] BGH, Urt. vom 12.11.1980, VIII ZR 293/79 - NJW 1981,275,276; *Palandt* § 328 Rn. 10; Staudinger/*Honsell* § 459 Rn 92; Prütting-Wegen-Weinreich/*Medicus-Stürner* § 328 Rn. 23.

[85] Primärschlüssel --> eindeutige Identifizierung des Fahrzeugs. Beim Hersteller gibt es somit ein „virtuelles Abbild" des Fahrzeugs mit seiner kompletten Service-Historie.

ein „*Merkblatt zur Datenerhebung, -verarbeitung, -übermittlung und -nutzung*“[86]. Darin teilt der Hersteller mit, dass alle notwendigen Daten zur Erfüllung der vertraglich eingegangenen Verpflichtungen (z.B: Garantievertrag) von der Vertragswerkstatt an die Volkswagen AG und ihre Markengesellschaften übermittelt werden. In dem „Merkblatt“ ist neben personenspezifischen Stammdaten (z.B: Name, Adresse) auch namentlich die Rede von „fahrzeugspezifischen Daten“, ohne jedoch klarzustellen, ob es sich dabei um Fahrzeugdaten i.e.S handelt bzw. ohne auf den faktischen Personenbezug dieser Daten einzugehen. Daraus lässt sich ableiten, dass die Volkswagen AG bei der Führung des elektronischen Servicehefts von einem Erlaubnistatbestand i.S.v. § 28 I Nr. 1 BDSG ausgeht und es daher keiner zusätzlichen Einwilligung[87] gem. § 4a BDSG bedürfe. Eine kritische Auseinandersetzung mit diesem Rechtsstandpunkt soll an dieser Stelle nicht weiter geführt werden. Auch soll die Frage offen bleiben, ob der Fahrzeughersteller nach Ablaufen des Garantievertrags den Erlaubnistatbestand § 28 I Nr. 1 BDSG aufrechterhalten kann bzw. eventuell im Anschluss ein berechtigtes Interesse gem. § 28 I Nr. 2 BDSG an der Fortführung des elektronischen Servicehefts geltend machen muss.

Des Weiteren gibt es gem. Verordnung (EG) Nr. 692/2008 Anhang XV für den Fahrzeughersteller die Verpflichtung, *Maßnahmen* für die „Übereinstimmung in Betrieb befindlicher Fahrzeuge“ mit den gültigen Abgasvorschriften zu treffen. Zu diesem Zweck wurde ein fahrzeugseitiges Abgasüberwachungssystem als Teil der Typengenehmigung standardisiert. Das Abgasüberwachungssystem erzeugt beim Überschreiten der europaweit harmonisierten Grenzwerte einen Eintrag im fahrzeugseitigen Fehlerspeicher. Als *Maßnahmen* sind u.A. einzelne, regelmäßige Stichproben an Fahrzeugen vorgesehen, sowie nicht näher spezifizierte Nachweise über die Einhaltung der Abgasgrenzwerte in Form von statistischen Daten über die gesamte Fahrzeugflotte. Zumindest für die Daten aus dem fahrzeugseitigen Abgasmesssystem kann man daher hier von einem Erlaubnistatbestand aufgrund einer Rechtsvorschrift zur Erhebung und Übermittlung an den Fahrzeughersteller gem. § 4 I BDSG ausgehen.

[86] https://www.audi.de/de/brand/de.html#layer=/de/brand/de/tools/navigation/layer/rechtliches/datenschutz.html [abgerufen am 08.11.2017]

[87] Beispielhaft: Der Volkswagen Konzern bietet abgekoppelt vom eigentlichen Kaufvertrag eine schriftliche „Datenschutzrechtliche Einwilligungserklärung“ an, welche sich auf „Servicehotlines“, „Kundenbefragungen“ und „persönlich zugeschnittene Kundeninformationen“ bezieht aber die Themen „Fahrzeugdaten“ und „elektronisches Serviceheft“ nicht ausdrücklich anspricht. Die Einwilligung berechtigt zur „Datenverarbeitung“ durch den Fahrzeughändler und durch den Fahrzeughersteller. Das Verweigern dieser Einwilligung hat keinen Einfluss auf die grundlegenden Funktionen des Fahrzeugs bzw. die Leistungen aus dem Garantievertrag. Das ist somit konform mit dem datenschutzrechtlichen Kopplungsverbot gem. § 28 3b BDSG. Eine Beurteilung auf Basis des zukünftig strengerem Kopplungsverbots gem. DSG-VO soll hier offen bleiben.

2. Anonymisierung der Fahrzeug-Identifikationsnummer

   Durch besondere technische Maßnahmen beim Auslesen und/oder beim externen Speichern der Daten kann die Verknüpfung zur Fahrzeug-Identifikationsnummer allerdings aufgelöst werden. Durch diese Anonymisierung der Fahrzeug-Identifikationsnummer verlieren die ausgelesenen Daten den Personenbezug und damit zunächst den Schutz durch das BDSG. Aus dieser Betrachtung heraus kann der Fahrzeughersteller daher die Übermittlung der Fahrzeugdaten von der Werkstatt an sein Datencenter praktisch beliebig ausdehnen.

   Allerdings sei hier der Vollständigkeit halber angeführt, dass sich ein Personenbezug zum Fahrzeughalter oder zu einem Dritten ferner auch dann noch ergeben kann, wenn die Fahrzeug-Identifikationsnummer nicht Teil der Datensätze ist. Dies ist unmittelbar einleuchtend bei Stand- bzw. Videobildern, die fremde Personen oder fremde KFZ Kennzeichen enthalten. Ebenso bei Telefonbucheinträgen, die naturgemäß Telefonnummern von unbeteiligten Dritten enthalten. Weniger offensichtlich ist ein Personenbezug bei sogenannten *Fahrerprofilen*. Beispielsweise ist das Schaltverhalten einer Person durch Gewohnheiten geprägt und daher in gewissem Umfang auch individuell. Es ist demnach nicht per se auszuschließen, dass langfristige Aufzeichnungen über die Schaltzeitpunkte in Relation zur Motordrehzahl nicht auch Daten sind, die aufgrund dieser Individualität eine Person bestimmbar machen. Das gilt umso mehr, als eine Vielzahl solcher individuellen Verhaltensmuster[88] im Fahrzeug aufgezeichnet werden und durch deren gegenseitige Verknüpfung zumindest theoretisch tatsächlich eine ausreichend eindeutige Bestimmbarkeit dieser Person vorliegt. Das Gegenargument, dass diese Fahrprofile durch Fahrerwechsel im Fahrzeug verfälscht werden, scheidet bei modernen Autos der Oberklasse bereits aus - diese erkennen unterschiedliche Fahrer ein und desselben Fahrzeuges[89] und können die Fahrertrennung daher schon bei der Aufzeichnung der Daten durchführen. Dies steigert die theoretische Bestimmbarkeit der Person und damit die datenschutzrechtliche Relevanz im Hinblick auf die erforderliche Interessensabwägung im Streitfall.

   In Verbindung mit Telematik-Services sei an dieser Stelle noch darauf hingewiesen, dass sich ein Personenbezug der übermittelten Daten streng genommen auch über die IP Adresse des Telekommunikations-Endgeräts des

[88] z.B: werden über die Funktion „Müdigkeitserkennung“ fahrerspezifische Steuerbewegungen im Sinne eines „machine learning“ verarbeitet.
[89] z.B: durch personifizierte Fahrzeugschlüssel.

Fahrzeughalters ergibt[90]. Daraus folgt: Auch wenn die Daten bereits vor deren Übermittlung an das Datencenter des Fahrzeugherstellers durch die Computersysteme im Fahrzeug anonymisiert wurden, so gibt es dennoch einen Ansatzpunkt für eine tiefere Überprüfung der datenschutzrechtlichen Konformität des gesamten Telematik-Dienstes.

3. Ergebnisse der datenschutzrechtlichen Analyse

Die Werkstatt darf zur Erfüllung ihres Serviceauftrags auf Fahrzeugdaten des Autos zugreifen. Die initiale Abfrage des Fehlerspeichers und eine *anlassbezogene* tiefere Analyse von weiteren Sensor- und Protokolldaten im Fahrzeug ist im Rahmen der Vertragserfüllung über die Erlaubnistatbestände des BDSG gedeckt. Für ein dauerhaftes Speichern der ausgelesenen, personenbezogenen Daten durch die Werkstatt gibt es hingegen keine unmittelbar erkennbare Rechtfertigung.

Anders ist die Situation bei statischen Benutzerdaten, wie z.B: der elektrischen Sitzeinstellung im Auto oder die vom Benutzer gespeicherten Radiokanäle. Diese Art von Daten wird i.A. nicht für eine technische Fehleranalyse am Fahrzeug notwendig sein. Auch ein berechtigtes Interesse auf Seiten der Werkstatt bzw. des Herstellers ist hier schwer zu konstruieren, zumal bei der Interessensabwägung durch den gesteigerten Persönlichkeitsgrad solcher Daten der Fahrzeughalter zu bevorteilen ist. Da diese Daten i.V.m der Fahrzeug-Identifikationsnummer ebenfalls personenbezogen sind, stehen dem Fahrzeughalter die Schutzkonzepte des BDSG zur Verfügung, und er kann verlangen, dass diese Daten nicht ohne zusätzliche Anonymisierungsschritte von der Werkstatt ausgelesen bzw. eingesehen werden (Schutzziel: Vertraulichkeit).

Wie oben gezeigt wird der Fahrzeughalter die Führung des elektronischen Servicehefts und die Übermittlung der Abgasmeßdaten an den Fahrzeughersteller akzeptieren müssen. Eine darüber hinausgehende Datenübermittlung von nicht-anonymisierten Fahrzeugdaten an den Hersteller, wie sie nachweislich erfolgt[91], erfordert eine umfangreiche Interessensabwägung i.S.v § 28 I Nr.2 BDSG. Die Fahrzeughersteller argumentieren hier mit Notwendigkeiten und beidseitigen Nützlichkeiten im Rahmen der Produktweiterentwicklung, Produktsicherheit, Planung von Ersatzteilvorhaltungen, Kundenbindung usw. Die Prüfung, ob nicht das schutzwürdige Interesse des Fahrzeughalters überwiegen könnte, liefert

[90] BGH, Urt. vom 16.05.2017 , VI ZR 135/13 - NJW 2017, 2416 - dazugehöriges Vorabentscheidungsverfahren: EuGH, Urt. vom 19.10.2016 C-582/14 - NJW 2016, 3579.
[91] c't Magazin für Computertechnik 2016/9 170,171; Fußnote 6.

zumindest auf einer theoretischen Ebene einen Angriffspunkt für eine rechtliche Abwehrmaßnahme durch den Fahrzeughalter. Dem Fahrzeughersteller wird man hier die Argumentationslast auferlegen, warum er diese berechtigten Interessen nicht mittels anonymisierten Daten befriedigen kann[92].

Da sich nach oben dargestellter Ansicht (Kapitel C.V) für den Fahrzeughalter kein Ausschließlichkeitsrecht an außerhalb seines Fahrzeugs gespeicherten Daten ergibt und der Schutz nach dem BDSG für anonymisierte Datensätze versagt, hat der Fahrzeughalter nach bisherigen Darstellung keine unmittelbaren rechtlichen Möglichkeit, gegen die Übermittlung und Nutzung von anonymisierten Daten auf Seiten des Fahrzeugherstellers vorzugehen. Das gilt allerdings nur bis zu dem Punkt, an welchem das Fahrerprofil so eindeutig wird, dass aus den Datensätzen wieder ein Personenbezug entsteht.

III. Schutz von Fahrzeugdaten durch Lauterkeitsrecht

Betriebs- und Geschäftsgeheimnisse sind über §§ 18,19 UWG gegen unbefugte Zugangsverschaffung geschützt. Daneben gibt es auch den Nachahmungsschutz gem. § 4 UWG als Leistungsschutzrecht.

Für Betriebs- und Geschäftsgeheimnisse (folgend: *Unternehmensgeheimnis*[93]) gibt es eine gefestigte Definition aus der Rechtsprechung[94]: Als solche Geheimnisse sind Tatsachen zu verstehen, die im Zusammenhang mit dem Geschäftsbetrieb stehen, nur einem eng begrenzten Personenkreis bekannt und damit nicht offenkundig sind. Der zweite Halbsatz umschreibt das „Geheimnis“ – zur Anerkennung eines schützenswerten Unternehmensgeheimnisses ist erforderlich, dass es ein wirtschaftliches Interesse an dessen Geheimhaltung gibt und dass ein bekundeter oder zumindest erkennbarer Wille zur Geheimhaltung besteht[95]. Im Angesicht der Umsetzung der sogenannten *Know-How* Richtlinie EU 2016/943 kann mit heutigem Zeitpunkt schon vertreten werden, dass eine strengere Interpretation bzw. Erweiterung des „Geheimhaltungswillens“ erforderlich ist bzw. werden wird. Die Richtlinie fordert als neues Kriterium das Vorhandensein von „angemessenen Geheimhaltungsschutzmaßnahmen“ und somit ein objektives Tatbestandsmerkmal. Die Richtlinie ist noch nicht in nationales Recht umgesetzt. Dem nationalen Gesetzgeber soll hier nicht vorgegriffen werden, jedoch kann anderseits auch nicht ausgeschlossen werden, dass die Rechtsprechung bereits vor Fristablauf der Umsetzung dieses zusätzliche Merkmal in die

[92] so auch: *Kunnert* CR 2016 S. 512; *Roßnagel* S. 285.
[93] *Dorner* CR 2014, 617, 622.
[94] BGH, Urt. vom 7.11.2002, I ZR 64/00 – NJW-RR 2003, 618, 620.
[95] *Zech* S. 232.

Gesetzesauslegung einfließen lässt – Eine vergleichbare Situation hat im Lauterkeitsrecht bereits zu solch einem richterlichen Vorgriff geführt[96].

Der Unternehmensbezug muss hinreichend konkret und für die operativen oder strategischen Abläufe des Geschäftsbetriebs hinreichend relevant sein, sodass ein wirtschaftlich geprägtes Geheimhaltungsinteresse begründet werden kann. Neben kaufmännischen kommen hier auch technische Informationen, z.B: Produktionsmethoden, in Frage. Das wirtschaftliche Interesse an der Geheimhaltung setzt aber nicht voraus, dass die Datensätze einen konkret bezifferbaren Wert besitzen[97]. Solche Unternehmensgeheimnisse können wiederum nur semantische Information sein und keine uninterpretierten Zeichenketten – es muss hinreichend bekannt sein, „was" die entsprechenden Daten darstellen sollen.

Für die weitere Betrachtung im Lauterkeitsrecht sei der Fahrzeughalter ein Unternehmer im Sinne von § 14 BGB – Das muss nicht notwendigerweise ein Taxiunternehmer sein, sondern kann jeder Unternehmer sein, der seinen PKW für geschäftliche Zwecke, z.B: Kundenbesuche, nutzt.

1. Fahrzeugdaten als Unternehmensgeheimnis aus Sicht des Fahrzeughalters

   Zunächst ist der Bezug zum Unternehmen des Fahrzeughalters herzustellen. Für einen Unternehmer, dessen Fahrzeug annahmegemäß ein Betriebsmittel ist und in welches er nicht bewusst unternehmensrelevante Daten einspielt, kommen nur wenige Datensätze im Fahrzeug als Unternehmensgeheimnis in Betracht. Sämtliche technische Daten des Fahrzeugs, wie der Fehlerspeicher oder technische Diagnosedaten, scheiden aus. Sie haben i.A. keinen Zusammenhang mit dem Geschäftsbetrieb des Unternehmers. Der Geschäftsbetrieb ist das eigentliche Schutzgut – Ein Auslesen dieser technischen Fahrzeugdaten und damit Kenntnismachung an Dritten hat aber keinen negativen Effekt auf die Geschäfte des Unternehmers.

   Die Zugehörigkeit von bestimmten Fahrzeugen zum Unternehmen, wie sie über die VIN und eine Halterabfrage durchgeführt werden kann, ist zwar u.U. eine Information mit Unternehmensbezug die auch für Mitbewerber interessant ist, aber eher keine Information im Zusammenhang mit dem eigentlichem Geschäftsbetrieb und aufgrund der Offenkundigkeit kein Geheimnis.

   Der aktuelle Kilometerstand des Fahrzeugs wäre bei einem Taxiunternehmer zwar eine Information im Zusammenhang mit dem Geschäftsbetrieb (im Sinne einer

[96] BGH, Urt. vom 05.02.1998, I ZR 211/95 – NJW 1998, 2208.
[97] MüKoLauterkeitsrecht/*Brammsen* § 17 Rn. 13.

Auslastung der Fahrzeuge), jedoch ist der Kilometerstand i.A. für jeden Fahrgast erkennbar, und es fehlt somit an einem erkennbaren Geheimhaltungswillen und erst Recht an Geheimhaltungsmaßnahmen.

Etwas anderes könnte gelten, wenn in dem Fahrzeug Positionsdaten des eingebauten GPS Systems dauerhaft gespeichert werden. Ein Auslesen der Positionsdaten liefert Rückschlüsse auf Kunden- und Lieferantenbesuche. Diese Positionsdaten sind einzeln betrachtet für sich alleine kein Geheimnis, da das Auto ja auch auf der Straße bzw. dem Parkplatz im Zuge eines Kundenbesuchs sichtbar ist. Das Geheimhaltungsinteresse und die Betriebsbezogenheit ergeben sich jedoch aus der Ansammlung von vielen solcher Einzeldaten[98] – ähnlich einer Kundenliste die ihren Wert auch erst aus der konzentrierten Ansammlung und konkreten Zusammenstellung von mehreren Kunden gewinnt. Kunden- und Lieferantenlisten von relevantem Umfang werden regelmäßig als Unternehmensgeheimnis eingeordnet[99]. Ein Schutz dieser Datensätze nach dem UWG stünde für natürliche Personen neben dem Schutz, der sich für hinreichend detaillierte Bewegungsprofile auch schon über das Datenschutzrecht ergibt. Für juristische Personen wäre der UWG Schutz allerdings das einzige Abwehrinstrument, da sich das Unternehmen als juristische Person nicht auf das BDSG berufen kann. Bekannt ist, dass Navigationssysteme im Auto die letzten Zieleingaben speichern. Ein dauerhaftes Speichern von GPS Positionsdaten in diversen Fahrsituationen bzw. beim Abstellen des Fahrzeugs wurde von Autoherstellern bereits tw. zugestanden[100] - unbekannt ist jedoch, ob diese Positionsdatenhistorie regelmäßig auch bei Werkstattbesuchen ausgelesen wird. Neben der nicht ganz unproblematischen Anerkennung der Bewegungsprofile als ausreichend aussagekräftiges und damit hinreichend relevantes Unternehmensgeheimnis haben wir es hier daher wohl eher mit einem theoretischen Schutzkonzept zu tun.

Ein anderer Spezialfall ist das Speichern von Telefonnummern im Fahrzeug. Moderne Fahrzeuge bieten an, auf Knopfdruck das gesamte Telefonbuch eines Mobiltelefons in den Fahrzeugspeicher zu übertragen. Bei einem Geschäftsmann wird dieses Telefonbuch notwendigerweise auch geschäftsrelevante Kontakte enthalten, deren Ansammlung je nach Umfang und Aussagekraft einen Geheimhaltungswert besitzen kann. Ist dies zu bejahen, dann ergibt sich eine

[98] Sogenanntes „Bewegungsprofil".
[99] BGH, Urt. vom 27. 4. 2006 , I ZR 126/03 - GRUR 2006, 1044; OLG Köln, Urt. vom 5. 2. 2010, 6 U 136/09 GRUR-RR 2010, 480; ArbG Hamburg Urt. vom 24.1.2013, 29 Ga 2/13 - BeckRS 2013, 68150.
[100] *Markey* Report „Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk" - https://www.markey.senate.gov//imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf Seite 8 [abgefragt am 05.12.2017]

ähnliche Situation wie oben in Verbindung mit statischen Nutzerdaten und dem Datenschutzrecht dargestellt: Die Werkstatt muss zur Erfüllung ihres Serviceauftrags auf Fahrzeugdaten zugreifen – Eine technische Trennung in erlaubte- bzw. verbotene Daten ist auf dieser Ebene schwierig, zumal § 17 UWG eine vorsätzliche Beschaffung und Kenntnisnahme des Geschäftsgeheimnisses erfordert. Dies könnte nur dann angenommen werden, wenn die Werkstatt ganz gezielt die Telefonbuchdaten zum Zwecke des Geheimnisverrats an Mitbewerber ausliest. Neben dem Schadensersatzanspruch gem. § 9 i.V.m § 17 II UWG steht dann auch ein Unterlassungsanspruch gem. § 8 i.V.m § 17 II UWG zur Verfügung, und zwar bereits vorab, sobald der Geheimnisverrat konkret droht.

Aus Sicht des Fahrzeughalters bleibt somit als Zwischenergebnis festzuhalten, dass die gespeicherten Daten im Fahrzeug nur in wenigen Spezialfällen ein Unternehmensgeheimnis darstellen – für diese speziellen Daten wird allerdings ein Schutz über § 17 UWG zugestanden.

2. Fahrzeugdaten als Unternehmensgeheimnis des Fahrzeugherstellers

Auch wenn im Rahmen dieser Arbeit bevorzugt die Position des Fahrzeughalters untersucht wird, soll in diesem Zusammenhang kurz dargestellt werden, ob an den Fahrzeugdaten nicht ein Unternehmensgeheimnis des Fahrzeugherstellers greifen kann. Im Fall der Zuerkennung könnte der Hersteller Daten bewusst vor seinem Kunden, dem Fahrzeughalter, zurückhalten bzw. sich auch gegen das Auslesen von Daten durch Fremdwerkstätten schützen. Beide Szenarien sind für den Fahrzeughalter aus folgendem Grund relevant: In naher Zukunft könnten sich Geschäftsmodelle entwickeln, bei denen der Fahrzeughalter die Möglichkeit bekommt, „seine“ Fahrzeugdaten nicht dem Fahrzeughersteller sondern einem unbeteiligten Drittunternehmen gegen Entgelt zur Verfügung zu stellen.

Für die Anerkennung eines Unternehmensgeheimnisses ist es nachteilig, dass der Hersteller die Maschine (=das Auto) an den Kunden übergibt und das verkörperte Geheimnis (die im Fahrzeug gespeicherten Daten) daher aus der sicheren Sphäre des Herstellers entfernt wird. Daher stellt man bereits heute für die Zuerkennung des Unternehmensgeheimnisses in solchen Fällen teilweise darauf ab[101], ob ein nicht unerheblicher Aufwand notwendig ist, um das Geheimnis zu ergründen (Stichwort: „Reverse Engineering“). Dieser Maßstab wird mit Umsetzung der *Know-How* Richtlinie EU 2016/943, welche konkrete Schutzmaßnahmen für das Unternehmensgeheimnis einfordert, annahmegemäß noch strenger werden[102]. In

[101] Harte-Henning/*Harte-Bavendamm* § 17 Rn. 2a; Ohly-Sosnitza/*Ohly* § 17 Rn. 6.
[102] Harte-Henning/*Harte-Bavendamm* § 17 Rn. 2a.

unserer Fallstudie „Werkstatt“ ergibt sich eine spezielle Situation: Die Verordnung (EG) 715/2007 schreibt vor, dass unabhängige Werkstätten alle notwendigen Geräte und Informationen bekommen müssen, um Service und Reparaturdienstleistungen an den Fahrzeugen durchführen zu können. Dabei geht es z.B: um Konstruktionszeichnungen aber auch um standardisierte Möglichkeiten zum Auslesen von Fahrzeugdaten. Im Hinblick auf die Daten und Informationen die durch diesen gesetzlich vorgeschriebenen Know-How Transfer zur Verfügung gestellt oder deren Kenntnisnahme ermöglicht wird, ist Offenkundigkeit anzunehmen und daher kein Unternehmensgeheimnis i.S.d UWG anzuerkennen.

Für Daten, die sich außerhalb dieses Offenkundigkeitsbereichs befinden und für die der Fahrzeughersteller besondere Schutzvorkehrungen vorgesehen hat, muss zunächst in statische und dynamische Fahrzeugdaten unterschieden werden.

Für den Bereich der statischen Fahrzeugdaten kommen im Zusammenhang mit einem möglichen Unternehmensgeheimnis die sogenannten *Konfigurationsdaten* in Frage[103]. Technisch kann man diese Konfigurationsdaten und ihre Inhalte als notwendigen Bestandteil der Software auffassen. Teilweise werden sie bei der ersten Inbetriebnahme der Software bzw. des gesamten Fahrzeugs auch noch individuell gesetzt oder verändert. Sie sind Teil des *Designs* der Maschine – dieses Design sollte über immaterialgüterrechtliche Konzepte geschützt werden. § 69a I UrhG schützt Computerprogramme einschließlich des *Entwurfsmaterials.* Während es beim Tatbestandsmerkmal *Computerprogramm* mittlerweile auch schon ein erweitertes Begriffsverständnis gibt[104], ist der Begriff des *Entwurfsmaterials* im Wesentlichen auf den Entwicklungsprozess der Software beschränkt[105] und scheidet als Oberbegriff für Konfigurationsdaten aus. Aber auch ein Schutz unter dem Begriff Software scheidet aus – dies ergibt sich schon aus §§ 4, 87a UrhG, wo Datenstrukturen und Daten namentlich erwähnt werden[106]. Wie bereits oben dargestellt, gibt es daher keinen urheberrechtlichen Schutz an den Konfigurationsdaten im Fahrzeug. Der Lauterkeitsschutz könnte diese Lücke füllen: Eine Anerkennung als Unternehmensgeheimnis i.S.v. § 17 UWG ist, sofern die oben genannten Voraussetzungen für ein solches gegeben sind, unproblematischer - § 17 UWG nennt keine spezifischen Erscheinungsformen und ist somit breiter anwendbar. Dazu kommt, dass Computerprogramme vor ihrer Aufnahme in das Urheberrecht schon als geschütztes Betriebsgeheimnis i.R.v §

[103] z.B: ein hoch-optimiertes Set von Konfigurationsparametern, welche ein mechanisches, am freien Fahrzeugzuliefermarkt erhältliches Bauteil besonders schonend im Hinblick auf erhöhte Langlebigkeit ansteuert.
[104] OLG Hamburg, Urt. vom 12.03.1998, 3 U 226/97 – NJW-RR 1999, 483.
[105] Spindler-Schuster/*Wiebe* UrhG § 69a Rn. 8.
[106] Wandtke-Bullinger/*Grützmacher* § 69a Rn. 14.

17 UWG anerkannt wurden[107]. Die Zuerkennung eines Unternehmensgeheimnisses für Konfigurationsdaten ist also möglich, wird im Einzelfall allerdings ausschließlich aufgrund der Relevanz des Datums im Sinne der Unternehmensbezogenheit auf Seiten des Fahrzeugherstellers bewertet werden können[108].

Im Anschluss gilt es zu untersuchen, ob ein Unternehmensgeheimnis zu Gunsten des Fahrzeugherstellers für dynamische Fahrzeugdaten in Betracht kommt. Gerade für diese Art von Daten kann es zu einem Interessenskonflikt zwischen Fahrzeughalter und Fahrzeughersteller kommen. Letzterer hat ein Interesse an Erkenntnissen zur eigenen Produktverbesserung bzw. strategischen Adaptierung seines Produktportfolios. Der Fahrzeughalter verspricht sich jedoch berechtigterweise bessere Ertragsmöglichkeiten, wenn er diese Daten auch Dritten für beliebige Zwecke anbieten kann. Annahmegemäß gibt es die technische Möglichkeit, diese Daten ohne Personenbezug, also anonymisiert oder pseudonymisiert zur verwerten und damit eine Kollision mit dem Datenschutzrecht zur vermeiden.

Zech spricht sich für die Möglichkeit aus, dass ein Hersteller einer komplexen Maschine die in dieser gespeicherten, von dieser erfassten oder sonst wie automatisch erzeugten Daten gegenüber seinem Kunden geheim hält[109]. Er führt weiter aus, dass bei automatisiert erzeugten Daten lediglich geklärt werden müsse, ob das Interesse an der Geheimhaltung durch den Berechtigten wirtschaftlich gerechtfertigt ist - mit Verweis auf Erwägungsgrund 8 der *Know-How* Richtlinie EU 2016/943: Ob das Datum nicht objektiv betrachtet *belanglos* ist. Die Wertigkeit von einzelnen Daten kann sich auch erst aus der konkreten Ansammlung gleicher oder ähnlicher Datensätze ergeben (vgl. „Big Data“). Mit Bezug auf das Fahrzeug stehen wir vor der Situation, dass der Betreiber der Maschine (der Fahrzeughalter) nicht identisch mit dem Hersteller der Maschine ist. Für die Zuerkennung eines Unternehmensgeheimnisses ist weiterhin der Zusammenhang mit dem Geschäftsbetrieb notwendig, dessen ungestörte Ausübung als Rechtsgut geschützt werden soll[110]. Hierfür soll laut *Zech* auch die Speicherung *im Rahmen* des Geschäftsbetriebs ausreichend sein[111]. Dieser *Rahmen* ist nicht in einem örtlichen Sinne zu verstehen. Der Umstand, dass Daten außerhalb der Geschäftseinrichtungen des Fahrzeugherstellers erzeugt werden, widerspricht der Zuerkennung eines Unternehmensgeheimnisses noch nicht –

[107] BayObLG, 4. Strafsenat, Urt. vom 28.08.1990 RReg. 4 St 250/89 – GRUR 1991, 694.
[108] Vgl. Beispiel in Fußnote 103, wo ein schützenswerter Wettbewerbsvorteil argumentiert werden könnte.
[109] *Zech* GRUR 2015, 1151, 1155; *Grützmacher* CR 2016, 485, 488.
[110] *Dorner* CR 2014, 617, 623.
[111] *Zech* GRUR 2015, 1151, 1155.

Annahmegemäß sind an der Maschine technische Schutzvorkehrungen getroffen, die die Offenkundigkeit verhindern. Aber ein Sphärenzusammenhang mit den operativen Geschäftsprozessen des Unternehmens ist sehr wohl zu fordern.

Eben diese Sphäre darf nicht beliebig ausgedehnt werden. Das ursprüngliche Kerngeschäft des Automobilherstellers ist die Produktion, der Vertrieb und die anschließende Betriebsaufrechterhaltung von Autos – in diesem Kerngeschäft kommt es auch zu der Übergabe der Fahrzeuge an die Fahrzeughalter. Durch einen Geheimnisverrat von dynamischen Fahrzeugdaten kommt es weder für die Produktion, das Verkaufsgeschäft noch für das Wartungsgeschäft des Herstellers zu negativen wirtschaftlichen Effekten - für die damit verbundene Zwecke (z.B: Produktoptimierung) bleibt der Wert dieser Daten für den Fahrzeughersteller trotz Geheimnisverrat gleich hoch. Ein Geheimnisverrat vermindert zwar annahmegemäß den Wert der erhobenen Daten, dieser Wertverlust ergibt sich aber erst durch den Weiterverkauf dieser Daten an unbeteiligte Dritte. Dieser „neue“ Geschäftsprozess steht in keinerlei Verbindung mit jenem der zwischen Fahrzeughalter und Fahrzeughersteller zur Übergabe und Betriebsaufrechterhaltung des Fahrzeugs geführt hat.

Den Begriff des Geschäftsbetriebs kann man außerdem nicht so weit ausweiten, dass eine unternehmensfremde Person, der Fahrzeughalter, mit der Maschine bestimmungsgemäß verfährt und die daraus entstehenden Fahrten im Zusammenhang mit dem Geschäftsbetrieb des Herstellers stehen. Jeglicher Einfluss, den der Fahrzeughersteller auf die Generierung dieser „Geheimnisse“ hatte, ist durch den Designschutz der Maschine abgegolten (z.B: die Algorithmen in der Software).

Im Ergebnis ist die Zuerkennung eines schützenswerten Geheimnisses bei der Generierung von dynamischen Fahrzeugdaten auf den Betrieb des Fahrzeugs innerhalb der operativen oder strategischen Geschäftsprozesse des Fahrzeugherstellers begrenzt – Das wäre bspw. zu bejahen für dynamische Fahrzeugdaten, die im Zuge von durch den Hersteller durchgeführten Testfahrten erzeugt werden, aber nicht für jene die beim Betrieb des Autos durch den Fahrzeughalter anfallen.

3. Nachahmungsschutz gem. § 4 UWG

Der ungehinderten Weitergabe der dynamischen Fahrzeugdaten durch den Fahrzeughalter an einen Dritten könnte noch der Nachahmungsschutz gem. § 4 Nr. 3 UWG entgegenstehen. Unkörperliche Gegenstände stehen als Waren

generell dem Nachahmungsschutz offen[112]. Das zeigt sich auch aus der Geschichte der Rechtsprechung, die Software[113] und Datenbankwerke[114] vor deren spezialgesetzlicher Aufnahme in das Immaterialgüterrecht schon über den Nachahmungsschutz des Lauterkeitsrechts geschützt hat. So eine Nachahmungshandlung kann prinzipiell auch eine Vervielfältigung von Daten sein[115]. Neben den spezialgesetzlichen Schutzgesetzen ist § 4 UWG grundsätzlich subsidiär anwendbar, allerdings ist zu berücksichtigen, dass außerhalb der zugewiesenen, spezialgesetzlichen Schutzkonzepte die wirtschaftliche Betätigung des Einzelnen grundsätzlich frei sein soll[116]. Die Anwendung des lauterkeitsrechtlichen Nachahmungsschutz bei der Übernahme von nicht urheberrechtlich geschützten Daten, wie hier der Fall, ist in diesem Spannungsfeld daher auf besondere unlauterkeitsbegründende Umstände zu reduzieren.

Ansprüche, die sich aus der Verletzung des Nachahmungsschutzes ergeben, können nur vom betroffenen Unternehmen gegen einen Mitbewerber erhoben werden. Der Fahrzeughalter, selbst wenn er Unternehmer ist, kommt als Mitbewerber nicht in Betracht. Es besteht kein konkretes Wettbewerbsverhältnis im Sinne eines nachgeahmten Produkts, denn der Fahrzeughalter kann nur „seine“ Rohdaten anbieten, während der Fahrzeughersteller darüber hinaus Abweichungen bzw. Gemeinsamkeiten sowie Statistiken über viele Fahrzeuge hinweg durchführen kann aus denen annahmegemäß zusätzliche Erkenntnisse entstehen.

Denkbar wäre allerdings, dass der Fahrzeughersteller mit einem Dritten („Datenhändler“) in ein Wettbewerbsverhältnis tritt. Diese Möglichkeit soll an dieser Stelle aber nicht weiter vertieft werden, da der Fahrzeughalter hiervon nicht mehr unmittelbar betroffen ist.

4. Zusammenfassung des lauterkeitsrechtlichen Schutzes

Für den Fahrzeughalter als Unternehmer ergibt sich nur in wenigen, theoretisch erdachten Spezialfällen ein Angriffspunkt für ein lauterkeitsrechtliches Schutzkonzept an den gespeicherten Daten im Fahrzeug.

Interessanter ist das Ergebnis in Bezug auf ein Unternehmensgeheimnis aus Sicht des Fahrzeugherstellers: Statische Fahrzeugdaten, die keine statischen Nutzerdaten sind, und als Teil des Designs der Maschine aufgefasst werden können, nicht offenkundig oder belanglos sind und einem berechtigten

[112] Ohly-Sosnitza/*Ohly* § 4 Rn. 3/27.
[113] OLG Frankfurt am Main, Urt. v. 21.07.1983 6 U 16/83 – GRUR 1983, 757.
[114] BGH, Urt. vom 06.05.1999 I ZR 199 / 96 – GRUR 1999, 923.
[115] OLG Frankfurt am Main, Urt. vom 22.03.2005 11 U 64/2004 - GRUR 2005, 299; *Zech* S.412.
[116] Ohly-Sosnitza/*Ohly* § 4 Rn. 3/2.

Geheimhaltungsinteresse unterliegen, sind ein Unternehmensgeheimnis i.S.v. § 17 UWG des Fahrzeugherstellers. Das ist eine sinnvolle Ergänzung von Schutzlücken die sich aus dem Immaterialgüterrecht ergeben. Im Falle der Zuerkennung gilt: Trotz der Speicherung auf „seinem“ Datenträger und der generellen Zuerkennung eines *Kenntnisnahme*-Rechts an den gespeicherten Daten kann der Fahrzeughalter demnach nicht die Aufhebung einer eventuell bestehenden, faktischen Zugangshürde zu jenen Daten verlangen. Dem Fahrzeughersteller stehen Unterlassungsansprüche gem. § 8 i.V.m §17 II UWG und Schadensersatzansprüche gem. § 9 i.V.m § 17 II UWG zu, falls sich der Fahrzeughalter oder ein Dritter Zugang zu diesen Daten selbstständig und vorsätzlich verschafft. Die Schutzziele Vertraulichkeit und Verfügbarkeit an diesen Daten stehen demnach nur dem Fahrzeughersteller zu. Im Falle einer Integritätsverletzung dieser Daten ist für den Fahrzeughalter aber über den eigentumsrechtlichen Schutz des Datenträgers sehr wohl ein Schadensanspruch gem. § 823 I BGB konstruierbar.

Wesentlich „wertvoller“ aus Sicht des Fahrzeughalters und eines unbeteiligten „Datenhändlers“ ist jedoch die Verfügungsmöglichkeit über die dynamischen Fahrzeugdaten. Diese sind kein Unternehmensgeheimnis des Fahrzeugherstellers. Der Fahrzeughalter ist hier einerseits privilegiert über den Eigentumsschutz – er kann den physischen Zugang zur Datenschnittstelle faktisch kontrollieren. Andererseits ist ihm der Fahrzeughersteller i.A. mit einem faktischen Ausschluss schon zuvorgekommen, denn er verhindert den Zugriff auf Daten außerhalb der standardisierten Datenstrukturen durch Verschlüsselung bzw. Passwortschutz. Dem Fahrzeughalter steht es zwar frei, Mittel und Wege zu finden, diese technischen Schutzmechanismen zu überwinden – Dabei besteht allerdings das Risiko, dass er sich damit ebenfalls Zugang zu Daten verschafft, die als Unternehmensgeheimnis des Fahrzeugherstellers einzustufen sind (siehe oben). Ob der Fahrzeughalter über sein Recht auf *Kenntnisnahme* die Entfernung des Zugriffsschutzes an den dynamischen Fahrzeugdaten vom Fahrzeughersteller verlangen kann, ist nach dem derzeitigen Stand der Analyse noch nicht beantwortbar - je nach technischer Realisierung ist hier jedenfalls auch die potentielle Offenlegung von Unternehmensgeheimnissen des Herstellers als Gegenargument zu berücksichtigen.

IV. Deliktrechtliche Schutzkonzepte aus dem allg. Zivilrecht

Nach der detaillierten Analyse auf spezialgesetzlicher Ebene soll nachfolgend das allg. Deliktrecht nach möglichen Schutzkonzepten durchsucht werden. Schon alleine aufgrund des Spezialitätsgrundsatzes ist einleuchtend, dass die hier

behandelten Schutzkonzepte einen subsidiären Charakter haben müssen. Diese Subsidiarität ergibt sich aber auch aus einer praktischen Sichtweise heraus, denn man wird zunächst versuchen, die Daten auf semantischer Ebene spezialgesetzlich auf ihre Schutzfähigkeit zu prüfen. Scheitert dies, dann hat man es eventuell mit einer Schutzlücke zu tun die man auf syntaktischer Ebene[117] mit Hilfe des allg. Zivilrechts schließen kann.

1. Deliktsrechtliche Schutzkonzepte an Daten gem. § 823 I BGB

   Wie bereits in Kapitel C.IV dargestellt, ist über den Umweg einer Integritätsverletzung am Datenträger der schreibende bzw. zerstörende Zugriff auf Daten gegen den Willen des Eigentümers des Datenträgers über § 823 I BGB geschützt - angesetzt wird hier an dem geschützten Rechtsgut „Eigentum“. Auch der vollständige Ausschluss der Nutzungsmöglichkeit *Kenntnisnahme* (vgl. Kapitel C.IV) ist über die Konstruktion des Besitzes geschützt.

   Das Schutzkonzept über den Umweg des Datenträgers versagt für das Schutzziel der Vertraulichkeit. Daher ist in einem weiteren Schritt zu fragen, ob dieses Schutzziel über eine Konstruktion hergestellt werden kann, die Daten als „sonstiges Recht“ i.S.v § 823 I BGB qualifiziert.

a) Vertraulichkeitsschutz gem. § 823 I BGB auf „Systemebene“

   Eine Argumentation in diese Richtung lässt sich aus dem vom BVerfG anerkannten „neuen“ Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[118] ableiten. Dieses wurde aus einer Erweiterung des allg. Persönlichkeitsrechtes abgeleitet. Autoren haben daraufhin versucht, die grundrechtliche Anerkennung in das Zivilrecht auf Basis von § 823 I BGB zu übertragen, indem sie einen ähnlichen Ansatz wie bei der erfolgreichen Rechtsfortbildung zum „eingerichteten Gewerbebetrieb“ verfolgen[119].

   Die BVerfG Entscheidung ist allerdings nur unproblematisch auf „Systemebene“ anzuwenden. Gegenstand der höchstrichterlichen Herleitung war das Schließen einer Schutzlücke, die verhindert, dass unberechtigte Dritte „Leistungen, Funktionen und Speicherinhalte des *Systems* nutzen“. Dies auch nur dann, wenn dieses System zumindest „persönlichkeitsrelevant“ ist, d.h. wenn jemand das System als „sein eigenes“ nutzt und daher mit einer hohen Wahrscheinlichkeit

[117] Als *syntaktische Ebene* gilt hier die *Zeichenkette*, also uninterpretierte Daten unabhängig von ihrem Informationsgehalt.
[118] BVerfG, Urt. vom 27.2.2008 , 1 BvR 370/07 - NJW 2008, 822.
[119] *Bartsch* CR 2008, 613, 614 ff; *Zech* S. 387; *Grützmacher* CR 2016, 485,490;Prütting-Wegen-Weinreich/*Schaub* § 823 Rn. 80.

Daten vorhanden sind, die zum persönlichen Lebensbereich zu zählen sind[120]. Auf das System „Auto“ kann man diese Einordnung unproblematisch anwenden.

Eine Beurteilung, ob eine etwaige Verletzung des Schutzgutes „Vertraulichkeit an Daten“ im Rahmen eines sonstigen Rechts von 823 I BGB vorliegt, muss mit einer Interessensabwägung beurteilt werden[121]. Dies wird zutreffend begründet unter Verweis auf die ähnlich gelagerten Schutzkonzepte im Rahmen der sonstigen Rechte § 823 I BGB, wie z.B: zum eingerichteten Gewerbebetrieb und dem Persönlichkeitsrecht. Gemäß diesen beiden Vorbildern ist das hier gefundene „sonstige Recht“ außerdem subsidiär zu anderen Schutzkonzepten (z.B: auf semantischer Ebene: Urheberrecht, Datenschutz, usw.) zu verstehen.
Teil dieser Interessensabwägung muss auch sein, ob der Betroffene zumutbare bzw. systemimmanente Schutzmittel angewendet hat. Bezogen auf die Fallstudie „Werkstatt“ muss der Fahrzeughalter damit rechnen, dass mit elektronischen Verfahren Daten aus seinem Auto ausgelesen werden. Schließlich gibt er alle Zugangsschutzmechanismen[122] , sowie auch den Besitz am Fahrzeug freiwillig auf. Auf der „Systemebene“ kann nicht weiter zwischen Daten unterschieden werden, deren Auslesen „notwendig“ und daher erlaubt ist – ein einmalig gewährter Zugang zum System eröffnet daher die Möglichkeit der Kenntnisnahme aller auslesbaren Daten. Personenbezogene Daten sind dabei, wie oben dargestellt, anderweitig geschützt.
Etwas anderes würde aber gelten, wenn ein unbeteiligter Dritter sich Zugang zum Auto verschafft und Daten über die OBD Schnittstelle ausliest. Über einen quasinegatorischen Unterlassungsanspruch analog §§ 823 I, 1004 BGB kann im Fall der Wiederholungsgefahr, bzw. vor der erstmalig unmittelbar bevorstehenden Störung, vorgegangen werden. In Analogie zum allg. Persönlichkeitsrecht wäre auch ein ersatzfähiger Schaden ableitbar: Es gibt zwar derzeit keine öffentlich zugänglichen Marktplätze, an denen der Fahrzeugeigentümer oder ein unberechtigter Datendieb konkrete Erlösaussichten für die Überlassung der Daten vorfindet. Gelingt allerdings der Nachweis für einen erfolgreichen „Verkauf“ der Daten, steht dem Ersatz eines Eingriffsgewinns[123] nichts entgegen.

[120] *Kutscha* NJW 2008, 1042, 1043; *Zech* S.388.
[121] *Bartsch* CR 2008, 613,616; *Zech* S. 387.
[122] Die OBD Schnittstelle befindet sich im Fahrgastraum.
[123] *Wendehorst* S.117.

b) Schutzkonzept § 823 I BGB auf „Datenebene“

Ein wesentlich wirksameres Schutzkonzept würde sich ergeben, wenn § 823 I BGB als sonstiges Recht auf den *Datenbestand* selbst anwendbar wäre[124]. Einer der Ausgangspunkte für die Argumentation ist die höchstrichterliche Klassifikation von „Datenbeständen als vermögenswertes Gut“[125].

Der Schutz würde vorerst subsidiär neben demjenigen stehen, der sich über den Umweg des eigentumsrechtlichen Schutzes an der Verkörperung der Daten am Datenträger ergibt[126]. Das erweiterte Schutzkonzept müsste allerdings auch den praxisrelevanten Fall umfassen, dass die Daten aus dem oben anerkannten Schutzbereich des Ursprungssystems bzw. des Ursprungsdatenträgers auf einen anderen Datenträger übertragen werden.

Dem Konzept steht vorerst entgegen, dass der so übermittelte Datenbestand sofort im eigentumsrechtlichen Schutzbereich des neuen Datenträgers „verschwinden“ würde – Annahmegemäß ist der Eigentümer des Zieldatenträgers eine andere Person als diejenige, der wir einen Schutz an der Kopie der Daten zugestehen wollen[127]. Um das oben postulierte Nebeneinander der beiden Schutzkonzepte (verkörperter Angriffspunkt *neben* unverkörperter Angriffspunkt) weiter aufrecht zu erhalten, benötigt man für den unkörperlichen Angriffspunkt eine hinreichend konkrete Zuweisung der gespeicherten Daten an den ursprünglich Berechtigten.

Das ist zum einen über den bereits angesprochenen „Skripturakt“[128] möglich. Zusätzlich wird man aber verlangen müssen, dass der Berechtigte einen virtuell ausschließlichen Zugang, z.B: mittels Passwortschutz, zu „seinem“ Speicherbereich hat. Diese zweite Forderung hat zum einen technische Gründe, ist aber auch als Element der sozialen Offenkundigkeit notwendig um den unkörperlichen Eingriffsbereich ausreichend genau abzugrenzen. Cloud-Services verfügen regelmäßig über einen abgeschlossenen, zugewiesenen Speicherbereich. Diesen Speicherbereich kann man nun als *virtuellen Datenträger* verstehen, an welchem der Berechtigte einen deliktsrechtlichen Schutz, auch gegen Dritte[129], geltend machen kann. In Wirklichkeit ergibt sich dadurch eine Konstruktion wie in Kapitel D.IV.a) dargestellt, denn der virtuelle Datenträger hat

[124] Befürwortend: Prütting-Wegen-Weinreich/*Schaub* § 823 Rn. 80; *Bartsch* CR 2010, 553, 555; BeckOKBGB/*Spindler* § 823 Rn. 183 ff; *Zech* S. 386; *Meier-Wehlau* NJW 1998, 1585; Ablehnend: Staudinger/*Hager* § 823 Rn. B192; *Härting* CR 2016, 646, 649.

[125] BGH, Urt. vom 02.07.1996, X ZR 64/94 – NJW 1996, 2924.

[126] BeckOK/*Spindler* § 823 Rn. 185.

[127] Diese Konstellation wird im Umfeld von Cloud-Services immer wichtiger.

[128] vgl. Kapitel C.II.

[129] Der Cloud-Service Provider hat regelmäßig vertraglich eingeräumte Zugriffsrechte auf den Datenbestand, z.B. um Backup-Dienste durchzuführen oder im Rahmen von technischen Wartungs- und Servicemaßnahmen (Stichwort „Systemadministration“).

für sich alleine eine „Systemeigenschaft“ und dieses System ist Angriffspunkt für das Grundrecht auf Vertraulichkeit und Integrität – zivilrechtlich abgebildet über das Einfallstor § 823 I BGB als sonstiges Recht. Auch die Übertragung des Schutzziels Verfügbarkeit ist, wie oben vertreten, über eine besitzähnliche Konstruktion als ständige Zugangsmöglichkeit zum „virtuellen Datenträger“ ableitbar.

Ein Teil der zustimmenden Literaturmeinungen[130] spricht bei genauer Lesart korrekterweise auch von einem Schutzrecht am Daten*bestand* im Zusammenhang mit § 823 I BGB, während ein Großteil dieser Autoren ein eigentumsähnliches Recht an Daten i.S.v §§ 903, 90 BGB weiterhin ablehnt. Diese Differenzierung ist, auch wenn sie explizit nicht durchgängig dargestellt wird, ganz wesentlich: Denn der *Datenbestand* steht weiterhin unmittelbar mit dem Berechtigten in Verbindung – er betreibt und pflegt diesen Datenbestand selbstständig und erlangt dadurch einen Schutz in Bezug auf die Nutzung und Geheimhaltung von einer funktionalen Perspektive *an* diesem Datenbestand. Das bedeutet aber umgekehrt, dass das Schutzkonzept nicht den Daten selbst anhaftet. Gegen den Datendieb der sich unberechtigt Zugang zum virtuellen Datenträger verschafft hätte der Berechtigte des Datenbestandes eine Handhabe, nicht aber gegen denjenigen, an welchen der Dieb die Daten, z.B: als Kopie, weitergeben hat[131]. An den Daten selbst gibt es weiterhin kein Ausschließlichkeitsrecht – es fehlt die güterrechtliche Zuordnung. Das Deliktsrecht kann diese eigentumsähnlichen Ausschließlichkeitsrechte nicht begründen, sondern schützt nur eine bereits erfolgte Zuordnung von eben diesen[132]. Eine solche wurde in Kapitel C jedoch bereits abgelehnt. Das in der Literatur geforderte *Recht am Datenbestand* im Schutzbereich von § 823 I BGB ist daher im Ergebnis auf einen abgeschlossenen, *systemähnlichen* Speicherbereich, an dem der Berechtigten einen offenkundigen Zugang hat, zu begrenzen.

Im Kapitel D.IV.a) wurde im Zusammenhang mit der Fallstudie „Werkstatt“ eine Berechtigung zum Auslesen der Daten durch den Werkstattsbetrieb angenommen[133]. Durch die Übertragung der Daten aus dem Auto heraus auf einen Computer in der Werkstatt verliert der Fahrzeugeigentümer nach der hier vertretenen Ansicht das Schutzkonzept an seinem Datenbestand. Auf dem Computer der Werkstatt hat er keinen, ihm zugeordneten Speicherbereich. Er nimmt auch den Skripturakt nicht selbst vor. Aus der Perspektive § 823 I BGB hat er demnach keine Handhabe dagegen, dass die Werkstatt Datensätze aus seinem

[130] vgl Fußnote 124.
[131] *Fischer* § 303a Rn. 6 - Eine mögliche Verfolgung unter dem Straftatbestand § 202d StGB „Datenhehlerei“ bleibt bei dieser Betrachtung unberücksichtigt.
[132] *Dorner* CR 2014, 617, 621.
[133] Weiterhin unter der Annahme, dass keine gegenteilige vertragliche Vereinbarung besteht.

Fahrzeug dauerhaft speichert und an Dritte (z.B: den Fahrzeughersteller) übermittelt.

2. Deliktsrechtliche Schutzkonzepte an Daten gem. § 823 II BGB i.V.m dem Strafrecht

Im Unterschied zum Zivilrecht enthält das Strafrecht spezifische Schutznormen für Daten, und zwar die Antragsdelikte §§ 202a, 202b, 202d, 303a, 303b StGB und das Offizialdelikt § 202c StGB. Diese sind Schutzgesetze i.S.v. § 823 II BGB und stehen daher prinzipiell für einen außervertraglichen Anspruch gegen einen „Täter" zur Verfügung. Dabei realisiert § 303a StGB die Schutzziele Datenintegrität und Verfügbarkeit (Wortlaut: „unterdrückt"), während § 202a StGB die Vertraulichkeit schützt.

Zum Integritätsschutz: Wie schon in Kapitel C.II angesprochen, ist die Festlegung eines zivilrechtlichen Schutzberechtigten nicht unproblematisch und geht aus dem StGB als solche nicht hervor. § 303a StGB fordert explizit die *Rechtswidrigkeit*. Aufgrund der wörtlichen Nennung einer ohnehin implizit in jeder Strafrechtsnorm vorhandenen Strafbarkeitsvoraussetzung muss man, i.V.m mit dem Bestimmheitsgebot, hier einen strengen Maßstab für die Bestimmung des Täters als Abgrenzung zum Berechtigten vornehmen. Nach h.M.[134] wird auf den „Skripturakt" abgestellt und erst in nachgelagerter Art und Weise auf die Eigentümerstellung an dem betroffenen Datenträger. Dieser Ansicht ist zu folgen, da der Eigentümer bereits über § 303a StGB, zumindest für Integritätsverletzungen, einen Schutz genießt. Der „Skribent" ist derjenige, der die Speicherung der Daten selbst unmittelbar bewirkt hat[135]. Dies ist bei einem passwortgeschützten Cloud-Speicher, den annahmegemäß nur der Berechtigte mit Daten befüllen kann, unproblematisch zu bejahen. Im Hinblick auf die im Fahrzeug gespeicherten dynamischen Fahrzeugdaten ist diese Zuweisung allerdings nicht ohne weiteres eindeutig - die Daten werden automatisch erzeugt. Eine „Bewirkung" durch den Fahrer des Fahrzeugs ist kausal gerade noch begründbar, aber das Kriterium „unmittelbar selbst" ist weder für den aktuellen Fahrzeugführer noch für den Fahrzeughalter unproblematisch subsumierbar. Denn aufgrund der Programmierung der entsprechenden Algorithmen könnte man auch argumentieren, dass der Fahrzeughersteller als „Skribent" anzusehen ist[136]. Obiger Ansicht folgend ist der Fahrzeughalter über den eigentumsrechtlichen Schutz § 823 I BGB am Datenträger daher besser vor Integritätsverletzungen an den

[134] BayObLG, Urt. vom 24.06.1993, 5 St RR 5/93 - JR 1994, 478; *Grützmacher* CR 2016;485, 491; *Zech* S.394; *Welp* IuR 1988 S.444; *Hoeren* MMR 2013,486,487; a.A. Schönke-Schröder/*Stree-Hecker* § 303a Rn 3.
[135] *Zech* S. 395.
[136] Unproblematischer dem Fahren bzw. Fahrzeughalter zuweisbar sind aber wohl die statischen Nutzerdaten im Fahrzeug.

gespeicherten Daten geschützt als über § 823 II i.V.m § 303a StGB. Dazu kommt, dass §303a StGB aufgrund mangelnder expliziter Nennung eines Fahrlässigkeitstatbestandes (§ 15 StGB) nur bei Vorsatz zur Anwendung kommt. Gem. der Systematik von § 823 II S.2 ist daher auch für die zivilrechtlichen Ansprüche eine vorsätzliche Rechtsgutverletzung erforderlich, wobei der Vorsatzbegriff aus dem Strafrecht Anwendung findet[137]. Eine fahrlässige Integritätsverletzung ist über § 823 II i.V.m § 303a StGB daher nicht geschützt, über die oben angeführten Konstruktionen (Eigentum, sonstiges Recht) mittels § 823 I BGB hingegen schon.

Vertraulichkeitsverletzungen an *fremden* Datenbeständen sind über § 823 II BGB i.V.m § 202a StGB geschützt. Die Strafrechtsnorm fordert allerdings neben dem Vorsatz einen faktisch wirksamen, besonderen Zugriffschutz, welcher im objektiven Tatbestand durch den Schädiger *überwindet* wird. Die Rechtsnorm stellt somit die Verschaffung des *Zugangs* zu den Daten unter Strafe – den Daten selbst haftet weiterhin kein Schutzkonzept an, welches auch außerhalb der geschützten Einheit zur Verfügung stünde. Im Ergebnis greift der Schutz daher wiederum auf „Systemebene“ und nicht auf Datenebene, wobei das „System“ auch vollständig virtualisiert sein kann (vgl. Cloud-Speicher). Als eine solche Überwindung eines Zugriffschutzes kann ein abgesperrtes Auto, welches ein Datendieb aufbricht um die OBD Schnittstelle anzuzapfen, problemlos eingeordnet werden[138]. In der Werkstatt-Situation versagt das Schutzkonzept, wie oben dargestellt, an der freiwilligen Aufgabe des Zugriffschutzes durch den Fahrzeughalter. Gegen das Weiterübermitteln der ausgelesenen Daten besteht keine Handhabe im Rahmen von § 202a StGB. Ähnliches gilt für den Straftatbestand Datenhehlerei gem. § 202d StGB – hier scheitert es daran, dass die Werkstatt die Datensätze nicht rechtswidrig erlangt hat.

Fraglich bleibt noch das Schutzziel der Verfügbarkeit – ausgedrückt durch das Tatbestandsmerkmal „unterdrückt“ in § 303a StGB. Zwar ist ein vollständiger Nutzungsausschluss des eigenen Datenträgers auch über das Eigentumsrecht bzw. das Besitzrecht gem. § 823 I BGB geschützt, jedoch könnte die Kombination § 823 II BGB i.V.m § 303a StGB hier einen erweiterten Schutz darstellen, der sich auch auf einzelne unterdrückte Datenelemente erstreckt. In Kapitel D.III.2 wurde festgestellt, dass die „herrenlosen“[139] dynamischen Fahrzeugdaten vom Fahrzeughersteller oft mit einer Verschlüsselung bzw. mit anderen

[137] Dauner-Langen/*Katzenmeier* § 823 Rn. 535.
[138] Die OBD Schnittstelle ist von außen nicht zugänglich. Auch das Eindringen in den Motorraum wäre ein Überwinden eines Zugriffschutzes.
[139] „Herrenlos“ deshalb, weil bislang keine spezialgesetzlichen Schutzkonzepte gefunden wurden.

Zugangsbarrieren versehen ist. Fraglich ist daher, ob dies eine rechtswidrige „Unterdrückung“ gegenüber dem Fahrzeughalter darstellt. Die Errichtung eines Zugangshindernisses kann eine Unterdrückung i.S.d. Vorschrift sein[140], fraglich ist allerdings deren Rechtswidrigkeit. Die „Fremdheit“ der Daten muss im Umfeld von §303a StGB streng beurteilt werden. Im Umkehrschluss muss die verletzte Berechtigung daher aus einem unmittelbaren Recht auf Verarbeitung, Löschung oder Nutzung abgeleitet sein[141] - ein bloßes Interesse am Inhalt der Daten genügt nicht[142]. Über das Eigentum am Datenträger ist der Fahrzeughalter hier in einer guten Position, um als „Berechtigter“ i.S.v. § 303a StGB angesehen zu werden. Seine Rolle als „Skribent“ ist allerdings, wie gezeigt, nicht eindeutig. Aufgrund dieser fehlenden Eindeutigkeit muss man die Erfüllung des Tatbestands §303a StGB wegen des Anbringens des Zugriffsschutzes durch den Fahrzeughersteller letztlich jedenfalls wegen fehlenden Vorsatzes verneinen. Der subjektive Tatbestand muss sich auf alle Tatbestandsmerkmale beziehen – somit auch auf die Kenntnis der fehlenden Verfügungsbefugnis. Dazu kommt, dass im Moment der Auslieferung der Zugangsschutz bereits besteht, aber noch gar keine schützenswerten dynamischen Fahrzeugdaten vorliegen. Somit ist auch die Kausalität des Eingriffs zu verneinen. Im Zwischenergebnis ergibt sich daher über § 823 II i.V.m § 303a StGB keine zusätzliche Möglichkeit für den Fahrzeughalter, gegen elektronischen Zugangsbarrieren an seinen Fahrzeugdaten rechtlich vorzugehen.

3. Ergebnis der deliktsrechtlichen Analyse

   Die deliktsrechtliche Analyse bestätigt die Ablehnung eines „Dateneigentumsrechts“ insofern, als deliktsrechtlich anerkannte bzw. herleitbare Schutzkonzepte an Daten in Wirklichkeit nur auf Systemebene unproblematisch anwendbar sind. § 823 II i.V.m § 303a StGB schützt zwar wörtlich die Integrität von *Daten*, allerdings ist - wie gezeigt - die Zuordnung zu einem Berechtigten außerhalb einer systemähnlichen Umgebung (z.B: Eigentum am Datenträger, virtueller Datenträger, abgeschlossenes IT System) schwierig. Ohne eindeutige Bestimmung des Berechtigten scheidet der Tatbestand § 303a StGB aber von vornherein aus – herrenlose Daten sind nicht geschützt. Die Schutzkonstruktionen zum Vertraulichkeitsschutz über § 823 I BGB bzw. § 823 II i.V.m § 202a sind ohne den Systembegriff ebenfalls nicht überzeugend argumentierbar.

[140] *Fischer* § 303a Rn. 10.
[141] *Fischer* § 303a Rn. 4a.
[142] Kindhäuser-Neumann-Paeffgen/*Zaczyk* § 303a Rn. 5.

Zusammenfassend kann daher festgehalten werden, dass durch die hier erfolgte Anerkennung eines Rechts am Datenbestand i.S.v. § 823 I BGB als sonstiges Recht für den Fahrzeughalter das Schutzziel der Vertraulichkeit an im Fahrzeug gespeicherten Daten erreicht wird, sofern er den faktischen Zugangsschutz nicht freiwillig bzw. leichtfertig aufgibt. Das ist eine Ausweitung des Schutzes verglichen mit jenem, den der Fahrzeughalter alleine durch die eigentumsrechtliche Betrachtung des Datenträgers hätte. Aus der Anerkennung folgt weiter, dass Fahrzeugdaten, die außerhalb des Fahrzeugs in einem dem Fahrzeughalter eindeutig zugewiesenen und abgrenzbaren virtuellen Speicherbereich (vgl. Cloud-Speicher) abgelegt werden, ebenfalls diesen Schutz erfahren. Dieses Schutzkonzept im Rahmen der „sonstigen Rechte“ überzeugt aus einer rechtsdogmatischen Sichtweise mehr, als wenn man die „verkörperten Daten“ als Erweiterung der Rechtsprechung des BGH[143] als Sache einordnet und an diesen einen eigentumsrechtlichen Schutz i.S.v. § 823 I BGB konstruiert. Solange man den Daten keine semantische Information zuweisen kann, gibt es für eine Zuerkennung der Sacheigenschaft an Daten auf einem Cloud-Speicher keine Ansatzpunkte und somit keinen Weg zur Anerkennung als eigentumsähnliches Rechtsgut im Schutzrahmen von § 823 I BGB.

Die gefundenen Schutzkonzepte an Daten im Cloud-Speicher kommen dem Fahrzeughalter im Kontext von sogenannten Telematik-Services zu Gute. Für diese Services ist immer eine vertragliche Vereinbarung zwischen dem Fahrzeughalter und dem Telematik-Betreiber - hier dem Fahrzeughersteller - notwendig. Hierbei werden ausgewählte Fahrzeugdaten während des Betriebs des Fahrzeugs über dessen Datenanbindung an das Backend des Telematik-Service-Providers übermittelt. Dem Fahrzeughalter wird dann ein Webportal angeboten, in welchem er standortunabhängig in diese übermittelten Daten Einsicht nehmen kann[144]. Auf dem Webportal werden in erster Linie aktuelle Zustandsdaten zu dem Fahrzeug angezeigt, aber seltener umfassende historische Datensätze. Dies ist dem Anwenderinteresse des Fahrzeughalters geschuldet. Aus einer technischen Perspektive werden allerdings alle Zustandsdaten zumindest zwischengespeichert – wie lange sie danach aufbewahrt werden, ist nicht bekannt. Allerdings hat sich herausgestellt[145], dass in der Praxis wesentlich mehr Daten übertragen werden als dem Benutzer des Telematik-Dienstes auf dem Webportal suggeriert wird. Das Webportal ist dem Fahrzeughalter über einen Zugriffsschutz eindeutig zugeordnet

[143] BGH, Urt. vom 15. 11.2006, XII ZR 120/04 - NJW 2007,2394.
[144] z.B. beim Produkt „Mercedes Me“ der Daimler AG: Zustand offene Türen, Zustand offene Fenster, Benzinstand, Reifendruck, diverse Warnmeldungen, Kilometerstand, aktuelle Fahrzeugposition (abschaltbar), Historie der letzten Fahrt, etc.
[145] siehe Fußnote 6, 8, 91.

und kann daher als „virtuelles System“ betrachtet werden. Ein Einbrechen und Ausspähen der Daten in diesem Webportal durch einen Datendieb ist über § 823 II BGB i.V.m § 202a StGB geschützt – alle Tatbestandsvoraussetzungen von § 202a StGB liegen vor. Als Berechtigte sind in diesem Fall sowohl der Betreiber des Webportals als auch der Fahrzeughalter anzusehen. Schwieriger ist eine Übertragung des Integritätsschutzes über § 823 II BGB i.V.m § 303a StGB, da überwiegend nur Zustandsdaten zur Verfügung stehen, die in einer dauerhaft gespeicherten Form keinen erkennbaren Wert haben. Deren Zerstörung bewirkt demnach i.A. keinen ersatzfähigen Schaden. Aus ähnlichen Gründen problematisch erscheint die Anerkennung eines Integritätsschutzes aus dem „Recht am Datenbestand“ gem. § 823 I BGB. Dieses Schutzziel wurde u.A. mit der Argumentation hergeleitet, dass eine Zerstörung von Daten deren Nutzwert vernichtet – das ist bei den Zustandsdaten am Webportal nicht der Fall, denn sie werden jederzeit aufs Neue durch die aktuellen Daten aus dem Auto überspielt. Die Schutzziele Vertraulichkeit und Verfügbarkeit sind aber problemlos über die Konstruktion § 823 I BGB abbildbar. Hier ist auch ein quasinegatorischer Unterlassungsanspruches über §§ 823 I, 1004 BGB zu bejahen. Letzterer hat in Form eines Beseitigungsanspruchs bei einer dauerhaften Zugangsbehinderung zum Webportal eine hohe Praxisrelevanz – die geforderte Interessensabwägung ist aber weiterhin zu berücksichtigen und wird für einen privaten Fahrzeughalter im Hinblick auf die Relevanz der dargestellten Daten des Öfteren auch negativ ausgehen.

V. Bereicherungsrechtliche Schutzkonzepte

In der untersuchten Fallstudie werden annahmegemäß im Falle eines Service- bzw. Reparaturauftrages Fahrzeugdaten ausgelesen und an den Fahrzeughersteller übermittelt. Mangels Vereinbarung im Garantievertrag bzw. mangels Bewusstsein des Fahrzeughalters über diesen Vorgang gibt es weder Gegenleistung noch Rechtsgrund für die Erlangung dieser Daten aus Sicht des Fahrzeugherstellers. Ein Schutzkonzept für den Fahrzeughalter könnte sich daher über eine Eingriffskondiktion gem. § 812 I S.1 Alt. 2 ergeben. Eine Eingriffskondiktion kommt beim Eingriff in den Zuweisungsgehalt eines Ausschließlichkeitsrechts in Betracht, wenn dieses übertragbar oder sonst wie wirtschaftlich verwertbar ist[146]. Der Fahrzeughalter hat jedoch, wie oben dargestellt, i.A. keinerlei Ausschließlichkeitsrechte an den Fahrzeugdaten – dies wurde u.A. auch mit dem nicht hinreichend konkretisiertem Zuweisungsgehalt begründet.

[146] *Zech* S.72.

Fraglich ist jedoch, ob in der speziellen Situation von dynamischen Fahrzeugdaten eine Eingriffskondiktion nicht auch ohne Ausschließlichkeitsrecht begründbar ist. Ansatzpunkt dafür ist die Anerkennung der generierten Daten als Gebrauchsvorteil der Sache „Auto“ gem. § 100 BGB[147] - Gebrauchsvorteile sind Nutzungen aus einer Sache und stehen bei Fehlen einer anderweitigen Regelung dem Eigentümer der Sache zu. Daraus leiten *Heun* und *Assion* ein „Erstnutzungsrecht“ an den Fahrzeugdaten ab – über dieses soll der Fahrzeughalter vertraglich verfügen können bzw. soll eine unberechtigt gezogene Nutzung zur *Herausgabe des Erlangten* verpflichten[148]. Der vertraglichen Dispositionsmöglichkeit über die generierten Daten durch den Fahrzeughalter kann zugestimmt werden – schließlich wurden an den dynamischen Fahrzeugdaten bislang keine entgegenstehenden Rechte Dritter festgestellt. Auch ein Wertersatz der unrechtmäßig gezogenen Nutzung wäre generell über § 812 I S.1 Alt. 2 i.V.m § 818 I,II BGB abbildbar. In der Fallstudie „Werkstatt“ wurde jedoch auf deliktrechtlicher Ebene festgestellt, dass der Fahrzeughalter den Zugriffsschutz zu den Fahrzeugdaten freiwillig aufgibt. Die Daten werden dann auf einen Computer in der Werkstatt kopiert und oftmals auch an den Fahrzeughersteller weitergeben. An der Kopie hat der Fahrzeughalter i.A. keinerlei Rechtsposition mehr - auch keine Rahmen- bzw. Abwehrrechte[149]. Ohne ursprüngliche Rechtsposition kann es aber auch keinen Eingriff i.S.d Bereicherungsrechts geben. Erträge, die der Fahrzeughersteller durch einen Weiterverkauf der Fahrzeugdaten erzielt, sind daher kein ungerechtfertigter Vorteil den es auszugleichen gilt.

[147] *Heun-Assion* CR 2015,812,818; *Zech* CR2015,137, 142; a.A. Studie BMVI „Eigentumsordnung für Mobilitätsdaten“ S.60.
[148] *Heun-Assion* CR 2015, 812, 818.
[149] Vorbehaltlich spezieller Datensätze die nach UWG oder Datenschutzrecht geschützt sein könnten.

E. Schlussbetrachtung

Anknüpfend an die Fragestellung aus der Einführung (Kapitel A): *Welche rechtlichen Schutzkonzepte an Fahrzeugdaten aus Sicht des Fahrzeughalters wurden gefunden? Gibt es daneben auch Einschränkungen in den Eigennutzungs- bzw. Verfügungsbefugnissen?*

Wie gezeigt sind die Ergebnisse zu trennen in:

- Syntaktische Ebene: Keine Unterscheidung nach der konkreten Aussagekraft bzw. Bedeutung des gespeicherten Datums („Zeichenkette“)
- Semantische Ebene: Spezialgesetzliche Vorschriften, die eine bestimmte Bedeutung des Datums zuerkennen und darauf aufbauend Rechte und Pflichten statuieren

I. Syntaktische Ebene – Zusammenfassung der Ergebnisse

Eine prinzipielle sachenrechtliche Einordnung von Daten als „Dateneigentum“ im Verständnis von § 903 BGB ist nicht herleitbar. Aufbauend auf der Eigentümerstellung an den Datenträgern im Fahrzeug ergibt sich für den Fahrzeughalter aber bereits eine Vielzahl von deliktsrechtlichen Schutzkonzepten und Befugnissen an den gespeicherten Daten. Soweit und solange den gespeicherten Daten keine fremden Schutzmechanismen auf semantischer Ebene zugewiesen sind (siehe nächstes Kapitel), kann der Eigentümer über den gedanklichen Umweg der Verkörperung der gespeicherten Daten beliebig mit ihnen verfahren und andere von der Einwirkung ausschließen – Gegen eine unberechtigte Kenntnisnahme bzw. Vervielfältigung kann sich der Fahrzeughalter alleine aus der Eigentümerstellung an dem Datenträger abseits des Vorenthaltens des physischen Zutritts allerdings nicht wehren. Gibt er die Eigentümerstellung an seinem Fahrzeug auf, z.B: durch Verkauf, verbleiben für ihn keinerlei Rechtspositionen an den Fahrzeugdaten.

Über die Anerkennung eines *Rechts am Datenbestand* gem. § 823 I BGB als sonstiges Recht im Zuge einer Rechtsfortbildung ergibt sich eine Erweiterung des Schutzkonzepts. Unter dem Vorbehalt einer Interessensabwägung lässt sich ein Vertraulichkeitsschutz gegen unberechtigtes Auslesen und Vervielfältigen konstruieren. Nach der hier vertretenen Ansicht muss der Datenbestand aber logisch zusammenhängend und durch einen (virtuellen) Zuordnungsmechanismus dem Datenberechtigten zugewiesen sein. Das ist im Fahrzeug selbst unproblematisch der Fall, geht jedoch i.A. dann verloren, wenn Daten aus dem Auto abfließen und in einer fremden Rechtssphäre gespeichert werden. Das ist besonders praxisrelevant im Hinblick auf die nachweislich stattfindende

Übermittlung von fahrzeugspezifischen Daten vom Werkstattbetrieb zum Fahrzeughersteller.

Mit der Übertragung des materiellen Computerstrafrechts §§ 202a, 303a ff. StGB auf das zivile Deliktsrecht im Rahmen von § 823 II BGB existiert bereits de lege lata ein Schutzkonzept für alle drei Schutzziele der Informationssicherheit. Im Ergebnis ergibt sich zwar mehr Rechtssicherheit als über die Konstruktion § 823 I BGB, allerdings ist nur eine vorsätzliche Schädigung des Datenbestandes geschützt. Eine Erweiterung des Schutzkonzepts auf einzelne Datenelemente außerhalb des „Systembegriffs" kann auch über diesen Weg nicht erreicht werden – hier scheitert es an der schwierigen Zuordnung des einzelnen Datenelements an einen „Berechtigten".

Für die beiden deliktischen Schutzkonstruktionen gilt allerdings einschränkend, dass der Fahrzeughalter seinen faktischen Zugangsschutz nicht aufgeben darf – tut er das, so verliert er jegliche Kontrolle über das Absaugen der Daten aus seinem Fahrzeugsystem. In diesem Zusammenhang wird auch ein möglicher bereicherungsrechtlicher Anspruch verneint.

Die gefundenen deliktsrechtlichen Schutzkonzepte lassen sich in eingeschränkter Art und Weise auch auf Cloud-Speicher anwenden – das ist besonders praxisrelevant in Verbindung mit sogenannten Telematik-Diensten. Hier kann sich der Kunde gegen unberechtigte Sperren und Fremdzugriffe in dem ihm zugeordneten Datenbereich zur Wehr setzen.

Diese „vorsichtige" und einschränkende Anerkennung von zivilrechtlichen Schutzkonzepten an Daten in Form von Rahmenrechten[150] und reinen Abwehrrechten[151] auf Systemebene passt gut in das Spannungsfeld mit dem *Grundrecht auf Informationsfreiheit*, abgeleitet aus Art. 5 I 1 2. Var. GG. Eine Anerkennung eines Schutzes an Daten außerhalb des (virtuellen) Systemkontextes käme mangels Abgrenzung und konkret benannter Handlungen einem Ausschließlichkeitsrecht an Daten gleich und bräuchte daher eine Rechtfertigung hinsichtlich der Einschränkung der Handlungsfreiheit Dritter. Dabei ist beim Gut der *Information* wegen Art.5 GG ein besonders hoher Maßstab anzulegen[152]. Der Gesetzgeber berücksichtigt dies auf *semantischer Ebene* durch Schutzkonzepte in Spezialgesetzen, wie z.B: im Urheberrecht oder im Patentrecht, und beschränkt die gewährten Ausschließlichkeitsrechte durch zeitliche Elemente oder anderen Verpflichtungen des Rechtsinhabers. Auf der technischen Ebene des Datums ist aber noch keine semantische Information vorhanden. Dies

[150] Sonstige Rechte i.S.v. § 823 I BGB mit Abwägungsvorbehalt und ohne güterrechtliche Zuweisung.
[151] § 823 II BGB i.V.m einem Schutzgesetz.
[152] *Zech* S.146.

erschwert die Konzeption von möglichen Beschränkungen des Ausschließlichkeitsrechts enorm. Hierfür wären nämlich die Erarbeitung einer durchgängigen Systematik und eine Abwägung mit Gemeininteressen erforderlich, welche im Zuge einer Rechtsfortbildung auf abstrakter Ebene nicht geleistet werden kann. Dies soll, dem Prinzip des sachenrechtlichen numerus clausus folgend, dem Gesetzgeber vorbehalten bleiben[153]. Der Rechtsfortbildung bleibt weiterhin die Möglichkeit der einzelfallgerechten Schutzlückenfüllung über Abwehr- und Rahmenrechte[154], allerdings jeweils unter der Bedingung einer Interessensabwägung. Als solches soll das „Schutzrecht am Datenbestand“ im Kontext von § 823 I BGB hier Anerkennung finden. Nach der hier vertretenen Ansicht jedoch nur auf Systemebene und nicht für das einzelne Datum – erst durch die gezielte Auswahl, Speicherung und Sammlung in einer *abgeschlossenen Umgebung* entsteht eine schützenswerte *Quasi-Semantik* für eine Ansammlung lediglich syntaktischer Information.

II. Semantische Ebene – Zusammenfassung der Ergebnisse

Während im Urheberrecht trotz des vielversprechenden Ansatzes über den Datenbankleistungsschutz gar keine Rechtspositionen an Fahrzeugdaten gefunden wurden, gibt es in wenigen Spezialfällen (z.B.: Bewegungsprofile, im Fahrzeug gespeicherte Unternehmensgeheimnisse) die Möglichkeit für lauterkeitsrechtliche Abwehrrechte – allerdings nur für den Fahrzeughalter als Unternehmer. Hier bleibt es wohl alles in allem bei einer eher theoretischen Schutzmöglichkeit.

Als stärkstes Schutzinstrument aus Sicht des Fahrzeughalters auf der semantischen Ebene wurde das Datenschutzrecht identifiziert. Sobald innerhalb eines Datenbestandes ein Personenbezug herstellbar ist, greifen die Betroffenenrechte aus dem BDSG – Darunter fallen Auskunftsansprüche, Löschansprüche und Schadenersatzansprüche. Das datenschutzrechtliche Schutzkonzept wird aber erst wirksam, sobald Daten aus dem Auto ausgelesen werden - wirkt dann aber weiter über alle Kopien und deren Speicherorte hinweg, also auch bis in das Datencenter des Fahrzeugherstellers. Durch die Anerkennung der Fahrzeug-Identifikationsnummer als personenbezogenes Datum sind Datensätze aus dem Fahrzeug ohne spezielle Anonymisierungsmechanismen praktisch immer personenbezogene Daten. Die vertragskonforme Abwicklung der betrachteten Fallstudie „Auto-Service in Werkstatt“ ist zwar über die BDSG Erlaubnistatbestände gedeckt, jedoch kommt es bei einer umfassenden und

[153] *Zech* CR 2015, 137, 145.
[154] *Peukert* S. 880 ff.

ausschweifenden Speicherung und Übermittlung von Fahrzeugdaten zu einem Interessenkonflikt mit dem Fahrzeughalter. Für diesen Konflikt gibt es im BDSG ein Rechtsinstitut und somit die Möglichkeit für die Zuerkennung der kodifizierten Abwehrmaßnahmen.

Wird der Personenbezug an den Daten vollständig (!) entfernt, verliert das BDSG seine Anwendbarkeit und es verbleiben nur noch die deliktsrechtlichen Schutzkonzepte auf der syntaktischen Ebene (Kapitel E.I).

III. Bewertung der Ergebnisse

Abgesehen vom Datenschutzrecht wurden kaum Rechtspositionen gefunden, die direkt an den Daten ein Schutzkonzept statuieren. Dies eröffnet andererseits für den Fahrzeughalter eine große Flexibilität auf vertragsrechtlicher Seite. Zwar wurden einzelne Datenelemente identifiziert, an denen ein lauterkeitsrechtliches Abwehrrecht für den Fahrzeughersteller besteht - die „wertvolleren" Elemente, die dynamischen Fahrzeugdaten, stehen jedoch formal uneingeschränkt unter schuldrechtlicher Verfügungsgewalt des Fahrzeughalters. Der Fahrzeughersteller wirkt dieser Verfügungsgewalt allerdings durch faktische Zugangsbarrieren überschießend entgegen. Hier wäre ein Ansatzpunkt für den Gesetzgeber gefunden, entweder durch weitere technische Standardisierung der Schnittstellen oder durch spezialgesetzliche Maßnahmen, z.B. im AGB Recht[155], einzugreifen und dadurch die Entstehung eines freien Datenmarktes zu unterstützen.

Ähnliches gilt auch für das Datenschutzrecht. Die Fahrzeughersteller informieren mittlerweile zwar transparenter und arbeiten tw. auch mit BDSG rechtskonformen Einwilligungserklärungen, jedoch ist für einen durchschnittlich verständlichen Besitzer weiterhin nicht erkennbar, wann welche Daten aus seinem Fahrzeug ausgelesen und verarbeitet werden. Durch die ausdrückliche Einwilligungserklärung für erweiterte und vertragsfremde Nutzungen trägt der Fahrzeughersteller zwar der gesteigerten Sensibilisierung für das Thema Datenschutz innerhalb der Verbrauchergemeinschaft Rechnung, interpretiert allerdings die BDSG Erlaubnistatbestände weitgehend zu seinen Gunsten bzw. dehnt den Schutz seiner vermeintlichen Unternehmensgeheimnisse großzügig aus und rechtfertig damit überschießende Zugangsbarrieren und lückenhafte Dokumentation. Die Datenschutz-Grundverordnung wird an dieser Situation nichts ändern – die Informationsasymmetrie zwischen Fahrzeughalter und Hersteller sowie die schwache Verhandlungsposition des Fahrzeugkäufers bleiben

[155] *Hornung-Goeble* CR 2015, 265, 271.

erhalten[156]. Ein gutes Beispiel dafür sind Telematik-Services: Diese bieten aus Sicht des durchschnittlichen Fahrzeughalters heute nur einen eingeschränkten Mehrwert – Dennoch werden speziell im hochpreisigen Fahrzeugsegment und getrieben durch Rabatt-Aktionen der Hersteller mehr und mehr Fahrzeuge damit ausgestattet[157]. Die Fahrzeugkäufer haben bei den Vertragsbedingungen dabei keinerlei Verhandlungsspielraum. Hier liegt der Verdacht nahe, dass der Fahrzeughersteller bereits heute von dem Datentransfer übermäßig profitiert und kein Interesse daran hat, dass der Fahrzeughalter auf einem freien Datenmarkt selbstständig als Anbieter aktiv wird.

Aus Sicht des Fahrzeughalters ist besonders nachteilig, dass sobald er einen Datentransfer mit der Werkstatt oder mit dem Fahrzeughersteller zulässt und keine zusätzlichen vertraglichen Bestimmungen einschlägig sind, er alle Rechtspositionen an anonymisierten Daten verliert.

Trotz der rechtlich guten Ausgangsposition des Fahrzeughalters in Bezug auf eine mögliche Eigenverwertung der in seinem Fahrzeug gespeicherten Fahrzeugdaten, ist er daher faktisch auf der vertragsrechtlichen Gestaltungsebene benachteiligt. Hier wäre ein möglicher Ansatzpunkt für eine gesetzliche Initiative. Ob der Vorschlag von BM DOBRINDT zur Schaffung eines umfassenden, sachenrechtsähnlichen Dateneigentums eine taugliche und interessengerechte Lösung ist, soll an dieser Stelle nicht weiter bewertet werden. Dies wird u.A. vor dem Hintergrund der Bestrebungen der EU Kommission[158] zu beurteilen sein, welche unter dem Schlagwort „fünfte Grundfreiheit“ eine Erhöhung der Datenmobilität von nicht-personenbezogenen Daten innerhalb des Binnenmarktes anstrebt.

Ich versichere, dass ich die Bachelorarbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen. Ich erkläre mich hiermit einverstanden, dass die Arbeit auf Verlangen der/des Prüfenden mit Hilfe eines Plagiatserkennungsprogrammes auf ggf. enthaltene Plagiate überprüft wird.

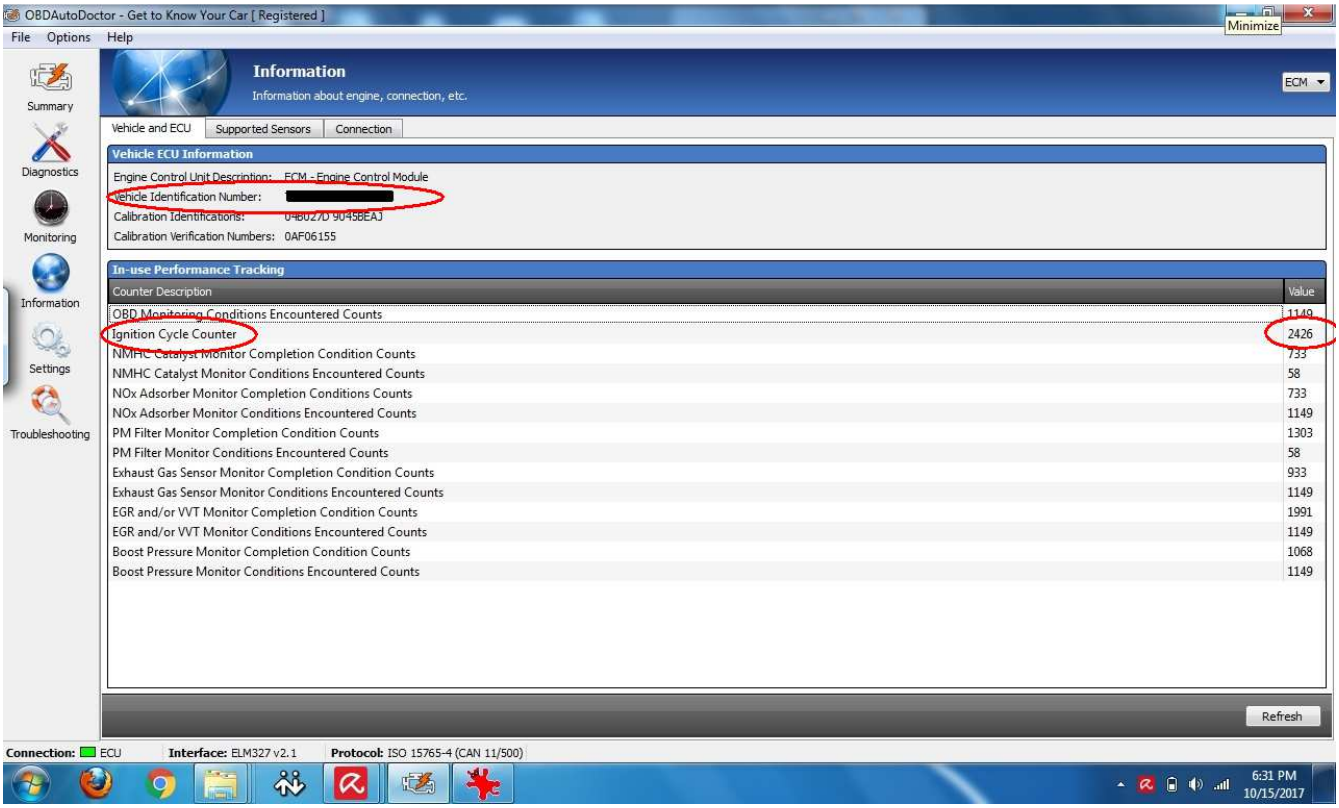
DI Christoph Jandegger

Wien, 11.12.2017

[156] *Hornung-Goeble* CR 2015, 265, 270.
[157] z.B: 2,2 Mio Fahrzeuge alleine von BMW und Mini bis inkl. Jänner 2015 - Quelle ADAC [a.a.O.].
[158] 2017/0228 (COD): “Proposal for a regulation on a framework for the free flow of non-personal Data”.

Anhang

Im Zuge der Erstellung dieser Arbeit wurde die Fallstudie „Werkstatt“ simuliert, indem aus einem Skoda Fabia III, Bj 2015 über die OBD Schnittstelle Daten ausgelesen wurden. Das dazu erforderliche Gerät ist am freien Markt um ca. 30 Euro erhältlich[159], ist jedoch auf das Auslesen von standardisierten Daten des Motorsteuergeräts („OBD-2“ gem. ISO 15031-6) beschränkt. Dazu kommt eine, ebenfalls am freien Markt erhältliche, Software für den Betrieb auf einem handelsüblichen Notebook[160]. Über fahrzeugherstellerspezifische Geräte bzw. Software ist ein wesentliches umfangreicheres Abbild der Fahrzeugdaten auslesbar. Im vorliegenden Fall war es jedoch ausreichend zu zeigen, dass mit einfachen Mitteln aussagekräftige[161] Fahrzeugdaten auslesbar sind und dass die Fahrzeug-Identifikationsnummer[162] als Teil der Datensätze immer zur Verfügung steht (Siehe Screenshot):



[159] Zum Einsatz kam das Produkt: *Tonwon OBDII Pro BLE4.0.*
[160] Zum Einsatz kam die Software: *OBD AutoDoctor.*
[161] Im unten dargestellten Beispiel wurde das Datum „Ignition Cycle Counter“ grafisch hervorgehoben – Dieser Datenwert zeigt die Anzahl aller jemals durchgeführten Motorstartvorgänge seit erstmaliger Inbetriebnahme des Fahrzeugs an.
[162] Im Zuge der Veröffentlichung dieser Arbeit wurde die Fahrzeug-Identifikationsnummer (*Vehicle Identification Number)* aus datenschutzrechtlichen Erwägungen geschwärzt.

Literaturverzeichnis

Bartsch, Michael, Die Vertraulichkeit und Integrität informationstechnischer Systeme als sonstiges Recht nach § 823 I BGB, Computer und Recht 2008, 613-617 **(zitiert: *Bartsch* CR 2008)**

Bartsch, Michael, Software als Rechtsgut - Zur Wahrnehmung von Software aus Sicht des Rechts, zur Begriffsbildung im Recht und zu den praktischen Konsequenzen, Computer und Recht 2010, 553-559 **(zitiert: *Bartsch* CR 2010)**

Bamberger, Georg/Roth, Herbert/Hau, Richard/Posceck, Roman, Beck Online Kommentar BGB, 43. Auflage, München 2017 **(zitiert: BeckOKBGB/*Bearbeiter*)**

Wolff, Heinrich Amadeus/Brink, Stefan, Beck Online Kommentar Datenschutzrecht, 22. Auflage, München 2017 **(zitiert: BeckOKDatenschutzrecht/*Bearbeiter*)**

Ahlberg, Hartwig/Götting, Horst-Peter, Beck Online Kommentar Urheberrecht, 17. Auflage, München 2017 **(zitiert: BeckOKUrhR/*Bearbeiter*)**

Boecken, Winfried/Düwell, Josef/Diller, Martin/Hanau, Hans, Gesamtes Arbeitsrecht – Kommentar, 1. Auflage, Baden-Baden 2016 **(zitiert: Boecken-Düwell-Diller-Hanau/*Bearbeiter*)**

Spaar, Dieter, Daten auf Rädern, c't Magazin für Computertechnik 2016/9, 170-172 (**zitiert: c't Magazin für Computertechnik 2016/9**)

Dauner-Lieb, Barbara/Langen, Werner, BGB Schuldrecht Kommentar Band 2, 3. Auflage, Baden-Baden 2016 **(zitiert: Dauner-Langen/*Bearbeiter*)**

Dorner, Michael, Grundfragen des modernen Daten- und Informationshandels, Computer und Recht 2014, 617-628 **(zitiert: *Dorner*)**

Dreier, Thomas/Schulze, Gernot, Urheberrechtsgesetz – Kommentar, 5. Auflage, München 2015 **(zitiert: Dreier-Schulze/*Bearbeiter*)**

Häberle, Peter, Strafrechtliche Nebengesetze – Kommentar, Band 1, einschl. 216. Ergänzungslieferung, München 2017 **(zitiert: Erbs-Kohlhaas/*Bearbeiter*)**

Fischer, Thomas, StGB Kommentar, 63. Auflage, München 2016 **(zitiert: *Fischer*)**

Nordemann, Axel, Kommentar zum Urheberrechtsgesetz, zum Verlagsgesetz und zum Urheberrechtswahrnehmungsgesetz, 11. Auflage, Stuttgart 2014 **(zitiert Fromm-Nordemann/*Bearbeiter*)**

Grosskopf, Lambert, Rechte an privat erhobenen Geo- und Telemetriedaten, Der IP Rechtsberater 2011, 259-261 **(zitiert: *Grosskopf*)**

Grützmacher, Malte, Dateneigentum – ein Flickenteppich, Computer und Recht 2016, 485-495 **(zitiert: *Grützmacher*)**

Haft, Fritjof, Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) - Teil 2: Computerdelikte, Neue Zeitschrift für Strafrecht 1987, 6-10 **(zitiert: *Haft*)**

Härting, Niko, Dateneigentum – Schutz durch Immaterialgüterrecht? , Computer und Recht 2016, 646-649 **(zitiert: *Härting*)**

Harte-Bavendamm, Henning/Henning-Bodewig, Frauke, UWG Kommentar, 4. Auflage, München 2016 **(zitiert: Harte-Henning/*Bearbeiter*)**

Hoeren, Thomas, Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht, Multimedia und Recht 2013, 486-491 **(zitiert *Hoeren*)**

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd, Handbuch Multimedia-Recht, 45. Auflage, München 2017 **(zitiert: *Hoeren-Sieber-Holznagel*)**

Hornung, Gerrit/Goeble, Thilo, Data Ownership im vernetzten Automobil, Computer und Recht 2015, 265-273 **(zitiert: *Hornung-Goeble*)**

Heun, Sven-Erik/Assion, Simon, Internet(recht) der Dinge, Computer und Recht 2015, 812-818 **(zitiert: *Heun-Assion*)**

Jlussi, Dennis, Industrie 4.0 und Dateneigentum, in: Industrie 4.0 in Eckpunkten, 2. Auflage, Hannover 2016 **(zitiert: *Jlussi)***

Kilian, Wolfgang, Strukturwandel der Privatheit, in: Gedächtnisschrift für Wilhelm Steinmüller, Berlin 2014, https://edoc.hu-berlin.de/handle/18452/18547 **(zitiert: *Kilian*)**

Kindhäuser, Urs/Neumann, Ulfried/Paeffgen, Ullrich, StGB Kommentar, 5. Auflage, Baden-Baden 2017 **(zitiert: Kindhäuser-Neumann-Paeffgen/*Bearbeiter*)**

Kunnert, Gerhard, Die datenschutzkonforme Vernetzung des Automobils, Computer und Recht 2016, 509-516 **(zitiert: *Kunnert*)**

Kutscha, Martin, Mehr Schutz von Computerdaten durch ein neues Grundrecht? , NJW 2008, 1042-1044 **(zitiert: *Kutscha*)**

Kühl, Kristian/Heger, Martin, Strafgesetzbuch – Kommentar, 28. Auflage, München 2014 (zitiert: **Lackner-Kühl/*Bearbeiter*)**

Meier, Klaus/Wehlau, Andreas, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585-1591 **(zitiert: *Meier-Wehlau*)**

Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina, Münchner Kommentar BGB, Band 3, 7. Auflage, München 2016 **(zitiert: *MüKoBGB*/Bearbeiter)**

Heermann, Peter/Schlingloff, Jochen, Münchener Kommentar zum Lauterkeitsrecht, Band 2, 2. Auflage, München 2014 **(zitiert: MüKoLauterkeitsrecht/*Bearbeiter*)**

Joecks, Wolfgang/Miebach, Klaus, Münchner Kommentar StGB, Band 5, 2. Auflage, München 2014 **(zitiert: *MüKoStGB*/Bearbeiter)**

Ohly, Ansgar/Sosnitza, Olaf, UWG Kommentar, 7. Auflage, München 2016 **(zitiert: Ohly-Sosnitza/*Bearbeiter*)**

Palandt, BGB Kommentar, 72. Auflage, München 2013 **(zitiert: *Palandt*)**

Peukert, Alexander, Güterzuordnung als Rechtsprinzip, 1. Auflage, Tübingen 2008 **(zitiert: *Peukert*)**

Prütting, Hanns/Wegen, Gerhard/Weinreich, Gerd, BGB Kommentar, 7. Auflage, Köln 2012 **(zitiert: Prütting-Wegen-Weinreich/*Bearbeiter*)**

Roßnagel, Alexander, Fahrzeugdaten – wer darf über sie entscheiden? , Straßenverkehrsrecht 8/2014, 281-287 **(zitiert: *Roßnagel*)**

Eser, Albin, Strafgesetzbuch Kommentar, 29. Auflage, München 2014 **(zitiert: Schönke-Schröder/*Bearbeiter*)**

Schulze-Heiming, Ingeborg, Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, 1. Auflage, Münster 1995 (**zitiert: *Schulze-Heiming)***

Simitis, Spiros, Bundesdatenschutzgesetz - Kommentar, 8. Auflage, Baden-Baden 2014 **(zitiert: Simitis/*Bearbeiter*)**

Specht, Louisa, Ausschließlichkeitsrechte an Daten - Notwendigkeit, Schutzumfang, Alternativen, Computer und Recht 2016, 288-296 (**zitiert: *Specht***)

Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien – Kommentar, 3. Auflage, München 2015 **(zitiert: Spindler-Schuster/*Bearbeiter*)**

Staudinger, Julius von, BGB Kommentar, Buch 3, Bearbeitung 2013, München 2013 **(zitiert: Staudinger/*Bearbeiter*)**

BM für Verkehr und digitale Infrastruktur, Eigentumsordnung für Mobilitätsdaten, Berlin 2017, http://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.html?nn=12830 **(zitiert: Studie BMVI)**

Volkmann, Uwe, Verfassungsmäßigkeit der Vorschriften des Verfassungsschutzgesetzes von Nordrhein-Westfalen zur Online Durchsuchung und zur Internet-Aufklärung, DVBl 2008, 590-593 **(zitiert: *Volkmann*)**

Wandtke, Artur Axel, Medienrecht: Praxishandbuch, Band 2, 2. Auflage, Berlin 2011 **(zitiert: Wandtke/*Bearbeiter*)**

Wandtke, Artur Axel/Bullinger, Wilfried, Praxiskommentar zum Urheberrecht, 4. Auflage, München 2014 **(zitiert: Wandtke-Bullinger/*Bearbeiter*)**

Wendehorst, Christiane, Anspruch und Ausgleich, 1. Auflage, Tübingen 1999 **(zitiert: *Wendehorst*)**

Welp, Jürgen, Datenveränderung § 303a StGB – Teil 1, IuR Sonderheft 1988, 443-449 **(zitiert: *Welp*)**

Zech, Herbert, Information als Schutzgegenstand, 1. Auflage, Tübingen 2012 (**zitiert: *Zech***)

Zech, Herbert, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“, Computer und Recht 2015, 137-146 ***(*zitiert: *Zech* CR 2015*)***

Zech, Herbert, „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151-1160 **(zitiert: *Zech* GRUR)**