abida
ASSESSING BIG DATA

DATENRECHTE – EINE RECHTS- UND SOZIALWISSENSCHAFTLICHE ANALYSE IM VERGLEICH DEUTSCHLAND - USA

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

01IS15016A-F

Prof. Dr. Louisa Specht
Prof. Dr. Wolfgang Kerber

ABIDA - ASSESSING BIG DATA

PROJEKTLAUFZEIT 01.03.2015-28.02.2019
ABIDA Gutachten; 01IS15016A

Westfälische Wilhelms-Universität Münster,
Institut für Informations-, Telekommunikations- und
Medienrecht (ITM), Zivilrechtliche Abteilung

Karlsruher Institut für Technologie,
Institut für Technikfolgenabschätzung
und Systemanalyse (ITAS)

Leibniz Universität Hannover
Institut für Rechtsinformatik
(IRI)

Technische Universität Dortmund,
Wirtschafts- und Sozialwissenschaftliche
Fakultät (WiSo) Techniksoziologie

Ludwig-Maximilians-Universität München,
Forschungsstelle für Information, Organisation
und Management (IOM)

Wissenschaftszentrum
Berlin für Sozialforschung

ABIDA - Assessing Big Data
Über das Gutachten

Das Gutachten wurde im Rahmen des ABIDA-Projekts mit Mitteln des Bundesministeriums für Bildung und Forschung erstellt. Der Inhalt des Gutachtens gibt ausschließlich die Auffassungen der Autoren wieder. Diese decken sich nicht automatisch mit denen des Ministeriums und/oder der einzelnen Projektpartner.

ABIDA lotet gesellschaftliche Chancen und Risiken der Erzeugung, Verknüpfung und Auswertung großer Datenmengen aus und entwirft Handlungsoptionen für Politik, Forschung und Entwicklung.

www.abida.de

Dieses Gutachten enthält zwei eigenständige Hauptteile (Teil I und Teil II), die zwar erhebliche Querbezüge zueinander aufweisen, die aber notwendigerweise bereits in der Methodik divergieren. Während der erste Hauptteil (Autor: *Louisa Specht*) eine rechtsvergleichende Abhandlung enthält, stellt sich der zweite Teil (Autor: *Wolfgang Kerber*) als eine sozialwissenschaftliche Untersuchung dar. Es wurde daher darauf geachtet, dass die in den verschiedenen Disziplinen geltenden formalen Standards (insb. die Fußnotengestaltung) eingehalten werden. In Teil III werden die in beiden Teilen gefundenen Ergebnisse thesenartig zusammengefasst.

TEIL I: RECHTSVERGLEICHENDE ANALYSE DES ZIVILRECHTLICHEN UMGANGS MIT DATEN IN DEN RECHTSORDNUNGEN DEUTSCHLANDS UND DER USA

1. EINLEITUNG

Unter dem Begriff des „Dateneigentums“ wird derzeit vor allem diskutiert, ob ausschließlichkeitsrechtliche Rechtspositionen an Daten de lege lata bestehen oder es ihrer Begründung de lege ferenda bedarf. Eigentum meint dabei im deutschen Recht die Befugnis, mit dem Eigentumsgegenstand zumindest im Grundsatz nach Belieben verfahren und andere von der Einwirkung ausschließen zu können, § 903 BGB. Eigentum kann nach deutschem Recht allein an Sachen und damit an körperlichen Gegenständen bestehen, § 90 BGB. Daten aber ist es immanent, dass es ihnen an einer Körperlichkeit mangelt. Körperlich ist allein ihr Trägermedium, d.h. die Festplatte oder der USB-Stick, auf dem sie gespeichert sind. Wohl ihr Trägermedium, nicht aber sie selbst können daher unter den Eigentumsbegriff des § 903 BGB fallen.

Der Begriff des „Dateneigentums“ wird aber auch in Verträgen verwendet, um Entscheidungsbefugnisse über Daten zu bezeichnen,[1] vereinzelt wird mit ihm sogar die Rechtsstellung des datenschutzrechtlich Betroffenen de lege ferenda beschrieben, dem jedenfalls nach z.T. vertretener Ansicht ein Vergütungsanspruch bei Verwendung der ihn betreffenden personenbezogenen Daten zugewiesen werden soll.[2] Auch im US-amerikanischen Recht wird der Begriff des „Dateneigentums“[3] primär im datenschutzrechtlichen Kontext verwendet, auch in Datenverarbeitungs- und Datenüberlassungsverträgen werden regelmäßig Befugnisse an Daten als „data ownership“ bezeichnet.[4] Diese Verwendung in verschiedenen Kontexten zeigt, dass die unter dem Begriff des „Dateneigentums“ unter Praktikern, in der Wissenschaft, aber auch auf politischer Ebene geführte Diskussion weitaus facettenreicher ist, als dogmatisch nur die Frage nach einer ausschließlichkeitsrechtlichen Zuweisung von Rechten an Daten zu betreffen. Es geht der Diskussion vielmehr insgesamt um den rechtlichen, v.a. den zivilrechtlichen Umgang mit Daten de lege lata und einen möglicherweise bestehenden Reformbedarf de lege ferenda. Dieser (zivil-)rechtliche Umgang mit Daten ist Gegenstand des vorliegenden Gutachtens.

---

[1] Vgl. z.B. *Boehm*, ZEuP 2016, 358, 379 ff. m.w. Nachw.; *Assion/Mackert*, PinG 2016, 161, 161: *„Data Ownership“*, die in Fn. 3 allerdings darauf hinweisen, dass die Verwendung des deutschen Begriffes *Eigentum* „irreführend“ wäre und sie daher in Verträgen den englischsprachigen Begriff verwenden.

[2] Vgl. v.a. Fezer, MMR 2017, 3, 5 ff.: „Das Recht des Nutzers auf einen individuellen Vermögensausgleich besteht gegenüber dem Unternehmen aus Gründen einer kommerziellen Vermarktung der verhaltensgenerierten Personendaten.“

[3] Vgl. z.B. *Schwartz*, 117 Harv. L. Rev. 2056, 2059 (2004); *Determann*, Datenrechte im US-amerikanischen Rechtsraum, in: Specht/Werry/Werry, Datenrecht in der Digitalisierung, im Erscheinen; *Samuelson*, 52 Stan. L. Rev. 1125 et seq. (2000); *Evans*, 42 Am. J.L. & Med. 651 (2016).

[4] Vgl. z.B. *Glazer et al.*, Practical Law Practice Note 4-532-4243 (2017).

Eine wesentlich von dieser Diskussion betroffene Fallgruppe ist sicherlich das vernetzte Fahrzeug, bei dem sowohl der Fahrzeughersteller als auch viele andere Stakeholder ein Interesse an den vielfältigen im Fahrzeug erzeugten Daten (bspw. über das Fahrverhalten des Nutzers) haben, um die angebotenen Dienste weiterzuentwickeln, das Fahrzeug zu reparieren oder auch, weil sich diese Daten lukrativ bspw. an Versicherungen weiterreichen lassen. Gleiches gilt für die im Smart Home produzierten Daten, etwa über das Heiz- oder Sicherheitsverhalten, den Strom- und Wasserverbrauch, die Bedienung von Rolläden oder automatisierten Schließmechanismen. Krankenkassen haben ein Interesse an den mittels Smart Devices, z.B. Fitnesstrackern, generierten Daten, um ihre Tarife gezielter dem individuellen Verhalten der Betroffenen anpassen zu können und damit das Eigenrisiko zu verringern. Dasselbe gilt für jegliche Bewegungs- und Verhaltensdaten, die über die mitgeführten Geräte, wie dem Handy, erhoben werden. Bewertungsportale und soziale Netzwerke haben ein Interesse an einem möglichst freien Umgang mit den ihnen zur Verfügung gestellten Daten, häufig mit dem Ziel der personalisierten (Echtzeit-)Werbung. Über Gesichtserkennungssysteme z.B. im Supermarkt, über Kundenkartenprogramme, digitalisierte Einkaufslisten, Cookie-Tracking, Clickstreamanalysen und andere Webtrackingmaßnahmen lassen sich passgenauen Persönlichkeitsprofile erstellen, die für das personalisierte Marketing von erheblicher wirtschaftlicher Bedeutung sind. Man könnte die Aufzählung betroffener Fallgruppen wohl endlos fortsetzen.[5]

Mit Blick auf diese Vielzahl möglicher Anwendungsfälle kann dieses Gutachten nicht auf jede sektorspezifische Regelung, die den Umgang mit Daten in bestimmten Bereichen betrifft, im Einzelnen eingehen. Es nimmt daher einen generalisierenden Blickwinkel ein, hebt aber sektorspezifische Regelungen dort hervor, wo sie in positiver oder negativer Hinsicht eine Vorbildfunktion auch für andere Bereiche haben könnten.

Das Gutachten gliedert sich insgesamt in zwei Hauptteile (Teil 1 und Teil 2), wobei der erste Teil eine rechtsvergleichende Untersuchung enthält und der zweite Teil aus sozialwissenschaftlicher (insbes. ökonomischer) Perspektive eine Analyse der Interessenkonflikte und Argumentationen von Stakeholdern bei den derzeit im Fokus stehenden Regulierungsansätzen zur Ausgestaltung des rechtlichen Umgangs mit Daten de lege ferenda enthält.

Der Rechtsvergleich bezieht sich auf die Rechtsordnungen Deutschlands und der USA, wo Rechtsbereiche unionsrechtlich harmonisiert sind (v.a. im Datenschutzrecht), werden auch unionsrechtliche Vorgaben einbezogen. Im Übrigen aber sind die Rechtsordnungen der einzelnen Mitgliedstaaten[6] oder auch nicht zur Europäischen Union gehörender Staaten[7] nicht vom Gutachtenauftrag umfasst. Dies gilt auch für alle öffentlich-rechtlichen Fragestellungen, die keinen Einfluss auf den zivilrechtlichen Umgang mit Daten haben. Relevant werden öffentlich-rechtliche Fragestellungen aber im Zuge der Begrenzung möglicher zivilrechtlicher Rechtspositionen an Daten, z.B. durch Vorgaben des Datenschutzrechts. Gegenstand des ersten Gutachtenteils ist damit die Frage, wie die Zivilrechtsordnungen Deutschlands und der

[5] Hierzu und weitergehend bereits: *Specht*, GRUR Int. 2017, 1040, 1041.

[6] Eine Untersuchung zu den Rechtsordnungen der übrigen Mitgliedstaaten findet sich aber hier: *Osborne Clarke LLP*, Legal study on ownership and access to data, 2016; zur Diskussion in Großbritannien vgl. aber: *Gärtner/Brimsted*, EIPR 2017, 461 ff.

[7] Zur Diskussion in der Schweiz vgl. aber: *Eckert*, 12 SJZ 245 (2016).

USA mit Daten umgehen. Dazu gehört die Erörterung vertragsrechtlicher Rechtspositionen ebenso wie die Frage nach wettbewerbsrechtlichen oder dinglichen Rechtspositionen, Immaterialgüterrechten, einem deliktischen Schutz von Daten, Zugangsrechten und anderen Beschränkungen eines zivilrechtlichen Umgangs mit Daten.[8]

Auf die vertragsrechtliche Ebene kommt es v.a. deshalb maßgeblich an, weil es für eine vertragliche Ausgestaltung des Datenhandels nicht unbedingt der Zuweisung ausschließlichkeitsrechtlicher Positionen an Daten bedarf. Dies zeigen nicht nur die einschlägigen gesetzlichen Vorschriften, wie §§ 433, 453, § 581 BGB, sondern z.B. auch der Vergleich mit TV-Formaten, an denen derartige Ausschließlichkeitsrechte nicht bestehen, an denen aber ebenfalls umfassend vertragliche Nutzungsrechte eingeräumt werden. Die faktische Zugangsbeschränkung zum Veranstaltungsort reicht hier aus, um die Sendeanstalten dazu anzuhalten, Verträge über die Anfertigung und die Ausstrahlung der Aufnahmen zu schließen und einen entsprechenden Preis hierfür zu zahlen.[9] Nicht vom Gutachtenauftrag umfasst ist der technische Schutz von Daten[10] sowie die Frage von Daten in der Insolvenz.[11] Nicht umfassend aufgegriffen (jedoch zumindest in Teil II kurz dargelegt) wird weiterhin eine sich derzeit v.a. in den USA etablierende Diskussion um einen mittelbaren Schutz von Daten über die Patentierbarkeit ihrer Erhebungsmethoden. Zu dieser Thematik ist kürzlich ein Urteil des US Supreme Courts ergangen,[12] die Diskussion über das Für und Wider einer solchen Patentierbarkeit von Datenerhebungsmethoden beginnt aber gerade erst,[13] und würde überdies im Umfang wohl einen eigenen Gutachtenauftrag füllen.

Konkret stellen sich daher im Rahmen dieses Gutachtenauftrags drei Fragen:

1. Was sind Daten und zwischen welchen Kategorien von Daten ist mit Blick auf die unterschiedlichen rechtlichen Anforderungen an ihren Umgang zu differenzieren?
2. Welchen Regelungsregimen unterliegt der Umgang mit Daten in den (Zivil-)Rechtsordnungen der Vergleichsstaaten de lege lata?
3. Welche Vorschläge für eine Ausgestaltung der Rechtsordnungen der Vergleichsstaaten in Bezug auf den zivilrechtlichen Umgang mit Daten de lege ferenda existieren und wie sind diese zu bewerten?

Das Gutachten wird in Teil 1 diese Fragen chronologisch abarbeiten.

---

[8] Vgl. hier insbesondere die Überblicksaufsätze von *Zech*, CR 2015, 137 ff.; *Berberich/Golla*, PinG 2016, 165 ff.; nicht Gegenstand dieses Gutachtens ist die technische Schutzmöglichkeit von Daten.

[9] *Drexl*, Designing Competitive Markets for Industrial Data -Between Propertisation and Access, 2016, MPI for Innovation & Competition ResearchPaper No. 16-13, abrufbar unter: https://ssrn.com/abstract=2862975, S. 29 m.w. Nachw., zuletzt abgerufen am 26.03.2018.

[10] Vgl. hierzu aber: *Hoppen*, CR 2015, 802 ff.; *Grützmacher*, CR 2016, 485, 492 ff.

[11] Vgl. hierzu: *Bräutigam/Klindt*, Digitalisierte Wirtschaft/Industrie 4.0, 2015, S. 27; *Becker*, GRUR-Newsletter 01/2016, S. 7, 10; *Röttgen*, Datenrechte im europäischen Rechtsraum, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

[12] Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107 (2013).

[13] Vgl. etwa: *Burk*, 21 B.U.J. Sci & Tech. L. 233-255 (2015).

2. DATEN UND DATENKATEGORIEN

2.1 DATEN UND INFORMATIONEN

Die Begriffe „Daten“ und „Informationen“ werden häufig synonym verwendet. Dies ist nicht nur eine explizit in der Literatur vertretene Auffassung,[14] sondern auch das Gesetz scheint vielerorts von einer synonymen Verwendung beider Begriffe auszugehen. So definiert etwa § 2 Abs. 3 Umweltinformationsgesetz (UIG) Umwelt*informationen* (…) als alle *Daten* über den Zustand von Umweltbestandteilen, Energie, Lärm etc., die DS-GVO formuliert in Art. 4 Nr. 1 DS-GVO personenbezogene *Daten* seien alle *Informationen*, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Und auch im US-amerikanischen Entwurf des Uniform Computer Information Transactions Act aus dem Jahr 1999 (UCITA) hieß es: *„Information means data (…).“*[15]

Nachdem aber insbesondere in der öffentlich-rechtlichen Literatur in Deutschland schon früh nach einer Abgrenzung beider Begriffe gesucht wurde,[16] wird heute überwiegend in Anlehnung an *Zech* zwischen verschiedenen Informationsebenen unterschieden. Danach umfasst die syntaktische Ebene allein die Zeichenebene, während auf einer weiteren semantischen Ebene die Bedeutung der Information liegt.[17] Auch *Druey* nahm in seinem Entwurf einer Grundlegung der Information als Gegenstand des Rechts 1996 die Abgrenzung von Daten und Informationen in diesem Sinne vor.[18] Dem wird auch hier im Wesentlichen zugestimmt, wobei zur Verdeutlichung der Begriff des Datums allein für die syntaktische Ebene gewählt wird, während der Informationsbegriff die semantische Ebene beschreibt. Daten sind danach

---

[14] *Determann*, Datenrechte im US-amerikanischen Rechtsraum, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, erscheint 2018; *Schmitz*, ZD 2018, 5 ff.

[15] § 102(a)(35) UCITA (Final Act with Comments, September 29th, 2000), abrufbar unter: http://www.uniformlaws.org/shared/docs/computer_information_transactions/ucita_final_02.pdf, zuletzt abgerufen am 23.02.2018; der Entwurf des UCITA wurde nur in zwei Bundesstaaten ratifiziert: Maryland und Virginia – die übrigen Bundesstaaten haben den UCITA verworfen, vgl. für Maryland: https://law.justia.com/codes/maryland/2016/commercial-law/title-22/subtitle-1/short-title-and-definitions./section-22-102/), für Virginia: Title 59.1 (Trade and Commerce) – Chapter 43 (UCITA) - § 59.1-501.2 (Definitions) (35).

[16] Vgl. etwa: *Vesting*, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: Hoffmann-Riem/Schmidt-Assmann/Voßkuhle, Grundlagen des Verwaltungsrechts, 2. Aufl. 2012, Bd. II, § 20 Rn. 1, 2; *Albers*, Informationelle Selbstbestimmung, 2005, S. 89 f.

[17] *Zech*, GRUR 2015, 1151, 1153; *ders.*, Information als Schutzgegenstand, 2012, S. 32.

[18] Vgl. *Druey*, Information als Gegenstand des Rechts – Entwurf einer Grundlegung, 1996, S. 6: „Die Information im syntaktischen Sinn trifft unabhängig von Sender und Empfänger quantitative Aussagen über die zwischen zwei Subjekten bewegte Information. Hierbei misst sie der relativ unwahrscheinlicheren Information einen höheren Informationsgehalt zu. Die semantische Dimension der Information geht davon aus, dass die Information in Zeichen codiert wird. Damit bedarf es bei Sender und Empfänger einen zusätzlichen Vorgang der Codierung, einer Umsetzung von Sinn in Zeichen und umgekehrt. Die semantische Erscheinungsweise von Information bedingt das Bestehen einer zweiten Informationsebene. Sender und Empfänger müssen sich über die Codierung bewusst sein (…). Die pragmatische Dimension letztlich stellt auf den Zweck der Information als Entscheidungsgrundlage für den Empfänger ab. Der Informationswert ist bei dieser Betrachtung wesentlich von der Verknüpfung mit anderen Informationen abhängig. Die Nachricht etwa, dass der Ätna ausbricht ist für denjenigen, der in Messina lebt relevanter als für den, der in Kopenhagen lebt.“

die auf einem Datenträger festgehaltenen Zeichen oder Zeichenfolgen.[19] Allerdings darf bei der Erörterung des Verhältnisses von syntaktischen Daten und semantischen Informationen die Aufgabe von Daten nicht verkannt werden. Sie dienen gewissermaßen als Informationsträger, indem sie ein Spektrum an Bedeutungsmöglichkeiten kodieren. Situationsbedingt und abhängig von den individuellen Fähigkeiten des Rezipienten kann ein Datum unterschiedlich interpretiert werden. So erlangt ein Wort in seinem Satzgefüge unterschiedliche Bedeutungen je nach Bildungsgrad des Rezipienten, territorialer Wortbedeutung oder Kontextverständnis.[20] Die syntaktische und semantische Ebene lassen sich insofern zwar theoretisch trennen, funktional ist aber die Bedeutung der syntaktischen für die semantische Ebene nicht zu leugnen. Ein Datum zeichnet sich funktional dadurch aus, dass ihm zwar nicht eine einzige und stets gleichbleibende Bedeutung innewohnt, es aber zur Kodierung mehrerer Bedeutungsmöglichkeiten dient, von denen der Rezipient im Rahmen eines Verständnisvorgangs eine dieser Bedeutungsmöglichkeiten selektiert.[21] Dem entspricht die Definition von Daten nach ISO als

> *„reinterpretable representation of information … in a formalized manner suitable for communication, interpretation, or processing".*[22]

Semantische Informationen sind im Verhältnis zu syntaktischen Daten[23] vor allem durch zwei Merkmale gekennzeichnet: Einen Informationsvorgang als Voraussetzung ihrer Entstehung sowie die inhaltliche Gleichsetzung mit einem vom Rezipienten selektierten Ausschnitt des Sinngehaltes der Informationsgrundlage.[24] Relevant wird dieses Verhältnis von Daten und Informationen z.B. bei der Frage der Mangelhaftigkeit von Daten, die sich u.a. daraus ergeben könnte, dass man von dem überlassenen Datum die gewünschte Information nicht ableiten kann. Wichtig ist die Differenzierung aber v.a. für den Gegenstand, dessen zivilrechtlicher

---

[19] *Sieber*, NJW 1989, 2569, 2572; *Willke*, Systemisches Wissensmanagement, 2. Aufl. 2001, S. 7; *Vesting*, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: Hoffmann-Riem/Schmidt-Assmann/Voßkuhle, Grundlagen des Verwaltungsrechts, 2. Aufl. 2012, Bd. II, § 20 Rn. 14; *Albers*, Umgang mit personenbezogenen Informationen und Daten, in: Hoffmann-Riem/Schmidt-Assmann/Voßkuhle, Grundlagen des Verwaltungsrechts, 2. Aufl. 2012, Bd. II, § 22 Rn. 11; *Becker*, ZGE 2017, 253, 256; *Grützmacher*, CR 2016, 485, 486: *„verschiedene Datensphären"*; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 19.

[20] Hierzu bereits ausführlich: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 20.

[21] Vgl. hierzu grundlegend: *Albers*, Informationelle Selbstbestimmung, 2005, S. 89 f. sowie *Beyer*, GRUR 1990, 399, 400 f.; vgl. hierzu ebenfalls: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung - Die zivilrechtliche Bedeutung des Datenhandels, 2012, S. 21

[22] ISO/IEC 2382:2015(en).

[23] Der Informationsbegriff an sich, der nicht allein das Verhältnis zu Daten betrachtet, ist freilich wesentlich komplexer, vgl. *Druey*, Information als Gegenstand des Rechts – Entwurf einer Grundlegung, 1996, S. 5 ff.

[24] *Druey*, Information als Gegenstand des Rechts – Entwurf einer Grundlegung, 1996, S. 5, der als weiteren Aspekt der Information den Zustand der Kenntnis nennt, was jedoch eher der Definition des Wissens entspricht; zur Wissensdefinition vgl. die anschließenden Ausführungen auf S. 25; ähnlich auch: *Beyer*, GRUR 1990, 399, 401; vgl. zum Informationsbegriff auch: *Dreier*, Informationsrecht in der Informationsgesellschaft, in: Bizer/Lutterbeck/Rieß, Umbruch von Regelungssystemen in der Informationsgesellschaft, Freundesgabe für Alfred Büllesbach, 2002, S. 65, 68 f.; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 23.

Umgang in diesem Gutachten erörtert wird. Es ist formal das Datum und nicht die Information, allerdings ist aufgrund der Funktion von Daten als Informationsgrundlage stets zu sehen, dass mit einer Regulierung von Daten auch die aus ihnen ableitbaren Informationen betroffen sein können.[25] Ebenso kann eine Regulierung auf der semantischen Ebene reflexartig auch die syntaktische Ebene betreffen, z.B. indem Löschungsansprüche gewährt werden, die sich auf der Zeichenebene auswirken. Der unter den Gliederungspunkten C, D und E erörterte rechtliche Umgang mit Daten betrifft daher ebenfalls sowohl die syntaktische, als auch die semantische Ebene.

2.2 PERSONENBEZOGENE DATEN

Die Verarbeitung personenbezogener Daten unterliegt den Regelungen des Datenschutzrechts, insbesondere der Datenschutz-Grundverordnung und den nationalen Datenschutzgesetzen (z.B. dem BDSG-Neu sowie den Landesdatenschutzgesetzen). Sowohl im Falle einer vertraglichen Vereinbarung über Datenverarbeitungsvorgänge, als auch für den Fall einer Begründung möglicher Ausschließlichkeits- oder Zugangsrechte an Daten sind diese Vorgaben zu beachten. Die Frage, wann ein Datum personenbezogen ist, ist daher überaus relevant für den zivilrechtlichen Umgang mit den betroffenen Daten. Die E-Privacy Verordnung findet dagegen auf Kommunikationsdaten Anwendung, unabhängig davon, ob diese einen Personenbezug aufweisen, oder nicht. Auch der über die Anwendbarkeit der E-Privacy Verordnung entscheidende Begriff der Kommunikationsdaten ist daher in einem nächsten Abschnitt (vgl. hierzu unter 2.3.) erläutert.

Gem. Art. 1 Abs.1, Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten

> *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind."*

Erwägungsgrund 26 zur DS-GVO erläutert, dass damit alle „Informationen" erfasst sind, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

> *„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.*
>
> *Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."*

[25] So zutreffend: *Wiebe/Schur*, ZUM 2017, 461, 470 f.

Bereits für den Anwendungsbereich der Datenschutzrichtlinie[26] hatte der EuGH entschieden, dass für eine Bestimmbarkeit der natürlichen Person nicht nur auf die Kenntnisse des für die Datenverarbeitung Verantwortlichen abgestellt werden kann, sondern auch die Kenntnisse Dritter herangezogen werden müssen, wenn der Verantwortliche auf diese Kenntnisse rechtmäßigerweise zugreifen kann. Zu diesem Ergebnis gelangte der EuGH durch Auslegung des ErwGr. 26 der Datenschutzrichtlinie, der in diesem Punkt im Wesentlichen ErwGr. 26 der Datenschutz-Grundverordnung entspricht. Ist also eine Identifizierung der Person gesetzlich verboten oder praktisch nicht durchführbar, z.B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten, Arbeitskraft etc. erfordern würde, ist nach Auffassung des EuGH das Risiko einer Identifizierung de facto zu vernachlässigen.[27] Der EuGH folgt damit weder der objektiven, noch der relativen Theorie des Personenbezugs, sondern nimmt eine vermittelnde Position ein. Herangezogen werden sollen lediglich solche Mittel, die auch vernünftigerweise berücksichtigt werden dürfen.[28] Dies folgt aus der autonomen Auslegung des Unionsrechts unter Berücksichtigung der Erwägungsgründe.[29] Über diese Vorgabe durfte schon im Anwendungsbereich der Datenschutzrichtlinie nicht hinausgegangen werden, weil bereits sie eine Vollharmonisierung intendierte.[30] Ein Datum darf insofern nicht schon in Anbetracht des Wunsches der Gewährleistung eines maximalen Schutzniveaus generell als personenbezogenes Datum qualifiziert werden.[31] Diese vermittelnde Ansicht liegt auch der DS-GVO zugrunde.[32] In Anbetracht der technischen Entwicklung, insbesondere der Möglichkeit von Big Data Analysen, werden aber eine Reihe von Daten auch nach dieser beschränkt-objektiven Theorie[33] des

---

[26] ErwGr. 8 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG v. 23.11.1995, L 281/31, S. 32.

[27] EuGH, Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 = NJW 2016, 3579 Tz. 46 – *Breyer*; vgl. auch: Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil C, Rn. 287.

[28] EuGH, Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 = NJW 2016, 3579 Tz. 45 – *Breyer*; so auch: *Brink/Eckhardt*, ZD 2015, 205, 210 ff.: „*absoluter Ansatz mit relativen Elementen*"; *Karg*, DuD 2015, 520, 525; Taeger/Gabel-*Buchner*, BDSG aF, 2. Aufl. 2013, § 3 Rn. 13; letztlich auch auf Basis von ErwGr. 26 DSRL: Art. 29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136 v. 20.06.2007, S. 17 f.; *Specht/Müller-Riemenschneider*, ZD 2014, 71, 73 f.

[29] Zur autonomen Auslegung der DS-GVO vgl. z.B. *Hofmann/Johannes*, ZD 2017, 221 ff.

[30] ErwGr. 8 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG 1995 v. 23.11.1995, Nr. L 281/31, S. 32; *Brühann*, EuZW 2009, 639, 642.

[31] *Specht/Müller-Riemenschneider*, ZD 2014, 71, 74; ähnlich: *Brink/Eckhardt*, ZD 2015, 205, 209.

[32] Sydow-*Ziebarth*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 4 Rn. 23; Kühling/Buchner-*Klar/Kühling*, DS-GVO, 1. Aufl. 2017, Art. 4, Rn. 27 ff.; Gola-*Gola* DS-GVO, 1. Aufl. 2017, Art. 4 Rn. 17 ff.; Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil C, Rn. 279 ff.; *Brink/Eckhardt*, ZD 2015, 205, 209; wohl auch: Paal/Pauly-*Ernst*, DS-GVO,2. Aufl. 2018, Art. 4 Rn. 8 ff.; weitergehend: Ehmann/Selmayr-*Klabunde*, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 4 Rn. 13; zum Streitstand vgl. *Bergt*, ZD 2015, 365 ff.; für einen „Abschied vom Personenbezug": *Schmitz*, ZD 2018, 5 ff.

[33] Zum Begriff vgl. *Specht/Müller-Riemenschneider*, ZD 2014, 71, 74.

EuGH personenbezogen sein. Daten Verstorbener und anonymisierte (nicht aber allein pseudonymisierte) Daten fallen allerdings nicht in den Anwendungsbereich der DS-GVO.[34]

Innerhalb der personenbezogenen Daten lässt sich weiter nach ihrer Sensitivität differenzieren. Die Verarbeitung sensibler personenbezogener Daten unterliegt dabei erhöhten Voraussetzungen gem. Art. 9 DS-GVO, § 22 BDSG-Neu. Ebenfalls unterscheiden lässt sich zwischen pseudonymisierten und nicht-pseudonymisierten Daten, wobei die Verarbeitung pseudonymisierter Daten z.T. erleichtert wird, beispielsweise im Falle der Durchbrechung des Zweckbindungsgrundsatzes.[35] Letztlich lässt sich sowohl für personenbezogene, als auch für nicht-personenbezogene Daten zwischen Rohdaten und angereicherten Daten unterscheiden, wobei im Falle eines Personenbezugs mit einer Anreicherung oder auch Zusammenführung von Daten die Gefährdung des informationellen Selbstbestimmungsrechtes steigt, weshalb jedenfalls im Rahmen der gesetzlichen Erlaubnistatbestände erhöhte Anforderungen an eine Verarbeitungsbefugnis zu stellen sind.

2.3 KOMMUNIKATIONSDATEN

Die am 10.01.2017 im Entwurf vorgelegte ePrivacy-Verordnung,[36] für die derzeit auf Vorschlag der bulgarischen Ratspräsidentschaft über Anpassungen wesentlicher Regelungen diskutiert wird,[37] normiert Einschränkungen der Verarbeitung auch für sogenannte elektronische Kommunikationsdaten, d.h. elektronische Kommunikationsinhalte und elektronische Kommunikationsmetadaten. Elektronische Kommunikationsinhalte wiederum sind definiert als Inhalte, die mittels elektronischer Kommunikationsdienste übermittelt werden, z.B. Textnachrichten, Sprache, Videos, Bilder und Ton, Art. 4 Abs. 3 lit. b). Kommunikationsmetadaten hingegen sind solche Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden. Dazu zählen die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation verwendeten Daten, die im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste erzeugten Daten über den Standort des Geräts sowie Datum, Uhrzeit, Dauer und Art der Kommunikation, Art. 4 Abs. 3 lit. c). Dabei werden auch juris-

[34] ErwGr. 26 und 27 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU 2016 v. 04.05.2016, Nr. L 119/1, S. 5.

[35] Der Zweckbindungsgrundsatz ist ein wesentlicher Grundsatz des europäischen Datenschutzrechts. Er verlangt die präzise Angabe eines legitimen Verarbeitungszwecks vor der Verarbeitung, der auch für Folgeverarbeitungsvorgänge grds. Nicht durchbrochen werden darf. Ausnahmen ergeben sich aber gem. Art. 6 Abs. 4, wenn die Verarbeitung zu einem anderen Zweck mit dem Primärzweck vereinbar ist. In diese Abwägung kann gem. Art. 6 Abs. 4 lit. e DSGVO auch die Tatsache der Pseudonymisierung eingestellt werden, was sich positiv für den Datenverarbeiter auswirkt.

[36] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM (2017) 10 final.

[37] Https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/recht/e_privacy_verordnung/Bulg.RatsP_zu_ePrivacyVO_v._22.03.2018.pdf

tische Personen[38] und auch nicht-personenbezogene Daten dem Anwendungsbereich der E-Privacy Verordnung unterworfen, insbesondere die sogenannte Machine-to-Machine-Kommunikation im Internet der Dinge.[39] Die E-Privacy Verordnung unterwirft auch diese Daten ähnlichen Erlaubnistatbeständen, wie sie nach der DS-GVO für personenbezogene Daten gelten. Soweit eine Verarbeitung der betroffenen Daten zulässig ist mit Einwilligung *„de[s] betreffende[n] Endnutzer[s]"*[40] stellt sich mit Blick auf die hier thematisierten Rechtsaspekte insbesondere die Frage, ob dies der Eigentümer des Endgerätes oder der individuelle Nutzer ist und ob demjenigen, der hier einwilligen soll, damit ein eigentumsähnliches Recht an den betroffenen Daten zugewiesen wird.

3. (ZIVIL-)RECHTLICHER UMGANG MIT DATEN DE LEGE LATA

In der Erörterung des zivilrechtlichen Umgangs mit Daten ist zunächst die Frage zu beantworten, ob das deutsche, das europäische oder das US-amerikanische Recht de lege lata Rechte an Daten kennt und wenn ja, in welcher Form. Dabei kommen sowohl Rechtspositionen i.S.d. Volleigentums, als auch einzelner Befugnisse in Betracht. Als Regulierungsobjekt lässt sich auf Einzeldaten oder auch auf Datenkonglomerate abstellen. Ein umfassendes, eigentumsähnlich gestaltetes Ausschließlichkeitsrecht an Daten kann dabei de lege lata nicht ausgemacht werden. Allein der Datenbankschutz gem. § 4 UrhG sowie das Datenbankherstellerrecht gem. § 87a UrhG gewähren Rechte an Datenbanken, auch sie schaffen aber keine Rechtspositionen an Einzeldaten. Dies ist in den USA, die keinen Schutz nicht-schöpferischer Datenbanken kennen, nicht anders. Abwehrrechte ergeben sich im deutschen Recht aus dem Geschäftsgeheimnisschutz sowie deliktsrechtlich, wobei ein „Recht am eigenen Datenbestand" als sonstiges Recht noch immer streitig ist;[41] abgestellt wird im Falle der Beeinträchtigung oder Löschung von Daten noch immer primär auf eine Verletzung des Eigentumsrechts am Trägermedium. Auch in den USA ergeben sich Ansprüche aus dem Trade-Secret-Schutz und dem Law of Torts. Zugriffsrechte auf Daten gewährt z.B. das Kartellrecht. Beide Rechtsordnungen kennen außerdem sektorspezifische Zugangsrechte. Daten können weiterhin sowohl im deutschen, als auch im US-amerikanischen Recht Gegenstand des Vertragsrechts sein, wobei sich im deutschen Vertragsrecht größere Schwierigkeiten v.a. mit Blick auf Typologie des Vertrags zur Ergehung personenbezogener Daten sowie Mängelrechte ergeben. Dies liegt im Wesent-

---

[38] Vgl. ErwGr. 3 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM (2017) 10 final, S. 14.

[39] Vgl. ErwGr. 12 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM (2017) 10 final, S. 16; explizit auch: ErwGr. 12 des Änderungstextes des EU-Rates zum Vorschlag der EU-Kommission, abrufbar unter: https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/recht/e_privacy_verordnung/ePrivacy-Verordnung_draft_EU-Rat_05122017.pdf, zuletzt abgerufen am: 22.02.2018.

[40] Vgl. etwa: Art. 6 Abs. 2 lit. c), Art. 8 Abs. 1 lit. b) des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM (2017) 10 final.

[41] Vgl. zum Streitstand die Ausführungen unter C. IV. 2.

lichen darin begründet, dass das Datenschutzrecht gerade auch den vertragsrechtlichen Umgang mit Daten begrenzt und in der deutschen und europäischen Rechtsordnung deutlich strenger ausgestaltet ist, als dies im US-amerikanischen Recht der Fall ist.

3.1 KEINE EIGENTUMS- ODER EIGENTUMSÄHNLICHEN RECHTSPOSITIONEN AN DATEN

Eigentum kann – nach deutschen Recht – allein an körperlichen Gegenständen bestehen, § 90 BGB. Nicht körperliche Daten unterliegen daher nicht dem Eigentumsrecht gem. § 903 BGB.[42] Z.T. wird jedoch – v.a. in der älteren Rechtsprechung zum Softwarekauf – angenommen, dass die Sacheigenschaft des Trägermediums auch die Sacheigenschaft der auf ihm gespeicherten Inhalte begründe.[43] Das Eigentumsrecht ordnet jedoch lediglich das Trägermedium einer Person zu. Eine rechtliche Zuordnung der auf ihm gespeicherten Daten ist damit noch nicht getroffen. Wie im Immaterialgüterrecht, z.B. im Urheberrecht, die Frage des Eigentums am Trägermedium von der Frage des Nutzungsrechts am Immaterialgut zu trennen ist, sind auch die Befugnisse zur Entscheidung über die Verwendung von Daten von der sachenrechtlichen Zuordnung des Speichermediums zu unterscheiden.[44] Im Falle personenbezogener Daten bestimmt das informationelle Selbstbestimmungsrecht, wer über die Verwendung der gespeicherten personenbezogenen Daten entscheiden darf. Denn die Einwilligung des Betroffenen ist unabhängig von der Eigentumslage am Trägermedium für eine datenschutzrechtskonforme Verwendung personenbezogener Daten erforderlich.[45] Auch kann das Datum durch die Digitalisierung jederzeit von seinem Trägermedium gelöst und selbständig gehandelt werden. Schon hieraus ergibt sich die Notwendigkeit, das Eigentum am Trägermedium von der Inhaberschaft möglicher Rechte an den auf ihm gespeicherten Daten zu unterscheiden.[46] Das Sacheigentum enthält auch kein Regelungsregime für nicht-rivale Güter, eine analoge Anwendbarkeit der sachenrechtlichen Vorschriften ist daher mangels vergleichbarer Interessenlage ausgeschlossen.

---

[42] Statt vieler: *Sattler*, in: Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, 2017, S. 27 ff.; *Roßnagel*, NJW 2017, 10, 11.

[43] BGH, Urt. v. 15.11.2006 - XII ZR 120/04, NJW 2007, 2394; vgl. hierzu auch umfassend: *Hieke*, InTeR 2017, 10, 12; Auer-Reinsdorff/Conrad-*Fischl*, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 17 Rn. 22 ff.; BeckOGK BGB-*Augenhofer*, Stand: 01.01.2018, § 474 Rn. 53; *Marly*, BB 1991, 432 ff.; *König*, NJW 1993, 3121.

[44] Vgl. *Kilian*, CR 2002, 921, 926.

[45] *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 77.

[46] *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 8, 20, 77; davon zu unterscheiden ist die Frage, ob das Speichern von Daten zu einem Eigentumserwerb am Trägermedium gem. § 950 Abs. 2 BGB führt, was zumindest für das Aufzeichnen von Gesprächsinhalten auf Tonbänder verneint wird, vgl. BGH, Urt. v. 10.07.2015 – V ZR 206/14, NJW 2016, 317 - *Kanzler Kohls Tonbänder*; auch im Falle eines solchen Eigentumserwerbs aber ist die Frage der Übertragbarkeit des Eigentums am Trägermedium zu trennen von der Einräumung von Nutzungsrechten an den gespeicherten Inhalten; zu den verschiedenen Zuordnungsmöglichkeiten vgl. auch: *Arkenau/Wübbelmann*, Eigentum und Rechte an Daten – Wem gehören Daten?, in: Taeger, Internet der Dinge: Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband 2015, S. 95 ff.

Im US-amerikanischen Recht existiert ebenfalls keine eigentumsrechtliche Position an Daten.[47] Zwar ist das Personal Property des US-amerikanischen Rechts nicht explizit auf körperliche Gegenstände beschränkt, typischerweise wird es aber auf solche angewandt. Daten und Informationen sind von ihm jedenfalls im Grundsatz nicht erfasst.[48] Zwar wird in den kalifornischen Datenschutzgesetzen vom „owner" bestimmter Daten gesprochen.[49] Der Gesetzgeber verdeutlicht aber in den Legaldefinitionen, dass er den Begriff des Eigentums gewählt hat, um auszudrücken, dass er sämtliche Daten, die ein Unternehmen über betroffene Personen hält, schützen,[50] nicht aber, dass er ein Dateneigentum zugunsten des die Daten haltenden Unternehmens begründen möchte.[51]

Allerdings wollen einige US-amerikanische Gesetze in Bezug auf Connected Cars den Fahrzeugeigentümern Befugnisse an auf einem event data recorder (EDR, Datenerfassungsgeräte für Kraftfahrzeuge, die kritische Sensor- und Diagnosedaten vor Kollisionen aufzeichnen) gespeicherten Daten zuweisen und sprechen hierbei von Eigentum:

> *"Except as specifically provided under subsection (d) of this section and subsections (f)-(i) of this section, the data on a motor vehicle event data recorder:*
> *(1) Is private;*
> *(2) Is exclusively owned by the owner of the motor vehicle."*[52]

Ohne die Zustimmung des Fahrzeugeigentümers dürfen die Daten jedenfalls im Grundsatz nicht aus dem EDR abgefragt werden.[53] Dieses Abwehrrecht differenziert nicht zwischen personenbezogenen und nicht-personenbezogenen Daten, sondern bezieht sich auf alle im EDR gespeicherten Daten. Ob hierdurch tatsächlich eigentumsähnliche Befugnisse an den betroffenen Daten zugewiesen werden sollen, insbesondere ob an diesen ausschließliche Nutzungsrechte eingeräumt und die eingeräumten Nutzungsrechte auch nach erstmaliger Entäußerung in den Rechtsverkehr dinglich ausgestaltet sein sollen, bleibt im Gesetzestext und den Begründungen allerdings unklar.

---

[47] *Determann*, California Privacy Law, 2016, p. 25.

[48] Ark. Code Ann. § 23-112-107 (West); vgl. hierzu auch: *Determann*, Datenrechte im US-amerikanischen Rechtsraum, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

[49] CAL. CIV. CODE § 1798.82(a).

[50] CAL. CIV. CODE § 1798.81.5(a), der besagt: "(1) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information. (2) For the purpose of this section, the terms "own" and "license" include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term "maintain" includes personal information that a business maintains but does not own or license."

[51] *Determann*, California Privacy Law - Practical Guide and Commentary, 3. Aufl. 2018, Kapitel 2:15.1., im Erscheinen; *ders.*, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

[52] Ark. Code Ann. § 23-112-107 (West)

[53] *Determann*, Datenrechte im US-amerikanischen Rechtsraum, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

3.2 GESCHÄFTSGEHEIMNISSCHUTZ

3.2.1 SCHUTZ VON GESCHÄFTSGEHEIMNISSEN IM DEUTSCHEN UND EUROPÄISCHEN RECHT

Im Lauterkeitsrecht ist neben dem mittelbaren Leistungsschutz der §§ 4 Nr. 3 lit. a) – c) UWG v.a. der Geheimnisschutz (§§ 17, 18 UWG) relevant.[54] Daten lassen sich durchaus als Geschäfts- und Betriebsgeheimnisse schützen. Die am 27.05.2016 vom Rat der Europäischen Union angenommene und bis Juni 2018 umzusetzende Geschäftsgeheimnisrichtlinie vereinheitlicht hier die Rechtslage im europäischen Rechtsraum.[55]

Ein Geschäfts- oder Betriebsgeheimnis ist nach dem bisherigen nationalen Verständnis jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem bekundeten, auf wirtschaftlichen Interessen beruhenden Willen des Betriebsinhabers geheim gehalten werden soll.[56] Dieses Begriffsverständnis wird jedoch durch die Geschäftsgeheimnisrichtlinie modifiziert. In Anlehnung an Art. 39 Abs. 2 TRIPS ist das Geschäftsgeheimnis künftig definiert als (1) geheime Informationen mit (2) kommerziellem Wert, die (3) Gegenstand angemessener Geheimhaltungsmaßnahmen sind.[57]

Erforderlich sind gegenüber dem bisherigen nationalen Verständnis nach der unionsrechtlichen Vorgabe v.a. angemessene Geheimhaltungsmaßnahmen, vgl. Art. 2 Nr. 1 lit. c) Geschäftsgeheimnisrichtlinie. Funktional entspricht dieses Merkmal wohl am ehesten dem bisherigen Geheimhaltungswillen,[58] allerdings besteht der Unterschied darin, dass an den Geheimhaltungswillen bislang in Rechtsprechung und Literatur nicht allzu hohe Anforderungen gestellt werden;[59] manche Stimmen wollen gar gänzlich auf ihn verzichten.[60] Welche Ge-

---

[54] Vgl. hierzu v.a. *Becker*, GRUR 2017, 346, 347 ff.

[55] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. EU 2016 v. 15.06.2016, Nr. L 157/1; vgl. hierzu u.a. *McGuire*, GRUR 2016, 1000 ff.; *Heinzke*, CCZ 2016, 179 ff.; *Klein/Wegener*, GRUR-Prax 2017, 394 ff.; *Kalbfus*, GRUR-Prax 2017, 391 ff.; *ders.* GRUR 2016, 1009 ff.; zur Qualifikation von Software als Ware i.S.d. CISG vgl. MüKo BGB-*Huber*, 7. Aufl. 2016, CISG Art. 1 Rn. 20.

[56] BGH, Urt. v. 15.03.1955 – I ZR 111/53, GRUR 1955, 424, 425 - *Möbelpaste*; BGH, Urt. v. 01.07.1960 – I ZR 72/59, GRUR 1961, 40, 43 - *Wurftaubenpresse*; BGH, Urt. v. 07.11.2002 – I ZR 64/00, GRUR 2003, 356, 358 – *Präzisionsmessgeräte*; BGH, Urt. v. 27.04.2006 – I ZR 126/03, GRUR 2006, 1044, 1046 – *Kundendatenprogramm*.

[57] Zu den einzelnen Voraussetzungen vgl. *Heinzke*, CCZ 2016, 179, 181 ff.

[58] *Kalbfus*, GRUR-Prax 2017, 391, 391.

[59] BGH, Urt. v. 27.04.2006 – I ZR 126/03, GRUR 2006, 1044 Tz. 19 – *Kundendatenprogramm*: Der Geheimhaltungswille ergibt sich aus der Natur der geheim zu haltenden Tatsache; *Heinzke*, CCZ 2016, 182 m.w. N. Vermutung des Geheimhaltungswillens.

heimhaltungsmaßnahmen dem Geheimnisinhaber noch als angemessen abverlangt werden können, bleibt einstweilen abzuwarten.[61]

Zu den Geschäftsgeheimnissen können auch und gerade Datenbestände gehören:

> *„Enthalten Kundenlisten die Daten von Kunden, zu denen bereits eine Geschäftsbeziehung besteht und die daher auch in Zukunft als Abnehmer der angebotenen Produkte in Frage kommen, stellen sie im Allgemeinen für das betreffende Unternehmen einen wichtigen Bestandteil seines „Good will" dar, auf dessen Geheimhaltung von Seiten des Betriebsinhabers meist großer Wert gelegt wird (…).“*[62]

Soweit die EU-Kommission ausführt, es sei zweifelhaft, ob Daten Geschäftsgeheimnisse darstellen könnten, so gelten ihre Zweifel allein Einzeldaten, nicht aber Datenkonglomeraten:

> *„It is doubtful that individual data generated by interconnected machines and devices could be regarded as "trade secret" in the sense of this Directive, mostly because of its lack of commercial value as individual data; however, combination of data (datasets) can be trade secrets under this Directive if all the criteria are met."*[63]

Allerdings führt der Geheimnisschutz nicht zu einem Ausschließlichkeitsrecht mit Nutzungs- und Ausschlussfunktion,[64] sondern gibt allein Abwehrrechte gegen und Schadensersatzansprüche bei Verletzung von Geschäfts- und Betriebsgeheimnissen.[65] Zivilrechtlich folgt dies aus § 823 Abs. 2 BGB i.V.m. § 17 UWG als Schutzgesetz. Zukünftig müssen aber auch alle anderen europäischen Staaten einen zivilrechtlichen Geheimnisschutz vorsehen, vgl. Art. 6 Abs. 1 Geheimnisschutzrichtlinie. Damit wird allerdings noch kein Verbotsrecht für die Nutzung einer Information als solcher gewährt, sondern allein ein Schutz gegen unlauteren Zu-

---

[60] *Maume*, WRP 2008, 1275, 1279 ff.; *Ohly*, GRUR 2014, 1, 5; *Kalbfus*, Know-how-Schutz in Deutschland zwischen Zivilrecht und Strafrecht – Welcher Reformbedarf besteht?, 2011, Rn. 148 ff.; *Kalbfus*, GRUR-Prax 2017, 391, 391 ff.

[61] Für ein moderates Verständnis, das auch aus Sinn und Zweck des Geheimnisschutzes zur Kostenreduktion der faktischen Geheimhaltung folgt: *Kalbfus*, GRUR-Prax 2017, 391, 392.

[62] BGH, Urt. v. 27.04.2006 – I ZR 126/03, GRUR 2006, 1044 Tz. 19 – *Kundendatenprogramm*.

[63] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD (2017) 2 final, p. 20.

[64] Hierzu umfassend: *McGuire*, GRUR 2016, 1000, 1003 ff.

[65] Köhler/Bornkamm/Feddersen-*Köhler*, UWG, 36. Aufl. 2018, § 17 UWG Rn. 2; Ohly/Sosnitza-*Ohly*, UWG, 7. Aufl. 2016, § 17 Rn. 1 ff.; vgl. auch: Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD (2017) 2 final, p. 20; zu den Ansprüchen vgl. *Heinzke*, CCZ 2016, 179, 180.

gang.[66] Auf schuldrechtlicher Ebene ist eine Nutzungsbeschränkung mit Wirkung inter partes aber ebenso möglich, wie die Einräumung von Nutzungsbefugnissen.[67]

Inhaber eines Geschäftsgeheimnisses ist nach Art. 2 Nr. 2 Geschäftsgeheimnisrichtlinie diejenige natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis ausübt.[68]

Neben dem gesetzlichen Geheimnisschutz lassen sich Daten auch über strafbewehrte Geheimhaltungsvereinbarungen schützen. Der Abschluss derartiger Geheimhaltungsvereinbarungen wird wohl als angemessene Geheimhaltungsmaßnahme zukünftig ohnehin auch für den gesetzlichen Geheimnisschutz erforderlich sein.[69]

3.2.2 SCHUTZ VON GESCHÄFTSGEHEIMNISSEN IM US-AMERIKANISCHEN RECHT

Im US-amerikanischen Rechtsraum wird ein Schutz von Daten im Wesentlichen über den Geschäftsgeheimnisschutz gewährt. Bereits das Restatement of Torts aus dem Jahr 1939 enthielt eine Regelung über die Haftung für eine Verletzung von Betriebsgeheimnissen. Sec. 757 des Restatement (First) of Torts 1939 definierte das Betriebsgeheimnis in Comment b. dabei wie folgt:

„A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers. […]"[70]

Seit 1985 gilt der Uniform Trade Secret Act (UTSA), eine Modellregelung, die von nahezu allen Bundesstaaten ohne oder mit nur geringen Änderungen übernommen wurde.[71] Lediglich

---

[66] *Klein/Wegener*, GRUR-Prax 2017, 394, 394; *Heinzke*, CCZ 2016, 179, 179.

[67] Zur Rechtsnatur des Know-How-Vertrages vgl. *Pfaff*, BB 1974, 565, 567 f.; Palandt-*Weidenkaff*, BGB, 77. Aufl. 2018, Einf v § 581 Rn. 8; OLG Hamm, Urt. v. 02.03.1993 – 7 U 39/92, NJW-RR 1993, 1270, 1270; *Cebulla*, Die Pacht nichtsächlicher Gegenstände, 1999, S. 189 f.; *Haedicke*, Rechtskauf und Rechtsmängelhaftung, 2003, S. 303 m.w.N.; *Martinek*, Moderne Vertragstypen, 1993, Bd. II, S. 234 ff.

[68] Vgl. hierzu auch: *Heinzke*, CCZ 2016, 179, 180; zu den sich bei der Zuordnung des durch den Geheimnisschutz Begünstigten ergebenden Problemen vgl. *Klein/Wegener*, GRUR-Prax 2017, 394, 394 ff.

[69] So zumindest: *Heinzke*, CCZ 2016, 179, 182 f.; zu Anforderungen und Grenzen vertraglicher Geheimhaltungsvereinbarung vgl. Auer-Reinsdorff/Conrad-*Conrad/Schneider*, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, § 11 Rn. 114 ff.; Hasselblatt-*Straßer*, MAH Gewerblicher Rechtsschutz, 5. Aufl. 2017, § 48 Rn. 27 f.

[70] Text abrufbar unter: http://www.lrdc.pitt.edu/ashley/RESTATEM.HTM, zuletzt abgerufen am 04.05.2017.

[71] *Glazer et al.*, Practical Law Practice Note 4-532-4243 (2017).

die Staaten New York und Massachusetts haben den UTSA bisher noch nicht implementiert.[72] Der UTSA definiert ein „Trade Secret" in section 1 (4) UTSA:

„Trade Secret means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

Auch das US-amerikanische Recht erfordert also angemessene Geheimhaltungsmaßnahmen, die europäische Vorgabe ist aber freilich autonom auszulegen. Auf völkerrechtlicher Ebene findet sich das Erfordernis angemessener Geheimhaltungsmaßnahmen in Art. 39 Abs. 2 lit. c) TRIPS.[73] Eine Misappropriation (unbefugte Nutzung und Preisgabe[74]) von Trade Secrets führt im US-amerikanischen Recht zu Unterlassungs- und Schadensersatzansprüchen.[75] Der „Diebstahl" von Trade Secrets wird auch strafrechtlich sanktioniert, vgl. § 1832 U.S. code.

Zu nennen in der Genese des Trade-Secret-Schutzes ist auch der am 11.05.2016 in Kraft getretene Defend Trade Secret Act (DTSA). Hierbei handelt es sich um eine bundesgesetzliche Regelung, die den sich ausschließlich mit strafrechtlichen Folgen befassenden Economic Espionage Act (EEA) aus dem Jahr 1996 um zivilrechtliche Regelungen ergänzt. Die sich aus dem Economic Espionage Act ergebende Definition eines Betriebsgeheimnisses entspricht dabei im Wesentlichen derjenigen des UTSA.[76] Die Regelungen von EEA und DTSA wurden normiert in den §§ 1831 ff. U.S. Code. Sie ergänzen die auf dem UTSA beruhenden Gesetze der Bundesstaaten und verdrängen sie gerade nicht. Der DTSA gibt Betroffenen vielmehr

---

[72] New York verwendet die Definition des Restatement First of Torts § 757 (1939), Massachusetts regelt diese Frage durch ein eigenes Gesetz.

[73] Vgl. hierzu auch: *Kalbfus*, GRUR-Prax 2017, 391, 391.

[74] *Determann*, Datenrechte im US-amerikanischen Rechtsraum, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

[75] Vgl. Section 2 and 3 UTSA nebst Begründung, abrufbar unter: http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf, zuletzt abgerufen am 04.05.2017 sowie §§ 1836 (3) U.S. Code.

[76] § 1839 (3) EEA the term: "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and
(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public".

die Möglichkeit, Ansprüche vor den Bundesgerichten geltend zu machen. Dies war bis zu seinem Inkrafttreten allein bei den Gerichten der Bundesstaaten möglich.[77]

Der Begriff der „Information", die als Betriebsgeheimnis geschützt werden kann, wird in den vorstehenden Gesetzen sehr weit verstanden. Er umfasst technische und nicht-technische Angaben, einschließlich Know-how, Methoden und sogar Ideen. Die Information muss auch nicht absolut geheim sein, vielmehr muss sich der Inhaber durch entsprechende Geheimhaltungsmaßnahmen um ihre Geheimhaltung bemühen.[78] Die Beweislast für diese Geheimhaltungsbemühungen wird dabei von demjenigen getragen, der sich auf das Vorliegen eines Betriebsgeheimnisses beruft. Aufgrund der sehr einfachen Übertragungsmöglichkeit von Daten und der genutzten Software vom Computer zu Computer scheint es erforderlich, dass Massendatenhersteller zum Zwecke der Geheimhaltung auf eine Kombination von physischen Barrieren und Geheimhaltungsvereinbarungen zurückgreifen, um im Falle eines Gerichtsverfahrens erfolgreich einen angemessenen Geheimhaltungsaufwand vortragen zu können.[79]

3.2.3 „HOT NEWS-" UND MISAPPROPRIATION-DOKTRIN

Handelt es sich um eine kostenintensive Zusammenstellung von Daten, so kann diese nach einem Urteil des US Supreme Court in der Rechtssache *International News Service v. Associated Press*[80] auch nach der sog. Misappropriation Doktrin (in diesem Zusammenhang auch als „Hot News" Doctrine bezeichnet) gegen eine unbefugte Übernahme von Wettbewerbern geschützt sein.[81] Gegenstand des Urteils war ein Streit zwischen zwei konkurrierenden Presseagenturen, von denen eine (Associated Press) während des ersten Weltkrieges Journalisten bezahlte, die Nachrichten vom Krieg in Europa an den Hauptsitz der Nachrichtenagentur übermittelten, die wiederum von dort an lokale Zeitungen weitergegeben wurden. Die konkurrierende Presseagentur (International News Service) entschloss sich dagegen, keine eigenen Journalisten zu bezahlen, die die Nachrichten generierten, sondern zu warten, bis die lokalen Presseunternehmen die von der Associated Press weitergeleiteten Nachrichten veröffentlichten. Sie griff diese dann schlicht auf. Möglich wurde dieses Geschäftsmodell durch die Zeitverschiebung innerhalb der USA, denn die International News Service erlangte die Nachrichten in einer früheren Zeitzone und telegraphierte sie in eine spätere Zeitzone, wo sie dann in den eigenen Zeitungen veröffentlicht werden konnten.[82] Die Associated Press hielt dies für die Verletzung ihrer Urheberrechte. Der Supreme Court urteilte zwar, dass

---

[77] *Lejeune*, CR 2016, 330, 339.

[78] *Lemley*, 61 Stan. L. Rev. 311, 317 (2008).

[79] *Prange*, Intellectual Property Magazine (2017), p. 42.

[80] International News Service v. Associated Press, 248 U.S. 215 (1918).

[81] Zu vorangegangener Rechtsprechung, die letztlich in die "Hot News" Doktrin mündete vgl. eingehend: *Ekstrand/Roush*, 35 Cardozo Arts & Ent. L. J. 303, 305 et seq. (2017).

[82] International News Service v. Associated Press, 248 U.S. 215 (1918); *Mattioli*, ZGE 2017, 299, 303; vgl. hierzu auch: *Balganesh*, 111 Colum. L. Rev. 419 (2011).

Nachrichten an sich nicht durch das US-amerikanische Urheberrecht geschützt werden können, jedoch unter gewissen Voraussetzungen ein „Quasi-IP-Recht" bestehe.[83] Gegen Wettbewerber kann dieses Recht als Abwehrrecht zum Schutz vor unberechtigtem Kopieren sogenannter „Hot News" geltend gemacht werden. Das Recht entsteht mit dem Aufgreifen der Nachricht und endet mit der Beendigung der wirtschaftlichen Werthaltigkeit der Nachricht.

> *„It is to be observed that the view we adopt does not result in giving to complainant the right to monopolize either the gathering or the distribution of the news, or, without complying with the copyright act, to prevent the reproduction of its news articles, but only postpones participation by complainant's competitor in the processes of distribution and reproduction of news that it has not gathered, and only to the extent necessary to prevent that competitor from reaping the fruits of complainant's efforts and expenditure, to the partial exclusion of complainant."*[84]

Der Schutz erstreckt sich also nur auf einen kurzen Zeitraum, in dem den Nachrichten aufgrund ihrer Aktualität ein wirtschaftlicher Wert zukommt.[85] Er wurde unter dem Gesichtspunkt gewährt, dass die Associated Press Arbeitsaufwand, Zeit und Geld erbringen musste, um die Nachrichten zu sammeln, und dass der International News Service sich diesen Arbeitsaufwand nicht ohne Zustimmung einverleiben dürfe.

Daten, die mit einem hohen Zeit- und Kostenaufwand zusammengestellt wurden, genießen auch dann, wenn es sich nicht um Nachrichten oder nachrichtenrelevante Daten handelt, einen Schutz vor diesem sog. freeriding. Dies richtet sich nach den State Laws on Misappropriation (Gesetze der Einzelstaaten zum Schutz vor missbräuchlicher Verwendung).[86] Damit es nicht zu einem Unterlaufen des urheberrechtlichen Schutzes kommt, sind allerdings zusätzliche Voraussetzungen erforderlich.[87]

- Der Kläger generiert oder sammelt Information auf seine Kosten
- Die Information ist zeitempfindlich
- Die Verwendung der Information durch den Beklagten erfolgt in Ausbeutung des Arbeitsaufwandes des Klägers (free riding on the plaintiff's efforts)

---

[83] *Ekstrand/Roush*, 35 Cardozo Arts & Ent. L. J. 303, 309 (2017); *Mattioli*, ZGE 2017, 299, 303.

[84] International News Service v. Associated Press, 248 U.S. 215 (1918).

[85] International News Service v. Associated Press, 248 U.S. 215 (1918).

[86] Siehe: National Basketball Association v. Motorola, Inc., 105 F.3d 841, 852-54 (2d Cir. 1997); United States Golf Assn. v. Arroyo Software Corp., 69 Cal. App. 4th 607, 611-12, 618 (1999); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 (AM. Law Inst. 1995); *Ginsburg*, 66 U. CIN. L. REV. 151, 157 ff. (1997); *Determann*, Datenrechte im US-amerikanischen Rechtsraum, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

[87] National Basketball Assoc. v. Motorola, Inc., 105 F.3d 841 (2d Cir. 1997).

- Der Beklagte steht im direkten Konkurrenzverhältnis mit dem Produkt oder der Dienstleistung, die durch die Kläger angeboten wird
- Die Ausbeutung durch den Konkurrenten reduziert den Anreiz für den Kläger, das Produkt oder die Dienstleistung anzubieten, dermaßen, dass die Existenz oder Qualität von Produkt oder Dienstleistung ernsthaft gefährdet würde

In der Entscheidung *Barclays Capital Inc. v. Theflyonthewall.com, Inc.*[88] wurden diese zusätzlichen Voraussetzungen nochmals verengt und als weiteres Element statuiert, dass die „Hot News" Doktrin nur dann eingreift, wenn gerade diejenigen Nachrichten, Daten o.ä., die von einem Unternehmen verbreitet wurden, von einem Dritten aufgegriffen und als eigene veröffentlicht werden. Es ist erforderlich, dass der Dritte in Konkurrenz zum ersten Unternehmen tritt, jedoch durch die Übernahme deutlich geringere Kosten hat.

> *„(...) we are mindful that the INS Court's concern was tightly focused on the practices of the parties to the suit before it: news, data, and the like, gathered and disseminated by one organization as a significant part of its business, taken by another entity and published as the latter's own in competition with the former."*

Leistner spricht vom Erfordernis eines „*echten free riding*".[89] Nicht aber soll die „Hot News" Doktrin eingreifen, wenn Daten mit eigenem Kostenaufwand aus Drittdaten eines konkurrierenden Unternehmens erstellt werden.[90] Die Misappropriation-Doktrinwird insofern nur sehr zurückhaltend angewandt.[91] Insbesondere existiert kein generelles Common Law Tort of Misappropriation.[92]

3.2.4 FTCA, UNFAIR COMPETITION LAWS UND UNIFORM DECEPTIVE TRADE PRACTICES ACT

Eine Unlauterkeit der Datenerhebung wird darüber hinaus in weiteren Einzelfällen angenommen, z.B. im Falle einer „betrügerischen" Erhebung sensibler personenbezogener Daten.[93] Verfolgt werden diese lauterkeitsrechtlichen Verstöße von der FTC. Täuschende Handelspraktiken sind darüber hinaus über die in allen Mitgliedstaaten existenten Unfair Competition Laws oder Uniform Deceptive Trade Practices Acts verboten. Allerdings ist es erforderlich, dass ein objektiv messbarer Schaden beim Betroffenen eintritt. Ist dies der Fall, so

---

[88] Barclays Capital Inc. v. Theflyonthewall.com, Inc., 650 F.3d 876, 901 (2d Cir. 2011).

[89] Teplitzky/Peifer/Leistner-*Leistner*, UWG, 2. Aufl. 2013, § 4 Rn. 16.

[90] National Basketball Assoc. v. Motorola, Inc., 105 F.3d 841 (2d Cir. 1997).

[91] Vgl. zu der vorhandenen Rechtsprechung eingehend: *Ekstrand/Roush*, 35 Cardozo Arts & Ent. L.J., 303 (2017).

[92] Restatement (Third) of unfair competition § 38 (AM. Law Inst. 1995).

[93] *Solove/Hartzog*, 114 Columbia L. Rev. 583, 640 (2014); *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 266.

können täuschende Handelspraktiken auch in Bezug auf Daten lauterkeitsrechtlich nach den jeweiligen Landesvorschriften sanktioniert werden.[94]

[94] *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 273.

3.3 SCHUTZ VON DATENBANKEN UND DATENBANKWERKEN

3.3.1 DATENBANKSCHUTZ NACH DEUTSCHEM UND EUROPÄISCHEM RECHT

Einzeldaten selbst haben keinen Werkcharakter und sind daher nach deutschem Urheberrecht nicht geschützt. Der unionsrechtlich durch die Datenbankrichtlinie harmonisierte Datenbankschutz gem. § 4 UrhG sowie das ebenfalls durch die Datenbankrichtlinie harmonisierte Datenbankherstellerrecht gem. § 87a UrhG intendieren zwar nicht den Schutz von Einzeldaten, wohl aber ihren Zusammenschluss im Rahmen eines Datenbankwerkes oder einer nicht-schöpferischen Datenbank, § 87a UrhG.[95]

3.3.1.1 DATENBANK

Eine Datenbank ist gem. § 87a Abs. 1 S. 1, § 4 Abs. 2 UrhG eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind. Erweist sich Auswahl oder Anordnung der Elemente als persönliche geistige Schöpfung, wird die Datenbank als Datenbankwerk gem. § 4 Abs. 1 UrhG geschützt. Ist dies nicht der Fall, besteht dennoch ein Leistungsschutzrecht gem. § 87a Abs. 1 S. 1 UrhG, wenn die Beschaffung, Überprüfung oder Darstellung der Daten eine nach Art oder Umfang wesentliche Investition erfordert. Geschützt wird hier nicht die individuelle schöpferische Leistung, sondern die Datenbank als solche sowie mittelbar die Investitionsleistung.[96] Inhaber des Datenbankherstellerrechtes ist daher derjenige, der das Investitionsrisiko trägt.[97] Dies können auch mehrere Beteiligte mit der Folge der Anwendbarkeit der §§ 705 ff. BGB sein.[98]

Die Elemente der Datenbank müssen unabhängig voneinander sein, d.h. sie müssen voneinander getrennt werden können, ohne dass der Wert ihres Inhaltes dadurch beeinträchtigt

---

[95] Zum Datenbankschutz vgl. insb. *Dorner*, CR 2014, 617, 622; *Ehlen/Brandt*, CR 2016, 570 ff.; *Ensthaler*, NJW 2016, 3473; *Hieke*, InTeR 2017, 10, 16 ff.; *Sattler*, in: Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, 2017, S. 27 ff.; *Ehmann*, K&R 2014, 394 ff.; *Elteste*, CR 2015, 447 ff.

[96] *Schmidt/Zech*, CR 2017, 417, 423.

[97] ErwGr. 41 S. 2 der Richtlinie 96/9/EG des Europäischen Parlaments und des Rates vom 11. März 1996 über den rechtlichen Schutz von Datenbanken, ABl. EG 1996 v. 27.03.1996, L 77/20, S. 23; BGH, Urt. v. 22.06.2011 – I ZR 159/10, GRUR 2011, 1018 Tz. 32 – *Automobil-Onlinebörse*; BGH, Urt. v. 26.03.2010 – I ZR 47/08, GRUR 2010, 1004 Tz. 22 – *Autobahnmaut*; BGH, Urt. v. 01.12.2010 – I ZR 196/08, GRUR 2011, 724 Tz. 26 – *Zweite Zahnarztmeinung II*; *Wiebe*, GRUR 2017, 338, 342; Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 6. Aufl. 2018, § 87a Rn. 19; Fromm/Nordemann-*Czychowski*, Urheberrecht, 11. Aufl. 2014, § 87a Rn. 25; Schricker/Loewenheim-*Vogel*, Urheberrecht, 5. Aufl. 2017, § 87a Rn. 70.

[98] Hierzu sowie zu möglichen Schwierigkeiten bei der Zuordnung des Rechts in vernetzten Wertschöpfungsketten vgl. *Wiebe*, GRUR 2017, 338, 342.

wird.[99] Die einzelnen Elemente der Datenbank dürfen nicht erst in ihrem Zusammenhang Sinn ergeben, wie dies etwa bei Büchern oder Musikstücken der Fall ist.[100] Bei Datensammlungen ist es jedenfalls häufig so, dass erst den in Bezug zueinander gesetzten Daten eine Aussage entnommen werden kann. Das einzelne Datum an sich ist nicht mehr als ein Zeichen, die semantische Information kann aus ihm bzw. aus mehreren in Bezug zueinander gesetzten Daten aber abgeleitet werden.[101] Sie ist letztlich die werthaltige Größe, während das einzelne Datum an sich in der Regel einen geringeren Wert haben wird.[102] Allerdings ist eine Reduktion des Wertes unschädlich, solange noch ein gewisser selbständiger Wert erhalten bleibt.[103] Maßgeblich ist dies aus Sicht eines jeden Dritten zu beurteilen, der sich für das Einzelelement interessiert.[104] Eine gänzliche Wertfreiheit wird man auch Einzeldaten nicht zusprechen können, weshalb das Kriterium der Unabhängigkeit der Elemente in der Regel erfüllt sein sollte.

Eine Sammlung liegt nur dann vor, wenn sie eine Vielzahl von Elementen enthält,[105] die ihrerseits nicht urheberrechtlich schutzfähig sein müssen.[106] Damit wird der Datenbankschutz gerade auch interessant als Schutzrecht für die Sammlung von Daten, an denen de lege lata keine ausschließlichkeitsrechtliche Rechtsposition besteht. Die Daten müssen allerdings für

---

[99] EuGH, Urt. v. 01.03.2012 – C-604/10, ECLI:EU:C:2012:115 = GRUR 2012, 386 Tz 26 f. – *Football Dataco u.a.*; BGH, Urt. v. 10.03.2016 – I ZR 138/13, GRUR 2016, 930 Tz. 19 – *TK 50 II*; BGH, Urt. v. 21.04.2005 – I ZR 1/02, GRUR 2005, 940, 941 – *Marktstudien*; Dreier/Schulze-Dreier, Urheberrechtsgesetz, 6. Aufl. 2018, § 87a Rn. 6; BeckOK UrhR-*Vohwinkel*, 18. Ed. (Stand: 01.11.2017), UrhG, § 87a Rn. 20 ff.; Wandtke/Bullinger-*Thum/Hermes*, Praxiskommentar zum Urheberrecht, 4. Aufl. 2014, § 87a Rn. 12.

[100] Fromm/Nordemann-*Czychowski*, Urheberrecht, 11. Aufl. 2014, § 87a Rn. 9; eine Sammlung von derartigen urheberrechtlich geschützten Werken kann aber wiederum Gegenstand des Datenbankschutzes sein, vgl. Wandtke/Bullinger-*Thum/Hermes*, Praxiskommentar zum Urheberrecht, 5. Aufl. 2018, § 87a Rn. 9.

[101] *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 21 ff.

[102] *Wiebe*, GRUR 2017, 338, 339.

[103] EuGH, Urt. v. 01.03.2012 – C-604/10, ECLI:EU:C:2012:115 = GRUR 2012, 386 Tz. 26 f. – *Football Dataco u.a.*

[104] EuGH, Urt. v. 29.10.2015 – C-490/14, ECLI:EU:C:2015:735 = GRUR Int. 2015, 1161 Tz. 27 – *Verlag Esterbauer*; EuGH, Urt. v. 09.11.2004 – C-444/02, ECLI:EU:C:2004:697 = GRUR 2005, 254 Tz. 34 – *Fixtures Marketing*; *Schmidt/Zech*, CR 2017, 417, 419.

[105] Wandtke/Bullinger-*Thum/Hermes*, Praxiskommentar zum Urheberrecht, 5. Aufl. 2018, § 87a Rn. 9, 11; BeckOK UrhR-*Vohwinkel*, 18. Ed. (Stand: 01.11.2017), UrhG, § 87a Rn. 28; Möhring/Nicolini-*Koch*, Urheberrecht, 3. Aufl. 2014, § 87a Rn. 8.

[106] Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 5. Aufl. 2015, § 87a Rn. 4; BeckOK UrhR-*Vohwinkel*, 18. Ed. (Stand: 01.11.2017), UrhG, § 87a Rn. 30; Fromm/Nordemann-*Czychowski*, Urheberrecht, 11. Aufl. 2014, § 87a Rn. 9.

einen Datenbankschutz gem. § 87a UrhG systematisch oder methodisch angeordnet sein.[107] Die Einzeldaten müssen durch Abfragemittel wiederauffindbar sein. Es kommt darauf an, dass sie auf der Zugriffsebene der Nutzer systematisch oder methodisch recherchierbar sind.[108] Ungeordnete Datenhaufen sind daher vom Datenbankschutz grds. nicht erfasst.[109] Kommt es allerdings lediglich auf die Recherchierbarkeit an, so ließe sich argumentieren, dass die Informationstechnologie die methodische Anordnung entbehrlich macht, solange die Daten auch bei ungeordneter Darstellung wieder aufgefunden werden können. Dies wird auch und gerade in Big-Data-Sachverhalten in der Regel der Fall sein.[110]

3.3.1.2 WESENTLICHE INVESTITIONSLEISTUNG

Letztlich muss die Investition in die Beschaffung, Überprüfung oder Darstellung getätigt werden und nach Art und Umfang wesentlich sein.[111] Hier sind v.a. zwei Dinge zu beachten: Zwar ist der Investitionsbegriff weit zu verstehen und ist nicht auf finanzielle Investitionsleistungen beschränkt.[112] Nicht erfasst wird aber der Aufwand für die Generierung von Daten, sondern allein die Investition, die der Beschaffung und Zusammenstellung von bereits vorhandenen Elementen gewidmet ist, wird berücksichtigt.[113] So ist beispielsweise die Aufstellung von Spielplänen für sportliche Ereignisse eine Erzeugung von Daten, während das Erfassen der Ergebnisse dieser Sportereignisse eine Datensammlung und -aufbereitung darstellt.[114] In einer Reihe von aktuellen Anwendungsfällen, z.B. solchen der Industrie 4.0, wird

---

[107] Die beiden Kriterien können alternativ vorliegen, vgl. hierzu sowie zu den Voraussetzungen alternativer bzw. methodischer Anordnung: EuGH, Urt. v. 09.11.2004 – C-444/02, ECLI:EU:C:2004:697 = GRUR 2005, 254 Tz. 30, 32 – *Fixtures Marketing*; Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 6. Aufl. 2018, § 87a Rn. 7.

[108] Wandtke/Bullinger-*Thum/Hermes*, Praxiskommentar zum Urheberrecht, 5. Aufl. 2018, § 87a Rn. 20, 21.

[109] Fromm/Nordemann-*Czychowski*, Urheberrecht, 11. Aufl. 2014, § 87a Rn. 11; Möhring/Nicolini-*Koch*, Urheberrecht, 3. Aufl. 2014, § 87a Rn. 14; Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 6. Aufl. 2018, § 87a Rn. 7; Wandtke/Bullinger-*Thum/Hermes*, Praxiskommentar zum Urheberrecht, 5. Aufl. 2018, § 87a Rn. 20, 24; *Wiebe*, GRUR 2017, 338, 340.

[110] *Schmidt/Zech*, CR 2017, 417, 420.

[111] Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 6. Aufl. 2018, § 87a Rn. 12; Wandtke/Bullinger-*Thum/Hermes*, Praxiskommentar zum Urheberrecht, 5. Aufl. 2018, § 87a Rn. 34; BeckOK UrhR-*Vohwinkel*, 18. Ed. (Stand: 01.11.2017), UrhG, § 87a Rn. 40 ff., 50 ff.

[112] Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 6. Aufl. 2018, § 87a Rn. 12; Schricker/Loewenheim-*Vogel*, Urheberrecht, 5. Aufl. 2017, § 87a Rn. 56; Spindler/Schuster-*Wiebe*, Recht der elektronischen Medien, 3. Aufl. 2015, UrhG, § 87a Rn. 7; Möhring/Nicolini-*Koch*, Urheberrecht, 3. Aufl. 2014, § 87a Rn. 19-25.

[113] Hoeren/Sieber/Holznagel-*Gaster*, Multimedia-Recht, 45. EL Juli 2017, Teil 7 Rn. 82.

[114] ÖstOGH, Urt. v. 24.03.2015 – 4 Ob 206/14 v, BeckRS 2015, 81041; EuGH, Urt. v. 09.11.2004 – C-203/02, ECLI:EU:C:2004:695 = GRUR 2005, 252 Tz. 19, 38 – *The British Horseracing Board u.a.*; EuGH, Urt. v. 09.11.2004 – C-444/02, ECLI:EU:C:2004:697 = GRUR 2005, 254 Tz. 38, 53 - *Fixtures-Marketing*; EuGH, Urt. v. 09.11.2004 – C-46/02, ECLI:EU:C:2004:694 = GRUR Int. 2005, 244 Tz. 34, 49 – *Fixtures Marketing*; vgl. dazu auch: *Heermann/John*, K&R 2011, 753; *Reinholz*, K&R 2012, 338; *Wiebe*, GRUR 2017, 338, 340.

allerdings in die Generierung von Daten investiert werden, eine Anwendbarkeit der §§ 87a ff. scheidet dann aus.[115]

Zweitens muss die Investition in qualitativer oder quantitativer Hinsicht („nach Art und Umfang") wesentlich sein. Zur Feststellung der Wesentlichkeit bedarf es einer wertenden Betrachtung, bei der klare Anhaltspunkte noch fehlen. Einzubeziehen ist sowohl der finanzielle, als auch der nicht zu beziffernde Aufwand an Mitteln, geistiger Leistung, Zeit etc. Je höher der Investitionsaufwand, desto eher ist von einem Schutz gem. § 87a UrhG auszugehen. Ausreichend ist es allerdings jedenfalls nach Auffassung der Rechtsprechung,

> *„wenn bei objektiver Betrachtung keine ganz unbedeutenden, von jedermann leicht zu erbringenden Aufwendungen erforderlich waren, um die Datenbank zu erstellen. Nicht notwendig sind Investitionen von substanziellem Gewicht."*[116]

Aufwendungen, die in den Erwerb einer fertigen Datenbank getätigt werden, sind keine berücksichtigungsfähige Investition.[117]

3.3.1.3 SCHUTZUMFANG

Geschützt ist die Datenbank an sich sowie wesentliche Teile[118] von ihr gegen eine unberechtigte Vervielfältigung, Verbreitung und öffentliche Wiedergabe. Nicht geschützt bleiben die Einzeldaten.[119] Auf die Übernahme der Anordnung kommt es nicht an.[120] Vor einer Vervielfältigung, Verbreitung und öffentlichen Wiedergabe unwesentlicher Teile der Datenbank ist der Rechteinhaber aber jedenfalls dann geschützt, wenn dies wiederholt und systematisch geschieht, vgl. § 87b S. 2 UrhG.[121] Die Schutzdauer beträgt 15 Jahre und beginnt mit der Veröffentlichung der Datenbank, respektive mit ihrer Herstellung, sofern sie nicht veröffentlicht wurde, vgl. § 87d UrhG.

---

115 Vgl. hierzu eingehend: *Grützmacher*, CR 2016, 485, 488.

116 BGH, Urt. v. 01.12.2010 – I ZR 196/08, MMR 2011, 676 Tz. 23 - *Zweite Zahnarztmeinung II*; vgl. zur teilweise abweichenden Auffassung in der Literatur v.a. *Schmidt/Zech*, CR 2017, 417, 423 m.w.Nachw.

117 BGH, Urt. v. 30.04.2009 – I ZR 191/05, GRUR 2009, 852 Tz. 24 – *Elektronischer Zolltari..f.*; Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 5. Aufl. 2015, § 87a Rn. 13; *Schmidt/Zech*, CR 2017, 417, 422.

118 Eine Übernahme von 10% der Datenbank ist hierfür nicht ausreichend, 50% hingegen schon, vgl. *Schmidt/Zech*, CR 2017, 417, 425; Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 5. Aufl. 2015, § 87b Rn. 7; Wandtke/Bullinger-*Thum/Hermes*, Praxiskommentar zum Urheberrecht, 5. Aufl. 2018, § 87b Rn. 15; BGH, Urt. v. 01.12.2010 – I ZR 196/08, MMR 2011, 676 Tz. 28 - *Zweite Zahnarztmeinung II*.

119 BeckOK UrhR-*Vohwinkel*, 18. Ed. (Stand: 01.11.2017), UrhG, § 87b Rn. 13; Dreier/Schulze-*Dreier*, Urheberrechtsgesetz, 5. Aufl. 2015, § 87b Rn. 7; Spindler/Schuster-*Wiebe*, Recht der elektronischen Medien, 3. Aufl. 2015, UrhG, § 87b Rn. 18.

120 BGH, Urt. v. 21.07.2005 – I ZR 290/02, CR 2005, 849 ff. – *HIT BILANZ*; *Grützmacher*, CR 2006, 14 ff.

121 Hierzu eingehend: *Grützmacher*, CR 2016, 485, 488; *Schmidt/Zech*, CR 2017, 417, 425.

3.3.2 DATENBANKSCHUTZ NACH US-AMERIKANISCHEM RECHT

Einzeldaten sind mangels Werkcharakter auch nach US-amerikanischem Recht nicht geschützt. Einen Schutz schöpferischer Datenbankwerke kennt das US-amerikanische Recht zwar, nicht aber auch einen Schutz nicht-schöpferischer Datenbanken entsprechend §§ 87a ff. UrhG.[122]

Früher existierte auch für nicht-schöpferische Zusammenstellungen von Daten ein Schutz unter der sog. Sweat of the Brow-Doktrin.[123] Grundgedanke dieses Prinzips war es, denjenigen, der durch seine eigene Arbeit, Anstrengung und Mühe ein Ergebnis geschaffen hat, vor unberechtigter Übernahme dieses Arbeitsergebnisses zu schützen, auch wenn es nicht urheberrechtlich schutzfähig war. Die "Sweat of the Brow-Doktrin" wurde jedoch durch den US Supreme Court in der Rechtssache *Feist Publications, Inc., v. Rural Telephone Service Co.* verworfen.[124]

> *"Original, as the term is used in copyright, means (...) that the work was independently created by the author (as opposed to copied from other works), and that it possesses at least some minimal degree of creativity. (...) It may seem unfair that much of the fruit of the compiler's labor may be used by others without compensation. As Justice Brennan has correctly observed, however, this is not "some unforeseen byproduct of a statutory scheme." Harper & Row, 471 U.S., at 589 (dissenting opinion). It is, rather, "the essence of copyright," ibid., and a constitutional requirement. The primary objective of copyright is not to reward the labor of authors, but "to promote the Progress of Science and useful Arts."*[125]

Allein solche Datenbanken genießen heute urheberrechtlichen Schutz, die eine gewisse Kreativität aufweisen, der Arbeitsaufwand allein soll dagegen kein ausreichender Schutzgrund mehr sein. Konkrete Einschätzungen und Datenbewertungen können allerdings einen ausreichend schöpferischen Charakter haben.[126] So wurden in *CCC Info v. Maclean Hunter Marketing Reports* die durch den Kläger veröffentlichten individuellen Einschätzungen von Gebrauchtwagenpreisen als Originalwerke gesehen.[127] Selbst eine Zusammenstellung von

---

[122] Dazu eingehend: *Mattioli*, ZGE 2017, 299, 303 ff.

[123] S. z.B. Emerson v. Davies, 8 F. Cas. (No. 4,436) (CCD Mass. 1845) oder West Pub. Co. v. Mead Data Cent., Inc., 616 F. Supp. 1571 (D. Minn. 1985).

[124] Feist Publications, Inc., v. Rural Telephone Service Co., 499 U.S. 340 (1991).

[125] Feist Publications, Inc., v. Rural Telephone Service Co., 499 U.S. 340 (1991) para. 10, 19.

[126] *Mattioli*, 99 Minn. L. Rev. 535 et seq. (2014).

[127] CCC Info v. Maclean Hunter Marketing Reports, Inc., 44 F.3d 61, 67 (2d Cir. 1994).

sechsstelligen Codes, die Zahnbehandlungen wiederspiegeln, sollen urheberrechtlich schutzfähig sein.[128]

3.4 DELIKTSRECHTLICHER SCHUTZ VON DATEN

Das Deliktsrecht ist unionsrechtlich weitgehend nicht harmonisiert.[129] Im deutschen Recht kommt zunächst ein Schutz vor der Löschung oder anderweitigen Beeinträchtigung von Daten gem. § 823 Abs. 2 BGB i.V.m. §§ 202a ff., 303a StGB in Betracht,[130] sofern die spezifischen Voraussetzungen der §§ 202a (Ausspähen von Daten), 202b (Abfangen von Daten), 202c (Vorbereiten des Ausspähens und Abfangens von Daten), § 202d (Datenhehlerei), 303a StGB (Datenveränderung) vorliegen. Denn §§ 202a ff., 303a StGB dienen dem Interesse des Dateninhabers, die Daten vor unbefugtem Zugriff zu schützen (§§ 202a ff. StGB),[131] sowie dem Interesse des Berechtigten an der unversehrten Verwendbarkeit von Daten (§ 303a StGB).[132] Dieser Individualschutz begründet ihren Schutzgesetzcharakter.[133] Auch die Verbotsvorschriften des Datenschutzrechts lassen sich als Schutzgesetze begreifen, ebenso wie der strafrechtliche Schutz gegen den Geheimnisverrat in besonderen Vertrauensverhältnissen, § 203 StGB. Im Falle einer sittenwidrigen Schädigung kommen Ansprüche gem. § 826 BGB in Betracht.

Ebenfalls im Einzelfall kann eine Löschung oder anderweitige Beeinträchtigung von Daten einen Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb begründen. Während es hierbei im Wesentlichen auf die Betriebsbezogenheit des Eingriffs ankommt, wird im Rahmen des § 823 Abs. 1 BGB ein Schutz vor Löschung und Beeinträchtigung von Daten auch ohne diese Voraussetzung über den Schutz des Eigentums am Trägermedium erreicht. Diskutiert wird auch ein Recht am eigenen Datenbestand.[134] Beide Modelle werden nachfolgend im Einzelnen dargestellt. Im US-amerikanischen Recht ergibt sich ein Schutz von Daten im Wesentlichen über die Privacy Torts, aber auch über den Breach of Confidentiality sowie über die Torts of Trespass to Chattels und Conversion.[135]

---

[128] American Dental Association v. Delta Dental Plans Association, 126 F.3d 977, 979 (7th Cir. 1997).

[129] Eine Ausnahme bildet beispielweise die Richtlinie des Rates 85/374/EWG vom 25. Juli 1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über die Haftung für fehlerhafte Produkte, ABl. EG 1985 v. 07.08.1985, Nr. L 210/29.

[130] Zu letzterem vgl. hierzu: *Faust*, 71. DJT 2016, S. A50; *Hieke*, InTeR 2017, 10, 14 ff.

[131] OLG Naumburg, Urt. v. 27.08.2014 – 6 U 3/14, CR 2016, 83, 83; *Fischer*, Strafgesetzbuch, 64. Aufl. 2017, § 202a Rn. 2; Schönke/Schröder-*Lenckner/Eisele*, Strafgesetzbuch, 29. Aufl. 2014, § 202a Rn. 1; Lackner/Kühl-*Heger*, StGB, 28. Aufl. 2014, § 202a Rn. 1.

[132] MüKo StGB-*Wieck-Noodt*, 2. Aufl. 2014, § 303a Rn. 2.

[133] Vgl. zum Ganzen: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 220 ff.

[134] BeckOK BGB-*Förster*, 44. Ed. (Stand: 01.11.2017), § 823 Rn. 141; *Meier/Wehlau*, NJW 1998, 1585, 1588 f.

[135] Vgl. Hierzu sogleich unter 3.4.3.

3.4.1 BEEINTRÄCHTIGUNG VON DATEN ALS EIGENTUMSVERLETZUNG AM TRÄGERMEDIUM

Im Falle einer Beschädigung oder Zerstörung von Daten wird z.T. angenommen, dies begründe eine Eigentumsverletzung am Trägermedium.[136] Eine solche über § 823 Abs. 1 BGB und § 1004 Abs. 1 BGB analog zu Unterlassungs- und Schadensersatzansprüchen führende Eigentumsverletzung ist zu bejahen bei Substanzverletzung, bei Entziehung der Sache, aber auch im Falle der Beeinträchtigung des bestimmungsgemäßen Gebrauchs.[137] Im Falle einer Löschung von auf einem Trägermedium gespeicherten Daten ließe sich eine Gebrauchsbeeinträchtigung annehmen, da der Eigentümer das Speichermedium nicht mehr nach seinem Belieben [also zum Abruf der geschädigten Daten] nutzen kann.[138] Der bestimmungsgemäße Gebrauch eines Speichermediums liegt (auch dann, wenn man sich auf den präzisen Einzelgegenstand und nicht auf Speichermedien insgesamt bezieht) allerdings mehr in seiner generellen Tauglichkeit zur Datenspeicherung und zum Datenabruf, denn in der Abrufmöglichkeit ganz bestimmter Daten.[139] Jedenfalls aber scheitert diese Hilfskonstruktion, wenn das Eigentum an dem Trägermedium nicht dem Anspruchsteller, sondern einem Dritten zusteht, z.B. weil dieser die von ihm verwendeten Daten auf einem externen Server speichert.[140]

3.4.2. RECHT AM EIGENEN DATENBESTAND

Meyer/Wehlau haben bereits 1998 ein „Recht am Datenbestand" angeregt,[141] das nach teilweise vertretener Auffassung jedoch auf den „verkörperten Datenbestand" beschränkt sein

---

[136] OLG Karlsruhe, Urt. v. 07.11.1995 - 3 U 15/95, NJW 1996, 200, 201; *Meier/Wehlau*, NJW 1998, 1585, 1588; *Rombach*, CR 1990, 101, 104, der darauf verweist, dass auch das Löschen von Tonbändern eine Eigentumsverletzung des Trägermediums sei; vgl. hierzu auch: *Gerstenberg*, NJW 1956, 540, 540; a.A. LG Konstanz, Urt. v. 10.05.1996 - 1 S 292/95, NJW 1996, 2662, 2662.

[137] BGH, Urt. v. 05.06.1990 - VI ZR 359/89, NJW-RR 1990, 1172, 1173; BGH, Urt. v. 11.01.2005 - VI ZR 34/04, NJW-RR 2005, 673, 674; Palandt-*Sprau*, BGB, 77. Aufl. 2018, § 823 Rn. 7; Erman-*Wilhelmi*, BGB, 15. Aufl. 2017, § 823 Rn. 25; Jauernig-*Teichmann*, Bürgerliches Gesetzbuch, 16. Aufl. 2015, § 823 Rn. 8; HK-BGB-*Staudinger*, 9. Aufl. 2017, § 823 Rn. 38, jeweils m.w.Nachw.

[138] OLG Karlsruhe, Urt. v. 07.11.1995 - 3 U 15/95, NJW 1996, 200, 201; vgl. auch: *Wehlau*, OLG Report 2004, abrufbar unter http://www.olg-report.de/media/komm0414.RTF, S. 1, zuletzt abgerufen am 30.10.2010; *Hieke*, InTeR 2017, 10, 14 m.w.Nachw.; *Spindler*, Daten im Deliktsrecht, in: Hilbig-Lugani/Jakob/Mäsch/Reuß/Schmid, Zwischenbilanz – Festschrift für Dagmar Coester-Waltjen zum 70. Geburtstag, 2015, S. 1183, 1185.

[139] Ähnlich: *Faustmann*, VuR 2006, 260, 261; *Hieke*, InTeR 2017, 10, 14; vgl. zum Ganzen: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 218 ff.

[140] *Wehlau*, OLG Report 2004, abrufbar unter: http://www.olg-report.de/media/komm0414.RTF, S. 1, zuletzt abgrufen am 30.10.2010; vgl. zum Ganzen: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 218 ff.

[141] *Meier/Wehlau*, NJW 1998, 1585 ff.

soll. Bei der Übertragung verlorene Daten sollen demnach nicht erfasst sein, erforderlich sei vielmehr eine Beeinträchtigung im Zustand ihrer Speicherung auf einem beliebigen Datenträger.[142] Um als sonstiges Recht i.S.d. § 823 Abs. 1 BGB in Betracht zu kommen, bedarf es jedoch einer Nutzungs- und Ausschlussfunktion dieses Rechts sowie einer Vergleichbarkeit mit den übrigen sonstigen Rechten.[143] Beides ist hier gegeben. Denn außerhalb gesetzlicher Sondervorschriften, wie dem Geheimnisschutz, urheberrechtlichen Vorschriften oder den erläuterten strafrechtlichen Vorschriften besteht mit dem Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme als Teilbereich des Allgemeinen Persönlichkeitsrechts seit der entsprechenden Bundesverfassungsgerichtsentscheidung[144] ein generelles Recht, andere von der Nutzung gespeicherter Daten auszuschließen.[145] Dieses Recht führt nicht nur zu einer generellen Abwehrbefugnis, sondern dürfte auch geeignet sein, die Vergleichbarkeit mit anderen über § 823 Abs. 1 geschützten Rechten herbeizuführen.

Ein sonstiges „Recht am eigenen Datenbestand" müsste allerdings hinreichend darauf reagieren, dass auch das informationelle Selbstbestimmungsrecht des Betroffenen als sonstiges Recht i.S.d. § 823 Abs. 1 BGB geschützt ist. Der Betroffene muss die ihn betreffenden personenbezogenen Daten auch dann selbst weiterverwenden dürfen, wenn sie in einem über § 823 Abs. 1 BGB geschützten Datenbestand eines Dritten gespeichert sind.[146] Dies ließe sich dadurch gewährleisten, dass eine durch den datenschutzrechtlichen Betroffenen vorgenommene positive Nutzung der Daten (eine durch den Betroffenen vorgenommene Beeinträchtigung des Datenbestandes könnte sicherlich anders beurteilt werden) nicht den Tatbestand des § 823 Abs. 1 BGB verwirklicht, jedenfalls aber die Rechtswidrigkeit negiert würde. Umgekehrt darf das Recht am eigenen Datenbestand nicht dazu führen, dass ein datenschutzrechtswidriger Umgang mit den zum Datenbestand gehörenden Daten nicht geahndet werden kann. Die Nutzungskomponente eines Rechts am eigenen Datenbestand müsste insoweit umfassend den Beschränkungen des Datenschutzrechts unterworfen werden. Die

---

[142] *Faustmann*, VuR 2006, 260, 262; allgemein für ein Recht am eigenen Datenbestand: *Spindler*, Daten im Deliktsrecht, in: Hilbig-Lugani/Jakob/Mäsch/Reuß/Schmid, Zwischenbilanz – Festschrift für Dagmar Coester-Waltjen zum 70. Geburtstag, 2015, S. 1183, 1184 ff.; *Berberich/Golla*, PinG 2016, 165, 168 f.: "Dateneigentum als sonstiges Recht"; *Hornung et al*., Eigentumsordnung für Mobilitätsdaten, 2017, S. 4: „Einführung einer Haftungsnorm zur Verbesserung des Integritätsschutzes von Daten"; *Grützmacher*, CR 2016, 485, 490; Prütting/Wegen/Weinreich-*Schaub*, BGB, 13. Aufl. 2018, § 823 Rn. 77; *Hörl*, ITRB 2014, 111, 112; *Spindler*, JZ 2016, 805, 813 f.; MüKo BGB-*Wagner*, 7. Aufl. 2017, § 823 Rn. 295; *Berberich/Golla*, PinG 2016, 165, 172 ff.; a.A. Staudinger-*Hager*, BGB. 2017, § 823 Rn. B192; *Spickhoff*, Der Schutz von Daten durch das Deliktsrecht, in: Leible/Lehmann/Zech, Unkörperliche Güter im Zivilrecht, 2011, S. 233, 243 ff.; *Faust*, 71. DJT 2016, S. A52 ff.; vgl. zum Streitstand auch: *Libertus*, MMR 2005, 507, 508 m.w.Nachw.; *Leible/Sosnitza*, K&R 2002, 51, 52.

[143] *Faust*, 71. DJT 2016, S. A79.

[144] BVerfG, Urt. v. 27.02.2008 – 1 BvR 370/07, ZUM 2008, 301 – *Online-Durchsuchung*.

[145] Ähnlich: *Heymann*, CR 2016, 650, 652; vgl. auch: *Bartsch*, CR 2008, 613 ff.

[146] Vgl. hierzu bereits: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, Teil 5.

Reichweite, mögliche Verletzungshandlungen sowie die Beschränkungen eines möglichen Rechts am eigenen Datenbestand müssten insofern sehr fein austariert werden.[147] Auch weitere Zugriffsrechte könnten zu einem Ausschluss der Rechtswidrigkeit der Verletzungshandlung führen.

Beschränkt man das Recht am eigenen Datenbestand aber auf die Manipulation, Löschung oder Beschädigung des Datenbestands sowie auf das Kopieren und die Weiterreichung desselben,[148] und wird dem informationellen Selbstbestimmungsrecht des Betroffenen ausreichend Rechnung getragen, so scheint ein Recht am eigenen Datenbestand jedenfalls dogmatisch sehr viel näher zu liegen, als entsprechende Datenschädigungen über eine Eigentumsbeeinträchtigung des Trägermediums zu erfassen. Bei Ausgestaltung eines solch beschränkten Rechts am eigenen Datenbestand wäre eine Normierung auf europäischer Ebene wünschenswert.[149]

Berechtigter eines solchen Rechts am eigenen Datenbestand könnte, je nach Ausgestaltung, derjenige sein, der die Speicherung tatsächlich veranlasst oder für den sie veranlasst wird (in einem Arbeits- und Auftragsverhältnis also je nach Weisungsgebundenheit der Arbeitgeber oder der Arbeitnehmer).[150]

3.4.3 US TORT LAW

3.4.3.1 PRIVACY TORTS

In den USA wird ein deliktsrechtlicher Schutz von Daten in engen Grenzen mittelbar über das Right to Privacy gewährt. Aus ihm erwachsen nach *Prosser* vier deliktsrechtliche privacytorts (1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs, 2. Public disclosure of embarrassing private facts about the plaintiff, 3. Publicity which places the plaintiff in a false light in the public eye, 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness[151]). Die intruson upon seclusion nach § 652 Restatement (Second) of Torts erfordert es, dass eine Person absichtlich körperlich oder auf andere Weise in die Abgeschiedenheit oder Angelegenheiten einer anderen Person eindringt und dies von

147 Gegen ein umfassendes Recht am eigenen Datenbestand, das auch dem Datensubjekt einen Umgang mit den ihn betreffenden personenbezogenen Daten verbietet: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, Teil 5.

148 Vgl. die Auflistung möglicher Verletzungshandlungen bei *Bartsch*, CR 2008, 613, 614 f.

149 *Osborne Clarke LLP*, Legal study on ownership and access to data, 2016.

150 Ähnlich: *Hörl*, ITRB 2014, 111, 112.

151 *Prosser*, 48 Calif. L. Rev. 383, 388-89 (1960); *Richards/Solove*, 98 Calif. L. Rev., 1887, 1889 et. seq. (2010).

einer vernünftigen Person als in hohem Maße beleidigend empfunden wird.[152] Erhebungen von frei im Internet verfügbaren Daten und ihre Weiterreichung werden jedoch nicht als tatbestandsverwirklichend erachtet, da mit Blick auf die Daten keine Zurückgezogenheit und damit keine berechtigten Privatsphäreerwartungen des Betroffenen bestünden.[153] Etwas anderes kann sich allerdings ergeben, wenn die Daten durch besondere Privatsphäreeinstellungen z.B. in sozialen Netzwerken nicht der gesamten Öffentlichkeit zugänglich sind.[154] Auch das Tort of Publicity given to private life gem. § 652D des Restatement (Second) of Torts ist aus diesem Grunde in der Regel nicht einschlägig.[155] Das Tort of Publicity Placing Person in false light gem. § 652E des Restatement (Second) of Torts hat schon ausweislich seiner Bezeichnung einen gänzlich anderen Anwendungsbereich.

Auch für eine unbefugte kommerzielle Nutzung i.S.d. der appropriation of name or likeness nach § 652C des Restatement (Second) of Torts ist die Datenerhebung und Weitergabe nicht ausreichend, selbst dann nicht, wenn es sich um die Weitergabe von Namen und Email-Adressen zu Zwecken der individuellen Werbeansprache handelt:

> *„The mail box, however noxious its advertising contents often seem to judges as well as other people, is hardly the kind of enclave that requires constitutional defense to protect `the privacies of life.' The short, though regular, journey from mail box to trash can is an acceptable burden, at least so far as the Constitution is concerned."*[156]

Das in einigen Staaten anerkannte Right to Publicity schützt allerdings die „Verwertung" der eigenen Person, in der Regel von Prominenten, und kann damit im Falle der unberechtigten Verwendung ihrer Daten zu Schadenersatzansprüchen führen.[157]

---

[152] *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 274.

[153] Zur berechtigten Privatheitserwartung vgl. auch: *Solove/Schwartz*, Information Privacy Law, 4th ed. 2011, p. 35.

[154] U.S. v. Gines-Perez, 214 F. Supp. 2d 205, 226 (D.P.R. 2002): "While it is true that there is no case law on point regarding this issue, it strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, *without taking any measures to protect the information* (…)Simply expressed, if privacy is sought, then public communication mediums such as the Internet are not adequate forums *without protective measures"*; Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 et seq. (9th Cir. 2002); Pabarcus, 38 Wm. Mitchell L. Rev. 397, 409, 412 et seq. (2011); Kühnl, Persönlichkeitsschutz 2.0, 2016, S. 274 ff.

[155] Vgl. hierzu: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 280 f.

[156] Shibley v. Time, Inc., 45 Ohio App. 2d 69, 72 et seq. (Ohio Ct. App. 1975); *Lamont* v. *Commissioner of MotorVehicles* (1967), 269 et seq. supp. 880; vgl. zu dieser Problematik auch: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 279 f.

[157] *McClurg*, 98 Nw. U.L. Rev. 63, 105 et seq. (2003); *Bergelson*, 37 U.C. Davis L. Rev. 379, 410 (2003); *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 279.

3.4.3.2 CONFIDENTIALITY TORT

Neben den Privacy Torts existiert in den USA auch ein deliktischer Schutz gegen das Offenbaren von Daten in Vertrauensverhältnissen (breach of confidentiality). Dieses Tort ist bei Weitem nicht so ausgeprägt, wie sein Pendant im englischen Recht aber es ist durchaus möglich, Ansprüche auf dieses Tort zu stützen.[158] Erforderlich hierfür ist ein Vertrauensverhältnis (z.B. das Verhältnis Arzt-Patient), in dem Inhalte im Vertrauen auf ihre Geheimhaltung offenbart werden. Werden diese Inhalte an einen Dritten weitergegeben/ihm offenbart, stehen demjenigen, der die Inhalte in dem spezifischen Vertrauensverhältnis offenbart hat, Ansprüche auf Ersatz des aufgrund der Weitergabe/Offenbarung erlittenen Schadens zu.[159] Das Confidentiality Tort ähnelt damit am ehesten unserem deliktischen Geheimnisschutz über § 823 Abs. 2 BGB i.V.m. 203 StGB, aber auch das über § 823 Abs. 1 BGB geschützte Allgemeine Persönlichkeitsrecht schützt in seiner Ausprägung des Indiskretionsschutzes vor einer Offenbarung derartiger Inhalte.[160]

3.4.3.3 TORT OF TRESPASS TO CHATTELS UND CONVERSION

Im Falle einer unautorisierten Nutzung von Daten, insb. im Falle des Screen-Scrapings[161] sprechen die US-amerikanischen Gerichte v.a. in jüngster Zeit außerdem Schadensersatzansprüche wegen des Torts of Trespass to Chattels zu.[162]

> *"Trespass to chattels "lies where an intentional interference with the possession of personal property has proximately cause injury." Trespass to chattels (...) was recently applied to cover the unauthorized use of long distance telephone lines. Specifically, the court noted "the electronic signals generated by the [defendants'] activities were sufficiently tangible to support a trespass cause of action." Thus, it appears likely that the electronic signals sent by BE to retrieve information from eBay's computer system are also sufficiently tangible to support a trespass cause of action. In order to prevail on a claim for trespass based on accessing a computer system, the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff."*[163]

---

158 *Richards/Solove*, 96 Georgetown Law Journal, 123, 158 (2007).

159 *Richards/Solove*, 96 Georgetown Law Journal, 123, 177 (2007).

160 Vgl. dazu: BeckOGK BGB-*Specht*, Stand: 01.08.2017, § 823 Rn. 1082.

161 EBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000); *Glazer et al.*, Practical Law Practice Note 4-532-4243 (2017).

162 Register.com, Inc. v. Verio, Inc., 356 F. 3d 393 (2d Cir. 2004).

163 EBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

Das ursprünglich ebenfalls für körperliche Gegenstände entwickelte Tort of Conversion wird von einigen Gerichten mittlerweile sogar explizit auch auf unkörperliche Güter angewendet. So sollen elektronische Aufnahmen[164] und seismische Daten[165], die auf Computern gespeichert sind, Gegenstand einer Klage aufgrund eines Tort of Conversion sein können.[166]

> *„Although intangible property interests do not strictly satisfy the merger test, which reflects the concept that such interests can be converted only by exercising dominion over the paper document that represents that interest, there is no compelling reason to prohibit conversion for redress of a misappropriation of intangible property. Electronic documents and records stored on a computer can easily be converted by mere computer entries. Because such information is of value regardless of whether the format in which the information is stored is tangible or intangible, the protections of the law should apply equally to both forms--physical and virtual."*[167]

Andere Gerichte lehnen die Anwendbarkeit des tort of Conversion auf elektronische Daten allerdings explizit ab.[168]

Im Einzelfall kann eine zivilrechtliche Klage auch auf eine Verletzung des Computer Fraud and Abuse Act (CFFA) stützen, obwohl es sich bei ihm eigentlich um ein Strafgesetz handelt, 18 USC § 1030 (a)(2)(C) und § 1030 (g):[169]

> *(a) (2) (C) Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer shall be punished (…)*
>
> *(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.*

3.5 VERTRAGSRECHTLICHER UMGANG MIT DATEN

Eine vertragliche Disposition über Daten kann selbst dann erfolgen, wenn keinerlei ausschließlichkeitsrechtliche Rechtspositionen an ihnen existieren.[170] Dies verdeutlicht § 453

[164] Thyroff v. Nationwide Mut. Ins., 8 N.Y. 3d 283 (N.Y. 2007).

[165] In re Yazoo Pipeline Co., LP, 459 B.R. 636 (Bankr. S.D. Tex. 2011).

[166] Vgl. zum Ganzen auch: *Glazer et al.*, Practical Law Practice Note 4-532-4243 (2017).

[167] 8 N.Y. 3d 283 (N.Y. 2007).

[168] Capitol Com´n, Inc. v. Capitol Ministries, 2013 WL 5493013 (E.D.N.C. Oct. 1, 2013); vgl. zum Ganzen auch: *Glazer et al*., Practical Law Practice Note 4-532-4243 (2017).

[169] Vgl. hierzu auch: *Glazer et al.*, Practical Law Practice Note 4-532-4243 (2017).

BGB, der einen Kaufvertrag auch über andere Gegenstände als Sachen und Rechte zulässt. Andere Vertragstypen erfordern ohnehin nicht die Körperlichkeit des Vertragsgegenstands im Sinne des Sachbegriffs des § 90 BGB.[171] Über das Vertragsrecht kann der Umgang mit Daten sehr flexibel gehandhabt,[172] z.B. zwischen den Vertragspartnern auf bestimmte Handlungen beschränkt werden.[173] Wird vertraglich das „Eigentum" an Daten geregelt, ist freilich nicht die vertragliche Verschaffung einer ausschließlichkeitsrechtlichen Rechtsposition gemeint, sondern die Bestimmung desjenigen, der im Vertragsverhältnis bestimmen dürfen soll, wie mit den betreffenden Daten umzugehen ist.[174] Nachteil des Vertragsrechtes ist es, dass es Abwehr- und Regressmöglichkeiten allein gegenüber dem Vertragspartner, nicht aber auch gegenüber Dritten begründet. Dies ist nach US-amerikanischem Recht nicht anders als nach deutschem Recht.[175]

3.5.1 VERTRAGSRECHTLICHER UMGANG MIT DATEN NACH DEUTSCHEM RECHT

3.5.1.1 PRIMÄRER UND SEKUNDÄRER DATENMARKT

Eine vertragliche Disposition über Daten ist nach deutschem Recht aufgrund des weiten Leistungsbegriffs des § 241 BGB[176] durchaus möglich. Der Datenhandel mit nichtpersonenbezogenen Daten lässt sich dabei auch weitgehend problemlos mit den de lege lata bereitstehenden Vertragstypen erfassen, so etwa z.B. über §§ 433, 453 oder § 631 im Falle einer punktuellen und als endgültig intendierten Datenüberlassung ggf. ergänzt um die vorherige Zusammenstellung oder Generierung der Daten, sowie über § 481 BGB im Falle der zeitlich begrenzten Datenüberlassung. Schwieriger ist die Erfassung einer vertraglichen Disposition über personenbezogene Daten. Aufgrund der datenschutzrechtlichen Beschränkung einer Verarbeitung personenbezogener Daten ergeben sich spezifische Probleme aus der erforderlichen Verzahnung von Datenschutz- und Vertragsrecht. Insbesondere die je-

---

170 BGH, Urt. v. 02.07.1996 – X ZR 64/94, NJW 1996, 2924,292; *Roßnagel*, NJW 2017, 10, 11; *Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblytè/Wiedemann*, GRUR Int. 2016, 914, 915.

171 Zu Verträgen über Daten vgl. umfassend: *Hoeren*, Big Data und Recht, 2014, S. 30 ff.

172 Vgl. zu den Möglichkeiten vertraglicher Gestaltung etwa: *Sahl*, PinG 2016, 146, 150; *Assion/Mackert*, PinG 2016, 161 ff.; *Kraus*, Datenlizenzverträge, in: Taeger, Internet der Dinge: Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband 2015, S. 537, 546 ff.; *Roßnagel*, NJW 2017, 10, 12 ff.; *Schefzig*, Die Datenlizenz, in: Taeger, Internet der Dinge: Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband 2015, S. 551, 554 ff.; *Specht*, JZ 2017, 763 ff.

173 Vgl. für das US-amerikanische Recht etwa: ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996).

174 Auf diese Weise sind auch und gerade Verträge nach US-amerikanischem Recht zu verstehen, in denen regelmäßig „the ownership of the data" bestimmt wird, vgl. etwa: *Faulkenberry*, 6 J. Health & Life Sci. L. 119 et seq. (2013); *Glazer et al.*, Practical Law Practice Note 4-532-4243 (2017).

175 Vgl. hierzu z.B. *Mattioli*, ZGE 2017, 299, 307.

176 MüKo BGB-*Bachmann*, 7. Aufl. 2016, § 241 Rn. 18; Jauernig-*Mansel*, Bürgerliches Gesetzbuch, 16. Aufl. 2015, § 241 Rn. 7; HK-BGB-*Schulze*, 9. Aufl. 2017, § 241 Rn. 3.

derzeitige Widerruflichkeit der datenschutzrechtlichen Einwilligung stellt das Vertragsrecht vor Herausforderungen.
Möchte man Verträge über die Überlassung und Verwertung von Daten de lege lata typisieren, ist zunächst zwischen primärem und sekundärem Datenmarkt zu differenzieren. Während der primäre Datenmarkt das Vertragsverhältnis zwischen dem Betroffenen und der datenerhebenden Stelle (Datenerhebungsvertrag) erfasst, bezeichnet der sekundäre Datenmarkt das Vertragsverhältnis zwischen der datenerhebenden Stelle und dem Datenerwerber (Datenüberlassungsvertrag/Datenverwertungsvertrag, sekundärer Datenmarkt).[177]

Auf dem primären Datenmarkt werden Daten als Gegenleistung hingegeben. Handelt es sich um personenbezogene Daten, ist die Erklärung der datenschutzrechtlichen Einwilligung Teil der Gegenleistung, wenn die Auslegung der Willenserklärungen der Vertragsparteien dies ergibt.[178] Als Beispiel genannt werden kann die Erhebung von Daten in Kundenkartenprogrammen oder in sozialen Netzwerken. Die Leistung, für deren Inanspruchnahme Daten und Einwilligung hingegeben werden, ist die Bereitstellung der Nutzungsmöglichkeit des sozialen Netzwerkes.[179] Diese Ansicht scheint sich zwar zunehmend durchzusetzen, ist jedoch nicht unbestritten. Zwar dürfte es schwierig sein, die Willenserklärungen in den benannten oder ähnlichen Geschäftsmodellen anders auszulegen, als dass die Einwilligung vertraglich geschuldete Gegenleistungspflicht ist, weil es dem Datenverarbeiter gerade darauf ankommt, die Daten auch verarbeiten zu dürfen und der Nutzer hierüber regelmäßig informiert wird. Es wird aber durchaus ebenso vertreten, es handele sich um einen Vertrag ohne Gegenleis-

[177] Vgl. hierzu umfassend: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[178] *Linardatos*, Daten als Gegenleistung, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen, nimmt dagegen an, dass es sich bei der Einwilligung um eine Wirksamkeitsvoraussetzung des Vertrags handelt.

[179] Röhricht/Graf von Westphalen/Haas-*Specht*, HGB, Plattformnutzungsverträge, Rn. 21, im Erscheinen; *Bräutigam*, MMR 2012, 635 ff.; *Specht*, JZ 2017, 763 ff.; *Metzger*, AcP 216 (2016), 817 ff.; *Sattler*, JZ 2017, 1036 ff.; *Langhanke/Schmidt-Kessel*, EuCML 2015, 218, 221 ff.; *Schmidt-Kessel/Grimm*, ZfpW 2017, 84 ff.; *Berger*, ZGE 2017, 340, 353; *Hoeren*, Big Data und Recht, 2014, S. 75 ff.; *Intveen*, ITRB 2018, 70 ff.; Bericht der Arbeitsgruppe „Digitaler Neustart" v. 15.05.2017, S. 15 f., 59, abrufbar unter: https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf, zuletzt abgerufen am 10.03.2018; wohl auch: *Faust*, 71. DJT 2016, S. A17 ff.; ebenfalls in diese Richtung neigend: LG Berlin, Urt. v. 22.01.2018 – 16 O 341/15; *Weichert*, Wem gehören die privaten Daten?, in: Taeger/Wiebe, Informatik – Wirtschaft – Recht, Regulierung in der Wissensgesellschaft, Festschrift für Wolfgang Kilian zum 65. Geburtstag, 2004, S. 281, 282, stellte bereits frühzeitig fest, dass eine Kommerzialisierung des Persönlichkeitsrechts durch Datenhandel durch BVerfG, Urt. v. 15.12.1999 – 1 BvR 653/96, NJW 2000, 1021 (*„Das Persönlichkeitsrecht ist nicht im Interesse einer Kommerzialisierung der eigenen Person gewährleistet"*) nicht ausgeschlossen ist; a.A. Hoeren/Sieber/Holznagel-*Redeker*, Multimedia-Recht, 44. EL 2017, Teil 12 Rn. 428; dagegen: Art. 29 Datenschutzgruppe, Guidelines to Consent under Regulation 2016/679 v. 28.11.2017, Dokumentennummer 17/EN WP259, S. 9.

tung[180] oder die Einwilligung stelle sich allein als Wirksamkeitsvoraussetzung in einem Vertrag dar, in dem die Gegenleistung allein in der Hingabe der Daten liege.[181]

Auf dem sekundären Datenmarkt werden bereits erhobene Daten an Drittunternehmen weitergereicht. Zumeist wird hierfür ein wirtschaftlicher Gegenwert erlangt, in der Regel ein Entgelt. Als Beispiele dienen sowohl die klassischen Adresshändler, aber auch andere Unternehmen, in deren Geschäftsbetrieb Daten erhoben werden, die sich entgeltlich an Dritte weiterreichen lassen. Hierzu gehören z.B. Hersteller von smarten Geräten, die Daten über unser Gesundheitsverhalten aufzeichnen und diese z.T. an Versicherungen weiterreichen. Hier bilden Daten in der Regel den Leistungsgegenstand.[182]

3.5.1.2 TYPOLOGIE UND ROLLE DER DATENSCHUTZRECHTLICHEN EINWILLIGUNG

Die Datenüberlassung auf dem sekundären Datenmarkt folgt dem Kaufrecht, dem Werkvertragsrecht oder aber dem Pachtvertragsrecht, je nachdem, ob Daten endgültig überlassen, zunächst generiert und anschließend endgültig überlassen oder zeitlich für eine nur begrenzte Dauer überlassen werden.[183]

Der primäre Datenmarkt ist dagegen schwieriger zu beurteilen. Ist die datenschutzrechtliche Einwilligung sowie die Hingabe der Daten als Gegenleistung geschuldet, wird in der Regel ein Vertrag mit doppeltem Typus vorliegen. Denn die Erklärung der Einwilligung ähnelt aufgrund ihrer Widerruflichkeit[184] dem Lizenzvertrag, der miet- bzw. pachtvertraglichen Regelungen folgt. Die Leistungserbringung ist je nach Ausgestaltung entweder ebenfalls miet- bzw. pachtvertragsrechtlich oder auch dienstvertragsrechtlich zu beurteilen (so bei der Zurverfügungstellung eines Zugangs zu sozialen Netzwerken), kaufvertragsrechtlich (punktuelle und endgültige Überlassung von Software, Musikdateien, E-Books etc.) oder auch nach anderen Vertragstypen.[185] Diese Lösung lässt es zu, dass die jeweils auf Leistung und Gegenleistung passenden Regelungen des Leistungsstörungsrechts zur Anwendung gelangen und

---

[180] Hoeren/Sieber/Holznagel/*Redeker*, Multimedia-Recht, 44. EL 2017, Teil 12 Rn. 428.

[181] *Linardatos*, Daten als Gegenleistung, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, erscheint 2018.

[182] Hierzu eingehend: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[183] *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 119 ff.; zutreffend auch: *Rank*, Daten als Leistungsgegenstand, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

[184] Art. 7 Abs. 3 DS-GVO.

[185] Ebenfalls im Wesentlichen auf die Regelungen des Pachtvertragsrechts abstellend: *Sattler*, JZ 2017, 1036, 1038.

damit z.B. die Folgen des Einwilligungswiderrufes stets unabhängig von der Leistung der Vertragsgegenseite gelöst werden könnten.

Ein solcher Widerruf ist in dieser Lösung vergleichbar mit einer nicht länger erfolgenden Zurverfügungstellung des Miet- bzw. Pachtgegenstands und führt in dieser Lösung daher stets zu einem außerordentlichen Kündigungsrecht gem. § 543 Abs. 2 Nr. 1 BGB.[186] Wird auch die Leistung des Datenverarbeiters im Rahmen eines Dauerschuldverhältnisses erbracht (z.B. im Rahmen von Nutzungsverträgen sozialer Netzwerke), endet das Vertragsverhältnis mit der außerordentlichen Kündigung ex nunc. Wurden endgültig und punktuell digitale Inhalte gegen Überlassung der Daten und Erklärung der Einwilligung zur Verfügung gestellt (so z.B. Software), so sind die erbrachten Leistungen rückabzuwickeln. Erworbene digitale Inhalte sind von demjenigen, der seine Einwilligung widerruft, zu löschen.[187]

Im sekundären Datenmarkt führt der Widerruf der Einwilligung vor Vertragsschluss dazu, dass der Vertrag nach § 134 BGB nichtig ist.[188]

3.5.1.3 PROBLEM DES KOPPELUNGSVERBOTES

Vor ganz erhebliche Probleme stellt das datenschutzrechtliche Koppelungsverbot die vertragliche Ausgestaltung des primären Datenmarktes. Anders als noch nach alter Rechtslage beschränkt die DS-GVO das Koppelungsverbot nicht auf spezifische Bereiche (wie dies etwas § 28 Abs. 3a BDSG a.F. und § 95 Abs. 5 TKG vorsahen), sondern sieht ein allgemeines Koppelungsverbot vor.[189] Dieses allgemeine Koppelungsverbot untersagt es, die Erfüllung eines Vertrags von einer Einwilligung in die Datenverarbeitung abhängig zu machen, die für die Vertragserfüllung nicht erforderlich ist. Eine Einwilligung (und nicht nur die als vertragliche Gegenleistung erklärte Einwilligung) wird aber regelmäßig Daten erfassen, die nicht für das Vertragsverhältnis erforderlich sind, weil für Datenverarbeitungen, die für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich sind, zumindest dann der Erlaubnistatbestand des Art. 6 Abs. 1 lit. b) DS-GVO eingreift, wenn sie auf Anfrage der betroffenen Person erfolgen. Wird die Richtlinie für digitale Inhalte verabschiedet, die „Daten als Gegenleistung“ explizit

---

[186] *Metzger*, AcP 216 (2016), 817, 864; *Specht*, JZ 2017, 763, 768; ähnlich bereits: *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 272; zur anfänglichen Unwirksamkeit der Einwilligung im Vertragsverhältnis vgl. *Specht*, JZ 2017,763 ff.

[187] Zu Lösungsmöglichkeiten bei Schwierigkeiten in der Rückabwicklung vgl. *Specht*, JZ 2017, 763 ff.; zum Ganzen vgl. ausführlich: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts,DGRI Jahrbuch 2017, erscheint 2018.

[188] LG Düsseldorf, Urt. v. 20.12.2013 – 33 O 95/13, ZD 2014, 200 ff.; *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[189] Statt Vieler: BeckOK DatenschutzR-*Stemmer*, 22. Ed. (Stand: 01.08.2017), Art. 7 Rn. 41.

vorsieht, gibt der europäische Gesetzgeber damit außerdem zu erkennen, dass er die Vorgaben der DS-GVO hierdurch modifizieren möchte.

Mit gewichtigen Stimmen aus der Literatur lässt sich aber ohnehin argumentieren, dass nicht jede als Gegenleistung erklärte datenschutzrechtliche Einwilligung per se einen Verstoß gegen das Koppelungsverbot begründen kann. Denn die Freiwilligkeit bezieht sich hier weniger auf die Einwilligung, als auf den Vertrag insgesamt. Der Maßstab, an dem dieses Verhalten zu messen ist, ist daher nicht primär Art. 7 Abs. 4 DS-GVO, sondern vielmehr Art. 102 AEUV bzw. § 19 GWB sowie §§ 134, 138 BGB.[190] Dies scheint auch vor dem Hintergrund korrekt zu sein, dass das Koppelungsverbot vor einer unfreiwilligen Datenverarbeitung schützen will und damit vor einem Fremdzwang. Nicht aber intendiert das Koppelungsverbot einen Schutz vor einer freiwilligen Selbstverpflichtung, wie sie regelmäßig durch eine rechtsgeschäftliche Selbstbindung erfolgt, solange dieser Vertrag nicht unfreiwillig abgeschlossen wird.[191] Zwar ist ErwGr. 43 S. 2, aus dem die Unzulässigkeit der Einwilligungserklärung als Gegenleistungspflicht im Vertrag geschlussfolgert wird („*Die Einwilligung gilt als nicht freiwillig erteilt, wenn (...) die Erfüllung eines Vertrags (...) von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.*)“ bei der historischen und teleologischen Auslegung von Art. 7 DS-GVO zu berücksichtigen, seine Formulierung aber wird man als widerlegliche Vermutung verstehen müssen.[192] Die Erklärung der Einwilligung als Gegenleistung im Vertrag ist daher durchaus möglich, solange Umstände, die die Freiwilligkeit einschränken (z.B. faktische Angewiesenheit auf den entsprechenden Dienst), nicht vorliegen.[193]

3.5.1.4 KLAGBARKEIT DER EINWILLIGUNG UND MÄNGELGEÄHRLEISTUNGSRECHT

Der Widerruf der Einwilligung kann auf dem primären Datenmarkt nicht zu Mängelgewährleistungsrechten führen, möchte man die Einwilligung als Instrument zur Gewährleistung informationeller Selbstbestimmung nicht antasten. Dies muss sich bereits aus dem Schutzzweck der Einwilligung ergeben. Die Einwilligung kann daher weder als Gegenleistung, noch

[190] Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 7 Rn. 21; Kühling/Buchner-*Buchner/Kühling*, DS-GVO, 1. Aufl. 2017, Art. 7 Rn. 48; Gola-*Schulz*, DS-GVO, 1. Aufl. 2017, Art. 7 Rn. 27; a.A. BeckOK DatenschutzR-*Stemmer*, 22. Ed. (Stand: 01.08.2017), Art. 7 Rn. 41; vgl. zu diesem Problemkomplex auch: *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 267 ff.; *Buchner*, DuD 2016, 155, 159; zu dieser Frage auch: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[191] Vgl. hierzu auch: Specht, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[192] *Schneider*, Datenschutz, 2017, S. 143.

[193] Eingehend: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

im Wege der Nacherfüllung klagbar sein.[194] Schadensersatzansprüche können im Falle des Einwilligungswiderrufs nicht entstehen, weil der Betroffene durch das Datenschutzrecht zu einem Vertragsbruch berechtigt ist.[195]

Sind die Daten aus anderen Gründen als der fehlenden Einwilligung im primären Datenmarkt mangelhaft, etwa weil sie die falsche Person betreffen, oder veraltet sind, kann der Datenschuldner aber sehr wohl entsprechend den anwendbaren Mängelgewährleistungsrechten in Anspruch genommen werden.[196]

Auf dem sekundären Datenmarkt ist der Datenüberlassungsvertrag ohne das Vorliegen der datenschutzrechtlichen Einwilligung gem. § 134 BGB nichtig.[197] Einen Rechtsmangel der Daten begründet es, wenn die Einwilligung in die Datenübermittlung zwar vorliegt, die Einwilligung in die vom Datenerwerber angestrebte Datenverarbeitung aber widerrufen wird oder bereits anfänglich nicht vorliegt, etwa, weil die Art der Datenverarbeitung nicht von der Einwilligung gedeckt ist (Speicherung auf Servern im Ausland, Auswertung etc.). Dürfen die Daten aufgrund datenschutzrechtlicher Verpflichtungen nicht mehr verarbeitet werden, z.B. weil der Grundsatz der Speicherbegrenzung dies ab einem bestimmten Zeitpunkt untersagt, oder die Zweckbindung der Daten den vom Datenerwerber angestrebten Zweck nicht erfasst, liegt ebenfalls ein Rechtsmangel vor, sofern dies bei Gefahrübergang absehbar und vertraglich nicht adressiert ist.[198]

Im sekundären Datenmarkt können Daten weiterhin mangelhaft sein, weil sie veraltet sind oder sich auf die falsche Person beziehen, oder auch dann, wenn Kontrolldaten in einen Datensatz aufgenommen werden (bewusst unzutreffende, eindeutig wiederzuerkennende Daten, die der Kontrolle dienen, ob nach Beendigung eines Vertragsverhältnisses ein Datensatz weitergenutzt wird) und eine entsprechende Vereinbarung im Kaufvertrag fehlt. Dies kann

---

[194] So auch: *Langhanke/Schmidt-Kessel*, EuCML 2015, 218, 221; *Schmidt-Kessel/Grimm*, ZfpW 2017, 84, 103; a.A. unter Verweis darauf, dass als Naturalobligationen allein solche Leistungen ausgestaltet sind, die der Gesetzgeber im Grundsatz missbilligt: *Sattler*, JZ 2017, 1036, 1040, wobei dieser Vergleich nur eingeschränkt trägt, denn missbilligen will der Gesetzgeber jedenfalls solche Einwilligungen, die auf nicht ausreichend informierter Grundlage erfolgen, was im Netz regelmäßig der Fall ist; *Sattler*, JZ 2017, 1036, 1040 weist zwar zutreffend darauf hin, dass dies möglicherweise einen falschen Anreiz für die datenerhebenden Unternehmen setzt, die Daten möglichst schnell, möglichst umfangreich wirtschaftlich zu auszuwerten und weiterzureichen. Dieser Anreiz besteht aber ohnehin aufgrund des erheblichen ökonomischen Wertes personenbezogener Daten selbst bei Klagbarkeit der datenschutzrechtlichen Einwilligung.

[195] So zutreffend: *Schmidt-Kessel/Grimm*, ZfpW 2017, 84, 103.

[196] *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[197] LG Düsseldorf, Urt. v. 20.12.2013 – 33 O 95/13, ZD 2014, 200 ff.; *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[198] *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

zur Mangelhaftigkeit des gesamten Datensatzes führen. Weiter ist denkbar, dass zu wenig Daten geliefert werden und dies eine Mangelhaftigkeit des Datensatzes begründet.[199]

[199] *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

3.5.2 VERTRAGSRECHTLICHER UMGANG MIT DATEN IM US-AMERIKANISCHEN RECHT

Das Common Law stellt wesentlich geringere Anforderungen an den vertragsrechtlichen Umgang mit Daten, als das deutsche Recht. Da der Datenschutz in den USA weniger hochgehalten wird, als in Deutschland und Europa und insbesondere kein generelles Einwilligungserfordernis in die Datenverarbeitung existiert, können Daten im US-amerikanischen Rechtsraum sowohl im Kontext vertraglicher Leistungspflichten, als auch als Gegenleistung geschuldet sein. Es gilt aber, im Common-Law-Vertragsrecht einige grundsätzliche Anforderungen zu beachten:

3.5.2.1 CONSIDERATION

Dem US-amerikanischen Vertragsrecht liegt der Gedanke zugrunde, dass ein Versprechen nur dann rechtlich durchsetzbar ist, wenn es aufgrund einer Gegenleistung (consideration) gegeben wird.[200] Diese consideration kann zwar im Grundsatz in jedem erdenklichen Tun oder Unterlassen bestehen:

> *„A valuable consideration, in the sense of the law, may consist either in some right, interest, profit, or benefit accruing to the one party, or some forbearance, detriment, loss, or responsibility, given, suffered or undertaken by the other."*[201]

Es sind aber spezifische Anforderungen an sie zu stellen. Sie muss nicht zwingend angemessen, jedoch rechtmäßig sein und darf weder in einer schon in der Vergangenheit erbrachten Gegenleistung („past consideration"), noch in einer bereits bestehenden Verpflichtung (pre-existing duty) bestehen.[202] Zwar existieren Ausnahmen zu diesen Grundsätzen, die jedoch hier nicht weiter relevant sind.[203] Im bilateral contract stehen sich zwei Versprechen gegenüber, sodass jedes die Gegenleistung für das andere bietet. Daneben ist es aber auch möglich, dass eine consideration in einer tatsächlichen Handlung liegt, z.B. im Versenden einer Ware.[204] Das Versprechen wird hier durch die Erbringung der Leistung bindend (unilateral contract). Ersetzt werden kann die consideration durch die sog. detriminal reliance, die eine

---

[200] *Hay*, US-amerikanisches Recht, 6. Aufl. 2015, S. 119 ff.; *Engle*, US contract law for German Jurists, 2013, p. 35 et seq.; *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 28 f.

[201] Currie v. Misa (1875) LR 10 Ex 153.

[202] *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 30; *von Bernstorff*, Einführung in das englische Recht, 4. Aufl. 2011, S. 49.

[203] Vgl. insb. die Nachweise bei *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 28 ff.

[204] *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 31; im Falle des Warenkaufs kann im Leistungsbeginn allerdings auch ein konkludentes Gegenversprechen gesehen werden, vgl. UCC, § 2-206 (1) comment 3.

Bindungswirkung auch einseitiger Versprechen anordnet, wenn nur so ein ungerechtes Ergebnis vermieden werden kann. Sie erinnert insofern an die equity[205] und unterliegt ähnlichen Grundsätzen.[206]

Auch im Verzicht auf einen Teil der Handlungsfreiheit kann eine geeignete Gegenleistung liegen.[207] Denkbar scheint insofern auch der Verzicht auf die Geltendmachung eines Opt-Out hinsichtlich einer Datenverarbeitung. Nicht nur die Hingabe von Daten an sich (unilateral contract), sondern auch das Versprechen hierzu und auch das Versprechen eines Unterlassens der Geltendmachung eines Opt-Out scheinen insofern im US-amerikanischen Vertragsrecht als consideration in Betracht zu kommen.[208]

3.5.2.2 SONDERREGELUNGEN FÜR DEN WARENKAUF

Die Sonderregelungen des Uniform Commercial Code (UCC), die für Warenkäufe gelten, sind nicht auf „information not associated with goods" anwendbar.[209] Da das US-amerikanische Recht jedenfalls nicht konsequent zwischen Daten und Informationen trennt, sind damit wohl auch und gerade Daten nicht vom Anwendungsbereich des Uniform Commercial Code (UCC) erfasst. Sowohl Software,[210] als auch Smart Products – wie z.B. Connected Cars – können hingegen in den Anwendungsbereich des UCC fallen.[211]

3.5.2.3 ANSPRÜCHE BEI NICHTERFÜLLUNG

Im Falle der Nichterfüllung einer vertraglichen Verpflichtung ist im Grundsatz regelmäßig Schadensersatz geschuldet. Ob dies gleichermaßen bei Geltendmachung eines Opt-Outs, bzw. bei Nichthingabe von als Leistung oder Gegenleistung geschuldeten personenbezogenen Daten gelten kann, ist – soweit ersichtlich – im US-amerikanischen Recht weder gerichtlich entschieden, noch Gegenstand der Diskussion in der Literatur. Auf Erfüllung kann der Nichtleistende allerdings ohnehin nur dann in Anspruch genommen werden, wenn der Rechtsschutz aus dem Common Law unzureichend ist und sich eine Erzwingung des Tuns oder Unterlassens daher aus der equity ergibt.[212] Regelmäßige Rechtsfolge ist dies nicht. Ein

---

[205] Bei der equity handelt es sich im Wesentlichen um Regelungen, die das Common Law ergänzen und v.a. dem Ausgleich besonderer Härten dienen.

[206] Vgl. dazu umfassend: *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 32 ff.

[207] Hamer v. Sideway, 27 N.E. 256 (N.Y. 1891); vgl. auch: *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 31.

[208] In diese Richtung für das englische Recht auch: *Millard*, Cloud Computing Law, 2013, 3.1 sowie 3.2.6.

[209] Vgl. § 2-103 (1)(k) UCC, sowie comment 7.

[210] Specht v. Netscape, 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d. Cir. 2002).

[211] Vgl. § 2-103 (1)(k) UCC, sowie comment 7; einen Überblick über die wichtigsten Regelungen des UCC gibt: *Hay*, US-amerikanisches Recht, 6. Aufl. 2015, S. 126 ff.

[212] *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 54.

wichtiges Beispiel aber ist die Möglichkeit der Inanspruchnahme auf Leistung bei Einzigartigkeit der Kaufsache.[213] Dies ließe sich auch auf Daten übertragen, die jedenfalls dann, wenn es sich um personenbezogene Daten handelt, in Bezug auf die Person, über die auf semantischer Ebene etwas ausgesagt werden soll, häufig einzigartig sein werden.

Im Rahmen eines Schadensersatzanspruches verlangt werden kann der Wert der nichterbrachten Leistung abzüglich des Wertes der Gegenleistung (actual damages) sowie der Schaden, den der Vertragsbruch darüber hinaus verursacht hat (consequential damages).[214] Auch der Vertrauensschaden sowie ein sog. nomineller Schaden können ersetzt werden, bedürfen hier aber nicht der weiteren Ausführung. Strafschadensersatzansprüche (punitive damages) können entstehen, wenn die Nichtleistung zugleich eine unerlaubte Handlung (Tort) verwirklicht.[215]

[213] *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 58 m.w.Nachw.

[214] *Engle*, US contract law for German Jurists, 2013, p. 107 et seq.; *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 56.

[215] *Engle*, US contract law for German Jurists, 2013, p. 126 et seq.; *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 56 ff.

3.6 BEREICHERUNGSRECHTLICHER UMGANG MIT DATEN

3.6.1 BEREICHERUNGSRECHTLICHER ZUWEISUNGSGEHALT

Bereicherungsrechtlich kommt im Falle eines nichtigen Vertrags über die Überlassung von Daten und die Einwilligung in ihre Verarbeitung zunächst ein Anspruch auf Herausgabe der faktischen Herrschaftsposition über die Daten in Betracht. Diese kann ein Vermögenswert sein, der über das Bereicherungsrecht kondiktionsfähig ist.[216] Konkret handelt es sich um einen Anspruch aus Leistungskondiktion. Er ist auf Wertersatz gerichtet, wenn eine Herausgabe in natura ausscheidet.[217]

Auch eine Eingriffskondiktion kommt in Betracht, wenn keine Leistungsbeziehung vorliegt. Im Fall von personenbezogenen Daten ergibt sich dies insbesondere bei Vorliegen einer Zwangskommerzialisierung, z.B. dann, wenn personenbezogene Daten ohne die Einwilligung des Betroffenen zur Erzielung von Einnahmen eines Dritten verwendet werden. Denn persönlichkeitsrechtlich determinierten Gütern, wie etwa dem Eigenbild, hat der BGH schon früh einen bereicherungsrechtlichen Zuweisungsgehalt zugesprochen.[218] Kommt es zur ungefragten kommerziellen Verwertung des Persönlichkeitsbestandteils (der Stimme, dem Bildnis etc.), stehen dem Betroffenen insofern Ansprüche aus Eingriffskondiktion zu. Ob dies auch für andere Persönlichkeitsdetails gelten kann, ist zwar streitig,[219] dem Argument, den persönlichkeitsrechtlich determinierten Gütern fehle es mangels vermögensrechtlicher Ausgestaltung insgesamt an einem bereicherungsrechtlichen Zuweisungsgehalt, folgt aber jedenfalls der BGH nicht. Maßgeblich sollte es darauf ankommen, ob die persönlichkeitsrecht-

---

[216] Stellungnahme des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht zur Frage des „Eigentums“ an Daten und Informationen, Stellungnahme 75/2016, S. 7.

[217] Vgl. hierzu: *Börding/Jülicher/Röttgen/v. Schönfeld*, CR 2017, 134, 134 f.

[218] BGH, Urt. v. 08.05.1956 - I ZR 62/54, GRUR 1956, 427 - *Paul Dahlke*; vgl. auch: BGH, Urt. v. 26.10.2006 - I ZR 182/04, GRUR 2007, 139; vgl. hierzu eingehend: *Hermann*, Der Werbewert der Prominenz, 2012.

[219] *Mestmäcker*, JZ 1958, 521, 525; *Raiser* JZ 1961, 465, 470 f.; BeckOK BGB-*Wendehorst*, 44. Ed. (Stand: 01.11.2017), § 812 Rn. 130; *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 361 ff.; *ders.* UFITA 39 (1963), 223 ff.; *Schwerdtner*, Das Persönlichkeitsrecht in der deutschen Zivilrechtsordnung, 1977, S. 241 ff.; NK-BGB-*v. Sachsen Gessaphe*, 3. Aufl. 2016, § 812 Rn. 86; *Canaris*, Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, in: Ahrens/von Bar/Fischer/Spickhoff/Taupitz, Festschrift für Erwin Deutsch zum 70. Geburtstag, 1999, S. 85, 88 m.w.Nachw.; *Funkel*, Schutz der Persönlichkeit durch Ersatz immaterieller Schäden in Geld, 2001, S. 168 ff.; *Kläver*, Bereicherungsrechtliche Ansprüche bei einer Verletzung des allgemeinen Persönlichkeitsrechts, 1999, S. 61 ff.; *Klüber*, Persönlichkeitsschutz und Kommerzialisierung, 2007, S. 122 f.; *Schlechtriem*, Bereicherung aus fremdem Persönlichkeitsrecht, in: Fischer/Gessler/Schilling, Strukturen und Entwicklungen im Handels-, Gesellschafts- und Wirtschaftsrecht: Festschrift für Wolfgang Hefermehl zum 70. Geburtstag, 1976, S. 445, 449 ff.; *Siemes*, AcP 201 (2001), 202. 219 ff.; *Balthasar*, NJW 2007, 664.

lich determinierten Güter einer kommerziellen Verwertung zugänglich sind.[220] Der bereicherungsrechtliche Zuweisungsgehalt betrifft dann eben diesen kommerziell verwertbaren Aspekt des persönlichkeitsrechtlich determinierten Gutes. Hat der Einzelne die Freiheit, über die Darstellung seiner Persönlichkeit zu bestimmen, kann er diese Bestimmung auch von der Zahlung eines Entgelts abhängig machen.[221] Insofern kommt neben dem Recht am eigenen Bild, dem Namensrecht, dem Recht am eigenen Wort (etc.) auch dem informationellen Selbstbestimmungsrecht ein bereicherungsrechtlicher Zuweisungsgehalt zu.[222]

3.6.2 ERLANGTES ETWAS UND FIKTIVE LIZENZGEBÜHR

Erlangt hat der ungefragt kommerziell Verwertende die Nutzungsmöglichkeit des Persönlichkeitsbestandteils, für die er nach den Grundsätzen der Lizenzanalogie Wertersatz leisten muss, § 818 Abs. 3 BGB.[223] Erforderlich ist hierfür nicht, dass der Betroffene zur Lizenzierung bereit war.[224] Denn

> *„der Zahlungsanspruch fingiert nicht eine Zustimmung des Betroffenen, er stellt vielmehr den Ausgleich für einen rechtswidrigen Eingriff in eine dem Betroffenen ausschließlich zugewiesene Dispositionsbefugnis dar."*[225]

Problematisch wird regelmäßig die Berechnung des Betrags sein, der für eine Datennutzung im Regelfall hätte bezahlt werden müssen. Er entspricht im Grundsatz jenem Entgelt, das der kommerzielle Verwerter hätte entrichten müssen, um die Einwilligung des Klägers zur Verwendung der ihn betreffenden personenbezogenen Daten zu erhalten.[226]

---

[220] NK-BGB-*v. Sachsen Gessaphe*, 3. Aufl. 2016, § 812 Rn. 86; *Canaris*, Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, in: Ahrens/von Bar/Fischer/Spickhoff/Taupitz, Festschrift für Erwin Deutsch zum 70. Geburtstag, 1999, S. 85, 88; *Funkel*, Schutz der Persönlichkeit durch Ersatz immaterieller Schäden in Geld, 2001, S. 173 ff.; *Kläver*, Bereicherungsrechtliche Ansprüche bei einer Verletzung des allgemeinen Persönlichkeitsrechts, 1999, S. 61 ff.; *Klüber*, Persönlichkeitsschutz und Kommerzialisierung, 2007, S. 122 f.; Prütting/Wegen/Weinreich-*Prütting*, BGB, 13. Aufl. 2018, § 812 Rn. 62; *Siemes*, AcP 201 (2001), 202, 219 ff.

[221] MüKo BGB-*Schwab*, 7. Aufl. 2017, § 812 Rn. 313.

[222] So auch: *Schmidt-Kessel/Grimm*, ZfpW 2017, 84, 105; vgl. zum bereicherungsrechtlichen Zuweisungsgehalt auch: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[223] Statt vieler: BGH, Urt. v. 26.10.2006 – I ZR 182/04, NJW 2007, 689, 690 – *Rücktritt des Finanzministers*; Dreier/Schulze-*Specht*, Urheberrechtsgesetz, 6. Aufl. 2018, §§ 33 ff. KUG Rn. 14 ff. m.w.Nachw.

[224] Ausdrückliche Aufgabe der vormaligen Rechtsprechung: BGH, Urt. v. 26.10.2006 – I ZR 182/04, NJW 2007, 689, 690 – *Rücktritt des Finanzministers*; a.A. noch BGH, Urt. v. 14.02.1958 – I ZR 151/56, GRUR 1958, 408 – *Herrenreiter*; BGH, Urt. v. 18.03.1959 – IV ZR 182/58, GRUR 1959, 430 - *Caterina Valente*.

[225] BGH, Urt. v. 26.10.2006 – I ZR 182/04, NJW 2007, 689 Tz. 12 – *Rücktritt des Finanzministers*; BGH, Urt. v. 01.12.1999 – I ZR 226/97, GRUR 2000, 715, 717 ff. – *Der blaue Engel*.

[226] Vgl. OLG Hamburg, Urt. v. 09.11.2004 – 7 U 18/04, ZUM 2005, 164, 167.

Denn der Wert von Daten und damit auch der Betrag, den der kommerzielle Verwerter für die Datenverwertung zu zahlen bereit ist, bestimmt sich nicht objektiv, sondern im Zusammenhang mit der konkreten Art der Verwertung sowie subjektiv für den jeweiligen Verwender. Dasselbe Problem ergibt sich jedoch auch im Falle der kommerziellen Verwertung anderer Persönlichkeitsmerkmale so auch im Falle des Rechts am Eigenbild. Die fiktive Lizenzgebühr ist im Zweifel gem. § 287 ZPO vom Gericht unter Berücksichtigung aller Einzelfallumstände zu schätzen.[227] Zu berücksichtigen sein sollten insbesondere die Art und die Vielfalt der Auswertung sowie die Auswertungsdauer.

3.6.3 ANSPRUCH AUF GEWINNHERAUSGABE

Interessant sein kann insbesondere bei der Verarbeitung personenbezogener Daten ohne Einwilligung des Betroffenen auch ein möglicher Gewinnherausgabeanspruch. Anerkannt ist, dass sich im Falle der nicht konsentierten Verwendung von Persönlichkeitsbestandteilen ein Geldentschädigungsanspruch ergeben kann, bei dessen Berechnung auch der mit der Persönlichkeitsrechtsverletzung erzielte Gewinn zu beachten ist.[228] Hier werden indes zwei Dinge miteinander vermischt: Die Geldentschädigung dient allein zum Ausgleich der Verletzung von immateriellen Bestandteilen des Persönlichkeitsrechts. Wird gerade durch die Persönlichkeitsrechtsverletzung aber die Auflage einer Zeitschrift etc. und damit auch der Gewinn des Datenverwerters gesteigert, so wird das Persönlichkeitsrecht des Betroffenen werblich verwendet. Damit sind die kommerziellen Bestandteile des Persönlichkeitsrechts betroffen, deren Verletzung unter den erhöhten Voraussetzungen der verschärften Haftung nach §§ 818 Abs. 4, 819 Abs. 1 BGB einen separaten Gewinnabschöpfungsanspruch begründet. Denn der Verweis des § 818 Abs. 4 auf die „allgemeinen Vorschriften“ meint zwar zunächst die §§ 291, 292 BGB, die wiederum überwiegend weiter in die Vorschriften des Eigentümer-Besitzer-Verhältnisses verweisen. Soweit die §§ 987 ff. eine Regelung enthalten, ist eine Anwendung der §§ 280 ff. neben § 292 Abs. 1, § 989 – aus Spezialitätsgründen gesperrt. Soweit die §§ 987 ff. aber keine Regelung enthalten, darf auf das allgemeine Schuldrecht zurückgegriffen werden.[229] Das gilt nach umstrittener aber zutreffender Ansicht auch für die *Herausgabe von Surrogaten* i.S.v. § 285,[230] der nach h.M. auch das commodum ex negotiatione cum re (den mit der geschuldeten Sache erzielten Erlös) erfasst und damit den

[227] So bereits zutreffend: OLG Hamburg, Urt. v. 09.11.2004 – 7 U 18/04, ZUM 2005, 164, 167.

[228] BGH, Urt. v. 15.11.1994 – VI ZR 56/94, NJW 1995, 861, 865 a.E – *Caroline von Monaco*; *Prinz*, NJW 1996, 953 ff.

[229] BeckOK BGB-*Wendehorst*, 44. Ed. (Stand: 15.06.2017), § 818 Rn. 84.

[230] BGH, Urt. v. 25.03.1982 – VII ZR 60/81, NJW 1982, 1585.

Weg für einen Gewinnabschöpfungsanspruch ebnet.[231] Gilt dies für andere Bestandteile des Persönlichkeitsrechts, so ist kein Grund ersichtlich, dies auch für das Informationelle Selbstbestimmungsrecht anzunehmen. Die Höhe des abzuschöpfenden Gewinns ist nach § 287 ZPO zu schätzen.[232]

3.6.4 UNJUST ENRICHMENT IM US-AMERIKANISCHEN RECHT

Im deutschen Recht hat das Bereicherungsrecht zwar eine wesentlich größere Bedeutung, auch das US-amerikanische Recht aber kennt das sog. unjust enrichment. Gemeint sein kann mit dieser Bezeichnung sowohl das allgemeine Billigkeitsprinzip, das die Idee der Restitution trägt, als auch ein konkreter Anspruchsgrund, wenn nicht die Rückabwicklung von Verträgen und auch nicht die Sanktionierung von Torts ausgesprochen werden soll, sondern aus anderen Gründen eine Bereicherung vorliegt, etwa aufgrund einer fehlgeleiteten Zahlung.[233]

---

[231] Hierzu bereits eingehend: *Canaris*, Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, in: Ahrens/von Bar/Fischer/Spickhoff/Taupitz, Festschrift für Erwin Deutsch zum 70. Geburtstag, 1999, S. 85, 91 ff.; BeckOK BGB-*Unberath*, 44. Ed. (Stand: 01.03.2011), § 285 Rn. 10; zum Streitstand umfänglich: BeckOGK BGB-*Dornis*, § 285 Rn. 71 ff.; NK-BGB-*Dauner-Lieb*, 3. Aufl. 2016, § 285 Rn. 9; BGH, Urt. v. 27.10.1982 – V ZR 24/82, NJW 1983, 929, 930; MüKo BGB-*Emmerich*, 7. Aufl. 2016, § 285 Rn. 22 f. m.w.Nachw.

[232] Für einen Gewinnabschöpfungsanspruch auch: *Schmidt-Kessel/Grimm*, ZfpW 2017, 84, 105.

[233] *Reimann*, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, S. 75.

4. GRENZEN EINES ZIVILRECHTLICHEN UMGANGS MIT DATEN DE LEGE LATA

Unabhängig davon, ob sich generalisierende oder sektorspezifische Rechtspositionen an Daten begründen lassen oder ob es auch zukünftig bei einem vertragsrechtlichen Umgang mit Daten bleibt, ohne dass Verfügungs- oder Zugriffsrechte zugeordnet werden, so unterliegt der Umgang mit Daten Grenzen. Hierbei zu nennen ist insbesondere das informationelle Selbstbestimmungsrecht, das Schutz durch die Datenschutz-Grundverordnung, das BDSG-neu sowie landes- und bereichsspezifische datenschutzrechtliche Regelungen erfährt. Diese Begrenzung des Umgangs mit Daten kann ganz erheblich ausfallen. Insbesondere im Bereich der Big-Data-Analyse fragt sich, ob es durch den Schutz der informationellen Selbstbestimmung nicht zu einer nahezu vollumfänglichen Entleerung von ausschließlichkeitsrechtlichen oder vertragsrechtlichen Befugnissen an Daten kommt.[234] Gleiches gilt für die Begrenzung möglicher Befugnisse an Daten durch Zugangsrechte.

4.1 BEGRENZUNG DURCH ZUGANGSRECHTE

In bestimmten privatwirtschaftlichen Sektoren aber auch gegenüber der öffentlichen Hand[235] bestehen schon heute Zugriffsrechte auf Daten, so etwa für sogenannte „in-vehicle"-Daten im vernetzten Auto,[236] um nachgelagerte Märkte, wie etwa den für Wartungs- und Reparaturdienstleistungen zu ermöglichen.[237] Auch die Payment Services Directive[238] enthält in Art. 67 Zugangsrechte u.a. des Zahlungsdienstnutzers zu Zahlungskontoinformationen[239] und kartellrechtlich werden Zugangsrechte in Form von Zwangslizenzen gewährt, wenn eine Verweigerung der Lizenzierung den Missbrauch einer marktbeherrschen-

---

234 *Specht*, GRUR Int. 2017, 1040 ff.

235 Z.B. nach den Informationsfreiheitsgesetzen. Sie werden hier aber nicht weitergehend erörtert, da dies nicht vom Gutachtenauftrag umfasst ist.

236 Verordnung (EG) Nr. 715/2007 des Europäischen Parlaments und des Rates vom 20. Juni 2007 über die Typengenehmigung von Kraftfahrzeugen hinsichtlich der Emission von leichten Personenkraftwagen und Nutzfahrzeugen (Euro 5 und 6) und über den Zugang zu Reparatur- und Wartungsinformationen für Fahrzeuge, ABl. EU 2007 v. 29.06.2007, Nr. L 171/1.

237 Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD(2017) 2 final, p. 25.

238 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABl. EU 2015 v. 23.12.2015, Nr. L 337/35.

239 Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABl. EU 2015 v. 23.12.2015, Nr. L 337/35.

den Stellung darstellt, Art. 102 AEUV.[240]

Auch wenn aktuell noch keine Fälle vorliegen, in denen über einen Zugangsanspruch zu Daten aus kartellrechtlicher Perspektive entschieden wurde, so wird jedenfalls bei der Bewertung der Marktstellung eines Unternehmens mittlerweile auch sein Zugang zu wettbewerbsrelevanten Daten berücksichtigt, § 18 Abs. 3a GWB.[241]

Im US-amerikanischen Recht gelten ähnliche Grundsätze für die compulsory licenses.[242] Im vernetzten Fahrzeug sind außerdem Zugriffsrechte zu Zwecken von Reparatur- oder auch von Emissionsprüfungen zu gewährleisten.[243] Auch im Medizinbereich existieren sektorspezifische Zugangsrechte.[244]

---

[240] EuGH, Urt. v. 29.04.2004 - C-418/01, ECLI:EU:C:2004:257 = MMR 2004, 456 – *IMS Health*; EuGH, Urt. v. 06.04.1995 - C-241/91 P und C 242/91 P, ECLI:EU:C1995:98 = GRUR Int 1995, 490 – *RTE und ITP/Kommission*; EuG, Urt. v. 17.09.2007 – T-201/04, ECLI:EU:T:2007:289 – *Microsoft*; EuGH, Urt. v. 16.7.2015 – C-170/13, ECLI:EU:C:2015:477 = GRUR 2015, 764 – *Huawei Technologies*; vgl. zum Missbrauch einer marktbeherrschenden Stellung in datenrelevanten Fällen umfassend: *Drexl*, Designing Competitive Markets for Industrial Data -Between Propertisation and Access, 2016, MPI for Innovation & Competition ResearchPaper No. 16-13, abrufbar unter: https://ssrn.com/abstract=2862975, S. 44 ff., zuletzt abgerufen am 23.04.2018.

[241] Vgl. hierzu etwa: *Paal/Hennemann*, NJW 2017, 1697, 1699; *Körber*, NZKart. 2016, 303 ff.; *ders.* NZKart. 2016, 348 ff.; *Beisenherz*, DuD 2015, 600 ff.

[242] Vgl. aus der umfangreichen Literatur insb. *Makous/Hamilton*, 2014 WL 1234517 (2014) m.w.Nachw. auch aus der Rechtsprechung.

[243] *Determann/Perens*,32 Berkeley Tech. L. J. 915, 978 (2017); abrufbar unter: http://btlj.org/data/articles2017/vol32/32_2/32_2_fullFile_web.pdf, zuletzt abgerufen am 21.02.2018.

[244] Vgl. hierzu etwa: *Evans*, 24 Health Matrix 11 (2014).

4.2 BEGRENZUNG DURCH DAS DATENSCHUTZRECHT

4.2.1 DATENSCHUTZ NACH DEUTSCHEM UND EUROPÄISCHEM RECHT

Der nationale Datenschutz richtet sich ab dem 25.05.2018 nach der Datenschutz-Grundverordnung (DS-GVO) sowie dem BDSG-Neu und weiteren bereichsspezifischen Regelungen.[245] Auch die Vorgaben der E-Privacy-Verordnung sind zu beachten, sollte diese verabschiedet werden. Da es sich bei der DS-GVO um eine EU-Verordnung handelt, ist sie gem. Art. 288 Abs. 2 AEUV[246] unmittelbar anwendbar.[247] Sie ändert das datenschutzrechtliche Regelungsregime nicht unwesentlich und soll daher im Folgenden kursorisch erläutert werden. Das nationale Recht hingegen gestaltet im Wesentlichen die Öffnungsklauseln/Spezifizierungsklauseln der DS-GVO aus und ist für die Zwecke dieses Gutachtens daher zu vernachlässigen. Die E-Privacy-Verordnung enthält spezielle Vorgaben zur Gewährleistung der Vertraulichkeit der Kommunikation und erfasst daher die Verarbeitung von Kommunikationsinhalten und Kommunikationsmetadaten,[248] stützt sich aber ebenfalls auf das Prinzip eines Verarbeitungsverbotes dieser Inhalte bzw. Daten, sofern nicht ein Erlaubnistatbestand oder eine Einwilligung der bzw. des Endnutzer(s) vorliegt. Welchen Inhalt die Erlaubnistatbestände letztlich haben werden, ist noch nicht final absehbar, insbesondere ist derzeit noch streitig, ob es einen abwägungsoffenen Erlaubnistatbestand ähnlich Art. 6 Abs. 1 lit. f) DS-GVO geben wird.[249]

Die DS-GVO hat das Ziel, das Datenschutzrecht innerhalb der europäischen Union zu vereinheitlichen, es v.a. auf ein gleichrangiges Niveau zu bringen.[250] Auch schon zuvor war das Datenschutzrecht durch die Datenschutzrichtlinie[251] angeglichen, erst die Datenschutz-Grundverordnung aber schafft durch ihre unmittelbare Anwendbarkeit einen tatsächlich in weiten Teilen vereinheitlichten Schutzstandard. Datenschutz ist dabei allerdings kein Selbstzweck, sondern er erfolgt zum Schutz des Persönlichkeitsrechts und der Privatsphäre.[252] Die Datenschutz-Grundverordnung verfolgt dabei einen risikobasierten Ansatz, d.h. sie macht die Beschränkungen und Verbote der Datenverarbeitung von einer Risikoanalyse abhängig.

---

[245] Auch das Kunsturhebergesetz (KUG) trifft gewissermaßen datenschutzrechtliche Regelungen, weil es Vorgaben für Bildnisse und damit Bilddaten enthält.

[246] Vertrag über die Arbeitsweise der Europäischen Union.

[247] *Schantz*, NJW 2016, 1841.

[248] Siehe hierzu auch 2.3

[249] Interinstitutional File: 2017/0003 (COD) v. 11.01.2018, p. 12 et seq.

[250] Schantz/Wolff-*Schantz*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil B, Rn. 198.

[251] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG v. 23.11.1995, Nr. L 281/31.

[252] *Härting*, Datenschutz-Grundverordnung, 2016, S. 34.

Je höher das Risiko für Persönlichkeitsrechte und Privatsphäre durch die Datenverarbeitung ausfällt, desto höher sind die Voraussetzungen für eine Ausnahme vom Verbotsprinzip, desto eher bleibt die Datenverarbeitung gänzlich verboten.[253]

4.2.1.1 ANWENDUNGSBEREICH DER DS-GVO

Gem. Art. 2 Abs. 1 DS-GVO erstreckt sich der sachliche Anwendungsbereich auf die Verarbeitung personenbezogener Daten im bereits erläuterten Sinne (siehe auch unter: 2.2.).[254] Für besonders sensible personenbezogene Daten sind spezielle Regelungen vorgesehen, so etwa in Art. 9 DS-GVO.[255] Umfasst sind Daten zur rassischen und ethnischen Herkunft, zur politischen Meinung sowie zur religiösen oder weltanschaulichen Überzeugung, zur Gewerkschaftszugehörigkeit, genetische sowie biometrische Daten, Gesundheitsdaten und Daten zum Sexualleben oder der sexuellen Orientierung. Die Verarbeitung dieser Daten ist nur unter sehr restriktiven Voraussetzungen möglich, Art. 9 Abs. 2 DS-GVO, § 22 BDSG-neu. Nicht vom sachlichen Anwendungsbereich der DS-GVO erfasst ist allerdings die Verarbeitung personenbezogener Daten zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.[256]

Der Begriff der Datenverarbeitung meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten, so z.B. die Datenspeicherung oder ihre Weitergabe, aber auch ihre Löschung oder anderweitige Vernichtung, vgl. Art. 4 Nr. 2 DS-GVO.

Die Anwendbarkeit der DS-GVO in territorialer Hinsicht ist nicht ausschließlich auf die Europäische Union begrenzt.[257] Ihr räumlicher Anwendungsbereich erstreckt sich auch auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der Union entgeltlich oder unentgeltlich Waren oder Dienstleistungen anzubieten, oder das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt. Auch dann, wenn die Verarbeitung durch einen Verantwortlichen in einem Land erfolgt, das aufgrund völkerrechtlicher Bestimmungen dem Recht eines EU-Mitgliedstaates unterliegt, ist die DS-GVO in territorialer Hinsicht anwendbar.[258]

---

253 Ähnlich: *Härting*, Datenschutz-Grundverordnung, 2016, S. 35.

254 Vgl. Art. 4 Nr. 1 DS-GVO; statt vieler: *Schantz*, NJW 2016, 1841, 1842.

255 Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil D, Rn. 700; Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 9 Rn. 1; Sydow-*Kampert*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 9 Rn. 1.

256 Vgl. Art. 2 Abs. 2 lit. c) DS-GVO, statt vieler hierzu: *Schantz*, NJW 2016, 1841, 1842 f.

257 *Schantz*, NJW 2016, 1841, 1842; *Laue*, ZD 2016, 463, 465.

258 Hierzu eingehend: *Schantz*, NJW 2016, 1841, 1842.

4.2.1.2 DATENSCHUTZRECHTLICHE GRUNDSÄTZE

Die Datenverarbeitung ist verschiedenen Grundsätzen unterworfen, v.a. dem Verbotsprinzip. D.h. eine Datenverarbeitung ist nur dann rechtmäßig, wenn eine Einwilligung in die entsprechende Datenverarbeitung vorliegt oder die Verarbeitung durch einen Erlaubnistatbestand gestattet wird.[259] Weiterhin zu beachten sind der Grundsatz der Rechtmäßigkeit, der Grundsatz von Treu und Glauben sowie der Transparenzgrundsatz (Art. 5 Abs.1 lit. a) DS-GVO), der Zweckbindungsgrundsatz (Art. 5 Abs. 1 lit. b) DS-GVO), der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c) DS-GVO), der Richtigkeit (Art. 5 Abs. 1 lit. d) DS-GVO), der Speicherbegrenzung (Art. 5 Abs. 1 lit e) DS-GVO), der Grundsatz von Privacy by design and default (Art. 25 DS-GVO), der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f) DS-GVO) sowie die Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO. Die wichtigsten datenschutzrechtlichen Grundsätze werden im Folgenden erläutert.

4.2.1.2.1 ZWECKBINDUNGSGRUNDSATZ

Der wesentlichste dieser Grundsätze ist die Zweckbindung der Datenverarbeitung.[260] Gem. Art. 5 Abs. 1 lit. b) DS-GVO bedarf es bei der Datenverarbeitung eines zuvor festgelegten, eindeutigen und legitimen Zweckes. Der Zweckbindungsgrundsatz gilt für Datenverarbeitungen jeglicher Art[261] und ergibt sich bereits aus Art. 8 GRCh. Er ist das beherrschende Prinzip des Datenschutzrechts.[262] Der Zweck darf nicht von der Rechtsordnung missbilligt sein, wobei auch ethische Erwägungen und gesellschaftliche Gewohnheiten zu berücksichtigen sind.[263] Er ist vor der Datenverarbeitung festzulegen, eine Verarbeitung zu noch unbekannten Zwecken scheidet aus.[264] Auch eine pauschale Zweckangabe ist nicht ausrei-

---

[259] Zum Verbotsprinzip vgl. u.a. *Härting*, Datenschutz-Grundverordnung, 2016, S. 80 ff.; Sydow-*Kampert*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 9 Rn. 5

[260] Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil D, Rn. 397; BeckOK DatenschutzR-*Schantz*, 22. Ed. (Stand: 01.02.2017), Art. 5 DS-GVO Rn. 12.

[261] Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil D, Rn. 397.

[262] *Dammann*, ZD 2017, 307, 311; Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 23: *„Dreh- und Angelpunkt"*; BeckOK DatenschutzR-*Schantz*, 22. Ed. (Stand: 01.02.2017), Art. 5 DS-GVO Rn. 13: *„beherrschendes Konstruktionsprinzip"*.

[263] Art. 29 Datenschutzgruppe, Opinion 03/2013 on purpose limitation v. 02.04.2013, 00569/13/EN WP203, S. 20, abrufbar unter: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>, zuletzt abgerufen am 09.09.2017; *Monreal*, ZD 2016, 507, 509; ein rechtlich missbilligter Zweck wäre etwa die Diskriminierung bestimmter Personengruppen aus rassistischen Motiven, vgl. *Helbig*, K&R 2015, 145, 146.

[264] BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, NJW 1984, 419, 422 – *Volkszählung*; BeckOK DatenschutzR-*Schantz*, 22. Ed. (Stand: 01.02.2017), Art. 5 DS-GVO Rn. 13.

chend.[265] Eine Weiterverarbeitung der personenbezogenen Daten zu einem anderen als dem ursprünglichen Zweck ist jedoch möglich.[266] Voraussetzung dafür ist, dass der Weiterverarbeitungszweck mit dem ursprünglichen Zweck vereinbar ist.[267] Für die Prüfung der Vereinbarkeit des ursprünglichen Zwecks mit dem Zweck, der die Weiterverarbeitung rechtfertigt, sind die in Art. 6 Abs. 4 DS-GVO normierten Kriterien heranzuziehen.[268] Eine Weiterverarbeitungsmöglichkeit von personenbezogenen Daten zu einem anderen als dem ursprünglichen Zweck erleichtert Art. 5 Abs.1 lit. b) 2. HS DS-GVO für die dort genannten Zwecke (im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke und statistische Zwecke) vorgesehen.[269]

4.2.1.2.2 GRUNDSATZ DER DATENMINIMIERUNG

Der Grundsatz der Datenminimierung verlangt, dass nach Art und Umfang nur die Daten verarbeitet werden, die für die Erreichung des Zwecks erforderlich sind.[270] Außerdem sind nur so viele Daten zu erheben, wie es der Zweck gebietet.[271] Es darf keine andere und gleichzeitig weniger belastende Möglichkeit gegeben sein, den Zweck, der mit der Datenverarbeitung verfolgt werden soll, zu erreichen.[272] Speicherfristen sind auf das Mindestmaß zu beschränken. Es sind regelmäßige Termine festzulegen, an denen zu kontrollieren ist, ob die Daten noch benötigt werden. Falls dies nicht der Fall ist, sind sie zu löschen. Hier überschneidet sich der Grundsatz der Datenminimierung mit dem Grundsatz der Speicherbegrenzung, und verstärkt diesen.[273]

---

[265] *Culik/Döpke*, ZD 2017, 226, 227; *Bergmann/Möhrle/Herb*, Datenschutzrecht, 50. EL 2016, § 4 Rn. 43; vgl. zum Ganzen auch: *Specht*, GRUR Int. 2017, 1040, 1043 f.

[266] Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 30; Sydow-*Reimer*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 5 Rn. 27; *Monreal*, ZD 2016, 507, 509.

[267] Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 30; *Monreal*, ZD 2016, 507, 509.

[268] Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil D, Rn. 410; BeckOK DatenschutzR-*Schantz*, 22. Ed. (Stand: 01.02.2017), Art. 5 Rn. 21.

[269] *Schantz*, NJW 2016, 1841, 1844; BeckOK DatenschutzR-*Schantz*, 22. Ed. (Stand: 01.02.2017), Art. 5 Rn. 22; Sydow-*Reimer*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 5 Rn. 27.

[270] *Härting*, Datenschutz-Grundverordnung, 2016, S. 28; Sydow-*Reimer*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 5 Rn. 29; BeckOK DatenschutzR-*Schantz*, 22. Ed. (Stand: 01.02.2017), Art. 5 Rn. 34.

[271] Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil D, Rn. 427.

[272] *Härting*, Datenschutz-Grundverordnung, 2016, S. 28.

[273] Vgl. hierzu insb. *Härting*, Datenschutz-Grundverordnung, 2016, S. 28.

4.2.1.2.3 GRUNDSATZ DER RICHTIGKEIT

Der Grundsatz der Richtigkeit verlangt vom Verantwortlichen, personenbezogene Daten auf ihre Richtigkeit hin zu überprüfen.[274] Damit ist nicht nur eine einmalige Prüfung gemeint, sondern eine dauerhafte Prüfung bis zur endgültigen Löschung der personenbezogenen Daten des Betroffenen.[275]

4.2.1.2.4 GRUNDSATZ VON INTEGRITÄT UND VERTRAULICHKEIT

Der Grundsatz von Integrität und Vertraulichkeit verlangt es, Schutzmaßnahmen gegen den unbefugten Zugriff auf die erhobenen personenbezogenen Daten des Betroffenen sowie auf die Systeme, mit denen die Daten verarbeitet werden, zu implementieren.[276] Der Grundsatz von Vertraulichkeit und Integrität wird näher ausgestaltet durch technische und organisatorische Maßnahmen in Art. 32 DS-GVO. Darüber hinausgehende konkrete Sicherheitsmaßnahmen lassen sich aus dem Grundsatz von Vertraulichkeit und Integrität aber wohl nicht ableiten.[277]

4.2.1.2.5 RECHENSCHAFTSPFLICHT

Der Verantwortliche hat gem. Art. 5 Abs. 2 DS-GVO bei jeder Verarbeitung von personenbezogenen Daten die zuvor benannten Grundsätze einzuhalten.[278] Er hat außerdem hierüber Rechenschaft zu leisten, d.h. er hat stets allumfassend das Nötige zu tun, um die Einhaltung der Grundsätze zu gewährleisten und muss dies im Zweifel auch nachweisen können.[279]

4.2.1.2.6 PRIVACY BY DESIGN UND DEFAULT

Nach Art. 25 Abs. 1 DS-GVO trägt der Verantwortliche die Pflicht, Maßnahmen zu treffen, die den Stand der Technik, die Implementierungskosten, die Art des Umfangs, die Umstände, die Zwecke der Verarbeitung, die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten der natürlichen Personen berücksichtigen. Der Verantwortliche

---

[274] Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 40.

[275] Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil D, Rn. 442.

[276] Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil D, Rn. 448; Sydow-*Reimer*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 5 Rn. 47 ff.; BeckOK DatenschutzR-*Schantz*, 22. Ed. (Stand: 01.02.2017), Art. 5 Rn. 35 f.

[277] *Härting*, Datenschutz-Grundverordnung, 2016, S. 29.

[278] Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 51; BeckOK DatenschutzR-*Schantz*, 22. Ed. (Stand: 01.02.2017), Art. 5 Rn. 37.

[279] Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 5 Rn. 52; *Wächter*, Datenschutz im Unternehmen, 5. Aufl. 2017, Rn. 7; Sydow-*Reimer*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 5 Rn. 53.

hat vor und während der Verarbeitung von personenbezogenen Daten die Konformität mit der DS-GVO durch technische Mittel zu gewährleisten.[280] Datenverarbeitungsvorgänge sind so zu programmieren, dass die in Art. 5 DS-GVO normierten Grundsätze, insbesondere der Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c) DS-GVO, eingehalten werden.[281] Der Wortlaut von Art. 25 Abs. 1 DS-GVO nennt als Beispiel einer solchen Maßnahme die Pseudonymisierung. Sinn und Zweck ist es, Datenschutzrisiken durch entsprechende Gestaltung der eingesetzten Technik nachhaltig zu reduzieren.[282]

Der in Art. 25 Abs. 2 DS-GVO normierte Grundsatz „Privacy by Default" ist ein Unterfall des Privacy by design-Grundsatzes und trägt Erkenntnissen Rechnung, wonach Nutzer Voreinstellungen nur in seltenen Fällen aktiv verändern. Daher sind bereits diese Voreinstellungen so auszugestalten, dass möglichst wenig personenbezogene Daten erhoben und verarbeitet werden. Mittels entsprechender Voreinstellungen soll der Gefahr vorgebeugt werden, dass die Betroffenen bei Nichtveränderung der Einstellungen ungewollt Daten preisgeben.[283]

4.2.1.3 EINWILLIGUNG UND ERLAUBNISTATBESTÄNDE

Ist die Datenverarbeitung nur mit Einwilligung oder unter Rückgriff auf einen Erlaubnistatbestand zulässig, so ist insbesondere auf die Regelungen der Art. 6, 7 und 8 DS-GVO zurückzugreifen. Eine Einwilligung muss dabei gem. Art. 7 DS-GVO auf informierter Grundlage erfolgen, d.h. dem Betroffenen müssen alle erforderlichen Informationen zur Verfügung gestellt werden, damit er eine informierte Entscheidung treffen kann.[284] Das Transparenzgebot verlangt nach einer verständlichen Sprache ohne unnötiges technisches oder fremdsprachiges Fachvokabular.[285] Außerdem muss der Einwilligende mindestens 16 Jahre alt sein, um wirksam einwilligen zu können. Eine ausreichende Informiertheit des Nutzers herzustellen, erweist sich in der Praxis häufig als schwierig, weil es durch erhebliche Mengen an Informationen zu einer Informationsüberlastung des Betroffenen kommen kann. Die Einwilligung muss weiterhin frei von Zwang erklärt werden. Dies entfällt, wenn dem Betroffenen keine andere Wahl bleibt, als in die Datenverarbeitung einzuwilligen, er also nicht einmal die Möglichkeit hat, sich gegen eine Einwilligung zu entscheiden.[286] Hier ist insbesondere das bereits

---

[280] *Schantz*, NJW 2016, 1841, 1846.

[281] Schantz/Wolff-*Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil E, Rn. 835 f.; Paal/Pauly-*Martini*, DS-GVO, 2. Aufl. 2018, Art. 25 Rn. 12; Sydow-*Mantz*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 25 Rn. 50; *Baumgartner/Gausling*, ZD 2017, 308, 312.

[282] Sydow-*Mantz*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art 25 Rn. 15.

[283] Paal/Pauly-*Martini*, DS-GVO, 2. Aufl. 2018, Art. 25 Rn. 46; *Baumgartner/Gausling*, ZD 2017, 308, 312.

[284] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 240.

[285] Paal/Pauly-*Ernst*, DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 81.

[286] *Specht*, JZ 2017, 763, 766; VG Berlin, Urt. v. 24.05.2011 – 1 K 133/10, BeckRS 2011, 52814; Roßnagel-*Sonntag*, Handbuch Datenschutzrecht, 2003, Kap. 4.8 Rn. 54; Spindler/Schuster-*Spindler/Nink*, Recht der elektronischen Medien, 3. Aufl. 2015, BDSG, § 4a Rn. 6.

erläuterte Koppelungsverbot zu berücksichtigen. Die Einwilligung ist jederzeit frei widerruflich.

Liegt eine Einwilligung nicht vor, so ist die Verarbeitung personenbezogener Daten gem. Art. 6 Abs. 1 S. 1 lit. b) zulässig, wenn sie der Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Die betroffene Person muss dabei Vertragspartei oder Anfragender bei der Durchführung der vorvertraglichen Maßnahme sein.[287] Außerdem kann eine Datenverarbeitung zulässig sein zur Erfüllung einer rechtlichen Verpflichtung, Art. 6 Abs. 1 S. 1 lit. c) DS-GVO, zum Schutz lebenswichtiger Interessen einer Person (Art. 6 Abs. 1 S. 1 lit. d) DS-GVO) und zur Erfüllung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung von Hoheitsgewalt (Art. 6 Abs. 1 S. 1 lit. e) DS-GVO).

Der wohl bedeutendste Erlaubnistatbestand findet sich in Art. 6 Abs. 1 S. 1, lit. f) DS-GVO. Danach ist eine Datenverarbeitung zulässig, wenn in einer Abwägung mit den Betroffeneninteressen die Interessen des Verantwortlichen an einer Datenverarbeitung überwiegen.

4.2.1.4 BETROFFENENRECHTE

Die Rechte des Betroffenen sind in Kapitel 3 in den Art. 12 – 23 DS-GVO normiert. Es handelt sich vor allem um Informationsrechte gem. Art. 13, 14 DS-GVO, das Auskunftsrecht gem. Art. 15 DS-GVO, das Recht auf Berichtigung fehlerhafter personenbezogener Daten gem. Art. 16 DS-GVO, das Löschungsrecht gem. Art. 17 DS-GVO, das Recht auf Einschränkung der Verarbeitung, Art. 18 DS-GVO, das Recht auf Datenportabilität, Art. 20 DS-GVO sowie um das Widerspruchsrecht gem. Art. 21 DS-GVO. Die Ausübungsmöglichkeit dieser Rechte hat der Verantwortliche – gegebenenfalls auch über die Einrichtung einer entsprechenden technischen Infrastruktur – sicherzustellen.

4.2.1.5 SCHADENSERSATZ UND SANKTIONEN

Jede betroffene Person hat gem. Art. 82 Abs. 1 DS-GVO einen Schadensersatzanspruch, sofern ihr wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entsteht. Voraussetzung ist ein Verstoß gegen die Verordnung, der Eintritt eines Schadens sowie die Kausalität zwischen beiden Erfordernissen.[288] Liegen die Voraussetzungen vor, haftet der Verantwortliche gem. Art. 82 Abs. 2 S. 1 DS-GVO für den entstandenen Schaden, ein Auftragsverarbeiter haftet allerdings gem. Art. 82 Abs. 2 S. 2 DS-GVO nur dann, wenn er gegen eine ihn aus der DS-GVO speziell treffende Pflicht verstößt. Das Vorliegen der Anspruchsvoraussetzungen hat der Geschädigte zu beweisen.[289] Art. 82 Abs. 4 und 5 DS-GVO regeln die gesamtschuldnerische Haftung, wenn mehrere Verantwortliche

[287] Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 6 Rn. 15; BeckOK DatenschutzR-*Albers*, 22. Ed. (Stand: 01.02.2017), Art. 6 Rn. 30.

[288] Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 6 ff.; dazu: *Wybitul/Haß/Albrecht*, NJW 2018, 113.

[289] *Spindler*, DB 2016, 937, 947; *Wybitul/Haß/Albrecht*, NJW 2018, 113, 116.

oder Auftragsdatenverarbeiter den Schaden verursacht haben sowie den daraus folgenden Regressanspruch. Auch die Geltendmachung weiterer Schadensersatzansprüche bleibt dem Verletzten möglich.[290]

Werden die Vorgaben der Datenschutz-Grundverordnung nicht eingehalten, ist gem. Art. 83 DS-GVO auch die Verhängung von Geldbußen möglich.[291] Nach ErwGr. 150 zur DS-GVO handelt es sich dabei um eine verwaltungsrechtliche Sanktion der Aufsichtsbehörde. Art. 83 Abs. 4 – 6 DS-GVO enthält Richtwerte zu ihrer Höhe: 10.000.000 bzw. 20.000.000,00€ oder 2% bzw. 4% des weltweiten Jahresumsatzes eines Unternehmens. Erforderlich ist aber regelmäßig eine Einzelfallprüfung.[292] Art. 83 Abs. 2 DS-GVO gibt Kriterien vor, anhand derer diese Einzelfallprüfung zu erfolgen hat,[293] z.B. Art, Schwere und Dauer des Verstoßes, Verschuldensgrad, Wiederholungsverstöße sowie die Zusammenarbeit mit der Aufsichtsbehörde.[294] Des Weiteren werden von der Aufsichtsbehörde die Kategorien der personenbezogenen Daten, die Art der Kenntniserlangung von dem Datenschutzverstoß sowie die Einhaltung von etwaigen bereits verhängten Abhilfemaßnahmen gem. Art. 58 Abs. 2 lit. a-i) DS-GVO berücksichtigt.[295] Aus Art. 84 DS-GVO folgt, dass die Mitgliedstaaten berechtigt, sind weitere Sanktionen nationalen Rechts vorzusehen.[296]

4.2.2 DATENSCHUTZ NACH US-AMERIKANISCHEN RECHT

Das Recht zur Kontrolle über die eigenen Daten ist ein Kernbestandteil des von *Warren/Brandeis*[297] entwickelten und 1965 vom US Supreme Court anerkannten Right to Privacy.[298] Verfassungsrechtlich wird dabei v.a. das Interesse des Einzelnen an der Geheimhaltung privater Angelegenheiten geschützt (interest in avoiding disclosure of personal matters).[299] Ob auch ein Right to Information Privacy anzuerkennen ist, wie dies insbesondere

---

[290] Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil F, Rn. 1246; Paal/Pauly-*Frenzel*, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 20; zur Sperrwirkung: Sydow-*Kreße*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 82 Rn. 27.

[291] *Neun/Lubitzsch*, BB 2017, 1538, 1540; vgl. auch: *Keppeler/Berning*, DStR 2018, 91.

[292] *Grünwald/Hackl*, ZD 2017, 556, 557; Sydow-*Popp*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 83 Rn. 11; vgl. auch: *Keppeler/Berning*, DStR 2018, 91.

[293] *Neun/Lubitzsch*, BB 2017, 1538, 1541.

[294] *Grünwald/Hackl*, ZD 2017, 556, 557; BeckOK DatenschutzR-*Holländer*, 22. Ed. (01.11.2017), Art. 83 Rn. 31 ff.

[295] *Grünwald/Hackl*, ZD 2017, 556, 557; BeckOK DatenschutzR-*Holländer*, 22. Ed. (01.11.2017), Art. 83 Rn. 26 ff.

[296] Schantz/Wolff-*Schantz/Wolff*, Das neue Datenschutzrecht, 1. Aufl. 2017, Teil F, Rn. 1136.

[297] *Warren/Brandeis*, 4 Harv. L. Rev. 193, 198 (1890).

[298] Griswold v. Connecticut, 318 U.S. 479 (1965).

[299] Whalen v. Roe, 429 US 589 (1977).

Solove/Schwartz[300] vertreten, ist weiterhin streitig.[301] Das Right to Privacy ist in der Verfassung einiger Bundesstaaten explizit anerkannt. Dabei richtet sich das in der kalifornischen Verfassung verankerte Right to Privacy explizit auch gegen das unnötige Ansammeln von Daten durch Private und dient außerdem dem Schutz vor missbräuchlicher Verwendung sowie vor einer Verwendung zu anderen Zwecken als denen, zu denen die Daten erhoben wurden:[302]

> *"California constitutional right of privacy prevents government and business interests from [1] collecting and stockpiling unnecessary information about us and from [2] misusing information gathered for one purpose in order to serve other purposes or to embarrass us".*[303]

Damit enthält das kalifornische Right to Privacy einen gewissen Zweckbindungsgrundsatz.

Das US-amerikanische Datenschutzrecht ist nicht bundesweit einheitlich geregelt. Das Bundesrecht enthält allein bereichsspezifische Regelungen, wie z.B. den Health Insurance Portability and Accountability Act (1996), den Children´s Online Privacy Protection Act (1998), den Fair and Accurate Transactions Act (2003) und den Electronic Communications Privacy Act (der aus dem Wiretap Act und dem Stored Communications Act besteht). Darüber hinaus existieren in den einzelnen Staaten zahlreiche eigene datenschutzrechtliche Regelungen, wobei die wichtigsten Regelungen wohl aus Kalifornien stammen.[304] Zu erwähnen ist etwa der California Online Privacy Protection Act 2003, der Websitebetreiber u.a. dazu verpflichtet, Datenschutzerklärungen bereit zu halten, die die Nutzer über die erfolgenden Datenverarbeitungen informieren.

Das US-amerikanische Recht geht insgesamt diametral entgegengesetzt zum europäischen Datenschutzrecht von einer grundsätzlichen Zulässigkeit der Datenverarbeitung aus.[305] Ein ausdrücklich geäußertes Einverständnis mit der Datennutzung ist insofern jedenfalls im Grundsatz nicht erforderlich.[306] Anders liegt dies allerdings dann, wenn das Datensubjekt berechtigterweise davon ausgehen durfte, dass eine Datenverarbeitung nicht stattfindet

---

[300] *Solove/Schwartz*, Information Privacy Law, 4th ed. 2011, p. 35.

[301] Dazu etwa: *Kang*, 50 Stan. L. Rev. 1193, 1230 Fn. 157 (1998); vgl. zum Ganzen auch umfassend: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 234 ff.

[302] Hill v. National Collegiate Athletic Assn., 7 Cal 4th 1, 36 (Cal. 1994); vgl. auch: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 238.

[303] Hill v. National Collegiate Athletic Assn., 7 Cal 4th 1, 36 (Cal. 1994).

[304] *Schwartz/Solove*, 86 N.Y.U. L. Rev. 1814-1894 (2011); *Solove/Schwartz*, 102 Cal. L. Rev. 877, 888 (2014); sowie: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 271 f.; zum Children's Online Privacy Protection Act of 1998 vgl. *Schwartz*, ZD 2011, 97, 98.

[305] *Determann*, California Privacy Law, 2016, p. 24.

[306] Siehe ähnlich z.B. *Ozer*, 36 N.Y.U. Rev. L. & Soc. Change 215, 224 (2012).

(reasonable expectation of privacy).[307] Unternehmen können diese berechtigte Erwartung durch eine entsprechende Information über die Datenerhebung zerstören, weshalb häufig von umfassenden Datenschutzerklärungen Gebrauch gemacht wird.[308] Auch existiert kein Grundsatz der Datenminimierung.[309] Einer Einwilligung des Datensubjektes bedarf es darüber hinaus allein dann, wenn ein Gesetz dies explizit vorsieht, wie z.B. im California Medical Information Act der Fall.[310] Bedarf es einer solchen Einwilligung, muss sie im Vorfeld der Datenverarbeitung und zumindest freiwillig, informiert und häufig explizit, durch aktives Tun ausgedrückt werden. Z.T. sind weitere Kriterien zu erfüllen, so z.B. die Schriftform.[311] Opt-Out-Einwilligungen sind aber in der Regel möglich.[312]

Der Begriff der personenbezogenen Daten ist im US-amerikanischen Recht wesentlich enger gefasst, als dies im deutschen und europäischen Recht der Fall ist,[313] aufgrund der bereichsspezifischen Regelungen sind zudem z.T. nur spezifische Personen (z.B. Verbraucher, Kinder, Patienten etc.) geschützt.[314] Durchgesetzt werden datenschutzrechtliche Ansprüche durch den Attorney General, durch Klagen Privater sowie durch die Federal Trade Commission.[315] Kalifornien hat darüber hinaus eine Aufsichtsbehörde für den Datenschutz eingerichtet[316] sowie eine Privacy Enforcement and Protection Unit.[317]

Dem US-amerikanischen Recht wesensimmanent ist ein stark ausgeprägter Schutz der Meinungsfreiheit, die häufig zur Rechtfertigung von Datenverarbeitungen herangezogen wird. Verfassungsrechtlich findet sich dieser Schutz im ersten Verfassungszusatz (First Amendment):

> *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the*

---

[307] Zu reasonable expectation of privacy, siehe: *Freiwald*, Stan. Tech. L. Rev. 3 (2007).

[308] *Determann*, California Privacy Law, 2016, p. 24.

[309] *Determann*, California Privacy Law, 2016, p. 36.

[310] Medizinische Daten dürfen nicht ohne die Einwilligung für Marketing-Zwecke verwendet werden, vgl. *Determann*, California Privacy Law, 2016, p. 361.

[311] *Determann*, California Privacy Law, 2016, p. 363 et seq.

[312] *Determann*, California Privacy Law, 2016, p. 368 et seq.

[313] *Determann*, Datenschutz: International Compliance Field Guide, 2017, S. XVII, XXV.

[314] *Determann*, California Privacy Law, 2016, p. 33.

[315] *Determann*, California Privacy Law, 2016, p. 36; zur Rolle der FTC ausführlich: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 248 ff.

[316] *Genz*, Datenschutz in Europa und den USA, 2004, S. 74 f.

[317] Ähnliche Einrichtungen finden sich auch in den Staaten Colorado, New York und Wisconsin, vgl. *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 273 m.w.Nachw.

people peaceably to assemble, and to petition the Government for a redress of grievances."

Von diesem Verfassungszusatz geschützt sein soll auch der Verkauf, die Weitergabe und sonstige Nutzung personenbezogener Daten zu Marketingzwecken. Mit diesem Argument wurde ein Gesetz, das eine Weitergabe personenbezogener Daten zu Marketingzwecken verbietet, für verfassungswidrig erklärt.[318]

> *"Speech remains protected even when it may "stir people to action," "move them to tears," or "inflict great pain." (…) The more benign and, many would say, beneficial speech of pharmaceutical marketing is also entitled to the protection of the First Amendment."*[319]

Die Einschränkung der Freiheit der Meinungsäußerung zu kommerziellen Zwecken unterliegt aber einem geringeren Rechtfertigungsaufwand als ihre Einschränkung zu anderen, z.B. politischen Zwecken.[320]

> *"To require a parity of constitutional protection for commercial and noncommercial speech alike could invite dilution, simply by a leveling process, of the force of the Amendment's guarantee with respect to the latter kind of speech. Rather than subject the First Amendment to such a devitalization, we instead have afforded commercial speech a limited measure of protection, commensurate with its subordinate position in the scale of First Amendment values, while allowing modes of regulation that might be impermissible in the realm of noncommercial expression."*[321]

Nicht jede Datenverarbeitung kann daher ohne weitere Abwägung über die Meinungsfreiheit gerechtfertigt werden,[322] zumal das Fourth Amendment jedenfalls dann Schutz vor einer Datenerhebung bietet, wenn eine begründete Privatheitserwartung besteht, der Betroffene diese nach außen erkennbar manifestiert und sie gesellschaftlich als vernünftig anerkannt ist.[323]

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but*

---

[318] Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011); vgl. zum Ganzen auch umfassend: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 218 ff.

[319] Sorrell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011).

[320] Ohalik v. Ohio State Bar Assn., 436 U.S. 447, 457 (1978).

[321] Ohalik v. Ohio State Bar Assn., 436 U.S. 447, 457 (1978).

[322] Vgl. dazu umfassend: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 220 ff. m.w.Nachw.

[323] Katz v. United States, 389 U.S. 347, 362 (1967); *Wittmann*, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, S. 93 f.; *Solove/Schwartz*, Information Privacy Law, 4th ed. 2011, p. 35; *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 227.

upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Ob die Third-Party-Doktrin, wonach der Betroffene dann keinen Schutz nach dem Fourth Amendment mehr beanspruchen kann, wenn er Daten freiwillig mitteilt, weil er damit das Risiko einer Weiterverbreitung eingeht, auch im digitalen Zeitalter Anwendung findet, ist derzeit noch nicht abschließend entschieden.[324]

[324] Dagegen etwa: U.S. v. Jones, 132 S. Ct. 945, 954, 957 (2012); *Tomain*, 83 U. Cin. L. Rev. 1, 17 et seq. (2014); *Schwartz*, 69. DJT 2012, S. O75 f.; *MacLean*, 24 Alb. L.J. Sci. & Tech. 47, 52 (2014); *Solove*, 53 Stan. L. Rev. 1393, 1435 (2001); zum Streitstand eingehend: *Kühnl*, Persönlichkeitsschutz 2.0, 2016, S. 227 ff. m.w.Nachw.

5. (ZIVIL-)RECHTLICHER UMGANG MIT DATEN UND BEGRENZUNGEN DIESES UMGANGS DE LEGE FERENDA

Ist der Umgang mit Daten de lege lata durchaus möglich, so fragt sich de lege ferenda, ob dieser Rechtsrahmen ausreicht oder ob es für eine adäquate Erfassung des Rechtsobjektes „Daten" einer weitergehenden Regulierung bedarf. Insbesondere fragt sich, ob ausschließlichkeitsrechtliche Positionen an Daten in Betracht kommen. Dogmatisch lassen sich möglicherweise Begründungsansätze sowohl aus dem Immaterialgüterrecht, als auch aus dem Datenschutz- oder dem Sachenrecht übertragen. Auch der Rechtsvergleich mit den USA könnte einen neuen Blickwinkel eröffnen. Darüber hinaus stellt sich die Frage, ob der vertragsrechtliche Umgang mit Daten ausreichender Regulierung unterliegt, oder ob hier Anpassungsbedarf besteht.

Im Hinblick auf diese Aspekte existieren bereits Regulierungsansätze, die im Folgenden dargestellt (I.) und sodann einer Analyse unterzogen werden sollen (II.).

5.1 REGULIERUNGSANSÄTZE

Als wesentliche Regulierungsansätze zu nennen sind derzeit:
a) der Entwurf der EU-Kommission für ein „Datenerzeugerrecht" bzw. ein „Dateneigentum"[325] wobei die Zuweisung der ausschließlichkeitsrechtlichen Position auch an mehrere Personen erfolgen kann,
b) ein vertragsrechtliches Modell zum Umgang mit Daten, das ebenfalls verschiedenartig ausgestaltetet werden kann, nämlich einerseits durch
- den Erhalt des Status quo ohne gesetzgeberisches Einschreiten
- den Entwurf eines „Guidance Document", das sich an der derzeitigen Gesetzeslage orientiert und den Vertragsparteien Hilfestellungen bei der Ausgestaltung von Zugriff auf und Nutzung von Daten gibt
- Standardvertragsklauseln für den Zugang zu und die Nutzung von Daten auf vertragsrechtlicher Grundlage
- gesetzliche Ausgestaltung (sektorspezifisch oder sektorübergreifend) nicht-zwingender vertraglicher Vorgaben für Zugang zu und Nutzung von Daten sowie Regelungen zur AGB-Kontrolle
c) Zugangsrechte zu Daten unter FRAND-Bedingungen.

[325] Vgl. zur Ausdifferenzierung des vormaligen Vorschlags eines Datenerzeugerrechts: Annex to the Synopsis Report Consultation on the „Building a European Data Economy" Initiative, p. 21 et. seq., abrufbar unter: http://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf; zuletzt abgerufen am: 26.03.2018.

All diese von der Europäischen Kommission vorgeschlagenen oder aufgegriffenen Ansätze zielen darauf ab, den Austausch von Daten zu befördern („free flow of data"). Im Mittelpunkt steht dabei auch und gerade die Herstellung von Rechtssicherheit.[326]

Weiterhin vorgeschlagen wird die Ausweitung bzw. Anpassung des urheberrechtlichen Datenbankschutzes gem. § 87a UrhG sowie die Ausweitung des lauterkeitsrechtlichen Schutzes von Daten. Auf eine Beteiligung des datenschutzrechtlich Betroffenen zielt der Ansatz von *Schwartmann/Hentsch*,[327] der eine Lizenzierungsmöglichkeit personenbezogener Daten entsprechend dem Urhebervertragsrecht vorschlägt und damit an Ansätze zur kommerziellen Ausgestaltung des Persönlichkeitsrechts anknüpft.[328] Eine Diskussion über die vertragsrechtliche Stellung des datenschutzrechtlich Betroffenen wird in den USA schon seit mehreren Jahrzehnten geführt. Hierbei wird zwar auch die Terminologie „data property" verwendet, sie ist aber vor dem Hintergrund gewählt, dass das US-amerikanische Datenschutzrecht keinen dem europäischen Datenschutzrecht entsprechenden starken Datenschutz des Betroffenen kennt und der Terminus „data property" daher gewissermaßen als gegenüber dem de lege lata bestehenden US-amerikanischen Datenschutzrecht stärkeres Kontrollrecht des Betroffenen verstanden wird.[329] Daneben existiert in den USA die Idee eines „datarights", das allerdings nicht Daten an sich, sondern die Methode ihrer Erhebung schützt, um die Datenqualität und die Qualität ihrer Auswertung zu sichern. Sektorspezifisch existieren durchaus auch weitere Ansätze zur Regulierung des zivilrechtlichen Umgangs mit Daten.[330]

5.1.1 DATENERZEUGERRECHT/DATENEIGENTUM

5.1.1.1 VORSCHLAG DER EU-KOMMISSION

Die EU-Kommission stellt in ihrem Staff Working Document SWD(2017) 2 final in Anlehnung an *Zech*[331] ein Datenerzeugerrecht an nicht-personenbezogenen Rohdaten vor. Personenbezogene Daten sollen von diesem Recht nicht erfasst sein. Auch soll sich ein solches

---

[326] Vergleiche zu sämtlichen Vorschlägen insb. Annex to the Synopsis Report Consultation on the „Building a European Data Economy" Initiative, p. 18 et seq., abrufbar unter: http://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf; zuletzt abgerufen am: 26.03.2018.

[327] *Schwartmann/Hentsch*, PinG 2016, 117 ff.; dagegen aber: *Bisges*, MMR 2017, 301.

[328] Vgl. hierzu etwa: *Dorner*, CR 2014, 617, 619 ff. m.w.Nachw.

[329] So z.B. bei *Bui*, 21 USF Intell. Prop. & Tech. L. J. 1 et seq. (2016); *Samuelson*, 52 Stan. L. Rev. 1125 et seq. (2000); *Evans*, 42 Am. J.L. & Med. 651 (2016); *dies.*, 25 Harv. J.L. & Tech. 69, 93 (2011); *dies.*, 19 Vand. J. Ent. & Tech. L. 243 (2016); vgl. auch: *Osborne Clarke LLP*, Legal study on ownership and access to data, 2016, p. 24.

[330] Hierzu sogleich unter 6.

[331] *Zech*, Data as a tradable commodity, in: De Franceschi, European Contract Law and the Digital Single Market, 2016, pp. 51 at 63.

Datenerzeugerrecht allein auf die syntaktische Ebene von Daten, nicht aber auf die semantische beziehen und damit allein die Zeichenebene, nicht die Informationsebene betreffen.[332] Als Inhaber eines solchen Rechts wurde ursprünglich v.a. derjenige in Betracht gezogen, der in die Erzeugung der Daten investiert hat und damit der Hersteller der Maschinen, der Gerätschaften oder Werkzeuge, die die Daten aufzeichnen, oder auch derjenige der Wirtschaftsteilnehmer, der die Maschinen, Gerätschaften oder Werkzeuge kauft oder mietet. All diesen Teilnehmern könnte ein Miteigentumsanteil an den erzeugten Daten zustehen.[333] Einen ähnlichen Zuordnungsvorschlag unterbreitet eine im Auftrag des Bundesministeriums für Verkehr und digitale Infrastruktur angefertigte Studie.[334]

Denkbar scheint der Kommission anstelle eines umfassenden Ausschließlichkeitsrechts mit Nutzungs- und Abwehrkomponente aber auch ein reines Abwehrrecht, das nichtpersonenbezogene Daten betrifft.[335] Es wäre damit ähnlich dem Geschäftsgeheimnisschutz ausgestaltet, ohne dabei aber auf das Erfordernis der Geheimhaltung angewiesen zu sein.[336]

In ihrer im September 2017 veröffentlichten Konsultation differenziert die Kommission die Gestaltungsmöglichkeiten eines möglichen Dateneigentums weiter aus. Insbesondere die Möglichkeit einer geteilten Zuweisung an den Hersteller und den Datenerzeuger, aber auch an den Nutzer selbst wird in Betracht gezogen.[337]

Ausgestalten ließe sich ein solches Recht an bestimmten Einzeldaten oder aber an Datenkonglomeraten.[338] Beschränkt sein soll das als IP-Recht sui generis[339] gestaltete Recht durch

---

[332] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD(2017) 2 final, p. 34 et seq.

[333] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD(2017) 2 final, p. 35; vgl. hierzu auch umfassend: *Sattler*, in: Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, 2017, S. 27 ff.

[334] *Hornung et al*., Eigentumsordnung für Mobilitätsdaten, 2017, S. 5: „Kernelemente eines solchen Datengesetzes wären die Verständigung auf einen einheitlichen Zuordnungsansatz – wie z. B. der in der neu entwickelte und dargestellte Zuordnungsansatz zum wirtschaftlich Berechtigen."

[335] Für die Ausgestaltung in Einzelbefugnissen auch: *Dreier*, in: Weller/Wendland, Digital Single Market: Bausteine eines digitalen Binnenmarktes, 2018, im Erscheinen.

[336] Vgl. hierzu: *Röttgen*, Datenrechte im europäischen Rechtsraum, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

[337] Annex to the Synopsis Report Consultation on the „Building a European Data Economy" Initiative, p. 22 et. seq.; abrufbar unter: http://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf; zuletzt abgerufen am: 26.03.2018; der Nutzer wird explizit auf S. 24 als möglicher Rechtsinhaber ausgewiesen.

[338] *Specht*, CR 2016, 288 ff.; zur Schwierigkeit der Abgrenzung, an welchen Daten ein Recht bestehen soll, vgl. auch: Bericht der Arbeitsgruppe „Digitaler Neustart" v. 15.05.2017, S. 10, abrufbar unter: https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf, zuletzt abgerufen am 10.03.2018.

eine Verpflichtung, die Daten in spezifischen Situationen zu teilen, z.B. wenn hieran ein öffentliches Interesse (etwa aus Umweltschutzgründen) besteht oder auch in Multi-Player-Sachverhalten, in denen Daten benötigt werden, um bestimmte Dienste zu erbringen (die EU-Kommission nennt etwa Smart-Metering-Informationen, die zum Betreiben von Diensten im Smart Home erforderlich sind).[340]

5.1.1.2 ALTERNATIVE GESTALTUNGSANSÄTZE

Auch in der Literatur wird über ein nicht unbedingt dem Datenerzeuger zustehendes „Dateneigentum" nachgedacht.[341] Für die Zuweisung eines solchen Rechtes stehen verschiedene Ansätze zur Diskussion, so etwa das Eigentum am Trägermedium, die datenschutzrechtliche Betroffenheit, die Investitionsleistung entsprechend § 87a UrhG sowie der akt.[342]

Die eigentumsrechtliche Lage am Trägermedium als Zuweisungskriterium der gespeicherten Inhalte heranzuziehen, scheint wenig überzeugend. Denn das Sacheigentum enthält kein Regulierungsregime dazu, wie mit Inhalten des Trägermediums zu verfahren ist,[343] ob und wie diese genutzt werden dürfen. Dies wird bereits durch das Urheberrecht deutlich, das die Einräumung von Nutzungsrechten erfordert, damit ein körperliches Werkexemplar z.B. vervielfältigt werden darf.[344] Auch stellen sich Daten nicht als Früchte der Sache (z.B. der Maschine) i.S.d. § 99 Abs. 2 BGB dar, durch die sie generiert werden.[345] Denn sie sind weniger ein Produkt der Maschine, als ein Produkt des Gegenstands oder der Person, über die sie

---

339 Annex to the Synopsis Report Consultation on the „Building a European Data Economy" Initiative, p. 22; abrufbar unter: http://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf; zuletzt abgerufen am: 26.03.2018.

340 Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD (2017) 2 final, p. 36.

341 Vgl. etwa: *Hoeren*, MMR 2013, 486 ff.

342 Zu den einzelnen Zuordnungsmöglichkeiten vgl. bereits umfassend: *Hoeren*, Big Data und Recht, 2014, S. 11 ff.; Leitlinien für eine Zuordnung geben auch: *Börding/Jülicher/Röttgen/v. Schönfeld*, CR 2017, 134, 136.

343 Vgl. hierzu bereits ausführlich: *Zech*, CR 2015, 137, 142; *Berberich/Golla*, PinG 2016, 165, 168 f.; ebenso: *Thalhofer*, GRUR-Prax 2017, 225; *Grützmacher*, CR 2016, 485, 487; für eine „mittelbare" Zuordnung von Daten anhand des Trägermediums aber: *Hieke*, InTeR 2017, 10, 12; *Härting*, CR 2016, 646, 647; zumindest missverständlich auch: *Assion*, CR 2016, 84, der davon spricht, die „Verfügungsrechte" an Daten würden im Zweifel dem Eigentümer des Trägermediums zustehen, dabei aber wohl die tatsächliche Möglichkeit, über die Verwendung personenbezogener Daten zu entscheiden, meint.

344 Vgl. hierzu bereits: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, S. 77.

345 So v.a. *Grosskopf*, IPRB 2011, 259, 260; vgl. auch: *Dorner*, CR 2014, 617, 619.

erhoben werden. Nach wohl h.M. lässt sich eine Maschine weder ausbeuten, noch kann sie Erzeugnisse abwerfen.[346]

Problematisch scheint ein Auseinanderfallen von Sacheigentum und möglichen Rechten der auf ihnen gespeicherten Inhalte auch nicht mit Blick auf § 950 BGB. Denn das Aufspielen von Daten auf ein Trägermedium ist zumindest dann, wenn dadurch der Datenträger nicht erst seine wirtschaftliche Bedeutung erlangt, keine Verarbeitung, die zur Bildung einer neuen Sache führt, an der der Verarbeiter Eigentum erwirbt.[347]

Dagegen erscheint das informationelle Selbstbestimmungsrecht, das einfach-gesetzliche Ausprägungen im Datenschutzrecht erfährt, zwar grundsätzlich geeignet, eine güterrechtliche Zuweisungsentscheidung zu treffen,[348] auch wenn es in seiner Grundkonzeption allein als dem Schutz ideeller Interessen dienend ausgestaltet ist. Der BGH erkennt seit der *Paul-Dahlke*-Entscheidung nämlich auch vermögenswerte Bestandteile des Persönlichkeitsrechts an,[349] seit seiner Entscheidung „*Marlene-Dietrich*" werden diese sogar als vererblich erachtet.[350] Dass einer solchen Zuweisungsfunktion auch vermögensrechtlicher Interessen das Volkszählungsurteil entgegenstehen soll, wird hier als nicht zutreffend erachtet. Denn dieses lässt sich gerade auch so interpretieren, dass dem Einzelnen zwar keine uneingeschränkte Herrschaft über die ihn betreffenden Daten gewährt werden kann, es einer weniger weitreichenden Befugnis, die durch entsprechende Schrankenregelungen begrenzt wird, aber nicht

---

[346] BGH, Urt. v. 17.01.1968 - VIII ZR 207/65, NJW 1968, 692, 693; BeckOGK BGB-*Mössner*, Stand: 15.02.2018, § 99 Rn. 5.4 m.w.Nachw.; selbst wenn sich Daten aber als Sachfrucht darstellen ließen, so regelte erst § 953 BGB ihre eigentumsrechtliche Zuordnung. § 953 BGB setzt jedoch die Eigentumsfähigkeit der Frucht bereits voraus und begründet diese nicht. Für eine analoge Anwendbarkeit auf nicht-rival zu nutzende Daten fehlt es an der Vergleichbarkeit der Rechts- und Interessenlage, vgl.: *Zech*, CR 2015, 137, 142; vgl. hierzu bereits eingehend: *Specht*, CR 2016, 288 ff.; ähnlich auch: *Hoeren*, MMR 2013, 486 ff.; *Hieke*, InTeR 2017, 10, 12.

[347] BGH, Urt. v. 10.07.2015 – V ZR 206/14, GRUR 2016, 109 Tz. 19. – *Kanzler Kohls Tonbänder*; jurisPK-BGB-*Vieweg/Lorz*, 8. Aufl. 2017, § 950 Rn. 15; die Anwendbarkeit von § 950 beim Aufspielen von Daten auf einen Datenträger ebenfalls verneinend: BeckOK BGB-*Kindl*, 44. Ed. (Stand: 01.11.2017) § 950 Rn. 5 aE; MüKo BGB-*Füller*, 7. Aufl. 2017, § 950 Rn. 10; Palandt-*Herrler*, BGB, 75. Aufl. 2018, § 950 Rn. 3; RGRK-*Pikart*, BGB, 12. Aufl. 1979, § 950 Rn. 10; *Soergel-Henssler*, BGB, 13. Aufl. 2002, § 950 Rn. 8; Staudinger-*Wiegand*, BGB, 2017, § 950 Rn. 9 aE; *Westermann/Gursky/Eickmann*, Sachenrecht, 8. Aufl. 2011, § 53 II 2 Rn. 7; *Kolb*, GRUR-RR 2014, 423, 424; a.A. noch: LAG Chemnitz, Urt. v. 17.01.2007 – 2 Sa 808/05, MMR 2008, 416 ff.; OLG Karlsruhe, Beschl. v. 06.10.1986 – 6 U 160/86, CR 1987, 19, 20.

[348] So auch: *Kilian*, CR 2002, 921, 926; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 203 f., 223 f.; *Hermann*, Der Werbewert der Prominenz, 2012; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, S. 76 f.; a.A. *Hoeren*, MMR-Beil. 1998, 6, 8; *Härting*, CR 2016, 646, 648.

[349] BGH, Urt. v. 08.05.1956 – I ZR 62/54, GRUR 1956, 427, 429 – *Paul Dahlke*.

[350] BGH, Urt. v. 01.12.1999 – I ZR49/97, NJW 2000, 2195 ff – *Marlene Dietrich*; zur vermögensrechtlichen Komponente des Persönlichkeitsrechts vgl. bereits umfassend: *Kilian*, Strukturwandel der Privatheit, in: Garstka/Koy, Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten, Wilhelm Steinmüller zum Gedächtnis, 2014, S. 195, 207 ff.

entgegensteht.[351] Die Betroffenheit i.S.d. § 7 DS-GVO kommt als Zuweisungskriterium möglicher ausschließlichkeitsrechtlich gestalteter Datenrechte allerdings überhaupt nur dort in Betracht, wo personenbezogene Daten in Rede stehen.[352] Für einen Rechtsrahmen, der auch für nicht-personenbezogene Daten gelten soll, taugt sie als Zuweisungskriterium daher nicht.[353]

§§ 87a ff. UrhG erfordern eine wesentliche Investition in die Beschaffung, Sammlung, Überprüfung, Aufbereitung oder Darbietung des Datenbankinhaltes. Eine Investition in die Erzeugung von Daten ist gerade nicht geschützt.[354] Zwar gewährt der Datenbankschutz kein Recht an den einzelnen Datenbankinhalten und kann daher nicht herangezogen werden, wenn es um die Begründung eines Ausschließlichkeitsrechts am Datum selbst geht. Er zeigt aber jedenfalls ein gesetzliches Modell auf, demjenigen, der wirtschaftliche Investitionen vornimmt, ausschließlichkeitsrechtliche Befugnisse zuzuweisen, auch wenn der Gegenstand der Investition sicherlich nicht vergleichbar ist.[355] Die Investitionsleistung kommt als Zuweisungskriterium eines Ausschließlichkeitsrechts an Daten daher durchaus in Betracht.

Weiterhin lässt sich aus den strafrechtlichen Vorschriften der §§ 202a-c, 303a StGB z.T. auf eine zivilrechtliche Zuweisung einer eigentumsähnichen Position an Daten schließen. Sie soll demjenigen zustehen, der auch strafrechtlich von diesen Vorschriften geschützt wird.[356] Dies ist derjenige, der den für die Entstehung von Daten erforderlichen Skripturakt vornimmt, die Speicherung also unmittelbar bewirkt.[357] Regelmäßig wird der Skripturakt dabei

---

[351] BVerfG, Urt. v. 15.12.1983 - 1 BvR 209/83, NJW 1984, 419, 422 – *Volkszählung*; vgl. hierzu bereits eingehend: *Specht*, CR 2016, 288 ff.; zutreffend auch: *Veil*, MMR 2017, 281, 282; für eine eigentumsrechtliche Zuordnung von Rechten an Daten zu dem Betroffenen: *Fezer*, MMR 2017, 3 ff.; *ders*. ZD 2017, 99; wohl auch: *Wandtke*, MMR 2017, 6, 11.

[352] Gänzlich ablehnend allerdings: *Berberich/Golla*, PinG 2016, 165, 168 f.

[353] So bereits umfassend: *Specht/Rohmer*, PinG 2016, 127.

[354] EuGH, Urt. v. 09.11.2004 - C-203/02, ECLI:EU:C:2004:695 = GRUR 2005, 244 – *The British Horseracing Board u.a.*; EuGH, Urt. v. 09.11.2004 - C-338/02, ECLI:EU:C:2004:696 = GRUR 2005, 252 – *Fixtures-Marketing*; EuGH, Urt. v. 09.11.2004 - C-444/02, ECLI:EU:C:2004:697 = GRUR 2005, 254 - *Fixtures-Marketing*; EuGH, Urt. v. 09.11.2004 - C-46/02, ECLI:EU:C:2004:694 = GRUR Int 2005, 244 - *Fixtures-Marketing*; eingehend: *Leistner*, JZ 2005, 408, 409; *Wiebe*, CR 2014, 1, 4; *Zech*, GRUR 2015, 1151, 1158; BeckOK UrhR-*Vohwinkel*, 18. Ed. (Stand: 01.11.2017), UrhG, § 87a Rn. 44.

[355] Vgl. auch hierzu bereits eingehend: *Specht*, CR 2016, 288 ff.

[356] OLG Naumburg, Urt. v. 27.08.2014 – 6 U 3/15, CR 2016, 83 ff.; *Hilgendorf*, JuS 1996, 509, 511; *Popp*, JuS 2011, 385, 386; *Hoeren*, MMR 2013, 486, 487; kritisch: *Heun/Assion*, CR 2015, 812, 813; Dölling/Duttge/Rössner-*Tag*, Gesamtes Strafrecht, 4. Aufl. 2017, § 202a Rn. 3; vgl. hierzu auch: *Berberich/Golla*, PinG 2016, 165, 171.

[357] Vgl. hierzu auch: *Dorner*, CR 2014, 617, 618; Kindhäuser/Neumann/Paeffgen-*Kargl*, Strafgesetzbuch, 5. Aufl. 2017, § 202a Rn. 7; BeckOK StGB-*Weidemann*, 37. Ed. (Stand: 01.02.2018) § 202a Rn. 8; krit: *Bräutigam/Klindt*, Digitalisierte Wirtschaft/Industrie 4.0, 2015, S. 24; differenzierend: *Grützmacher*, CR 2016, 485, 491.

von der Person vorgenommen, die das die Speicherung bewirkende Programm ausführt.[358] Auch innerhalb eines Arbeits- oder Dienstverhältnisses, in dem Daten im Auftrag erstellt werden, soll zunächst der Auftragnehmer Berechtigter sein, bis er die Daten aushändigt.[359]

> *„'Skribent' und damit originär Berechtigter an den Daten soll derjenige sein, der durch Eingabe oder Ausführung eines Programms Daten selbst erstellt. Dieses Kriterium ist insofern dogmatisch und praktisch brauchbar, weil es gerade an die spezifische Dateneigenschaft anknüpft. Der „Skribent" ist der technische „Ersteller" der Daten, zunächst unabhängig davon, auf wessen Medium die Speicherung geschieht und wer geistig den Inhalt geprägt hat."*[360]

Auch dieses Kriterium wird aber in Mehrpersonenverhältnissen, in denen notwendigerweise mehrere Personen verschiedene oder auch gemeinsame Skripturakte vornehmen, zu Zuordnungsproblemen führen.[361]

5.1.2 ERWEITERUNG DES DATENBANKSCHUTZES GEM. § 87A URHG

Insbesondere *Wiebe* schlägt vor, anstelle einer ausschließlichkeitsrechtlichen Position an Daten den Datenbankschutz gem. § 87a UrhG extensiver auszulegen, als dies bisher geschieht. Konkret geht es ihm um die Abgrenzung der Berücksichtigungsfähigkeit der Kosten für eine Datensammlung und eine Datenerzeugung, von der die Anwendbarkeit des Datenbankschutzes de lege lata abhängt. Eine Investition in die Datenerzeugung ist de lege lata nicht möglich, um die Voraussetzungen des § 87a UrhG zu erfüllen. Erforderlich ist vielmehr eine Investition in die Sammlung bereits vorhandener Daten. Sind separate Aufwendungen für die Datensammlung nicht nachzuweisen, greift der Datenbankschutz insofern nicht.[362] *Wiebe* spricht sich dafür aus, diese Abgrenzung künftig wie folgt vorzunehmen: Bloß beschaffte und zusammengestellte Daten (Datensammlung) sind in der Natur bereits vorhanden und werden einzig gemessen und gesammelt. Sie müssen aber für eine Anwendbarkeit des § 87a UrhG nicht bereits gemessen sein. Auch eine Investitionsleistung in ihre Messung und Zusammenstellung sollte als ausreichend erachtet werden. Denn diese Daten können von jedem Dritten mit demselben Aufwand ebenso gemessen und zusammengestellt werden. Dies gilt etwa für Wetterdaten oder geographische Daten. Erzeugte Daten dagegen sind ihrer Natur nach niemandem als dem Datenerzeuger bekannt, weil ihnen erst durch diesen über-

---

[358] Vgl. für weitere Beispiele: *Röttgen*, Datenrechte im europäischen Rechtsraum, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen.

[359] Str. dagegen: *Fischer*, Strafgesetzbuch, 64. Aufl. 2017, § 303a Rn. 6; dafür: OLG Nürnberg, Beschl. v. 23.01.2013 – 1 Ws 445/12, ZD 2013, 282, m. Anm. *Schröder*, ZD 2013, 284; vgl. auch: *Zech*, GRUR 2015, 1151, 1159; *Hoeren*, MMR 2013, 486, 487.

[360] *Hoeren*, MMR 2013, 486, 487.

[361] *Spindler*, ZGE 2017, 399, 402.

[362] *Wiebe*, GRUR 2017, 338, 341 m.w.Nachw.

haupt zur Existenz verholfen wird.[363] Danach würden z.B. Messdaten über die Bodenbeschaffenheit lediglich aufgezeichnet und folglich lediglich ein bereits vorhandener Wert gemessen, der schon in der Natur existiert. Ihre Messung und Zusammenstellung könnte bei dieser Auslegung Gegenstand einer Investition i.S.d. § 87a UrhG sein.[364] Auch eine Reihe anderer maschinenerzeugten Daten, z.B. Sensordaten aus dem Connected Car, ließe sich bei dieser Auslegung vom Datenbankherstellerrecht umfassen.[365]

Ebenfalls extensiv auszulegen sein soll die Verletzungshandlung der Entnahme unwesentlicher Teile in wiederholter und systematischer Weise, § 87b S. 2 UrhG, die generalisierend auf automatisierte Auswertungen im B2B-Bereich Anwendung finden könnte.[366] Der extensiven Auslegung auf Tatbestandsseite könnte durch Normierung einer kurzen Schutzdauer begegnet werden.[367]

5.1.3 VERFÜGUNGSBEFUGNIS ÜBER KOMMUNIKATIONSDATEN

Die E-Privacy-Richtlinie intendiert ausweislich der Entwurfsbegründung ein „Verfügungsrecht" des Endnutzers sowohl für personenbezogene, als auch für nicht-personenbezogene Daten zu schaffen:

> *„Die Umsetzung der e-Datenschutz-Richtlinie hat sich bezüglich der Verfügungsbefugnis des Endnutzers über seine Daten als unwirksam erwiesen. Deshalb ist die Umsetzung dieses Grundsatzes durch eine zentrale Einholung der Nutzereinwilligung über die Software mit Anzeige der Informationen über die Einstellungen zur Privatsphäre erforderlich, damit das angestrebte Ziel erreicht werden kann."*[368]

Die englische Sprachfassung ist hier etwas neutraler, stellt jedoch ebenfalls darauf ab, dass der einzelne Nutzer zur Entscheidung über die Datennutzung befähigt werden soll:

> *"The implementation of the ePrivacy Directive has not been effective to empower end-users. Therefore the implementation of the principle by centralising consent in software and prompting users with information about the privacy settings thereof, is necessary to achieve the aim."*

---

[363] *Wiebe*, GRUR 2017, 338, 341 m.w.Nachw.

[364] Ebenso: *Schmidt/Zech*, CR 2017, 417, 422.

[365] *Wiebe*, GRUR 2017, 338, 341.

[366] *Wiebe*, GRUR 2017, 338, 344.

[367] *Wiebe*, GRUR 2017, 388, 344.

[368] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) v. 10.01.2017, COM (2017) 10 final, S. 5.

Soweit es aber um nicht-personenbezogene Daten und insbesondere, wenn es um Machine-to-Machine-Kommunikation geht, stellt sich die Frage, wer hier „verfügungsbefugt" sein soll. Der Endnutzer soll sich nach Art. 2 Nummer 14 der Richtlinie über den europäischen Kodex für die europäische Kommunikation bestimmen und ist hier definiert als ein Nutzer, der keine öffentlichen Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellt. Auch hierdurch ist aber noch nicht geklärt, ob es sich jeweils um den Eigentümer des die Daten aufzeichnenden Gerätes oder einen möglicherweise vom Eigentümer zu unterscheidenden Nutzer handelt. Sollte auf den tatsächlichen Nutzer, nicht auf den Eigentümer des Endgerätes abgestellt werden, dürfte dies Zuordnungsschwierigkeiten in der Praxis nach sich ziehen, auch wenn der Endnutzer im Falle der Machine-to-Machine-Kommunikation in der Regel der Eigentümer des Gerätes sein dürfte. Die von der Ratspräsidentschaft vorgeschlagene Möglichkeit der Einwilligung „at the time of subscription"[369] spricht allerdings ohnehin eher dafür, dass als Endnutzer generell der Eigentümer des Endgerätes angesehen werden soll. Dann aber stellt sich die Frage nach dem Verhältnis zu den aus der DS-GVO folgenden Befugnissen des Betroffenen.[370]

Ohne die Einwilligung des Endnutzers darf auf die – auch nicht-personenbezogenen Daten – jedenfalls grundsätzlich nicht zugegriffen werden. Der Endnutzer entscheidet über die Datenverarbeitung. Ob hierdurch tatsächlich ein „Verfügungsrecht" zugeordnet werden soll und wie diese Rechtsposition im weiteren Rechtsverkehr ausgestaltet sein soll, dazu enthält die E-Privacy-Verordnung keine weiteren Anhaltspunkte. Eine solche Interpretation scheint tendenziell zu weitgehend. Ebensowenig existieren Anhaltspunkte dafür, ob es gestattet sein soll, Dritten exklusive Rechtspositionen an den betreffenden Daten einzuräumen.

5.1.4 LAUTERKEITSRECHTLICHER LEISTUNGSSCHUTZ FÜR DATEN AUßERHALB DES KNOW-HOW-SCHUTZES

Neben einer Erweiterung des Datenbankschutzes gem. § 87a UrhG wird auch eine Erweiterung des lauterkeitsrechtlichen Schutzes angedacht. Insbesondere *Becker* gibt hier zu bedenken, dass sich ein unmittelbarer Leistungsschutz (Schutz gegen die Nachahmung selbst ohne dass es auf unlauterkeitsbegründender Umstände ankäme) v.a. für Daten mit gesellschaftlicher oder wirtschaftlicher Relevanz, die nur mit erheblichem Aufwand zu gewinnen sind und die keinen sondergesetzlichen Schutz genießen, gegenüber einer anderweitigen Anerkennung von Rechtspositionen an Daten gewissermaßen als „lowest hanging fruit" erwiese. Einen unmittelbaren Leistungsschutz über das UWG will er allerdings allein dann gewähren,

[369] Interinstitutional File: 2017/0003 (COD) v. 11.01.2018, p. 8.

[370] Ob letztlich die Machine-to-Machine-Kommunikation tatsächlich von der E-Privacy-Verordnung erfasst werden wird, ist noch nicht abschließend geklärt, sondern derzeit Gegenstand der Konsultation der Mitgliedstaaten, vgl. insoweit Interinstitutional File: 2017/0003 (COD) v. 11.01.2018, p. 8 et seq.

wenn kein legitimes Interesse an einer freien Nutzung besteht.[371] Auch *Leistner* verweist auf die aus ökonomischer Perspektive nicht zu verkennende Vorzugswürdigkeit eines solchen unmittelbaren Leistungsschutzes entsprechend der Misappropriation-Doktrin gegenüber der Zuweisung neuer Ausschließlichkeitsrechte, sofern

> *„ein Fall im Vergleich zum bestehenden immaterialgüterrechtlichen Schutzsystem echte Zusatzelemente aufweist, die dazu führen, dass die Zulassung der Nachahmung bei verobjektivierter (…) Betrachtung die Anreize für die Herstellung der Originalleistung so reduzieren würde, dass die Existenz derartiger Angebote im Markt grundsätzlich gefährdet wäre.*[372]

Ein jedenfalls mittelbarer Leistungsschutz (Schutz nicht unmittelbar gegen die Nachahmung, sondern gegen die Umstände des Angebotes) für Daten kann sich bereits de lege lata über den Nachahmungsschutz (§ 4 Nr. 3 lit. a)–c) UWG) ergeben, sofern die wettbewerbliche Eigenart von Daten bejaht wird. Dies ist de lege lata deshalb kritisch, weil die Kriterien zur Bestimmung der wettbewerblichen Eigenart für physisch in ihrer Gestaltung wahrnehmbare Güter entwickelt wurden und daher z.B. vornehmlich an optische Merkmale anknüpfen.[373] Eine Weiterentwicklung dieser Kriterien auf Datenmärkte scheint angezeigt, denn Daten sind in Anbetracht ihrer sich durch einen außerordentlich geringen Zeit- und Kostenaufwand auszeichnenden Übernahmemöglichkeit besonders anfällig für Nachahmungen.[374] Ausschlaggebend für die wettbewerbliche Eigenart könnte es daher statt optischer Merkmale sein, ob die Daten aus Sicht des Verkehrs nur von einem bestimmten Anbieter stammen können.[375] Im Nachahmungstatbestand ist dagegen darauf zu achten, dass hier nicht ein zu weit reichender lauterkeitsrechtlicher Schutz erreicht wird. Denn der BGH stellt für den Nachahmungsschutz darauf ab, ob das Originalprodukt in der Nachahmung wiedererkennbar ist.[376] Für Daten wäre das sehr weitgehend, da bei einer Reihe von Endprodukten erkennbar sein dürfte, dass und auf welchen Daten(-sätzen) sie beruhen.[377]

Der lauterkeitsrechtlich Geschützte ist eng verwandt mit dem durch ein Datenerzeugerrecht oder auch dem durch eine Ausweitung des Datenbankherstellerschutz Begünstigten: Es ist allein derjenige, der selbst etwas Nachahmungsfähiges erschafft, auch wenn Investitions-

---

[371] *Becker*, GRUR 2017, 346, 357.

[372] Teplitzky/Peifer/Leistner-*Leistner*, UWG, 2. Aufl. 2013, § 4 Rn. 37; zum Erfordernis besonderer Umstände vgl. auch: BGH, Urt. v. 21.02.2002 – I ZR 265/99, GRUR 2002, 629, 631; – *Blendsegel*.

[373] BGH, Urt. v. 06.05.1999 – I ZR 199/96, GRUR 1999, 923, 927 – *Tele-Info-CD*, dazu auch: *Leistner*, MMR 1999, 636, 641; *Becker*, GRUR 2017, 346, 348.

[374] So zutreffend: *Becker*, GRUR 2017, 346, 354.

[375] *Becker*, GRUR 2017, 346, 354 f., der zusätzlich darauf abstellt, dass die Daten „eine bestimmte marktrelevante Qualität aufweisen" müssen.

[376] BGH, Urt. v. 23.09.2015 – I ZR 105/14, GRUR 2015, 1214 Tz. 78 – *Goldbären*.

[377] Hierzu und für Beispiele vgl. *Becker*, GRUR 2017, 346, 349.

und Organisationsleistungen berücksichtigt werden, das Leistungsergebnis also nicht unmittelbar aus der Hand des Berechtigten stammen muss.[378]

5.1.5 DATENSCHULDRECHT

Auch ohne die Zuweisung von ausschließlichkeitsrechtlichen Rechtspositionen und lauterkeitsrechtlichem Schutz ist ein vertragsrechtlicher Umgang mit Daten möglich. Soll den Vertragsparteien ein möglichst einfacher Weg der vertraglichen Vereinbarung ermöglicht werden, um die Transaktionskosten für derartige Vertragsschlüsse zu vermindern, ließe sich dies sowohl durch das angedachte Guidance-Document, als auch durch Standardvertragsklauseln oder nicht zwingende gesetzliche Vorgaben für den Zugang zu und die Nutzung von Daten erreichen. Sie gelten, sofern die Vertragsparteien für den betroffenen Bereich keine Regelung getroffen haben. Nicht zwingende gesetzliche Regelungen würden dabei in ungleichen Machtverhältnissen allerdings schlicht abbedungen, weshalb zum Ausgleich möglicher Machtungleichgewichte zumindest ergänzende Vorgaben zur AGB-Kontrolle angedacht werden.[379]

Jede dieser Optionen ließe sich sowohl für den vertraglichen Umgang sowohl mit personenbezogenen, als auch mit nicht-personenbezogenen Daten realisieren, wobei im Falle eines Personenbezugs das Datenschutzrecht zu berücksichtigen wäre, was auch dazu führen kann, gesetzliche Regelungen in diesem Bereich zwingend ausgestalten zu müssen (vgl. hierzu die Analyse unter 5.2). Die Standardvertragsklauseln und gesetzlichen Vorgaben im B2B-Bereich ließen sich durchaus weniger streng gestalten als im B2C-Bereich.[380]

Insgesamt geht es den vorbenannten Ansätzen v.a. darum, den Handel mit nicht-personenbezogenen Daten u.a. durch Herstellung von Rechtssicherheit und die Reduktion der Transaktionskosten zu vereinfachen. Ein jedenfalls z.T. anderes Ziel wird verfolgt, wenn in Regulierungsansätzen für personenbezogene Daten vorgeschlagen wird, Verträge über Daten ähnlich dem Urhebervertragsrecht auszugestalten. Zwar geht es auch hier einerseits um die Gewährleistung von Rechtssicherheit bei der Ausgestaltung neuer gesellschaftlich und politisch erwünschter Geschäftsmodelle.[381] Vorgeschlagen wird insbesondere die Einführung einer dem § 44a UrhG entsprechenden Regelung zur Erhebung von Daten, wenn diese unmittelbar anschließend einem Anonymisierungsvorgang unterzogen und die Ausgangsdaten gelöscht werden.[382] Zusätzlich soll von einer entsprechenden Ausgestaltung

---

[378] *Becker*, GRUR 2017, 346, 354.

[379] Zu einem entsprechenden Vorschlag im US-amerikanischen Recht vgl. *Franklin/Reichman*, 147 U. Pa. L. Rev. 875 et seq. (1999).

[380] Für nicht-zwingende Standardvertragsklauseln: Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD (2017) 2 final, pp. 31, 32.

[381] *Schwartmann/Hentsch*, PinG 2017, 117, 125.

[382] *Specht*, GRUR Int. 2017, 1040, 1047.

aber andererseits auch der Betroffene profitieren. *Schwartmann/Hentsch* führen etwa an, eine entsprechende Ausgestaltung könne zu mehr Datensparsamkeit führen, wobei sie eine Erklärung schuldig bleiben, wie diese Datensparsamkeit durch eine dem Urheberrecht entsprechende Ausgestaltung des Datenschutzrechtes gelingen soll.[383] Im Falle einer urheberrechtsähnlichen Ausgestaltung des Datenschutzrechtes aber könnte man jedenfalls den Grundsatz der angemessenen Vergütung, § 32 UrhG, fruchtbar machen (dazu kritisch in der Analyse unter 7.).[384] Darüber hinaus wird das Datenschuldrecht insbesondere mit Blick auf die derzeit im Entwurf vorliegende Richtlinie für Digitale Inhalte erörtert. Aber auch ohne ihre Verabschiedung zwingt die Auslegung von Verträgen nach den Maßstäben der §§ 133, 157 BGB zumindest dann, wenn eine Leistung in Anspruch genommen werden kann, weil über diejenigen Daten, die zur Erbringung der Leistung ohnehin erforderlich sind, weitere Daten überlassen werden, zu einer Anerkennung von Daten als Gegenleistung im Vertrag. Nur sehr wenige Ansätze beschäftigen sich auch darüber hinaus mit der umfassenden Normierung eines „Datenschuldrechts“[385] (Hierzu ausführlich in der Analyse unter 7.).

5.1.6 REGULIERUNGSANSÄTZE IM US-AMERIKANISCHEN RECHT

In der Vergangenheit wurde der Terminus des Dateneigentums in den USA primär verwendet, um mit ihm eine gegenüber der über das Datenschutzrecht gewährten Position zu verstärkende Rechtsstellung des Betroffenen zu beschreiben.[386] In den USA liegt der Fokus der aktuellen Diskussion um den Umgang mit Daten nicht so sehr auf der Zuweisung von Ausschließlichkeits- und Zugangsrechten,[387] sondern primär auf der Frage, wie die datenschutzrechtliche Stellung des Betroffenen in der Digitalisierung gehandhabt werden soll.[388] Darüber hinaus existieren aber auch einige wenige Ansätze für die Begründung eigener Rechtspositionen an Daten sowie einer Übertragung der „Hot News“-Doktrin auf Big-Data-Sachverhalte.

5.1.6.1 „OWNERSHIP“ AN LANDWIRTSCHAFTLICHEN DATEN

Diskutiert wird insbesondere ein „Ownership“ an Daten im landwirtschaftlichen Bereich, das demjenigen zugewiesen werden könnte, der mit sensorausgestatten Geräten landwirtschaft-

---

383 *Schwartmann/Hentsch*, PinG 2017, 117, 125.

384 *Specht*, GRUR Int. 2017, 1040, 1042.

385 Hierzu aber eingehend: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

386 *Osborne Clarke LLP*, Legal study on ownership and access to data, 2016, p. 24.

387 Vgl. aber zu Zugangsrechten im Medizinbereich: *Evans*, 24 Health Matrix 11 (2014).

388 *Mattioli*, ZGE 2017, 299, 303, 307; zur bereits lange existenten Diskussion um eine Stärkung des Datenschutzes in den USA vgl. *Samuelson*, 52 Stan. L. Rev. 1125 et seq. (2000).

liche Arbeit tätigt und dabei z.B. Daten über die Bodenbeschaffenheit generiert.[389] Hier besteht Sorge, dass die Nutzungsbefugnisse an den Daten durch vertragliche Vereinbarung den Geräteherstellern zugewiesen werden, die die Vertragsbedingungen durch ihre starke Stellung im Markt faktisch diktieren könnten. Mittlerweile liegt ein Statement von 13 im Markt tätigen landwirtschaftlichen Unternehmen vor, die sich positiv zu einem möglichen den Landwirten zustehenden „Ownership" an Daten äußern. Überdies soll ein Anspruch auf Portabilität der Daten gewährleistet werden.[390] Auch hier ergeben sich allerdings nicht unerhebliche Zuordnungsprobleme eines solchen Eigentumsrechts.[391] Faktisch ergibt sich eine ähnliche Situation wie in der E-Privacy-Verordnung. Ob sich die Position der Landwirte allein auf ihr Verhältnis zu den Datenverarbeitern und damit auf den primären Datenmarkt beziehen soll oder ob die Rechtsposition verdinglicht ausgestaltet sein und sich daher auf den sekundären Datenmarkt erstrecken soll, dazu werden keine Angaben gemacht.

5.1.6.2 FORTBILDUNG DER „HOT NEWS"-DOKTRIN

Die „Hot News"-Doktrin wurde zunächst in der Entscheidung *National Basketball Association v. Motorola*[392] und *Barclays Capital Inc. V. Theflyonthewall.com, Inc.*[393] in der dargelegten Form eingeschränkt (siehe dazu auch unter 3.3.2). Für Big-Data-Sachverhalte, bei denen gerade die Auswertung großer, bereits vorhandener Bestände an Daten in Rede steht und für die daher die „Hot-News"-Doktrin in der Regel nicht eingreift, soll aber nach Vorschlag von *Ekstrand/Roush* die „Hot News"-Doktrin einen Schutz vor der Nutzung von Daten bieten, wenn diese nicht als fair use gerechtfertigt ist.[394] Dabei soll die Zeitempfindlichkeit der Informationen eine besondere Rolle spielen. Dieser Vorschlag knüpft an verschiedene Vorschläge zur Reform der „Hot News"-Doktrin an,[395] bezieht sich aber spezifisch auf Big-Data-Sachverhalte. Bereits im Zusammenhang mit dem Vorschlag der Einführung eines Datenbankschutzes in den USA gab es Anregungen, Daten, die einen Wert im Markt haben, gegen die Nutzung durch Dritte zu schützen. Vorgeschlagen wurde insbesondere eine Sperrfrist für die Verwendung fremder Datenbestände einzuführen, gleichzeitig aber gewisse Daten-

---

[389] Vgl. hierzu z.B. *Rasmussen*, 17 Minn. J.L. Sci. & Tech. 489 et seq. (2016); *Ferrell*, 21 Drake J. Agric. L. 13 et seq. (2016); *Walter*, 2 Drake J. Agric. L. 431 (1997).

[390] *Privacy and Security Principles for Farm Data*, Am. Farm Bureau Fed'n (May 5, 2015), abrufbar unter: https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data, zuletzt abgerufen am 26.03.2018; vgl. auch: *Ferrell*, 21 Drake J. Agric. L. 13 et seq. (2016).

[391] *Manning*, 11 J. Food L. & Pol'y 113 et seq. (2015).

[392] National Basketball Assoc. v. Motorola, Inc., 105 F.3d 841 (2d Cir. 1997).

[393] Barclays Capital Inc. v. Theflyonthewall.com, Inc., 650 F.3d 876, 901 (2d Cir. 2011).

[394] Die Kriterien, nach denen sich ein solcher „fair use" richten soll, finden sich bei *Ekstrand/Roush*, 35 Cardozo Arts & Ent. L.J. 303, 337 et seq. (2017).

[395] Vgl. etwa: *Reichman/Samuelson*, 50 Vand. L. Rev. 51 (1997).

inhaber (insb. Sole-Source-Provider) zu einer Lizenzierung der Datenbestände zu fairen und nicht-diskriminierenden Bedingungen zu verpflichten.[396]

5.1.6.3 „DATARIGHT" NACH MATTIOLI

Mattioli schlägt außerdem die Normierung eines „dataright" vor, das im Wesentlichen darauf gerichtet ist, einen Anreiz für die Offenlegung von Daten und den Methoden ihrer Erhebung und Auswertung zu geben.[397] Danach würde demjenigen, der die Daten erhebt, das ausschließliche Recht zugestanden, die Daten zu nutzen, während die Vervielfältigung und Verbreitung der Daten nicht vom Ausschließlichkeitsrecht umfasst sein soll und daher grundsätzlich durch jedermann vorgenommen werden dürfte. Der Schutz könnte sich auf einzelne Daten oder Datenkorpora erstrecken.

Ziel ist es, einen fehlerfreien „secondary data use" v.a. in der Forschung zu ermöglichen, um diese hierdurch voranzutreiben. Ein solcher „secondary data use" kann umso erfolgreicher betrieben werden, wenn ein möglichst großer Anteil an (Forschungs-)Daten offengelegt wird. Dies zeigt beispielsweise die Stanford Drug Study, in der durch die Weiterverwendung von Daten aus Online-Sucheinträgen schädliche Wechselwirkungen zwischen Medikamenten festgestellt werden konnten. Durch die Auswertung dieser Online-Suchdaten wurde festgestellt, dass Nutzer, die nach den Medikamenten Paxil und Prevastatin gesucht haben, mit großer Wahrscheinlichkeit auch nach mit Hypoglykämie verbundenen Begriffen suchten. Dies führte die Wissenschaftler zu der später experimental bestätigten Hypothese, dass diese zwei Medikamente bei kombinierter Einnahme unerwünschte Nebeneffekte verursachen.[398]

Ein fehlerfreier „secondary data use" erfordert aber v.a. die Offenlegung der Methoden der Datenerhebung und -verarbeitung und ihres Kontextes. Denn werden Daten ohne die Offenlegung von Einzelheiten über ihre Erhebung weiterverarbeitet, kann es zu evidenten Fehlschlüssen kommen. Wertet man etwa die Status-Updates von Usern sozialer Netzwerke aus einer Zeit aus, zu der ein Hurrikan die Ostküste der Vereinigten Staaten trifft, stellt man fest, dass der Großteil der online publizierten Status-Updates aus urbanen Gebieten kommt, weil in diesen Gebieten eine große Anzahl von Usern sozialer Netzwerke leben. Nur eine viel kleinere Zahl der Status-Updates kommt aus Gebieten, die tatsächlich vom Hurrikan getroffen wurden, weil hier die Userzahl von Online-Netzwerken deutlich reduzierter ist. Eine hypothetische Datenbank, die jedes Online-Update mit dem Namen des Hurrikans enthält, würde, wenn sie anschließend von einem Dritten ausgewertet würde, fälschlicherweise da-

---

[396] Vgl. etwa: *Reichman/Samuelson*, 50 Vand. L. Rev. 51 (1997); vgl. auch: *Osborne Clarke LLP*, Legal study on ownership and access to data, 2016, p. 80 et seq.

[397] *Mattioli*, 99 Minn. L. Rev. 535, 538 (2014).

[398] *White/Tatonetti/Shah/Altman/Horvitz*, J Am Med Inform Assoc 404 et seq. (2013); *Mattioli*, 99 Minn. L. Rev. 535, 540 (2014).

rauf schließen lassen, dass vor allem die urbanen Regionen von dem Hurrikan betroffen waren, denn die meisten Status-Updates entstammten schließlich diesen Regionen. Wenn aber die Methode der Datenerhebung bekannt wäre (Suche nach jedem Online-Status der den Namen des Hurrikans enthält, unabhängig von der tatsächlichen Betroffenheit der Region), könnte diese Fehleinschätzung vermieden werden.[399]

5.1.7 VORSCHLÄGE ZUR AUSGESTALTUNG DER BESCHRÄNKUNGEN DES RECHTLICHEN UMGANGS MIT DATEN

Beschränkungen des rechtlichen Umgangs mit Daten ergeben sich de lege lata, wie dargelegt, insbesondere durch das Datenschutzrecht sowie durch Zugangsrechte zu Daten. Im datenschutzrechtlichen Bereich existieren im Wesentlichen zwei Vorschläge zur Ausgestaltung seines Verhältnisses zum zivilrechtlichen Umgang mit Daten de lege ferenda: Z.T. wird eine Beibehaltung der datenschutzrechtlichen Prinzipien und insbesondere der jederzeitigen Widerruflichkeit der Einwilligung gefordert, dem v.a. das Vertragsrecht angemessen Rechnung tragen müsse. Hier ist insbesondere die Problematik der Auswirkungen einer jederzeitigen Widerruflichkeit der Einwilligung vertragsrechtlich abzubilden.[400] Vorgeschlagen wird jedoch auch, die jederzeitige Widerruflichkeit der Einwilligung im Vertragsverhältnis einzuschränken, um eine rechtssichere Grundlage für Datenverarbeitungen auf vertraglicher Grundlage zu schaffen.[401]

Zugangsansprüche ließen sich v.a. sektorspezifisch auf weitere Bereiche erstrecken, wo eine Notwendigkeit für derartige Ansprüche festgestellt wird. Hingewiesen wird allerdings darauf, dass sie einen fairen Interessenausgleich gewährleisten müssten. Nicht jeder, der Daten innehat, kann gezwungen werden, sie zu jedwedem Zweck jedwedem Dritten zur Verfügung zu stellen.[402] Denn eine Reihe von Geschäftsmodellen beruhen mittlerweile fast ausschließlich auf einem Datenbestand, so z.B. soziale Netzwerke.[403] Eine generelle Zugangsverschaf-

---

399 *Hardy*, Why Big Data is not truth, NY Times, June 1st, 2013, abrufbar unter: https://bits.blogs.nytimes.com/2013/06/01/why-big-data-is-not-truth/?_r=0, zuletzt abgerufen am 04.05.2017; *Mattioli*, 99 Minn. L. Rev., 535, 540, 536, 547 (2014).

400 *Schmidt-Kessel/Grimm*, ZfpW 2017, 84, 102 ff.; *Specht*, JZ 2017, 763 ff.

401 *Sattler*, JZ 2017, 1036 ff.; *Linardatos*, Daten als Gegenleistung, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erschienen.

402 Vgl. hierzu: OLG Frankfurt a.M., Urt. v. 23.02.2017 – 6 U 31/16, BeckRS 2017, 108160 und hierzu: *Klein*, GRUR-Prax 2017, 243; vgl. hierzu auch: *Wiebe/Schur*, ZUM 2017, 461, 468: *„Solange der Staat nicht die Verantwortung für Informationsmärkte und deren Infrastruktur komplett übernommen hat, dürfte eine verfassungsrechtliche Pflicht zur positiven Öffnung privater Informationsquellen nicht begründbar sein;“* auch die EU-Kommission strebt kein generelles und allumfassendes Datenzugangsrecht an: Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD(2017) 2 final, p. 37 et seq.

403 *Drexl*, Designing Competitive Markets for Industrial Data -Between Propertisation and Access, 2016, MPI for Innovation & Competition ResearchPaper No. 16-13, abrufbar unter: https://ssrn.com/abstract=2862975, S. 41, zuletzt abgerufen am 26.03.2018.

fungspflicht würde diese Geschäftsmodelle sicherlich in ihrem Bestand gefährden. Eine Vereinbarkeit mit den Grundrechten ist zu gewährleisten.[404] Wird auf diese Vorgaben indes Acht gegeben, ließe sich durch die Normierung von Zugangsansprüchen im Gegensatz zu einer rein kartellrechtlichen Gewährung von Zugangsmöglichkeiten eine ex-ante-Regulierung anstreben,[405] was sicherlich zu einer begrüßenswerten Rechtssicherheit beitragen würde.

[404] Vgl. dazu v.a. *Wiebe*, CR 2017, 87, 92 ff.

[405] Demgegenüber reagiert das Kartellrecht auf einen Marktmachtmissbrauch und reguliert damit ex-post, vgl. *Drexl*, Designing Competitive Markets for Industrial Data -Between Propertisation and Access, 2016, MPI for Innovation & Competition ResearchPaper No. 16-13, abrufbar unter: https://ssrn.com/abstract=2862975, S. 44, zuletzt abgerufen am 26.03.2018.

5.2 ANALYSE

5.2.1 REGELUNGSGEGENSTAND

In der Analyse der vorgestellten Regulierungsansätze stellt sich zunächst die Frage, ob sich eine mögliche Regulierung allein auf nicht-personenbezogene Daten beschränken oder ebenso personenbezogene Daten erfassen soll. Hier erscheint eine Trennung zwischen nicht-personenbezogenen und personenbezogenen Daten in der Mehrzahl der Fälle nicht sinnvoll. Denn einerseits ist der Begriff des Personenbezugs im Datenschutzrecht sehr weit,[406] sodass eine Vielzahl der betroffenen Daten personenbezogen sind. Andererseits können selbst nicht-personenbezogene Daten durch Hinzufügung weiterer Daten zu personenbezogenen Daten werden, sodass es widersinnig scheint, bei der Etablierung von Rechten an Daten zwischen personenbezogenen und nicht-personenbezogenen Daten zu differenzieren.[407] Letztlich wird ein Datenbestand in der Regel sowohl aus personenbezogenen, als auch aus nicht personenbezogenen Daten bestehen. Hieraus können eine Vielzahl von Problemen entstehen, sodass es sinnvoll erscheint, wenn mögliche Rechtspositionen an Daten oder auch Zugangsrechte entweder sowohl personenbezogene als auch nicht-personenbezogene Daten adressieren oder aber rechtssichere Möglichkeiten einer Beseitigung des Personenbezugs etabliert werden (z.B. Standards zur Anonymisierung).[408]

Bereits das Datenschutzrecht unterscheidet aber verschiedene Datenkategorien, namentlich die sensiblen und die nicht-sensiblen personenbezogenen Daten, Art. 6 bzw. 9 DS-GVO sowie anonymisierte und nicht-anonymisierte Daten. Diese Unterscheidung muss sich sowohl bei der Zuweisung möglicher ausschließlichkeitsrechtlicher, als auch vertraglicher Rechtspositionen an Daten sowie bei der Etablierung von Zugangsrechten fortsetzen. Denn auch die Gewährung des Zugangs zu Daten ist eine datenschutzrechtlich relevante Handlung, die sich unmittelbar an den Vorgaben des Datenschutzrechts zu orientieren hat. Die ePrivacy-Verordnung, die als weitere Kategorie die Unterscheidung zwischen Kommunikationsdaten und anderen Daten einführt, ist ebenfalls zu beachten, sollte sie verabschiedet werden.

5.2.2 AUSSCHLIEßLICHKEITSRECHTLICHE ZUWEISUNG VON DATEN

Die Zuweisung möglicher ausschließlichkeitsrechtlicher Positionen an Daten stand in der europäischen Diskussion lange Zeit im Fokus, in den USA ist hier demgegenüber allenfalls eine Randdiskussion zu verzeichnen. Dort steht v.a. das Datenschutzrecht im Mittelpunkt der Er-

[406] Zur Reichweite des Personenbezugs vgl. insbesondere EuGH, Urt. v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779 = NJW 2016, 3579 – *Breyer*; Ehmann/Selmayr-*Klabunde*, Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 4 Rn. 5 ff.; Sydow-*Ziebart*, Europäische Datenschutz-Grundverordnung, 1. Aufl. 2017, Art. 4 Rn. 7 ff.; Paal/Pauly-*Ernst*, DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 3 ff.; Gola-*Gola*, DS-GVO, 1. Aufl. 2017, Art. 4 Rn. 3 ff.

[407] Vgl. hierzu bereits eingehend: *Specht*, GRUR Int. 2017, 1040, 1042.

[408] Hierzu eingehend: *Specht*, GRUR Int. 2017, 1040, 1047.

örterungen. Gegenüber der Normierung von Ausschließlichkeitsrechten vorzugswürdig erweisen könnte sich das flexiblere Schutzsystem des Wettbewerbsrechts. Wird auf eine Verhinderung der Amortisation als Grund für eine unmittelbare Schutzgewährung abgestellt, wie dies in der US-amerikanischen Misappropriation-Doktrin der Fall ist, so führte dies gewissermaßen zu einem wettbewerbsrechtlichen Investitionsschutz.[409]

5.2.2.1 DATENERZEUGERRECHT/DATENEIGENTUM

Der Entwurf eines Datenerzeugerrechts zielt darauf ab, den Handel mit nicht-personenbezogenen Daten zu verbessern.[410] Es sollen, um mit *Zech* zu sprechen *„klare Spielregeln"* auf dem Markt mit nicht-personenbezogenen Daten gelten.[411] Dies gilt auch und gerade vor dem Hintergrund, dass eine vertragsrechtliche Ausgestaltung des Datenhandels zwar möglich ist, das Vertragsrecht aber unionsrechtlich nicht harmonisiert ist und daher bereits innerhalb der Europäischen Union eine Vielzahl unterschiedlicher Regelungen gelten.[412] Das Datenerzeugerrecht/Dateneigentum ist jedoch umfassender Kritik ausgesetzt,[413] tatsächlich ist es allerdings durchaus möglich, dass Ausschließlichkeitsrechte den Handel mit Daten befördern, wenn nicht abdingbare Beschränkungen und Ausnahmen vorgesehen werden.[414] Dies zeigt das UsedSoft-Urteil des EuGH, das einen Markt für Gebrauchtsoftware geschaffen hat, der zuvor über vertragliche Vereinbarungen verhindert wurde.

Die Beantwortung der Frage, ob eine ökonomische Notwendigkeit für ein solches Ausschließlichkeitsrecht existiert, ist nicht Gegenstand des Gutachtenauftrags.[415] Ein Kopierproblem, das behoben werden soll, besteht jedenfalls nicht aktuell und wird sicherlich auch zukünftig jedenfalls nicht generell auftreten.[416] Sobald sich ein solches aber für bestimmte Sektoren ergibt, wäre auch die ökonomische Notwendigkeit erneut zu diskutieren. Denn über den deliktischen Schutz des Trägermediums kann zwar ein Löschen oder ein anderwei-

---

409 Harte-Bavendamm/Henning-Bodewig-*Sambuc*, UWG, 4. Aufl. 2016, Rn. 62.

410 Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD (2017) 2 final, p. 36.

411 *Zech*, GRUR 2015, 1151, 1153.

412 *Van Asbroeck/Debussche/César*, White Paper 2017 – Data ownership in the context of the European data economy: proposal for a new right, pp. 112, 119.

413 Vgl. etwa: Bericht der Arbeitsgruppe „Digitaler Neustart" v. 15.05.2017, S. 7 ff. m.w.Nachw., abrufbar unter: https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf, zuletzt abgerufen am 10.03.2018; *Steinrötter*, MMR 2017, 731 ff.

414 *Farkas*, 23 Rev. Prop. Inmaterial 5, 12 (2017).

415 Zu Anreizwirkungen vgl. aber: *Heymann*, CR 2016, 650, 653 ff.

416 Zur fehlenden ökonomischen Rechtfertigung von Ausschließlichkeitsrechten an Daten vgl. v.a. *Kerber*, 47 IIC 759 (2016); *ders./Frank*, Data Governance Regimes in the Digital Economy: The Example of Connected Cars, 2017; *Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblytė/Wiedemann*, GRUR Int. 2016, 914, 915; *Spindler*, ZGE 2017, 399, 401.

tiges Zerstören oder Verändern von Daten erfasst werden, der eigentumsrechtliche Schutz des Trägermediums endet aber dort, wo Daten nicht zerstört oder verändert, sondern lediglich kopiert werden.[417]

Hervorgehoben sein soll, dass ausschließlichkeitsrechtliche Positionen an Daten nicht notwendigerweise als allumfassendes, eigentumsähnliches Recht ausgestaltet sein müssen, sondern durchaus auch nur einzelne Nutzungs- und Abwehrbefugnisse umfassen könnten.[418] Dies wird in der Diskussion um ein Datenerzeugerrecht z.T. verfälscht dargestellt. Auch könnte ein Ausschließlichkeitsrecht nicht-exklusiv ausgestaltet sein, d.h. mehreren Personen zustehen, dennoch aber eine Abwehrkomponente gegenüber Nichtberechtigten enthalten.[419] Dies zieht nun auch die EU-Kommission in Betracht.[420] Erst im Falle einer ökonomischen Notwendigkeit einer solchen Rechtsposition aber stellte sich die Frage seiner Zuweisung überhaupt, für deren Beantwortung die o.g. Modelle zur Verfügung stehen. Nicht ausgeschlossen ist es etwa, dass sich zukünftig sektorspezifischer Regulierungsbedarf ergibt.

Sollte sich eine ökonomische Notwendigkeit für ein Ausschließlichkeitsrecht ergeben, scheint ein solches Recht – wie immer es auch ausgestaltet sein würde – verfassungsrechtlich zumindest dann denkbar, wenn die Grundrechte und Interessen von Rechtsinhabern und der Allgemeinheit durch Schranken und Zugangsrechte ausreichend berücksichtigt würden.[421]

5.2.2.2 EXTENSIVE AUSLEGUNG DES DATENBANKSCHUTZES

Auch eine Erweiterung des Datenbankschutzes gem. § 87a UrhG kann sicherlich dort, wo eine ökonomische Notwendigkeit einer solchen Rechtsnotwendigkeit festgestellt werden kann, sinnvoll sein.[422]

---

[417] So zutreffend: *Härting*, CR 2016, 646, 647.

[418] *Dreier, in:* Weller/Wendland, Digital Single Market: Bausteine eines digitalen Binnenmarktes, 2018, im Erscheinen; *Specht*, CR 2016, 288 ff.

[419] *Van Asbroeck/Debussche/César*, White Paper 2017 – Data ownership in the context of the European data economy: proposal for a new right, p. 121.

[420] Annex to the Synopsis Report Consultation on the „Building a European Data Economy" Initiative, p. 22 et. seq., abrufbar unter: http://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf; zuletzt abgerufen am: 26.03.2018.

[421] Wiebe/Schur, ZUM 2017, 461, 473: „So wäre ein Datenrecht, das zu einer breiten Monopolisierung von Informationen führt, nicht mit der Verfassung vereinbar. Im Spannungsverhältnis zwischen einem Recht an Daten und der Informationsfreiheit bedarf es jedenfalls gewichtiger Inhaltsbeschränkungen für ein mögliches Eigentumsrecht"; zu möglichen Schranken vgl. insb. Wiebe, CR 2017, 87, 90; Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD(2017) 2 final, p. 35 et seq.

[422] Gegen eine ökonomische Notwendigkeit der Ausweitung des Datenbankschutzes aber: *Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblytė/Wiedemann*, GRUR Int. 2016, 914, 915.

Hierbei ist allerdings – ebenso wie für ein mögliches Datenerzeuger- oder anderweitig eigentumsähnlich ausgestaltetes Recht an Daten– anzumerken, dass durch all diese Rechtspositionen die faktische Stellung des Dateninhabers rechtlich noch gestärkt würde. Bei extensiver Auslegung des Datenbankherstellerrechts erforderlich ist daher, ebenso wie im Falle der Zuweisung anderer Ausschließlichkeitsrechte an denjenigen, der ohnehin faktisch über die Verwendung der Daten bestimmen kann, auch eine substanzielle Erweiterung des Schrankenkatalogs sowie allgemeine Zugriffsrechte, nicht nur im Wege des Kartellrechts.[423]

Ob sich das Leistungsschutzrecht des Datenbankherstellers noch weitergehend ausgestalten ließe, als dies derzeit angedacht wird (wenn auch nicht im Wege der Auslegung, dann doch jedenfalls durch einen gesetzgeberischen Akt) ist sicherlich eine Frage des Regulierungszieles. Einerseits wurde der Ausschluss des Investitionsschutzes in die Datenerzeugung auch und gerade mit der Notwendigkeit der Vermeidung einer Monopolisierung von Daten begründet.[424] Dieser Gefahr muss jedoch nicht zwingend durch einen gänzlichen Ausschluss der Datenerzeugung aus dem Datenbankherstellerrecht Rechnung getragen werden, ihr ließe sich ebenso durch die Normierung entsprechender Zugangsrechte begegnen. Die schwierige Abgrenzung von Datensammlung und Datenerzeugung führt in der Praxis zu Rechtsunsicherheit, die politisch gerade vermieden werden soll.[425] Erachtet man außerdem die im Rahmen der Schrankenbestimmungen für jedermann freie Datennutzung jedenfalls als Sekundärzweck des Datenbankschutzes und möchte man eine solche Freiheit der Datennutzung fördern, könnte auch dies als Argument für einen möglichst weiten Anwendungsbereich in Kombination mit ebenfalls weiten Schrankenbestimmungen herangezogen werden.[426] Andererseits kann Nutzungsfreiheit auch ohne ein Ausschließlichkeitsrecht gesetzlich normiert werden, sodass es eines solchen nicht unbedingt bedarf. Überdies würde die Berücksichtigung von Investitionen in die Datenerzeugung einen Anreiz zur Erzeugung von Daten begründen, was de lege lata gerade nicht der Fall sein soll.[427] Diese Aspekte sind zu berücksichtigen, sollte eine mögliche Ausweitung des Datenbankschutzes de lege ferenda in Betracht kommen.

5.2.2.3 US-AMERIKANISCHES „DATARIGHT“

Die Erwägungen im US-amerikanischen Recht zugunsten eines „datarights“ haben einen gänzlich anderen Zweck als die im europäischen Rechtsraum diskutierten Vorschläge. Ob die

---

[423] So zutreffend: *Wiebe*, GRUR 2017, 338, 345.

[424] *Leistner*, K&R 2007, 457, 458 ff.; *Schmidt/Zech*, CR 2017, 417, 421.

[425] BMWi, Weißbuch Digitale Plattformen, 2017, S. 66.

[426] Vgl. hierzu etwa: *Schmidt/Zech*, CR 2017, 417, 426.

[427] EuGH, Urt. v. 09.11.2004 – C-203/02, ECLI:EU:C:2004:695 = GRUR Int. 2005, 247 Tz. 31 ff. – *The British Horseracing Board u.a.*; vgl. auch: *Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblytė/Wiedemann*, GRUR Int. 2016, 914, 915.

Offenlegung von Daten und den Methoden ihrer Erhebung tatsächlich über das vorgeschlagene „dataright“ erreichbar ist, scheint zumindest streitbar. Soll lediglich das Nutzungsrecht zugewiesen werden, nicht aber das Vervielfältigungs- und Verbreitungsrecht, fragt sich, wie eine unberechtigte Nutzung in der Praxis bewiesen werden soll. Einen Anreiz zur Veröffentlichung entsprechender Daten kann ein Recht wohl nur dann geben, wenn es auch entsprechend durchsetzbar ist.

Inhaltlich wäre ein solches US-amerikanisches „dataright“ ebenso wie andere Ausschließlichkeitsrechte an Daten vor das Problem gestellt, wie der Datenproduzent bestimmt werden soll. Ist dies derjenige, der die Mittel herstellt (Gerätschaften, Software etc.), mit denen die Daten erhoben werden, derjenige, der die Daten erhebt oder ist der Datenproduzent nicht vielmehr derjenige, von dem die Daten stammen, die natürliche Person also, über deren Verhalten die Daten etwas aussagen oder in deren Eigentum die Gerätschaft steht, mit der die personenbezogenen Daten erhoben werden?

Auch wäre ein US-amerikanisches „dataright“ ebenso wie der zivilrechtliche Umgang mit Daten generell vor die Frage gestellt, wie es mit geltendem Datenschutzrecht in Einklang zu bringen ist. Zwar ist das US-amerikanische Datenschutzrecht weniger streng ausgestaltet als das europäische Datenschutzrecht, eine gänzlich freie Datenverarbeitung lässt aber auch das US-amerikanische Datenschutzrecht nicht zu. Ob überhaupt ein Anreiz gegeben werden sollte, personenbezogenen Daten stärker zu veröffentlichen und zu verbreiten, darf auch insgesamt bezweifelt werden. Die Datenschutz-Grundverordnung strebt mit dem Grundsatz der Datenminimierung und der Speicherbegrenzung das exakte Gegenteil an. Das gilt besonders für sensible Daten, z.B. Gesundheitsdaten.

5.2.3 DATENSCHULDRECHT UND DATENSCHUTZRECHT

5.2.3.1 REGULIERUNGSBEDARF?

Ein möglicher Regulierungsbedarf im Vertragsrecht lässt sich aus drei Richtungen betrachten: Erstens könnten angemessene gesetzliche Rahmenbedingungen den Datenverkehr erleichtern, indem sie ihn auf rechtssichere Grundlage stellen und so Transaktionskosten verringern. Zweitens könnten Regelungen zur Klauselkontrolle jedenfalls in gewissem Maße Machtungleichgewichte zwischen den Vertragsparteien ausgleichen. Allerdings fehlen zu beiden Aspekten bislang tiefergehende empirische Studien, die genauer analysieren, ob sich der bisherige vertragsrechtliche Rahmen tatsächlich als Hemmnis für den Handel mit Daten erweist.
Drittens aber ist auch die datenschutzrechtliche Perspektive zu betrachten, denn der vertragsrechtliche Umgang mit Daten ist bereits de lege lata nicht auf nicht-personenbezogene Daten beschränkt. Hier ist nicht einmal abschließend geklärt, welche Leistung und Gegenleistung in einem Datenerhebungs- bzw. Datenüberlassungsvertrag geschuldet ist, geschweige denn, welche Rechtsfolgen ein Einwilligungswiderruf auf das zugrundeliegende Vertragsverhältnis haben könnte. Kann auch hier nur gemutmaßt werden, dass dies zu er-

heblicher Rechtsunsicherheit auf den betroffenen Datenmärkten führt, weil auch hier umfassende empirische Studien fehlen, so besteht im Datenschuldrecht zumindest deshalb gesetzgeberischer Handlungsbedarf, weil die Willenserklärungen der Vertragsparteien in einer Vielzahl datengetriebener Geschäftsmodelle nach zivilrechtlichen Grundsätzen nicht anders ausgelegt werden können, als dass die datenschutzrechtliche Einwilligung als Gegenleistung im Vertrag geschuldet ist. Für diese Fälle ist zwingend zu klären, wie datenschutzrechtliche Vorgaben in eine den Grundsätzen der Privatautonomie folgende Rechtsordnung eingebettet werden sollen.[428]

5.2.3.2 GUIDANCE DOCUMENT, STANDARDVERTRAGSKLAUSELN UND GESETZLICHE AUSGESTALTUNG VON PRIMÄREM UND SEKUNDÄREM DATENMARKT

Stünden einzig nicht-personenbezogene Daten in Rede, würde die Ausgestaltung eines Datenschuldrechts vermutlich recht leicht gelingen. Da es aber aus den benannten Gründen wenig Sinn macht, vertragliche Vorgaben differenziert nach personenbezogenen und nicht-personenbezogenen Daten zu entwickeln, sind die Besonderheiten des Datenschutzrechts in einem möglichen Datenschuldrecht mit zu berücksichtigen.

5.2.3.2.1 REGULIERUNG DES SEKUNDÄREN DATENMARKTES

Orientiert werden könnte sich für eine vertragliche Ausgestaltung einerseits am Geschäftsgeheimnisschutz und andererseits am Urheberrecht. Der Geschäftsgeheimnisschutz taugt dabei im Wesentlichen für den sekundären B2B-Datenmarkt.[429] Solange weder an Daten, noch an Geschäftsgeheimnissen Ausschließlichkeitsrechte mit Nutzungs- und Abwehrfunktion bestehen, ähneln sich beide Vertragsgegenstände, sodass für die Entwicklung eines gesetzlichen Rahmens, Standardvertragsklauseln oder eines Guidance Documents für den sekundären Datenmarkt möglicherweise zumindest teilweise an den ausdifferenzierten Verträgen zur Nutzung von Geschäftsgeheimnissen Anklang genommen werden könnte. Auch für den primären B2B-Datenmarkt könnten diese Standardvertragsklauseln taugen. Entwickelt werden könnten derartige Regelungen durch eine aus Praxis, Wissenschaft und Politik besetzte Expertenkommission.[430]

---

[428] Hierzu eingehend: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit - Eckpfeiler eines neuen Datenschuldrechts, abrufbar unter: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Specht_Datenschuldrecht4.pdf, zuletzt abgerufen am 03.05.2018.

[429] Vgl. für Maschinendaten: *Sattler*, in: Sassenberg/Faber, Rechtshandbuch Industrie 4.0 und Internet of Things, 2017, S. 27, 49 ff.

[430] Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD (2017) 2 final, p. 31.

Die Intensität der Beschränkung der Privatautonomie steigert sich stufenweise vom Guidance Document, über Standardvertragsklauseln, bis zu gesetzlich vorgegebenen, nicht zwingenden und schließlich zwingenden Regelungen. Verfassungsrechtlich bedarf jeder Eingriff in die über Art. 2 Abs. 1 GG gewährleistete Privatautonomie einer Rechtfertigung. Ein zu weitgehender Eingriff kann sich als unverhältnismäßig erweisen, weshalb auch für eine Regulierung des Vertragsrechts zunächst nach einem legitimen Zweck gefragt werden muss. Machtungleichgewichte der Vertragsparteien können dabei zu einer Einschränkung der materialen Privatautonomie der unterlegenen Vertragspartei führen, die es rechtfertigt, in die Privatautonomie der überlegenen Vertragspartei durch gesetzliche Regulierung einzugreifen. D.h. Einschränkungen der Privatautonomie dienen zugleich ihrer Sicherung. Es handelt sich um eine grundrechtsdogmatische Anomalie, da ein einziges Grundrecht gewissermaßen mit sich selbst kollidiert. Die Garantie der Privatautonomie in Art. 2 Abs. 1 GG wandelt sich bei struktureller Unterlegenheit einer Vertragspartei daher von einem Freiheitsrecht in eine Freiheitsschranke.[431]

Die konkrete Wahl des Mittels (Guidance Document, Standardvertragsklauseln, zwingende oder nicht-zwingende gesetzliche Vorgaben) muss sich als geeignet, erforderlich und angemessen für die Erfüllung des konkreten Regulierungszwecks darstellen. Insofern scheint auch hier ein sektorspezifisches Vorgehen ratsam. Ergeben sich in spezifischen Sektoren strukturelle Unterlegenheitsszenarien, lässt sich durchaus über eine intensivere Regulierung nachdenken. Das Ziel der Rechtssicherheit ließe sich dagegen sicherlich bereits über entsprechende sektorspezifische Guidance Documents unterstützen.

5.2.3.2.2 REGULIERUNG DES PRIMÄREN DATENMARKTES

Angesichts der verfolgten Interessen auf dem primären B2C-Datenmarkt ist hier wohl eher über eine Anklangnahme beim Urhebervertragsrecht nachzudenken. *Schwartmann/Hentsch* befürworten auch für eine solche sich am Urhebervertragsrecht orientierende Ausgestaltung eines (auch) personenbezogene Daten umfassenden Datenschuldrechts ein Dateneigentum.[432] Richtig daran ist, dass das informationelle Selbstbestimmungsrecht de lege lata als reines Persönlichkeitsrecht ausgestaltet ist, das sich durch Unübertragbarkeit[433], Unpfändbarkeit[434], Unvererblichkeit[435] und Unverzichtbarkeit[436] auszeichnet.[437] Vermögensrechte

---

[431] *Isensee*, Vertragsfreiheit im Griff der Grundrechte – Inhaltskontrolle von Verträgen am Maßstab der Verfassung, in: Hübner/Ebke, Festschrift für Bernhard Großfeld zum 65. Geburtstag, 1999, S. 485, 508; vgl. auch: *Canaris*, AcP 200 (2000), 273, 299.

[432] *Schwartmann/Hentsch*, PinG 2016, 117, 122 f.

[433] *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995, S. 8.

[434] *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 132.

[435] BGH, Urt. v. 20.03.1968 - I ZR 44/66, NJW 1968, 1773 – *Mephistopheles*.

[436] *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 132.

hingegen werden geprägt durch Veräußerlichkeit, Vererblichkeit, Pfändbarkeit und Verzichtbarkeit.[438] Persönlichkeitsrechte wurden und werden z.T. noch heute insoweit als antinomischer Gegensatz zu den dem Eigentumsrecht unterliegenden Vermögensrechten erachtet.[439] Wird nach einer urheberrechtsähnlichen Ausgestaltung des Datenschutzrechts verlangt,[440] so ist eine Ausgestaltung des informationellen Selbstbestimmungsrechts als Vermögensrecht aber nicht zwingend erforderlich. Denn übertragen werden könnte dieses Recht ohnehin weder translativ, noch können ausschließliche Rechtspositionen eingeräumt werden. Dem sperrt sich das informationelle Selbstbestimmungsrecht schon aufgrund seiner Menschenwürdekomponente.[441] Eingeräumt werden könnten insofern auch bei eigentumsrechtlicher Ausgestaltung des Persönlichkeitsrechts allein einfache Lizenzen, was indes keinen Vorteil gegenüber einer auch bei nicht-eigentumsrechtlicher Ausgestaltung des informationellen Selbstbestimmungsrechts möglichen schuldrechtlichen Gestattung zur Nutzung von Daten hätte.[442] Auch bei nicht-eigentumsrechtlicher Ausgestaltung des informationellen Selbstbestimmungsrechtes ließen sich in einem möglichen Datenschuldrecht dem Urheberrecht entsprechende Schrankenbestimmungen zugunsten des Datenschuldners oder auch eine Verpflichtung zu einer angemessenen Vergütung normieren (kritisch dazu in der Analyse unter 7.). Der Ausgestaltung eines dem Betroffenen zuzuordnenden Dateneigentums bedarf es hierfür nicht.

5.2.3.2.3 KONKRETE INHALTE EINES DATENSCHULDRECHTS

Primärer und sekundärer Datenmarkt lassen sich zwar theoretisch mit den zur Verfügung stehenden Vertragstypen erfassen, was bereits eingehend dargelegt wurde. Regulierungsbedarf ergibt sich aber für die Ausgestaltung des primären Marktes mit personenbezogenen

---

[437] *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 91 m.w.Nachw.; für eine vermögensrechtliche Ausgestaltung spricht sich v.a. *Kilian* aus; vgl. zuletzt: *Kilian*, CR 2012, 169, 173 ff.

[438] *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995, S. 9; vgl. auch: *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 132.

[439] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 214; *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995, S. 4, jeweils m.w.Nachw.; a.A.: *von Gierke*, Deutsches Privatrecht, Bd. I, 1936, S. 706; *Hubmann*, Das Persönlichkeitsrecht, 1967, S. 132 f., die jeweils darauf abstellen, dass neben den ideellen Bestandteilen das Persönlichkeitsrecht auch kommerzielle Bestandteile aufweise; *Götting*, Persönlichkeitsrechte als Vermögensrechte, 1995, S. 7: Persönlichkeitsrechte betrafen immer schon auch Rechtspositionen, die zwar in einer engen Verbindung zur Persönlichkeit stehen, bei denen es aber auch und zum Teil sogar vorrangig um den Schutz wirtschaftlicher Interessen geht; vgl. hierzu auch: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 91.

[440] So etwa auch: *Berger*, ZGE 2017, 340, 352.

[441] *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, Kapitel 6.

[442] Hierzu bereits ausführlich: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, Kapitel 6; zur Möglichkeit der schuldrechtlichen Gestattung: *Sattler*, JZ 2017, 1036, 1043 ff.

Daten. Willenserklärungen, die auf den Abschluss eines Vertrags gerichtet sind, mit dem einerseits die Erbringung einer Leistung vereinbart wird, die Vertragsgegenseite aber gleichzeitig verpflichtet wird, Daten, die nicht für die Erbringung dieser Leistung erforderlich sind, zu überlassen und ihre Verarbeitung zu gestatten, können nach den Grundätzen von §§ 133, 157 BGB jedenfalls bei Registrierung der Nutzer in der Regel nicht anders ausgelegt werden, als dass die Überlassung der Daten und die Erklärung der datenschutzrechtlichen Einwilligung als Gegenleistung geschuldet sind. Wenn dies aber der Fall ist, müssen die datenschutzrechtlichen Grundsätze im Interesse eines effektiven Persönlichkeitsrechtsschutzes des Betroffenen in das Zivilrecht transportiert werden. Neben dieser erforderlichen Verzahnung von Datenschutzrecht und Vertragsrecht (Widerruflichkeit der Einwilligung, Folgen eines Widerrufs, Klagbarkeit der Einwilligung, Nacherfüllungsverlangen etc.)[443] sind v.a. Grundsatzfragen zu klären, etwa die Anwendbarkeit der §§ 312 ff. BGB, die Buttonlösung, § 312j Abs. 3, 4 BGB, die Möglichkeit der Ausübung von Zurückbehaltungsrechten und das Konkurrenzverhältnis zwischen vertraglichen Schadensersatzansprüchen und solchen aus der Datenschutz-Grundverordnung.[444] Die Entwicklung eines Datenschuldrechts ist nicht Gegenstand des Gutachtenauftrags, es wird aber jedenfalls die Möglichkeit der Anlehnung eines solchen Datenschuldrechts an das Urheberrecht erörtert. Denn die hierin enthaltende Grundforderung nach einer angemessenen Vergütung des Betroffenen ist eine solche, die in der Diskussion unter das Stichwort des „Dateneigentums“ gefasst wird.[445]

Auch in den USA gehen die Überlegungen dahin, den primären Datenmarkt auf vertraglicher Basis angemessener zu erfassen und hier über „default rules“ zu einem angemessenen Interessenausgleich zu kommen. Anklang nehmen möchte das US-amerikanische Recht dabei auch für den primären Datenmarkt nicht beim Urheberrecht, sondern beim Trade-Secret-Schutz. Dies liegt allerdings in der Schwäche des US-amerikanischen Datenschutzrechts begründet, das kein grundsätzliches Verbot der Datenverarbeitung kennt. Über die Anlehnung an Lizenzierungspraktiken des Geschäftsgeheimnisschutzes, denen ein grundsätzliches Unterlizenzierungsverbot immanent ist, soll es daher gelingen, ein Weitergabeverbot (bzw. eine Geheimhaltungspflicht) auch für personenbezogene Daten zu etablieren.[446] Die Angemessenheit der Vergütung soll dem Markt überlassen werden.

Vertraut man indes nicht darauf, dass der Markt den angemessenen Preis für personenbezogene Daten schon ausreichend regeln wird, ließe sich daran denken, Regelungen entspre-

---

[443] Vg. Hierzu eingehend: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[444] Vgl. hierzu bereits ausführlicher: *Schmidt-Kessel/Grimm*, ZfpW 2017, 84, 102 ff.; *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, abrufbar unter:https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Specht_Datenschuldrecht4.pdf, zuletzt abgerufen am 03.05.2018

[445] *Fezer*, ZD 2017, 99 ff.

[446] *Samuelson*, 52 Stan. L. Rev. 1125, 1157 (2000).

chend § 32 UrhG auch in einem „Datenschuldrecht“ zu verankern. Die Angemessenheit ließe sich auch hier durch die Einrichtung von Entscheidungsgremien ähnlich den in § 36 UrhG benannten Vereinigungen durch gemeinsame Vergütungsregeln bestimmen. An eine Regelung zur angemessenen Vergütung könnte man insbesondere deshalb denken, weil die Einwilligung als Gegenleistung im Vertrag nicht der AGB-Kontrolle unterliegt und daher der Preis für die Erklärung durch AGB nicht kontrolliert werden kann; der AGB-Kontrolle unterliegen einzig die für die Einwilligung erforderlichen Informations- und Transparenzvorgaben.[447]

Aus ökonomischer Perspektive lässt sich gegen einen Anspruch auf angemessene Vergütung entsprechend § 32 UrhG allerdings argumentieren, dass der Betroffene, anders als der Urheber, keine eigene Leistung erbracht hat, die etwaige Ansprüche rechtfertigen könnte.[448] Ob es hierfür ausreichen kann, dass der Betroffene eine Datenverarbeitung und damit eine Kommerzialisierung seiner selbst erleidet und damit eine Opferleistung erbringt,[449] oder aber ob die Heranziehung des Leistungskriteriums in diesem Kontext gänzlich ungeeignet ist, weil es allein eine Güterzuordnung konstituiert,[450] es im Falle des § 32 UrhG aber um die Herstellung von Vertragsgerechtigkeit geht, soll hier nicht weiter erörtert werden. Denn zuzugeben ist jedenfalls, dass ein solcher Anspruch einen nicht unerheblichen Verwaltungsaufwand nach sich ziehen würde.[451] Darüber hinaus besteht eine gewisse Wahrscheinlichkeit, dass Unternehmen diese Vergütungsansprüche der Betroffenen schlicht einpreisen, wenn es um den Verkauf ihrer datenerhebenden Produkte geht, sodass eine Vergütung jedenfalls im Ergebnis nicht zu einem Vermögenszuwachs des Betroffenen führen würde. Auch darf bezweifelt werden, ob ein solcher Anspruch nicht Fehlanreize zu einer noch stärkeren Datenpreisgabe setzt.

Explizit soll hier keine Empfehlung für oder gegen einen solchen Vergütungsanspruch ausgesprochen, sondern nur auf die Möglichkeit eines solchen Anspruchs und auf mögliche durch ihn entstehende Probleme hingewiesen werden. Sehr viel wichtiger als die Etablierung eines solchen Vergütungsanspruches scheint es aber zu sein, das datenschutzrechtliche Problem nicht ausreichender Informiertheit der Betroffenen zu lösen, das häufig einen gegenüber der fehlenden Vergütung sehr viel wesentlicheren Beitrag dazu leisten dürfte, dass sich diese übervorteilt fühlen, wenn Dritte mit der Verarbeitung der sie betreffenden personenbezogenen Daten Vorteile erzielen.[452]

---

[447] So zutreffend ebenfalls: Sattler, JZ 2017, 1036, 1045.

[448] So etwa: *Bisges*, MMR 2017, 301, 303 ff.

[449] *Hermann*, Der Werbewert der Prominenz, 2012.

[450] Vgl. hierzu: *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, S. 93 ff.

[451] *Bisges*, MMR 2017, 301, 304.

[452] Dazu eingehend: *Specht/Bienemann*, Visualisierung von Information – Ein Weg aus dem Privacy Paradox?, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, im Erscheinen, m.w.Nachw.

Verträge über unbekannte Nutzungsarten i.S.d. § 31a UrhG scheinen mit dem das Datenschutzrecht prägenden Zweckbindungsgrundsatz dagegen nicht in Einklang zu stehen. Möchte man den Zweckbindungsgrundsatz lockern, um z.B. Big-Data-Anwendungen rechtskonform zu ermöglichen, die sich gerade dadurch auszeichnen, dass Daten in einer zuvor nicht bekannten Art und Weise zusammengeführt und ausgewertet werden, ist dies eine rechtspolitische Entscheidung, die durch Fruchtbarmachung einer dem § 31a UrhG entsprechenden Regelung gelingen könnte, die den Zweckbindungsgrundsatz aber nicht unerheblich einschränken würde. Eine dem § 32c UrhG entsprechende Regelung wird nicht benötigt, solange der Zweckbindungsgrundsatz in seiner jetzigen Form fortbesteht und Verträgen über unbekannte Nutzungsarten entgegensteht. Ein Bestsellerparagraph, nach dem der Nutzer für den Fall, dass mit den ihn betreffenden personenbezogenen Daten besonders hohe Gewinne erzielt werden, zu vergüten ist, dürfte im Falle der Nutzung von Daten nicht erforderlich sein. Die mit einem solchen Nachvergütungsanspruch einhergehenden Auskunftsansprüche gem. §§ 32d und e UrhG, nach denen der Nutzer über den Umfang der Werknutzung und die hieraus gezogenen Erträge und Vorteile zu beauskunften ist, würden in Anbetracht der Vielzahl von verarbeiteten Daten zu einem nicht mehr zu vertretenden Aufwand für den Datenverarbeiter führen und nicht in einem angemessenen Verhältnis zu den mit dem jeweiligen Einzeldatum erzielten Gewinnen stehen. Auch Regelungen entsprechend den §§ 33, 34, 35 UrhG sind nicht erforderlich, da ausschließliche Rechte an personenbezogenen Daten nicht eingeräumt werden können und die Weiterübertragung personenbezogener Daten (nebst der Befugnis ihrer Verwendung) im Datenschutzrecht durch das Verbotsprinzip und die entsprechenden Erlaubnistatbestände bereits geregelt ist.

5.2.4 BESCHRÄNKUNG EINES ZIVILRECHTLICHEN UMGANS MIT DATEN

5.2.4.1 BESCHRÄNKUNG DURCH ZUGANGSRECHTE

Werden Ausschließlichkeitsrechte an Daten zugewiesen, bedürfen diese Ausnahmen und Beschränkungen zugunsten verschiedener Interessen. Die bereits de lege lata existierenden Zugangsansprüche auf staatliche Informationen, etwa durch die Informationsfreiheitsgesetze, oder auch im Automotive-Bereich wurden bereits dargelegt.[453]

Wo sich die Notwendigkeit ergibt,[454] könnten de lege ferenda Zugangsansprüche generell oder sektorspezifisch, entgeltlich oder unentgeltlich ausgestaltet werden, sie könnten han-

[453] Vgl. hierzu 4.1.

[454] Beispielsweise könnten Daten für die Entwicklung neuer Produkte oder das Anbieten von Dienstleistungen erforderlich sein, das betroffene Unternehmen aber außerstande, die Daten selbst zu erzeugen, vgl. hierzu auch: *Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblytė/Wiedemann*, GRUR Int. 2016, 914, 917; für weitere Beispiele vgl. auch: *Spindler*, ZGE 2017, 399, 402.

delbar oder personengebunden sein.[455] In jedem Fall aber müssen derartige Zugangsansprüche einen fairen Interessenausgleich gewährleisten und dürfen nicht per se gegen jeden bestehen, der Daten faktisch innehat.[456] Eine Vereinbarkeit mit den Grundrechten, v.a. mit der Berufsfreiheit, ist hier zu gewährleisten.[457] Im Gegensatz zu einer rein kartellrechtlichen Ausgestaltung von Zugangsmöglichkeiten ließe sich durch die Normierung von Zugangsansprüchen[458] dort, wo diese im gesamtgesellschaftlichen Interesse notwendig sind, eine ex-ante-Regulierung realisieren. Dies erfordert freilich vorab eine politische Einigung auf diese Bereiche und die Bedingungen, unter denen Zugang gewährt werden soll.[459] Die EU-Kommission schlägt eine Gewährleistung von Zugangsansprüchen unter FRAND-Bedingungen vor.[460] Gebunden sein müssen alle diese Zugangsansprüche an die Vorgaben des Datenschutzrechtes, denn die Zugangsgewährung ist eine Datenverarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO.

Im Bereich personenbezogener Daten existieren nicht nur Zugangsrechte (Auskunftsrechte), sondern auch ein Recht auf Datenportabilität. Ein solches Recht auf Datenportabilität wird

---

[455] Vgl. hierzu auch: Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD(2017) 2 final, p. 36 et seq.; vgl. auch die Empfehlungen der OECD, abrufbar unter: http://www.oecd.org/sti/ieconomy/enhanced-data-access.htm, zuletzt abgerufen am: 13.02.2018; für die Einführung von Zugangsansprüchen durch den Gesetzgeber auch: *Grützmacher*, CR 2016, 485, 492.

[456] Vgl. hierzu: OLG Frankfurt a.M., Urt. v. 23.02.2017 – 6 U 31/16, BeckRS 2017, 108160 und hierzu: *Klein*, GRUR-Prax 2017, 243; vgl. hierzu auch: *Wiebe/Schur*, ZUM 2017, 461, 468: *„Solange der Staat nicht die Verantwortung für Informationsmärkte und deren Infrastruktur komplett übernommen hat, dürfte eine verfassungsrechtliche Pflicht zur positiven Öffnung privater Informationsquellen nicht begründbar sein;"* auch die EU-Kommission strebt kein generelles und allumfassendes Datenzugangsrecht an: Commission Staff Working Document on the free flow of data and emerging issues of the European data economy p.o. 10.01.2017, SWD(2017) 2 final, p. 37 et seq.

[457] Vgl. dazu v.a. *Wiebe*, CR 2017, 87, 92 ff.

[458] Demgegenüber reagiert das Kartellrecht auf einen Marktmachtmissbrauch und reguliert damit ex-post, vgl. *Drexl*, Designing Competitive Markets for Industrial Data -Between Propertisation and Access, 2016, MPI for Innovation & Competition ResearchPaper No. 16-13, abrufbar unter: https://ssrn.com/abstract=2862975, S. 44, zuletzt abgerufen am 26.03.218.

[459] Zu Zugangsrechten zu Daten vgl. auch: *Becker*, ZGE 2017, 253, 256 f.; zu Umfang und Begrenzungsmöglichkeiten vgl. Max Planck Institute for Innovation and Competition, Position Statement of 26 April 2017 on the European Commission's „Public Consultation on Building the European Data Economy", S. 9 ff.

[460] Annex to the Synopsis Report Consultation on the „Building a European Data Economy" Initiative, p. 24 et. seq., abrufbar unter: http://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf; zuletzt abgerufen am: 26.03.2018.

auch für nicht-personenbezogene Daten angedacht,[461] um Wechselkosten und die hiermit verbundenen Lock-in-Effekte zu reduzieren.[462] Es könnte jedoch auch zu einem Anreiz für den Datenverarbeiter führen, Daten vermehrt selbst zu erheben, was einem freien Fluss von Daten abträglich wäre. Zu spezifizieren ist im Falle einer gesetzlichen Ausgestaltung eines solchen Rechts insbesondere, ob es sich allein auf die explizit durch den Nutzer bereitgestellten Daten oder auch auf die durch Auswertung dieser Daten gewonnenen Erkenntnisse beziehen soll.

5.2.4.2 BESCHRÄNKUNG DURCH DAS DATENSCHUTZRECHT

Auch das Datenschutzrecht muss weiterhin eine begrenzende Funktion erhalten. Dies hat es bereits heute für jedweden Umgang mit personenbezogenen Daten, ob diese nun auf vertrags-, ausschließlichkeits- oder zugangsrechtlicher Grundlage erfolgen.

Vor Tendenzen zur Einschränkung der Widerruflichkeit der im Vertag erteilten Einwilligung darf hier gewarnt sein. Das informationelle Selbstbestimmungsrecht bedarf gerade im digitalen Zeitalter einer Stärkung, nicht einer Schwächung und zwar auch und gerade, weil Datensammlungen und -auswertungen ein so erhebliches Missbrauchspotential innewohnt. Die Grundrechte wirken mittelbar auch im Zivilrecht und sperren eine Einschränkbarkeit der Widerruflichkeit jedenfalls im Grundsatz. Den Staat treffen entsprechende Schutzpflichten. Ist bereits die Einwilligung als Instrument zur Gewährleistung tatsächlicher Selbstbestimmung nur sehr beschränkt geeignet, so würde ein Entfallen ihrer Widerruflichkeit das Konzept der informationellen Selbstbestimmung gänzlich erodieren. Eine Einschränkung der Widerruflichkeit einer als vertraglichen Gegenleistung geschuldeten Einwilligung[463] oder gar eine gänzliche Aufhebung[464] sollte daher hinreichend bedacht sein. Zwar ist eine Widerruflichkeit der Einwilligung auch in anderen persönlichkeitsrechtlich relevanten Bereichen im Vertrag eingeschränkt, wie etwa im Bereich des Rechts am eigenen Bild.[465] Allerdings sind die Fall-

---

461 So bereits für den Bereich der Connected Cars: *Drexl*, Designing Competitive Markets for Industrial Data - Between Propertisation and Access, 2016, MPI for Innovation & Competition ResearchPaper No. 16-13, abrufbar unter: https://ssrn.com/abstract=2862975, S. 57, zuletzt abgerufen am 26.03.2018; vgl. auch: *Reimsbach-Kounatze*, Maximising the economic and social value of data, DSTI/CDEP(2016)4, abrufbar unter: http://predipubcn.sistemaip.net:8096/intranet-tmpl/prog/img/local_repository/koha_upload/DSTI-CDEP(2016)4-ENG.pdf, zuletzt abgerufen am 22.02.2018; Regulation of the European Parliament and of the Council on a framewort for the free flow of non-personal data in the European Union, COM(2017) 495 final; *European Commission*, Digital Single Market strategy – Mid-term review, 2017 - http://eur-lex.europa.eu/content/news/digital_market.html (12.12.2017).

462 Hierzu eingehend: *Schnurr et al.*, Marktmacht durch Daten, in: Specht/Werry/Werry, Handbuch Datenrecht in der Digitalisierung, erscheint 2018.

463 *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 270 ff.

464 So etwa: *Sattler*, JZ 2017, 1036 ff.

465 So z.B. bei der vertraglichen Einwilligung in die Verbreitung und öffentliche Schaustellung des Rechts am eigenen Bild, vgl. z.B. Dreier/Schulze-*Specht*, Urheberrechtsgesetz, 6. Aufl. 2018, § 22 KUG Rn. 32 ff.

konstellationen nicht vergleichbar. Insbesondere in dem für die vertragliche Einwilligung in die Nutzung des Rechts am eigenen Bild relevanten Bereich der Model-Release-Verträge, spielt eine fehlende Informiertheit des Betroffenen (anders als im Datenschutzrecht) regelmäßig eine nur untergeordnete Rolle.[466]

Anzumerken ist auch, dass die Anerkennung der schuldvertraglichen Einwilligung als Gegenleistung im Vertrag nach den Vorgaben der Richtlinie für digitale Inhalte nicht zu einem Weniger an Datenschutz führen und daher die Bestimmungen der Datenschutzrichtlinie nicht berühren soll.[467] Auch dies spricht dafür, die Widerruflichkeit der Einwilligung auch dann nicht anzutasten, wenn sie als schuldvertragliche Einwilligung erklärt wird.[468]

Insofern ergäben sich keine Änderungen zu der bereits de lege lata beschränkenden Funktion des Datenschutzrechts in einem gesetzlich ausgestalteten Datenschuldrecht de lege ferenda. Dies soll indes nicht darüber hinwegtäuschen, dass Anpassungen des Datenschutzrechts zwingend erforderlich scheinen, möchte man das informationelle Selbstbestimmungsrecht auch im digitalen Zeitalter weiterhin angemessen schützen und den Datenverkehr dennoch nicht gänzlich ersticken.

Unzulänglichkeiten des geltenden Datenschutzrechts werden zu Recht sowohl aus Betroffenen-, als auch aus Unternehmensperspektive artikuliert: Die Betroffenen beklagen eine fehlende Informiertheit über die Folgen einer Datenhingabe und die Erklärung der datenschutzrechtlichen Einwilligung. Nicht selten scheinen die Datenschutzerklärungen den Betroffenen eher zu überfordern, denn zu informieren. Es kommt zum information overload, der nicht selten in einem gänzlichen Abbruch der Informationsaufnahme respektive in einer Informationsvermeidung endet. Auch das Koppelungsverbot scheint in der Praxis den Betroffenen nicht davor bewahren zu können, dass er sich gewissermaßen gezwungen sieht, personenbezogene Daten im Austausch gegen eine Leistung des Vertragspartners hinzugeben.

Aus Unternehmensperspektive stellt sich v.a. das Problem, selbst dann im Stadium des Generierens personenbezogener Daten das Datenschutzrecht beachten zu müssen, wenn die Daten anschließend anonymisiert werden. Aufgrund der Rechtsunsicherheit, welche Anforderungen an eine für die Einwilligung ausreichende Informationsvermittlung zu stellen sind, sowie durch das Abwägungserfordernis im Erlaubnistatbestand des Art. 6 Abs. 1 lit. f) DS-GVO, stehen die Unternehmen vor dem Problem, für ihr Geschäftsmodell teils erhebliche Datenbestände erheben zu müssen, hierbei aber auf sehr unsicherer Rechtsgrundlage zu

---

[466] Vgl. zum Ganzen bereits eingehend: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

[467] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte v. 09.12.2015, COM (2015) 634 final, Begründung S. 13.

[468] Vgl. zum Ganzen bereits eingehend: *Specht*, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, erscheint 2018.

agieren. Die Vorgaben der E-Privacy-Verordnung verstärken diese Rechtsunsicherheit zusätzlich.

Reformbedarf besteht insofern etwa bei der für eine informierte Einwilligung erforderlichen Informationsvermittlung, wo daran gedacht werden könnte, Informationen zunehmend durch Visualisierung zu vermitteln[469] oder technische Lösungen, wie Einwilligungsassistenten, stärker zu fördern. Die für ihre Anwendbarkeit erforderliche Standardisierung der Informationsvermittlung ließe sich ebenfalls durch die Entwicklung einheitlicher, maschinenlesbarer Bildsymbole realisieren. Dem Schutz der Betroffenen könnte auch ein Recht auf datenerhebungsfreie Produkte dienen (auch hier müssten aber freilich die zur Bereitstellung der Funktionen erforderlichen Daten, nicht aber darüber hinausgehende Daten erhoben werden dürfen),[470] wobei auch ein solches Recht nicht ohne eine Reform der datenschutzrechtlichen Einwilligung auskommt, wohl aber kumulativ zu dieser dienlich ist. Denn geltend machen würde ein solches Recht wohl allein der ohnehin datenschutzrechtlich sensible Nutzer, während bei den übrigen Nutzern zunächst einmal Aufmerksamkeit für datenschutzrechtliche Belange generiert sowie die für eine datenschutzrechtlich wirksame Einwilligung die Information nutzerfreundlich zugeführt werden müsste. Dies gilt umso mehr für den Fall, dass sich der Preis für ein datenerhebungsfreies Produkt im Verhältnis zum selben aber datenerhebenden Produkt erhöht. Andererseits ließe sich darüber nachdenken, ob eine Datenverarbeitung jedenfalls dann erleichtert und auf rechtssichere Grundlage[471] gestellt werden könnte, wenn die erhobenen Daten unmittelbar nach ihrer Erhebung anonymisiert werden. Eine Schrankenregelung entsprechend Art. 5 Abs. 1 InfoSoc-Richtlinie bzw. § 44a UrhG verbunden mit Standards zur Anonymisierung wäre hierfür ein Mittel.[472] Der Reformbedarf des Datenschutzrechtes ist nicht Gegenstand des Gutachtenauftrags, er sollte aber mitbedacht werden, wenn über die Normierung von Rechtspositionen an Daten – ob nun ausschließlichkeitsrechtlicher, vertragsrechtlicher oder zugangsrechtlicher Natur – nachgedacht wird. Denn de lege lata kann das Datenschutzrecht jede dieser Rechtspositionen für den Verantwortlichen wertentleeren, wenn es ihm jede Verarbeitungsmöglichkeit entzieht oder nur auf sehr unsicherer Rechtsgrundlage – einer Einwilligung oder Abwägungsentscheidung – gewährt.[473] Dies gilt umso mehr, wenn die ePrivacy-Verordnung künftig weitere Anforderungen an die Verarbeitung personenbezogener und nicht-personenbezogener Daten stellt.

---

[469] Vgl. hierzu zutreffend: *Lutterbeck*, Das informationelle Selbstbestimmungsrecht auf dem Prüfstand, abrufbar unter: http://lutterbeck.org/data/uploads/lutterbeck_isr-28092010-1.1.pdf, zuletzt abgerufen am: 14.02.2018.

[470] *Becker*, JZ 2017, 170, 175 ff.

[471] Die Herstellung von Rechtssicherheit ist auch ein Anliegen des BMWi, vgl. Weißbuch Digitale Plattformen, 2017, S. 66.

[472] *Specht*, GRUR Int. 2017, 1040, 1047.

[473] Hierzu eingehend: *Specht*, GRUR Int. 2017, 1040, 1042 ff.

6. ZUSAMMENFASSUNG

Stehen Rechtspositionen an Daten in Rede, so sind Daten als betroffenes Rechtsobjekt zunächst abzugrenzen von Informationen. Ebenfalls ist die Frage des Personenbezugs eines Datums zu beantworten. Während sich Daten auf der syntaktischen Ebene als Zeichen darstellen, liegen Informationen auf der semantischen Ebene. Eine Regulierung der syntaktischen Ebene kann sich aber aufgrund der Funktion von Daten, Bedeutungsgehalte zu kodieren, auf die semantische Ebene auswirken. Gleichzeitig ist auch eine reflexhafte Beeinflussung der syntaktischen Ebene im Falle einer Regulierung auf semantischer Ebene denkbar. Die Personenbezogenheit eines Datums ist äußerst weit und besteht bereits dann, wenn sich das Datum auf eine bestimmbare Person bezieht, wobei auch Kenntnisse Dritter unter gewissen Umständen für die Bestimmbarkeit der Person herangezogene werden können. Daten lassen sich außerdem nach ihrer Sensitivität (Art. 9 DS-GVO) kategorisieren. Relevant sind weiterhin eine mögliche Pseudonymisierung sowie eine Anreicherung/Zusammenführung von Daten. Die E-Privacy-Verordnung kategorisiert weiterhin in Kommunikationsmetadaten und Kommunikationsinhalte, für die eigenständige Vorgaben gelten.

De lege lata existiert ein „Dateneigentum“ ebenso wenig wie eigentumsähnliche Rechtspositionen an Daten. Dies gilt gleichermaßen für das deutsche, wie für das US-amerikanische Recht. Abwehrrechte werden allerdings in beiden Rechtsordnungen über den Geschäftsgeheimnisschutz sowie das Deliktsrecht gewährt. Im US-amerikanischen Recht besteht ein wettbewerbsrechtlicher Schutz außerdem in engen Grenzen über die Misappropriation Doktrin.

Das Deliktsrecht ist unionsrechtlich kaum harmonisiert, im deutschen Recht aber ergeben sich deliktsrechtliche Ansprüche im Falle der Löschung und anderweitigen Beeinträchtigung von Daten v.a. gem. § 823 Abs. 2 BGB i.V.m. 303a StGB. Eine Beeinträchtigung und Löschung von Daten wird aber auch als Verletzung des Eigentumsrechts am Trägermedium erachtet. Über die Anerkennung eines Rechts am eigenen Datenbestand als sonstiges Recht gem. § 823 Abs. 1 BGB besteht weiterhin Streit. Im US-amerikanischen Recht kann sich ein deliktischer Schutz partiell über die Privacy Torts ergeben, über das Misappropriation Tort, das Confidentiality Tort sowie über das Tort of Trespass to Chattels und das Tort of Conversion.

Datenbankwerke und nicht-schöpferische Datenbanken unterliegen den Vorschriften der §§ 4, 87a UrhG. Auch die USA kennen einen Schutz schöpferischer Datenbankwerke, ein Schutz nicht-schöpferischer Datenbanken existiert im US-amerikanischen Recht allerdings nicht. In beiden Rechtsordnungen bestehen urheberrechtliche Befugnisse weiterhin nicht an Einzeldaten.

Sowohl in den Rechtsordnungen Deutschlands, als auch der USA können Daten allerdings Gegenstand von Verträgen sein, wobei sich in beiden Rechtsordnungen Probleme bei der

Verzahnung von Datenschutz- und Vertragsrecht ergeben, die in der deutschen Rechtsordnung aber wesentlich erheblicher ausfallen. Bilden Daten und datenschutzrechtliche Einwilligung die Gegenleistung in einem Vertrag, ist v.a. die Frage zu klären, wie ein Einwilligungswiderruf vertragsrechtlich abzubilden ist.

Begrenzungen erfährt der rechtliche Umgang mit Daten in den Rechtsordnungen Deutschlands und der USA durch Zugriffsrechte in sektorspezifischer und kartellrechtlicher Ausprägung sowie durch das Datenschutzrecht, das im europäischen Rechtsraum wesentlich stärker zugunsten des Betroffenen ausgeprägt ist, als in den USA.

Zur Ausgestaltung des rechtlichen Umgangs mit Daten liegen verschiedene Regulierungsansätze vor, allen voran der Vorschlag der EU-Kommission, in Anlehnung an *Zech* ein Datenerzeugerrecht zu etablieren. Auch andere Ansätze zur Begründung eines Dateneigentums aber sind zu nennen. Dies ist insbesondere die Ausgestaltung eines Dateneigentums analog § 903 BGB, das dem strafrechtlich durch die §§ 202a ff. StGB Geschützten zugewiesen werden soll (*Hoeren*). Daneben wird über eine Erweiterung des Datenbankschutzes (*Wiebe*) sowie des lauterkeitsrechtlichen Schutzes von Daten (*Becker*) nachgedacht. In Rede steht auch eine Beteiligung des Betroffenen an den mit den ihn betreffenden personenbezogenen Daten generierten Gewinnen (*Fezer; Schwartmann/Hentsch*) sowie in den USA über die Ausgestaltung eines „datarights" (*Mattioli*), das einen Anreiz zur Offenlegung von Daten und den Methoden ihrer Erhebung geben soll.

Sämtliche Regulierungsansätze unterliegen dabei dem Vorbehalt ihrer (v.a. rechtlichen und ökonomischen) Notwendigkeit sowie verfassungsrechtlicher Rechtfertigung. Sie sollen hier um einen weiteren ergänzt sein: Regulierungsbedarf ergibt sich aus Betroffenenperspektive derzeit v.a. für die Formulierung eines Datenschuldrechts für den primären Datenmarkt. Dieser Regulierungsbedarf besteht aufgrund veränderter Vertragsinhaltssituationen. Willenserklärungen, die auf den Abschluss eines Vertrags gerichtet sind, mit dem einerseits die Erbringung einer Leistung vereinbart wird, die Vertragsgegenseite aber gleichzeitig verpflichtet wird, Daten, die nicht für die Erbringung dieser Leistung erforderlich sind, zu überlassen und ihre Verarbeitung zu gestatten, können nach den Grundätzen von §§ 133, 157 BGB in einer Vielzahl von Fällen nicht anders ausgelegt werden, als dass die Überlassung der Daten und die Erklärung der datenschutzrechtlichen Einwilligung als Gegenleistung geschuldet sind. Wenn dies aber der Fall ist, müssen die datenschutzrechtlichen Grundsätze im Interesse eines effektiven Schutzes des informationellen Selbstbestimmungsrechtes des Betroffenen in das Zivilrecht transportiert werden.

LITERATURVERZEICHNIS TEIL I

Ahlberg, Hartwig/Götting, Horst-Peter, Beck´scher Online-Kommentar Urheberrecht, Stand: 01.11.2017, C.H.Beck – München

Albers, Marion, Informationelle Selbstbestimmung, 2005, Nomos – Baden-Baden

Albers, Marion, Umgang mit personenbezogenen Informationen und Daten, S. 107-234, in: Hoffmann-Riem, Wolfgang/Schmidt-Assmann, Eberhard/Voßkuhle, Andreas, Grundlagen des Verwaltungsrechts, Bd. II., 2. Aufl. 2012, C.H.Beck – München

Am. Farm Bureau Fed'n, Privacy and Security Principles for Farm Data, May, 5, 2015 (https://www.fb.org/issues/technology/data-privacy/privacy-and-security-principles-for-farm-data)

Arkenau, Judith/Wübbelmann, Judith, Eigentum und Rechte an Daten – Wem gehören Daten?, S. 95-110, in: Taeger, Jürgen, Internet der Dinge: Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband 2015, OIWiR – Oldenburg

Art. 29 Datenschutzgruppe, Opinion 03/2013 on purpose limitation v. 02.04.2013, 00569/13/EN/WP203 (<http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>)

Assion, Simon, Anmerkung zum Urteil OLG Naumburg, Urt. v. 27.08.2014 – 6 U 3/14, CR 2016, 84-85

Assion, Simon/Mackert, Lea Noemi, Verträge über Daten: Eine Praxischeckliste, PinG 2016, 161-164

Auer-Reinsdorff, Astrid/Conrad, Isabell, Handbuch IT- und Datenschutzrecht, 2. Aufl. 2016, C.H.Beck – München

Balganesh, Shyamkrishna, "Hot News": The Enduring myth of property in the news, 111 Colum L. Rev. 419-497 (2011)

Balthasar, Stephan, Eingriffskondiktion bei unerlaubter Nutzung von Persönlichkeitsmerkmalen – Lafontaine in Werbeannonce, NJW 2007, 664-666

Bamberger, Heinz Georg/Roth, Herbert/Hau, Wolfgang/Poseck, Roman, Beck´scher Online-Kommentar BGB, 44. Ed. Stand: 01.11.2017

Bartsch, Michael, Die Vertraulichkeit und Integrität informationstechnischer System als sonstiges Recht nach § 823 Abs. 1 BGB, CR 2008, 613-617

Baumgartner, Ulrich/Gausling, Tina, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, ZD 2017, 308-313

Becker, Maximilian, Schwerpunkt: Rechte and Industrial Data und die DSM-Strategie, GRUR-Newsletter 01/2016, 7-11 (http://www.grur.org/uploads/media/2016-01_GRUR_Newsletter.pdf)

Becker, Maximilian, Lauterkeitsrechtlicher Leistungsschutz für Daten, GRUR 2017, 346-355

Becker, Maximilian, Rights in Data – Industry 4.0 and the IP Rights of the Future, ZGE 2017, 253-265

Beisenherz, Maja, Im toten Winkel der Kartellbehörde – Personenbezogene Daten und Datenschutz in der Fusionskontrolle, DuD 2015, 600-605

Berberich, Matthias/Golla, Sebastian, Zur Konstruktion eines „Dateneigentums" – Herleitung, Schutzrichtung, Abgrenzung, PinG 2016, 169-176

Bergelson, Vera, It´s Personal But is it Mine? – Toward Property Rights in Personal Information, 37 U.C. Davis L. Rev. 379-451 (2003)

Berger, Christian, Property Rights to Personal Data? – An Exploration of Commercial Data Law, ZGE 2017, 340-355

Bergmann, Lutz/Möhrle, Roland/Herb, Armin, Datenschutzrecht, 50. EL. 2016, Boorberg – Stuttgart
Bergt, Matthias, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts, ZD 2015, 365-371
Beyer, Hans, Der Begriff der Information als Grundlage für die Beurteilung des technischen Charakters von programmbezogenen Erfindungen, GRUR 1990, 399-410
Bisges, Marcel, Personaldaten, Wertzuordnung und Ökonomie, MMR 2017, 301-306
BMWi, Weißbuch Digitale Plattformen, 2017 (https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/weissbuch-digitale-plattformen.pdf?__blob=publicationFile&v=22)
Boehm, Franziska, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358-387
Börding, Andreas/Jülicher, Tim/Röttgen, Charlotte/v. Schönfeld, Max, Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, CR 2017, 134-140
Bräutigam, Peter, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635-641
Bräutigam, Peter/Klindt, Thomas, Digitalisierte Wirtschaft /Industrie 4.0, 2015 (https://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf)
Brink, Stefan/Eckhardt, Jens, Wann ist ein Datum ein personenbezogenes Datum?, ZD 2015, 205-212
Brühann, Ulf, Mindeststandards oder Vollharmonisierung ds Datenschutzes in der EG, EuZW 2009, 639-644
Buchner, Benedikt, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155-161
Buchner, Benedikt, Informationelle Selbstbestimmung im Privatrecht, 2006, Mohr Siebeck – Tübingen
Bui, Jacqueline, Lack of Privacy Regulations in the Fitness and Health Mobile App Industry: Assessing the Health Insurance Portability and Accountability Act (HIPPAA) for Meeting the Needs of User Data Collection, 21 USF Intell. Prop. & Tech. L. J. 1-20 (2016)
Burk, Dan L., Patents as Data Aggregators in personalized medicine, 21 B.U.J. Sci & Tech. L. 233-255 (2015)
Canaris, Claus-Wilhelm, Wandlungen des Schuldvertragsrechts – Tendenzen zu seiner „Materialisierung" AcP 200 (2000), 273-364
Canaris, Claus-Wilhelm, Gewinnabschöpfung bei Verletzung des allgemeinen Persönlichkeitsrechts, S. 85-109, in: Ahrens, Hans-Jürgen/von Bar, Christian/Fischer, Gerfried/Spickhoff, Andreas/Taupitz, Jochen, Festschrift für Erwin Deutsch zum 70. Geburtstag, 1999, Heymanns – Köln
Cebulla, Mario, Die Pacht nichtsächlicher Gegenstände, 1999, De Gruyter – Berlin
Culik, Nicolai/Döpke, Christian, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226-230
Dammann, Ulrich, Erfolge und Defizite der EU-Datenschutz-Grundverordnung, ZD 2016, 307-314
Dauner-Lieb, Barbara/Langen, Werner, NomosKommentar Bürgerliches Gesetzbuch – BGB, Bd. 2: Schuldrecht, 3. Aufl. 2016, Nomos – Baden-Baden
Determann, Lothar, California Privacy Law, 2016, Amer Lawyer Media – New York City
Determann, Lothar, California Privacy Law, 3. Aufl. 2018, im Erscheinen, Amer Lawyer Media – New York City
Determann, Lothar, Datenschutz: International Compliance Field Guide, 2017, C.H.Beck – München

Determann, Lothar/Perens, Bruce, Open Cars, 32 Berkeley Tech. L. J. 915-988 (2017) (http://btlj.org/data/articles2017/vol32/32_2/32_2_fullFile_web.pdf)
Determann, Lothar, Datenrechte im US-amerikanischen Rechtsraum, in: Specht, Louisa/Werry, Susanne/Werry, Nikola, Datenrecht in der Digitalisierung, im Erscheinen, Erich Schmidt – Berlin
Deutscher Anwaltverein, Stellungnahme durch den Ausschuss Informationsrecht zur Frage des „Eigentums" an Daten und Informationen, Stellungnahme 75/2016, (https://anwaltverein.de/de/newsroom/sn-75-16-frage-des-eigentums-an-daten-und-informationen)
Digitaler Neustart, Bericht der Arbeitsgruppe v. 15.05.2017 (https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf)
Dölling, Dieter/Duttge, Gunnar/Rössner, Dieter, Gesamtes Strafrecht, 4. Aufl. 2017, Nomos – Baden-Baden
Dorner, Michael, Big Data und „Dateneigentum", CR 2014, 617-628
Dreier, Thomas, Informationsrecht in der Informationsgesellschaft, S. 65-76, in: Bizer, Johann/Lutterbeck, Bernd/Rieß, Jochen, Umbruch von Regelungssystemen in der Informationsgesellschaft, Freundesgabe für Alfred Büllersbach, 2002, Stuttgart (http://www.alfred-buellesbach.de/PDF/Freundesgabe.pdf; http://www.alfred-buellesbach.de/PDF/08_Dreier.pdf)
Dreier, Thomas, Eigentum an Daten?, in: Weller, Matthias/Wendland, Matthias, Digital Single Market: Bausteine eines digitalen Binnenmarktes, 2018 (im Erscheinen)
Dreier (Thomas)/Schulze (Gernot), Urheberrechtsgesetz, 6. Aufl. 2018, C.H.Beck – München
Drexl, Josef/Hilty, Reto M./Desaunettes, Luc/Greiner, Franziska/Kim, Daria/Richter, Heiko/Surblytė, Gintarė/Wiedemann, Klaus, Ausschließlichkeits- und Zugangsrechte an Daten, GRUR Int. 2016, 914-918
Drexl, Josef/Hilty, Reto M./Globocnik, Jure/Greiner, Franziska/Kim, Daria/Richter, Heiko/Slowinski, Peter R./Surblytė, Gintarė/Walz, Axel/Wiedemann, Klaus, MPI for Innovation and Competition, Position Statement of 26 April 2017 on the European Commission´s "Public Consultation on Building the European Data Economy" (https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf)
Drexl, Josef, Designing Competitive Markets for Industrial Data – between propertisation and access, 2016, MPI for Innovation and Competition Research Paper No. 16-13 (https://ssrn.com/abstract=2862975)
Druey, Jean Nicolas, Information als Gegenstand des Rechts – Entwurf einer Grundlegung, 1996, Schulthess – Zürich
Eckert, Martin, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, 112 SJZ 245-249 (2016)
Ehlen, Theresa/Brandt, Elena, Die Schutzfähigkeit von Daten – Herausforderungen und Chancen für Big Data Anwender, CR 2016, 570-575
Ehmann, Timo, Big Data auf unsicherer Grundlage – was ist „wesentlich" beim Investitionsschutz für Datenbanken?, K&R 2014, 394-400
Ehmann, Eugen/Selmayr, Martin, Datenschutz-Grundverordnung, 2017, C.H.Beck – München
Ekstrand, Victoria Smith/Roush, Christopher, From "Hot News" to "Hot Data": The Rise of "Fintech," the Ownership of Big Data, and the Future of the Hot News Doctrine, 35 Cardozo Arts & Ent. L. J. 303-340 (2017)

Elteste, Ulrike, Screen Scrapping: Wechselwirkungen zwischen Datenbankrecht und Vertragsrecht, CR 2015, 447-451
Engle, Eric, US Contract law for German Jurists, 2013, CreateSpace – South Carolina
Ensthaler, Jürgen, Industrie 4.0 und die Berechtigung an Daten, NJW 2016, 3473-3478
Erman, Walter, BGB, 15. Aufl. 2017, Otto Schmidt – Köln
Europäische Union, Interinstitutional File 2017/0003 (COD) v. 11.01.2018 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5165_2018_INIT&from=EN)
European Commission, Commission staff working document on the free flow of data and emerging issues of the European data economy, 10.01.2017, SWD (2017) 2 final (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002&from=NL)
European Commission, Digital Single Market strategy – mid term review, 2017 (http://eur-lex.europa.eu/content/news/digital_market.html)
European Commission, Annex to Synopsis Report Consultation on the "Building a European Data Economy"-Initiative, 2017 (http://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf)
Evans, Barbara J., Barbarians at the Gate: Consumer-Driven Data Commons and the Transformation of Citizen Science, 42 Am. J. L. & med. 651-685 (2016)
Evans, Barbara J., Much Ado About Data Ownership, 25 Harv. J. L. & Tech. 69-130 (2011)
Evans, Barbara J., Power to the People: Data Citizens in the Age of Precision Medicine, 19 Van. d. J. Ent. & Tech. L. 243-266 (2016)
Evans, Barbara J., Sustainable Access to Data for Postmarketing Medical Product Safety Surveillance under the Amended HIPAA Privacy Rule, 24 Health Matrix 11-47 (2014)
Farkas, Thomas J., Data Created by the Internet of Things: The New Gold without Ownership, 23 Rev. Prop. Inmaterial 5-17 (2017)
Faulkenberry, Regina M., Reviewing and Negotiating Cloud Computing Vendor Contracts, 6 J. Health & Life Sci. L. 119-154 (2013)
Faust, Florian, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, 71. Deutscher Juristentag, Bd. I, 2016, S. A1-A92, C.H.Beck – München
Faustmann, Jörg, Der deliktische Datenschutz, VuR 2006, 260-263
Ferrell, Shannon L., Legal Issues on the Farm Data Frontiert Part I: Managing First-Degree Relationships in Farm Data Transfers 21 Drake J. Agric L. 13-57 (2016)
Fezer, Karl-Heinz, Dateneigentum – Theorie des immaterialgüterrechtlichen Eigentums an verhaltensgenerierten Personendaten der Nutzer als Datenproduzent, MMR 2017, 3-5
Fezer, Karl-Heinz, Dateneigentum der Bürger, ZD 2017, 99-105
Fischer, Thomas, Strafgesetzbuch, 64. Aufl. 2017, C.H.Beck – München
Franklin, Jonathan/Reichman, Jerome H., Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information, 147 U. Pa. L. Rev. 875-970 (1999)
Freiwald, Susan, First Principles of Communications Privacy, Stan. Tech. L. Rev. 3-75 (2007)
Fromm, Friedrich K./Nordemann, Wilhelm, Urheberrecht, 11. Aufl. 2014, Kohlhammer – Stuttgart
Funkel, Thorsten, Der Schutz der Persönlichkeit durch Ersatz immaterieller Schäden in Geld, 2001, C.H.Beck – München
Gärtner, Anette/Brimsted, Kate, "Let´s talk about data ownership", EIPR 2017, 461-466

Genz, Alexander, Datenschutz in Europa und den USA, 2004, Deutscher Universitätsverlag – Wiesbaden
Gerstenberg, Ekkehard, Löschen von Tonbändern als neuer strafrechtlicher Tatbestand, NJW 1956, 540-545
Ginsburg, Jane C., Copyright, Common Law, and Sui Generis Protection of Databases in the United States and Abroad, 66 U. Cin. L. Rev. 151-176 (1997)
Glazer, Daniel et. al, Data as IP and Data License Agreements, Practical Law Practice Note 4-532-4243 (2017) (http://www.friedfrank.com/siteFiles/Publications/Data%20as%20IP%20and%20Data%20License%20Agreements%20(1).pdf)
Götting, Horst-Peter, Persönlichkeitsrechte als Vermögensrechte, 1995, Mohr Siebeck – Tübingen
Gola, Peter, DS-GVO, 2017, C.H.Beck – München
Grosskopf, Lambert, Rechte an privat erhobenen GEO- und Telemetriedaten, IPRB 2011, 259-261
Grünwald, Andreas/Hackl, Jens, Das neue umsatzbezogene Sanktionsregime der DS-GVO, ZD 2017, 556-560
Grützmacher, Malte, Zum Datenbankschutz von Musikcharts, CR 2006, 14-16
Grützmacher, Malte, Dateneigentum – ein Flickenteppich, CR 2016, 485-495
Gsell, Beate/Krüger, Wolfgang/Lorenz, Stephan/Reymann, Christoph, Beck´scher Online-Großkommentar BGB, Stand: 01.01.2018
Haedicke, Maximilian, Rechtskauf und Rechtsmängelhaftung, 2003, Mohr Siebeck – Tübingen
Hardy, Quentin, Why Big Data is not the truth, NY Times, June 1st, 2013 (https://bits.blogs.nytimes.com/2013/06/01/why-big-data-is-not-truth/?_r=0)
Härting, Niko, „Dateneigentum" – Schutz durch Immaterialgüterrecht?, CR 2016, 646-649
Härting, Niko, Datenschutz-Grundverordnung, 2016, Otto Schmidt – Köln
Harte-Bavendamm, Henning/Henning-Bodewig, Frauke, Gesetz gegen den unlauteren Wettbewerb (UWG), 4. Aufl. 2016, C.H.Beck – München
Hasselblatt, Gordian N., Münchener Anwaltshandbuch Gewerblicher Rechtsschutz, 5. Aufl. 2017, C.H.Beck – München
Hay, Peter, US-amerikanisches Recht, 6. Aufl. 2015, C.H.Beck – München
Heermann, Peter W./John, Martin, Lizenzierbarkeit von Spielplänen im deutschen Ligasport, K&R 2011, 753-760
Heinzke, Philippe, Richtlinie zum Schutz von Geschäftsgeheimnissen, CCZ 2016, 179-183
Helbig, Thomas, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 2015, 145-150
Herberger, Maximilian/Martinek, Michael/Rüßmann, Helmut/Weth, Stephan/Würdinger, Markus, Juris PraxisKommentar-BGB, Bd. III, 8. Aufl. 2017, Juris – Saarbrücken
Hermann, Tobias, Der Werbewert der Prominenz, 2012, Nomos – Baden-Baden
Heun, Sven-Erik/Assion, Simon, Internet(recht) der Dinge, CR 2015, 812-818
Heymann, Thomas, Rechte an Daten, CR 2016, 650
Hieke, Robert, Big Data, InTeR 2017, 10-20
Hilgendorf, Eric, Grundfälle zum Computerstrafrecht, JuS 1996, 509-512
Hoeren, Thomas, Big Data und Recht, 2014, C.H.Beck – München
Hoeren, Thomas, Dateneigentum, MMR 2013, 486-491
Hoeren, Thomas, Information als Gegenstand des Rechtsverkehrs – Prolegomena zu einer Theorie des Informationsrechts, MMR-Beilage 1998, 6-11

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd, Handbuch Multimedia-Recht, 45. EL. Juli 2017, C.H.Beck – München
Hörl, Bernhard, Schadensersatz für Datenverlust, ITRB 2014, 111-113
Hofmann, Johanna M./Johannes, Paul C., DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs, ZD 2017, 221-226
Hoppen, Peter, Sicherung von Eigentumsrechten an Daten, CR 2015, 802-806
Hornung, Gerrit et al, BMVI-Studie: Eigentumsordnung für Mobilitätsdaten, 2017 (http://www.bmvi.de/SharedDocs/DE/Artikel/DG/studie-mobilitaetsdaten-fachkonsultation.html)
Hubmann, Heinrich, Das Persönlichkeitsrecht, 1967, Boehlau – Münster
Hubmann, Heinrich, Der Bereicherungsanspruch im Persönlichkeitsrecht, UFITA 39 (1963), 223-236
Intveen, Michael, Vertragsrechtliche Aspekte der Bereitstellung digitaler Daten, ITRB 2018, 70-75
Isensee, Josef, Vertragsfreiheit im Griff der Grundrechte – Inhaltskontrolle von Verträgen am Maßstab der Verfassung, S. 485-514, in: Hübner, Ulrich/Ebke, Werner F., Festschrift für Bernhard Großfeld zum 65. Geburtstag, 1999, Recht und Wirtschaft – Heidelberg
Jauernig, Othmar, Bürgerliches Gesetzbuch: BGB, 16. Aufl. 2015, C.H.Beck – München
Joecks, Wolfgang/Hefendehl, Roland, Münchener Kommentar zum Strafgesetzbuch, Bd. 3, §§ 263-358 StGB, 2. Aufl. 2014, C.H.Beck – München
Kalbfus, Björn Helge, Know-how-Schutz in Deutschland zwischen Zivilrecht und Strafrecht – Welcher Reformbedarf besteht?, 2011, Heymanns – Köln
Kalbfus, Björn Helge, Angemessene Geheimhaltungsmaßnahmen nach der Geschäftsgeheimnis-Richtlinie, GRUR-Prax 2017, 391-393
Kalbfus, Björn Helge, Die EU-Geschäftsgeheimnis-Richtlinie, GRUR 2016, 1009-1017
Kang, Jerry, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193-1294 (1998)
Karg, Moritz, Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520-526
Keppeler, Lutz/Berning, Wilhelm, Die Bußgeldrisiken nach Art. 83 der Datenschutz-Grundverordnung – auch ein Risiko für den Jahresabschluss?!, DStR 2018, 91-96
Kerber, Wolfgang, Governance of Data: Exclusive Property vs. Access, 47 IIC 759-762 (2016)
Kerber, Wolfgang/Frank, Jonas, Data Governance Regimes in the Digital Economy: The Example of Connected Cars, 2017
Kilian, Wolfgang, Strukturwandel der Privatheit, S. 195-224, in: Garstka, Hansjürgen/Koy, Wolfgang, Wovon – für wen – wozu. Systemdenken wider die Diktatur der Daten, Wilhelm Steinmüller zum Gedächtnis, 2014, Helmholtz-Zentrum für Kulturtechnik – Humboldt Universität zu Berlin
Kilian, Wolfgang, Informationelle Selbstbestimmung und Marktprozesse, CR 2002, 921-929
Kilian, Wolfgang, Personal Data: The Impact of Emerging Trends in the Information Society, CR 2012, 169-175
Kindhäuser, Urs/Neumann, Ulfrid/Paeffgen, Hans-Ullrich, NomosKommentar Strafgesetzbuch – StGB, Bd. 2, §§ 80-231, 5. Aufl. 2017, Nomos – Baden-Baden
Kläver, Magdalene, Bereicherungsrechtliche Ansprüche bei einer Verletzung des allgemeinen Persönlichkeitsrechts, 1999, Dr. Kovac – Hamburg

Klein, Fabian, Marktteilnehmer erhalten keinen Zugriff auf Rohdaten, GRUR-Prax 2017, 243
Klein, Fabian/Wegener, Theresa, Wem gehören Geschäftsgeheimnisse?, GRUR-Prax 2017, 394-396
Klüber, Rüdiger, Persönlichkeitsschutz und Kommerzialisierung, 2007, Mohr Siebeck – Tübingen
Köhler, Helmut/Bornkamm, Joachim/Feddersen, Jörn, Gesetz gegen den unlauteren Wettbewerb: UWG mit PAngV, UKlaG, DL-InfoV, 36. Aufl. 2018, C.H.Beck – München
König, Michael, Software (Computerprogramme) als Sache und deren Erwerb als Sachkauf, NJW 1993, 3121-3124
Körber, Thorsten, „Ist Wissen Marktmacht"? Überlegungen zum Verhältnis von Datenschutz, „Datenmacht" und Kartellrecht – Teil 1, NZKart 2016, 303-310
Körber, Thorsten, „Ist Wissen Marktmacht"? Überlegungen zum Verhältnis von Datenschutz, „Datenmacht" und Kartellrecht – Teil 2, NZKart 2016, 348-356
Kolb, Stefan, Anmerkung zum Urteil des OLG Köln (Urt. v. 1.8.2014; GRUR-RR 2014, 419), GRUR-RR 2014, 423-424
Kraus, Michael, Datenlizenzverträge, S. 537-550, in: Taeger, Jürgen, Internet der Dinge: Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband 2015, OIWiR – Oldenburg
Kühling, Jürgen/Buchner, Benedikt, DS-GVO, BDSG, 2. Aufl. 2018, C.H.Beck – München
Kühnl, Christina, Persönlichkeitsschutz 2.0, 2016, De Gruyter – Berlin
Lackner, Karl/Kühl, Kristian, StGB, 28. Aufl. 2014, C.H.Beck – München
Langhanke, Carmen/Schmidt-Kessel, Martin, Consumer Data as Consideration, EuCML 2015, 218-223
Laue, Philip, Öffnungsklauseln in der DS-GVO – Öffnung wohin?, ZD 2016, 463-467
Leible, Stefan/Sosnitza, Olaf, Schadensersatzpflicht wegen Virenbefall von Disketten, K&R 2002, 51-52
Leistner, Matthias, Der Schutz von Telefonverzeichnissen und das neue Datenbankherstellerrecht, MMR 1999, 636-642
Leistner, Matthias, Zur Auslegung des Datenbankherstellerrechts, JZ 2005, 408-411
Leistner, Matthias, „Last exit" withdrawal?, K&R 2007, 457-465
Lejeune, Mathias, Der neue EU Richtlinie zum Schutz von Know-How und Geschäftsgeheimnissen, CR 2016, 330-342
Lemley, Mark A., The Surprising Virtues of Treating Trade Secrets as IP Rights, 61 Stan. L. Rev. 311-354 (2008)
Libertus, Michael, Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren, MMR 2005, 507-512
Linardatos, Dimitrios, Daten als Gegenleistung, in: Specht, Louisa/Werry, Susanne/Werry, Nikola, Handbuch Datenrecht in der Digitalisierung, im Erscheinen, Erich Schmidt – Berlin
Lutterbeck, Bernd, Das informationelle Selbstbestimmungsrecht auf dem Prüfstand, 28. 09.2010, (http://lutterbeck.org/data/uploads/lutterbeck_isr-28092010-1.1.pdf)
MacLean, Charles E., Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age, Unless Congress Continually Resets the Privacy Bar, 24 Alb. L. J. Sci. & Tech. 47-80 (2014)
Makous, David N./Hamilton, Mina I., Compulsory IP Licensing and Standards-Setting, Standard-Essential Patens and F/Rand, Aspatore (2014), 2014 WL 1234517)
Manning, Lauren, Setting the Table for Feast or Famine: How Education Will Play A Deciding Role in The Future of Precision Agriculture, 11 J. Food L. & Pol'y 113-156 (2015)

Marly, Jochen P., Die Qualifizierung der Computerprogramme als Sache nach § 90 BGB, BB 1991, 432-436
Martinek, Michael, Moderne Vertragstypen, Bd. II, 1993, C.H.Beck – München
Mattioli, Michael, Data Policy in the United States: New Challenges, ZGE 2017, 299-316
Mattioli, Michael, Disclosing Big Data, 99 Minn. L. Rev. 535-584 (2014)
Maume, Philipp, Know-how-Schutz – Abschied vom Geheimhaltungswillen? WRP 2008, 1275-1280
McClurg, Andrew J., A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 Nw. U. L. Rev. 63-144 (2003)
McGuire, Mary-Rose, Der Schutz von Know-how im System des Immaterialgüterrechts, GRUR 2016, 1000-1008
Meier, Klaus/Wehlau, Andreas, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585-1591
Mestmäcker, Ernst-Joachim, Eingriffserwerb und Rechtsverletzung in der ungerechtfertigten Bereicherung, JZ 1958, 521-526
Metzger, Alex, Dienst gegen Daten: Ein synallagmatischer Vertrag, AcP 216 (2016), 817-865
Millard, Christopher, Cloud Computing Law, 2013, Oxford University Press – Oxford
Mitglieder des Bundesgerichtshofs, RGRK, Das Bürgerliche Gesetzbuch: mit besonderer Berücksichtigung der Rechtsprechung des Reichsgerichts und des Bundesgerichtshofs, 12. Aufl. 1979, De Gruyter – Berlin
Möhring, Philipp/Nicolini, Käte, Urheberrecht, 3. Aufl. 2014, C.H.Beck – München
Monreal, Manfred, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO, ZD 2016, 507-512
Neun, Andreas/Lubitzsch, Katharina, EU-Datenschutz-Grundverordnung – Behördenvollzug und Sanktionen, BB 2017, 1538-1544
OECD, Empfehlungen der OECD, Maximising the economic and social value of data (http://www.oecd.org/sti/ieconomy/enhanced-data-access.htm)
Ohly, Ansgar, Der Geheimnisschutz im deutschen Recht: heutiger Stand und Perspektiven, GRUR 2014, 1-11
Ohly, Ansgar/Sosnitza, Olaf, UWG, 7. Aufl. 2016, C.H.Beck – München
Osborne Clarke LLP, Legal Study on ownership and access to data, 2016
Ozer, Nicolas A., Putting Online Privacy above the Fold: Building a Social Movement and Creating Corporate Change, 36 N.Y.U. Rev. L. & Soc. Change 215-282 (2012)
Paal, Boris P./Hennemann, Moritz, Big Data im Recht, NJW 2017, 1697-1701
Paal, Boris P./Pauly, Daniel A., Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl. 2018, C.H.Beck – München
Palandt, Otto, BGB, 77. Aufl. 2018, C.H.Beck – München
Pabarcus, Adam, Are Private Spaces on Social Networking Websites Truly Private – The Extension of Intrusion upon Seclusion, 38 Wm. Mitchell L. Rev. 397-432 (2011)
Pfaff, Dieter, Der Know-how-Vertrag im bürgerlichen Recht, BB 1974, 565-570
Popp, Andreas, Informationstechnologie und Strafrecht, JuS 2011, 385-392
Prange, David A., Big data and trade secrets: part 2, Intellectual Property Magazine 42 (2017) (https://www.intellectualpropertymagazine.com/resources/issue/?issueDate=February2017)
Prinz, Matthias, Geldentschädigung bei Persönlichkeitsrechtsverletzungen durch Medien, NJW 1996, 953-958
Prosser, William L., Privacy, 48 Calif. L. Rev. 383-423 (1960)

Prütting, Hanns/Wegen, Gerhard/Weinreich, Gerd, BGB, 13. Aufl. 2018, Luchterhand – München
Raiser, Ludwig, Der Stand der Lehre vom subjektiven Recht im Deutschen Zivilrecht, JZ 1961, 465-473
Rank, Alisa, Daten als Leistungsgegenstand, in: Specht, Louisa/Werry, Susanne/Werry, Nikola, Handbuch Datenrecht in der Digitalisierung, im Erscheinen, Erich Schmidt – Berlin
Rasmussen, Neal, From Precision Agriculture to Market Manipulation: A New Frontier in the Legal Community, 17. Minn. J. L. Sci & Tech. 489-516 (2016)
Reichman, Jerome H./Samuelson, Pamela, Intellectual Property Rights in Data?, 50 Vand. L. Rev. 51-166 (1997)
Reimann, Mathias, Einführung in das US-amerikanische Privatrecht, 2. Aufl. 2004, C.H.Beck – München
Reimsbach-Kounatze, Christian, Maximising the economic and social value of data, (DSTI/CDEP(2016)4 (http://predipubcn.sistemaip.net:8096/intranet-tmpl/prog/img/local_repository/koha_upload/DSTI-CDEP(2016)4-ENG.pdf)
Reinholz, Fabian, Anmerkung zum Urteil des EuGH vom 1.03.2012 (C-604/10, K&R 2012, 335) – Zur Frage des Datenbank-Schutzes für Fußball-Spielpläne, K&R 2012, 338-340
Richards, Neil M./Solove, Daniel J., Privacy´s Other Path: Recovering the Law of Confidentiality, 96 Georgetown Law Journal 123-182 (2007)
Richards, Neil M./Solove, Daniel J., Prosser´s Privacy Law: A Mixed Legacy, 98 Calif. L. Rev. 1887-1924 (2010)
Röhricht, Volker/Graf von Westphalen, Friedrich/Haas, Ulrich, HGB, 5. Aufl. 2018, im Erscheinen, Otto Schmidt – Köln
Röttgen, Charlotte, Datenrechte im europäischen Rechtsraum, in: Specht, Louisa/Werry, Susanne /Werry, Nikola, Handbuch Datenrecht in der Digitalisierung, im Erscheinen, Erich Schmidt – Berlin
Rombach, Wolfgang), Killer-Viren als Kopierschutz, CR 1990, 101-106
Roßnagel (Alexander, Rechtsfragen eines Smart Data-Austauschs, NJW 2017, 10-15
Roßnagel, Alexander, Handbuch Datenschutzrecht, 2003, C.H.Beck – München
Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 2, 7. Aufl. 2016, C.H.Beck – München
Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 3, 7. Aufl. 2016, C.H.Beck – München
Säcker, Franz Jürgen/Rixecker, Roland/Oetker, Hartmut/Limperg, Bettina, Münchener Kommentar zum Bürgerlichen Gesetzbuch, Bd. 6, 7. Aufl. 2017, C.H.Beck – München
Sahl, Jan Christian, Gesetz oder kein Gesetz, das ist hier die Frage – Zur Notwendigkeit gesetzlicher Regulierung in der Datenökonomie, PinG 2016, 146-151
Samuelson, Pamela, Privacy as Intellectual Property, 52 Stan. L. Rev. 1125-1174 (2000)
Sassenberg, Thomas/Faber, Tobias, Rechtshandbuch Industrie 4.0 und Internet of Things, 2017, C.H.Beck – München
Sattler, Andreas, Personenbezogene Daten als Leistungsgegenstand, JZ 2017, 1036-1046
Schantz, Peter, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841-1847
Schantz, Peter/Wolff, Heinrich Amadeus, Das neue Datenschutzrecht, 2017, C.H.Beck – München
Schefzig, Jens, Die Datenlizenz, S. 551-566, in: Taeger, Jürgen, Internet der Dinge: Digitalisierung von Wirtschaft und Gesellschaft, DSRI Tagungsband 2015, OIWiR – Oldenburg
Schlechtriem, Peter, Bereicherung aus fremdem Persönlichkeitsrecht, S. 445-466, in: Fischer, Robert/Gessler, Ernst/Schilling, Wolfgang, Strukturen und Entwicklungen im

Handels-, Gesellschafts- und Wirtschaftsrecht: Festschrift für Wolfgang Hefermehl zum 70. Geburtstag, 1976, C.H.Beck – München
Schmidt-Kessel, Martin/Grimm, Anna, Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten, ZfPW 2017, 84
Schmidt, Kirsten Johanna/Zech, Herbert, Datenbankherstellerschutz für Rohdaten?, CR 2017, 417-426
Schmitz, Barbara, Der Abschied vom Personenbezug, ZD 2018, 5-8
Schneider, Jochen, Datenschutz, 2017, C.H.Beck – München
Schnurr, Daniel et al., Marktmacht durch Daten, in: Specht, Louisa/Werry, Susanne/Werry, Nikola, Handbuch Datenrecht in der Digitalisierung, im Erscheinen, Erich Schmidt – Berlin
Schönke, Adolf/Schröder, Horst, Strafgesetzbuch, 29. Aufl. 2014, C.H.Beck – München
Schricker, Gerhard/Loewenheim, Ulrich, Urheberrecht, 5. Aufl. 2017, C.H.Beck – München
Schröder, Markus, Anmerkung zur Entscheidung des OLG Nürnberg vom 23.01.2013 (1 Ws 445/12; ZD 2013, 282) – Zum Schutz der Datenverfügungsbefugnis, ZD 2013, 284-285
Schulze, Reiner/Dörner, Heinrich/Ebert, Ina/Hoeren, Thomas/Kemper, Rainer/Saenger, Ingo/Schreiber, Klaus/Schulte-Nölke, Hans/Staudinger, Ansgar, Handkommentar Bürgerliches Gesetzbuch: BGB, 9. Aufl. 2017, Nomos – Baden-Baden
Schwartmann, Rolf/Hentsch, Christian-Henner, Parallel aus dem Urheberrecht für ein neues Datenverwertungsrecht, PinG 2016, 117-126
Schwartz, Paul M., Property, Privacy, and Personal Data, 117 Harv. L. Rev. 2056-2128 (2004)
Schwartz, Paul M., „Personenbezogene Daten" aus internationaler Perspektive, ZD 2011, 97-98
Schwartz, Paul M., Referat, 69. Deutscher Juristentag, Bd. II, 2012, S. O73-O97, C.H.Beck – München
Schwartz, Paul M./Solove, Daniel J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814-1894 (2011)
Schwerdtner, Peter, Das Persönlichkeitsrecht in der deutschen Zivilrechtsordnung, 1977, Schweitzer – Berlin
Sieber, Ulrich, Informationsrecht und Recht der Informationstechnik, NJW 1989, 2569-2580
Siemes, Christiane, Gewinnabschöpfung bei Zwangskommerzialisierung der Persönlichkeit durch die Presse, AcP 201 (2001), 202-231
Soergel, Hans-Theodor, BGB, Bd. 14, 13. Aufl. 2002, Kohlhammer – Stuttgart
Solove, Daniel J., Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan. L. Rev. 1393-1462 (2001)
Solove, Daniel J./Hartzog, Woodrow, The FTC and the New Common Law of Privacy, 114 Columbia L. Rev. 583-676 (2014)
Solove, Daniel J./Schwartz, Paul M., Information Privacy Law, 4. Ed. 2011, Apsen Publisher – Philadelphia
Solove, Daniel J./Schwartz, Paul M., Reconciling Personal Information in the United States and European Union, 102 Cal. L. Rev. 877-916 (2014)
Specht, Louisa, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, 1040-1047
Specht, Louisa, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen, CR 2016, 288-296

Specht, Louisa, Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?, JZ 2017, 763-770
Specht, Louisa, Datenverwertungsverträge zwischen Datenschutz und Vertragsfreiheit – Eckpfeiler eines neuen Datenschuldrechts, DGRI Jahrbuch 2017, im Erscheinen, Otto Schmidt – Köln
Specht, Louisa, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung – Die zivilrechtliche Erfassung des Datenhandels, 2012, Heymanns – Köln
Specht, Louisa/Bienemann, Linda, Visualisierung von Information – Ein Weg aus dem Privacy Paradox?, in: Specht, Louisa/Werry, Susanne/Werry, Nikola, Handbuch Datenrecht in der Digitalisierung, im Erscheinen, Erich Schmidt – Berlin
Specht, Louisa/Müller-Riemenschneider, Severin, Dynamische IP-Adressen: Personenbezogene Daten für den Webseitenbetreiber, ZD 2014, 71-75
Specht, Louisa/Rohmer, Rebecca, Zur Rolle des informationellen Selbstbestimmungsrechts bei der Ausgestaltung eines möglichen Ausschließlichkeitsrechts an Daten, PinG 2016, 127-132
Spickhoff, Andreas, Der Schutz von Daten durch das Deliktsrecht, S. 233-245, in: Leible, Stefan/Lehmann, Matthias/Zech, Herbert, Unkörperliche Güter im Zivilrecht, 2011, Mohr Siebeck – Tübingen
Spindler, Gerald, Daten im Deliktsrecht, S. 1183-1192, in: Hilbig-Lugani, Katharina/Jakob, Dominique/Mäsch, Gerald/Reuß, Philipp/Schmid, Christoph U., Zwischenbilanz – Festschrift für Dagmar Coester-Waltjen zum 70. Geburtstag, 2015, Gieseking – Bielefeld
Spindler, Gerald, Die neue EU-Datenschutz-Grundverordnung, DB 2016, 937-947
Spindler, Gerald, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, JZ 2016, 805-816
Spindler, Gerald, Data and Property Rights, ZGE 2017, 399-405
Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien, 3. Aufl. 2015, C.H.Beck – München
Steinrötter, Björn, Vermeintliche Ausschließlichkeitsrechte an binären Codes, MMR 2017, 731-736
Sydow, Gernot, Europäische Datenschutz-Grundverordnung, 2017, Nomos – Baden-Baden
Taeger, Jürgen/Gabel, Detlev, BDSG (aF) und Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2013, Recht und Wirtschaft – Frankfurt a.M.
Teplitzky, Otto/Peifer, Karl-Nikolaus/Leistner, Matthias, UWG, Bd. II, 2. Aufl. 2013, De Gruyter – Berlin
Thalhofer, Thomas, Recht an Daten in der Smart Factory, GRUR-Prax 2017, 225-227
Tomain, Joseph A., Online Privacy & the First Amendment: An Opt-in Approach to Data Processing, 83 U. Cin. L. Rev. 1-72 (2014)
Van Asbroeck, Benoit/Debussche, Julien/César, Jasmien, White Paper 2017 – Data ownership in the context of the European data economy: proposal for a new right
Veil, Winfried, Was ist eigentlich Datenpolitk?, MMR 2017, 281-282
Vesting, Thomas, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, S. 1-34, in: Hoffmann-Riem, Wolfgang/Schmidt-Assmann, Eberhard/Voßkuhle, Andreas, Grundlagen des Verwaltungsrechts, Bd. II. 2. Aufl. 2012, C.H.Beck – München
Von Bernstorff, Christoph Graf, Einführung in das englische Recht, 4. Aufl. 2011, C.H.Beck – München
Von Gierke, Otto, Deutsches Privatrecht, Bd. I, 1936, Duncker & Humblot - Berlin

Von Heintschel-Heinegg, Bernd, Beck´scher Online-Kommentar StGB, 37. Ed. Stand: 01.02.2018, C.H.Beck – München
Von Staudinger, Julius, Kommentar zum Bürgerlichen Gesetzbuch: Staudinger BGB – Buch 2: Recht der Schuldverhältnisse, §§ 823, 2017, De Gruyter – Berlin
Von Staudinger, Julius, Kommentar zum Bürgerlichen Gesetzbuch: Staudinger BGB – Buch 3: Sachenrecht, §§ 925-984, 2017, De Gruyter – Berlin
Wächter, Michael, Datenschutz im Unternehmen, 5. Aufl. 2017, C.H.Beck – München
Walter, James R., A Brand New Harvest: Issues Regarding Precision Agriculture Data Ownership and Control, 2 Drake J. Agric. L. 431-446 (1997)
Wandtke, Artur-Axel, Ökonomischer Wert von persönlichen Daten, MMR 2017, 6-12
Wandtke, Artur-Axel/Bullinger, Winfried, Praxiskommentar zum Urheberrecht, 4. Aufl. 2014, C.H.Beck – München
Warren, Samuel D./Brandeis, Louis D., The Right to Privacy, 4 Harv. L. Rev.193-220 (1890)
Weichert, Thilo, Wem gehören die privaten Daten?, S. 281-298, in: Taeger, Jürgen/Wiebe, Andreas, Informatik – Wirtschaft – Recht, Regulierung in der Wissensgesellschaft, Festschrift für Wolfgang Kilian zum 65. Geburtstag, 2004, Nomos – Baden-Baden
Wehlau, Andreas, Haftung für Datenverlust – der Datenbestand als sonstiges Recht i.S.d. § 823 Abs. 1 BGB, OLG Report 2004, K27-K31 (http://www.olg-report.de/media/komm0414.RTF)
Westermann, Harm Peter/Gursky, Karl-Heinz/Eickmann, Dieter, Sachenrecht, 8. Aufl. 2011, C.F.Müller – Heidelberg
White, Ryen W./Tatonetti, Nicholas P./Shah, Nigam H./Altman, Russ B./Horvitz, Eric, Web-scale pharmacovigilance: listening to signals from the crowd, J. Am Med Inform Assoc 404-408 (2013)
Wiebe, Andreas, Der Schutz von Datenbanken – ungeliebtes Stiefkind des Immaterialgüterrechts, CR 2014, 1-10
Wiebe, Andreas, Von Datenrechten zu Datenzugang – Ein rechtlicher Rahmen für die europäische Datenwirtschaft, CR 2017, 87-93
Wiebe, Andreas, Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338-245
Wiebe, Andreas/Schur, Nico, Ein Recht an industriellen Daten im verfassungsrechtlichen Spannungsverhältnis zwischen Eigentumsschutz, Wettbewerbs- und Informationsfreiheit, ZUM 2017, 461-473
Willke, Helmut, Systemisches Wissensmanagement, 2. Aufl. 2001 Lucius & Lucius – Stuttgart
Wittmann, Philipp, Der Schutz der Privatsphäre vor staatlichen Überwachungsmaßnahmen durch die US-amerikanische Bundesverfassung, 2014, Nomos – Baden-Baden
Wolff, Heinrich Amadeus/Brink, Stefan, Beck´scher Online-Kommentar Datenschutzrecht, 21. Ed. Stand: 01.08.2017
Working Paper, Art. 29-Datenschutzgruppe, Stellungnahme 4/2007, WP 136 v. 20.06.2007
Working Paper, Art. 29-Datenschutzgruppe, Guidelines to Consent under Regulation 2016/679, 17/EN WP259 v. 28.11.2017
Wybitul, Tim/Haß, Detlef/Albrecht, Jan Philipp, Abwehr von Schadensersatzansprüche nach der Datenschutz-Grundverordnung, NJW 2018, 113-118
Zech, Herbert, Data as a Tradeable Commodity, S. 51-80, in: De Franceschi, Alberto, European Contract Law and the Digital Single Market, 2016, intersentia – Cambridge
Zech, Herbert, Information als Schutzgegenstand, 2012, Mohr Siebeck – Tübingen

Zech, Herbert, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“, CR 2015, 137-146
Zech, Herbert, Industrie 4.0 – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151-1160

TEIL II: RECHTE AN DATEN IN DER DIGITALEN ÖKONOMIE: ANALYSE ÖFFENTLICHER DISKUSSIONSPROZESSE UND DER IN IHNEN VERWENDETEN ARGUMENTATIONEN

1. FRAGESTELLUNG UND METHODISCHE VORGEHENSWEISE

Aufgabe dieses Teils des Gutachtens ist eine Analyse von öffentlichen Diskussionsprozessen und den in ihnen verwendeten Begründungsmustern zur Frage der Ausgestaltung von Rechten an Daten. Hintergrund sind die gravierenden wirtschaftlichen, politischen und sozialen Umwälzungen, die aus dem technologischen Fortschritt der digitalen Revolution folgen. In diesem Prozess der digitalen Transformation spielen – neben Algorithmen und Künstlicher Intelligenz (KI) – Daten eine Schlüsselrolle als neue kritische Ressource, deren Nutzung eine Fülle von innovativen Produkten und Dienstleistungen ermöglicht, gleichzeitig aber auch bisher unbekannte Gefahren und Herausforderungen hervorbringt, die einer gesellschaftlichen Regelung bedürfen. Dies manifestiert sich in der Diskussion über Big Data mit ihren vielen Facetten, von der (gerade auch auf Daten beruhenden) Marktmacht großer US-Techfirmen wie Google, Facebook und Amazon, über die vielfältigen innovativen Nutzungsmöglichkeiten (bspw. Internet of Things/IoT), auch für öffentliche Interessen (wie Gesundheit, Smart Cities etc.), Auswirkungen der Automatisierung auf Arbeitsplätze (robotics), bis hin zu den Gefahren für den Schutz der Privatsphäre. Sowohl die EU als auch viele Mitgliedstaaten (u.a. Deutschland) haben deshalb begonnen, umfassende Strategien in Bezug auf die Digitalisierung von Wirtschaft und Gesellschaft zu entwickeln, die in vielfältige spezifische Diskussionen bzgl. unterschiedlichster Politikbereiche münden. Allerdings stehen viele dieser Diskussionsprozesse über notwendige Anpassungen der rechtlichen Rahmenbedingungen an die Bedürfnisse und Gefahren einer digitalen Ökonomie (und Gesellschaft) und der dabei zu lösenden Probleme erst am Anfang. Dies ist auch auf unser mangelndes Wissen über die Funktionsweise dieser digitalen Transformation zurückzuführen. Ein weiterer Grund sind die Schwierigkeiten, angesichts der Schnelligkeit und Unvorhersehbarkeit des Weiteren technischen Fortschritts verlässliche Aussagen über die adäquaten rechtlichen Regelungen für eine zukünftige digitale Wirtschaft und Gesellschaft zu machen. Dabei werden sich auch die Gesellschaft und damit die öffentliche und politische Diskussion erst sehr langsam der Tragweite der Konsequenzen der in alle Lebensbereiche hineinreichenden Digitalisierung bewusst, sodass die Diskussion über viele spezifische, aber auch grundsätzliche Fragen noch stark unterentwickelt ist.

Während im ersten Teil des Gutachtens die rechtliche Analyse des Umgangs mit Daten und der diesbezüglichen regulatorischen Vorschläge im Mittelpunkt der Untersuchung stehen, werden in diesem zweiten Teil aus einer sozialwissenschaftlichen (insbesondere ökonomi-

schen) Perspektive die öffentlichen Diskussionen über rechtliche Gestaltungsvorschläge in Bezug auf Rechte an Daten analysiert. Hierbei werden wir uns auf drei spezifische aktuelle Diskussionen fokussieren, nämlich die Diskussion über die zu verabschiedende ePrivacy-Verordnung, die Diskussion über Eigentums- bzw. Zugangsrechte bzgl. Nicht-personenbezogener Daten sowie die gerade erst beginnende Diskussion um die Rechte an Daten des vernetzten Autos als wichtiges Anwendungsbeispiel für den Umgang mit Daten in IoT-Kontexten. Die Untersuchung wird sich dabei jeweils auf die Analyse der Interessen der Stakeholder und ihrer Argumente in Hinblick auf die zur Diskussion stehenden regulatorischen Vorschläge konzentrieren. Da dies aber ein Mindestgrundverständnis der jeweiligen Problemstellungen und der in ihnen entstehenden Konflikte erfordert, ist immer auch eine Problemanalyse notwendig, für die eine ökonomische Perspektive besonders geeignet ist. Allerdings ist es nicht Aufgabe dieses Gutachtens, eine ökonomische Analyse der Regelungsoptionen für diese drei Problembereiche durchzuführen, um daraus Folgerungen für rechtspolitische (und damit aus ökonomischer Sicht auch wirtschaftspolitische) Empfehlungen zu ziehen. Vielmehr geht es vor allem darum, die von den verschiedenen Stakeholdern in die jeweils relevanten Regulierungsdiskussionen eingebrachten Argumentationen herauszuarbeiten und vor dem Hintergrund ihrer Interessen und zentraler gesellschaftlicher Wertvorstellungen (wie bspw. der Schutz der Privatsphäre oder Sicherheit) zu analysieren. Besonders wichtig ist dabei auch die Frage der Klassenbildung von unterschiedlichen Arten von Daten, für die in der digitalen Ökonomie und Gesellschaft jeweils unterschiedliche Regelungen bezüglich ihrer Generierung und ihres Verarbeitens und Nutzens für unterschiedliche Zwecke gelten sollen. Die in der EU besonders wichtige Unterscheidung in personen- und nicht-personenbezogene Daten ist hierfür nur ein Beispiel. In der Studie werden wir sehen, dass viele kontroverse Diskussionen sich auf die Bildung von Klassen von Daten und Grenzziehungen zwischen unterschiedlich zu behandelnden Klassen von Daten bzw. den Grad des Zugangs zu bzw. der Verfügungsmacht über Daten beziehen.

Im Vordergrund stehen dabei vor allem die grundlegenden Konflikte zwischen (1) den Interessen von Individuen, ihre Privatsphäre zu schützen (und damit personenbezogene Daten anderen Akteuren nicht zugänglich zu machen), (2) den Interessen von Unternehmen zur Verbesserung ihrer Produkte und Dienstleistungen (insbesondere auch für Innovationen) einen möglichst umfangreichen (und kostengünstigen) Zugang zu Daten zu gewinnen und (3) der Gesellschaft bzw. dem Staat. Diese möchten zwar auf der einen Seite auch die Privatsphäre der Individuen schützen, auf der anderen Seite aber ebenfalls den Zugang zu möglichst vielen Daten erleichtern, um eine Vielzahl von staatlichen Politiken, bspw. in Bezug auf Infrastruktur, Verkehr, Energieversorgung, Umweltschutz, Sicherheit sowie Gesundheitsversorgung zu verbessern, aber auch um durch Schaffung der Voraussetzungen für eine sich dynamisch entwickelnde digitale Ökonomie Arbeitsplätze und Wohlstand in Deutschland und Europa zu sichern (insbesondere auch durch Steigerung der internationalen Wettbewerbsfähigkeit). Dabei stellt sich aber nicht nur die Frage, in welchem Umfang in diesen Konfliktfeldern Daten zugänglich gemacht werden, sondern auch unter welchen Bedingungen dies geschieht, insbesondere auch unter dem Aspekt, ob und in welchem Umfang hierfür auch (monetäre und nichtmonetäre) Gegenleistungen erfolgen, oder – allgemeiner ge-

fragt – wie die umfangreichen Vorteile, die aus der Verwendung von Daten gewonnen werden können, in der Gesellschaft verteilt werden. Alle diese Fragen sind auch eng verknüpft mit der Frage von Machtverschiebungen innerhalb der Gesellschaft durch unterschiedliche Verfügungsmacht über die im Rahmen von Big Data gesammelten und produzierten Daten.

Die Konfliktlinien bzgl. der Problematik Rechte an Daten oder der faktischen Verfügungsmacht über Daten zeigen sich jedoch nicht nur auf dieser Makroebene zwischen den Individuen, der Wirtschaft und dem Staat bzw. der Gesellschaft, sondern auch konkret in einer Vielzahl von spezifischen Sektoren und Kontexten, bezüglich derer zur Zeit Diskussionen über Rechte an Daten entstehen. Hierbei geht es oft auch um Konflikte zwischen Unternehmen in komplexen B2B-Kontexten, wie sie in informationsmäßig integrierten Wertschöpfungsketten (und -netzen) sowie vor allem auch in IoT-Anwendungen zunehmend auftreten und thematisiert werden. Hier erheben oft unterschiedliche Stakeholder Anspruch auf die Nutzung (und kommerzielle Verwertung) der jeweils gleichen Daten, wobei bisher oft völlig ungeklärt ist, wie Rechte an Daten bzw. der Umgang mit der faktischen Verfügungsmacht über Daten (bspw. über Verträge und Zugangsrechte) ausgestaltet werden sollen, um eine angemessene Balance zwischen den verschiedenen Interessen herzustellen. Ein besonders interessantes Beispiel hierfür ist die Frage nach den Rechten bzgl. der Vielzahl von Daten, die im vernetzten Auto entstehen.

Für die Untersuchung wurde methodologisch folgende Vorgehensweise gewählt. Die empirische Basis zur Analyse der teils sehr kontroversen Diskussionen sind aktuelle Positionspapiere und Stellungnahmen von Unternehmensverbänden, staatlichen Institutionen, gesellschaftlich relevanten Gruppen wie bspw. Verbraucherverbände und Datenschützer, sowie Diskussionspapiere, Studien und offizielle Dokumente, die von der EU-Kommission, Regierungsstellen sowie Regulierungsbehörden veröffentlicht wurden, insbesondere zu den in der Diskussion befindlichen Regulierungsvorschlägen. Für zwei der analysierten Diskussionen (Reform der ePrivacy-Richtlinie und zur Communication "Building a European data economy") hat die EU-Kommission eine offizielle Konsultation durchgeführt, um Stellungnahmen von Stakeholdern und anderen interessierten Parteien einzuholen. Für die Diskussion über Daten im vernetzten Fahrzeug sind Stellungnahmen im Kontext der C-ITS Plattformdiskussion entstanden. Dabei wurde Wert darauf gelegt, möglichst aktuelle (nahe an der derzeitigen Regulierungsdiskussion befindliche) Positionspapiere und Stellungnahmen in die Analyse aufzunehmen. Die Analyse dieser Dokumente bezieht sich zum einen auf die Interessen unterschiedlicher Stakeholder sowie allgemeine gesellschaftliche Werte in Bezug auf die Ausgestaltung von Rechten an Daten und zum anderen auf die darin verwendeten Argumente, seien es juristische, ökonomische oder solche, die direkt an gesellschaftlichen Werten ansetzen. In den Abschnitten, in denen die einzelnen Diskussionen analysiert werden, finden sich jeweils detailliertere Angaben zu den jeweils verwendeten Dokumenten.

Dieser zweite Teil des Gutachtens gliedert sich in folgende Abschnitte: In Abschnitt 2 werden zunächst die drei untersuchten Diskussionen näher vorgestellt und in den größeren Diskussionskontext über digitale Ökonomie und Daten gestellt. Der kurze Abschnitt 3 präsen-

tiert grundlegende Klassifizierungen von Daten, die bei der weiteren Analyse in allen drei Diskussionen eine zentrale Rolle spielen. Hierauf folgen in den drei Hauptabschnitten 4, 5 und 6 des Gutachtens die eigentlichen Analysen der Diskussionen in den drei Bereichen e-Privacy-Reform, Rechte an nicht-personenbezogenen Daten sowie Daten in vernetzten Fahrzeugen. Abschnitt 7 enthält in knapper Form eine kurze Analyse der Diskussion in den USA. Eine zusammenfassende Analyse der wichtigsten Argumentationen in den analysierten Diskussionen findet sich im abschließenden Abschnitt 8.

2. ZUR STRUKTURIERUNG DER DISKUSSION UM RECHTE AN DATEN IN EINER DIGITALEN WIRTSCHAFT UND GESELLSCHAFT

Die wissenschaftliche und öffentliche Diskussion über Digitalisierung und Daten ist komplex, unübersichtlich und hat sich in unterschiedlichen Entwicklungslinien vollzogen, die hier nicht systematisch nachgezeichnet werden können. Zentral ist allerdings die exponentielle Zunahme der Menge an generierten Daten aus unterschiedlichsten Quellen, die in Kombination mit stark sinkenden Kosten der Speicherung und Kommunikation von Daten eine bisher nie dagewesene Ansammlung von Daten erlauben, die wiederum durch Datenanalyse zu einer Fülle von neuen Erkenntnissen führen (Big Data). Unbestritten ist, dass gerade diese Datenmassen zu vielen neuen innovativen Problemlösungen führen können (Data-Driven Innovation).[474] Gleichzeitig besteht aber auch ein Konsens darüber, dass viele dieser gesammelten Daten sehr detaillierte Informationen aus der Privatsphäre von Individuen enthalten können. Die daraus mögliche Erstellung von Konsumentenprofilen kann auf der einen Seite auf individuelle Personen zugeschnittene ("personalisierte") Produkt- und Dienstleistungsangebote ermöglichen, auf der anderen Seite aber auch dazu benutzt werden, Verbraucher durch Ausnutzung individueller Schwächen (behavioral targeting) oder personalisierter Preise (Abschöpfung der Konsumentenrente) zu schädigen.[475] Insofern sind Daten zu einer zentralen und für die Wettbewerbsfähigkeit von Unternehmen oft kritischen Ressource geworden, wobei allerdings auch die zentrale Bedeutung von Fähigkeiten zur Analyse von Daten, von neuen Methoden der Künstlichen Intelligenz (KI) und von Algorithmen, einbezogen werden muss.

Für besonders viele Diskussionen hat auch der disruptive Charakter von vielen neuen digitalen Geschäftsmodellen gesorgt, da sie in einem Schumpeterschen Prozess der "schöpferischen Zerstörung" viele alte, wohletablierte Geschäftsmodelle erfolgreich angegriffen haben und diese teilweise ersetzen oder zu ersetzen drohen. Insofern geht die digitale Revolution mit einer umfassenden Umstrukturierung der Wirtschaft einher. Hierbei spielen Plattformmärkte eine ganz besondere Rolle, da die auf Plattformen auftretenden direkten und indirekten Netzwerkeffekte in bestimmten Bereichen wie Suchmaschinen oder Sozialen Medien

[474] Vgl. OECD (2015), Monopolkommission (2015).

[475] Vgl. zur Diskussion über Preisdiskriminierung und personalisierte Preise Fudenberg & Villas-Boas (2012) sowie zu behavioral targeting Hoffmann, Inderst & Ottaviani (2013) sowie Acquisti et al. (2016).

das Auftreten von quasi-monopolistischen Marktstellungen wie bei Google und Facebook ermöglichen ("winner takes all").[476] Besonders wichtig ist in diesem Zusammenhang, dass Firmen wie Google, Facebook, aber bspw. auch Amazon Daten aus sehr unterschiedlichen Quellen gewinnen, zusammenführen und so in besonderer Weise Vorteile aus der Auswertung und Nutzung dieser Daten gewinnen können, die anderen Unternehmen nicht im gleichen Maße zur Verfügung stehen. Insofern gibt es bereits seit einigen Jahren eine zunehmende Diskussion in der Wettbewerbspolitik, inwieweit die Verfügung über große Mengen an bestimmten Daten zur Entstehung von Marktmacht und gravierenden Wettbewerbsproblemen führen kann. Die Diskussion über die Marktmacht von Google hat insbesondere durch den EU-Wettbewerbsfall "Google-Shopping" auch stark die politische und öffentliche Diskussion erfasst. Insofern gibt es eine intensive Debatte über die Frage, ob die bisherigen wettbewerbsrechtlichen Regelungen für die Lösung von Wettbewerbsproblemen in der digitalen Ökonomie ausreichen oder ob neue wettbewerbsrechtliche Lösungen gefunden werden müssten. Wichtig für unsere Diskussion ist, dass hierbei zunehmend die Frage in den Mittelpunkt rückt, inwieweit gerade die Verfügung über Daten eine zentrale Ursache von Wettbewerbsproblemen in der digitalen Ökonomie ist und wie deshalb bspw. bei der Missbrauchsaufsicht über marktbeherrschende Unternehmen oder in der Fusionskontrolle die Verfügung über Daten für die Feststellung von Marktmacht berücksichtigt werden sollte, bzw. ob und wie die Sicherstellung eines Zugangs zu Daten eine Lösungsmöglichkeit für Wettbewerbsprobleme sein kann.[477]

Neben dieser wettbewerbspolitischen Diskussion kreist eine weitere zentrale Diskussion der Datenproblematik um die Frage, ob und unter welchen Bedingungen das Sammeln dieser riesigen Mengen von Daten, insbesondere über das Internet, und deren Nutzung ein Problem für Internetnutzer und Verbraucher darstellt, vor allem aufgrund der vielen Informationen über die Privatsphäre von Personen. Im Mittelpunkt steht dabei primär das Geschäftsmodell von vielen Serviceanbietern wie Google, Facebook u.a., die den Nutzern oft attraktive "kostenlose" Dienstleistungen anbieten, die nicht durch Geld sondern faktisch durch Nutzerdaten bezahlt werden, deren Nutzung wiederum das Angebot von sehr gezielten Werbeaktivitäten an Werbetreibende ermöglicht ("targeted advertising"). Hierbei ist in der Diskussion inzwischen die ökonomische Argumentation akzeptiert worden, dass es sich nicht um "kostenlose" Angebote an die Nutzer handelt, sondern dass das Erlauben des Sammelns von Nutzerdaten eine "Gegenleistung" darstellt.[478] Sowohl aus einer verbraucherpolitischen als auch datenschutzrechtlichen Perspektive ist dabei die wichtige Diskussion entstanden, ob

[476] Vgl. zu Plattformmärkten und ihren ökonomischen Grundlagen Evans & Schmalensee (2007) und Monopolkommission (2015, Rdnr. 30-63); zur Diskussion über disruptive Innovationen De Streel & LaRouche (2015).

[477] Vgl. Monopolkommission (2015), Graef (2015), Stucke & Grunes (2016), Autorité de la Concurrence & Bundeskartellamt (2016).

[478] Vgl. Monopolkommission (2015) zum Geschäftsmodell von "free services"; zur rechtlichen Diskussion über "Daten als Gegenleistung" vgl. Schweitzer & Peitz (2017), Specht (2017) sowie in Teil I des Gutachtens auf S. 39 ff.

und unter welchen Bedingungen die Nutzer solcher Dienste rationale und wohlinformierte Entscheidungen über die Zurverfügungstellung von Nutzerdaten treffen können. Dies bezieht sich auch auf das Sammeln von Informationen über "Cookies" und andere Formen des "Trackings" des Surfverhaltens von Internetnutzern. Durch die bereits seit einiger Zeit geführte Diskussion über das "privacy paradox", d.h. dass sich viele Internetnutzer faktisch in ihrem Verhalten bzgl. der Weitergabe ihrer Daten anders verhalten als sie in Umfragen über die Wichtigkeit des Schutzes ihrer privaten Daten angeben,[479] sind inzwischen große Bedenken laut geworden, dass die bisherige Lösung durch spezifische Einwilligungen der Weitergabe von Daten der Nutzer an diese Serviceanbieter eventuell nicht ausreichend funktioniert, um einen adäquaten Schutz der Privatsphäre zu erreichen. Hieraus folgt eine breite Diskussion um die spezifischen Anforderungen, die an eine gültige Einwilligung gestellt werden ("notice and consent"-Lösungen),[480] aber auch eine wesentlich grundsätzlichere Diskussion darüber, welcher Stellenwert dem Instrument der individuellen Einwilligung für die Frage der Zulässigkeit des Sammelns und der Verarbeitung von Daten überhaupt zukommen soll.[481]

Durch das sich gerade entwickelnde Internet of Things (IoT) als wichtiger weiterer Schritt in der digitalen Transformation entstehen zurzeit zusätzliche neue Diskussionen, die weit über die obige Diskussion hinausgehen. Das Internet der Dinge zeichnet sich dadurch aus, dass Schritt für Schritt eine Vielzahl von bisher bereits existierenden, sowie völlig neuen Maschinen und Geräten mit unterschiedlichen Arten von datengenerierenden Sensoren ausgestattet werden und gleichzeitig als smarte vernetzte Geräte in ständiger Verbindung mit dem Internet bzw. mit anderen vernetzten Geräten stehen werden. Die Anwendungen können dabei sowohl innerhalb von integrierten Produktions- und Distributionsketten (und -netzen) im B2B-Bereich (wie bspw. Smart Manufacturing), im privaten Bereich von Konsumenten und Haushalten (wie bspw. Smart-Home-Anwendungen, smarte Uhren oder Fitnessarmbänder oder das vernetzte Auto) oder in öffentlichen und halböffentlichen Räumen (wie in Supermärkten oder bei Smart-City-Anwendungen) auftreten.[482] Dieser Schritt zum Internet der Dinge impliziert insbesondere, dass Daten für die Online-Welt nicht nur generiert werden, wenn eine Person aktiv über ihren Computer oder ein Smartphone in das Internet geht, d.h. die Suchmaschine benutzt, im Internet surft oder sich bei Facebook einloggt, sondern dass potentiell überall in der Offline-Welt ständig mit dem Internet vernetzte Geräte Daten über ihre Umgebung generieren, transferieren und weiterverarbeiten können. Dies bedeutet, dass die Offline-Welt datenmäßig zunehmend in die Online-Welt integriert wird. Die daraus ent-

[479] Zur Diskussion über das Privacy Paradox vgl. Norberg et al. (2007), Acquisti & Großklag (2007), Kokolakis (2015), Borgesius (2015), Hermstrüwer (2016).

[480] Zur Diskussion über die Problematik von "notice and consent"-Lösungen vgl. Borgesius (2015), European Data Protection Supervisor (2014), Luzak (2014), Hermstrüwer (2017) sowie grundsätzlich aus ökonomischer Sicht Acquisti et al. (2016, 479 f.).

[481] Vgl. bspw. Solove (2013).

[482] Vgl. PwC (2017).

stehende weitere Beschleunigung der Produktion von Daten wird die Möglichkeit eröffnen, neue Produkte und Dienstleistungen zu entwickeln, Produktions- und Distributionsprozesse zu optimieren sowie zu innovativen Verbesserungen bei der Erfüllung staatlicher Aufgaben führen (bspw. im Bereich von Verkehrssteuerung, Gesundheit und Sicherheit). Die Diskussion über das Internet der Dinge zeigt aber auch, dass sehr viele Fragen über die adäquaten rechtlichen Rahmenbedingungen ungelöst sind. Dies bezieht sich nicht nur auf Fragen der Cybersicherheit, Interoperabilität/Standardisierung und Haftung, sondern vor allem auch auf die Frage, wer die faktische Kontrolle über bzw. Rechte an diesen generierten Daten haben soll, sowie auf die durch das Internet der Dinge (durch die Möglichkeit einer flächendeckenden 24/7-Überwachung) sich nochmals massiv neu stellenden Frage nach dem Schutz der Privatsphäre individueller Personen.[483] Diese Diskussion ist insofern von besonderer Bedeutung, als die Frage nach einem Eigentumsrecht an Daten bzw. Zugangsrechten zu Daten erst in Bezug auf solche maschinengenerierten Sensordaten systematisch gestellt wurde.

Diese breiteren Diskussionen in Bezug auf Daten (Datenmacht in der Wettbewerbspolitik, Daten als Gegenleistung in Verbraucherpolitik/Datenschutzpolitik, Internet der Dinge) stellen einen wichtigen Hintergrund dar für die spezifischen Diskussionen über die Ausgestaltung von rechtlichen Fragen über den Umgang mit Daten, die in diesem Teil des Gutachtens konkret analysiert werden. Im Folgenden werden diese drei Diskussionen kurz vorgestellt und miteinander in Beziehung gesetzt:

ePrivacy-Reform: Nach der Entscheidung über die Verabschiedung der Datenschutz-Grundverordnung (DS-GVO), die im Mai 2018 in Kraft tritt, war es notwendig, die bisherige ePrivacy-Richtlinie von 2002, die die rechtlichen Regeln für den Schutz von Daten in der elektronischen Kommunikation umfasst, einer grundlegenden Revision zu unterziehen.[484] Konkret geht es dabei insbes. um den Schutz von Inhalten von Kommunikation, Kommunikationsmetadaten, Regeln für Cookies und Tracking, Verarbeitung von Informationen aus den Endgeräten von Verbrauchern (insbes. Smartphones) sowie die Regelung von Direktmarketing mittels elektronischer Kommunikation. Diese Reform der ePrivacy-Richtlinie ist besonders umstritten, weil sich bei ihr in besonderer Weise der Konflikt zwischen dem Schutz von Privatsphäre bzw. der Vertraulichkeit von Kommunikation und der starken Nachfrage verschiedener wirtschaftlicher Interessengruppen an der Nutzung von Daten über die Kommunikation bzw. von Informationen aus den mobilen Endgeräten von Verbrauchern zeigt, mit denen die sich entwickelnde digitale Wirtschaft eine Vielzahl von neuen Angeboten an Dienstleistungen entwickeln könnte. Gleichzeitig aber können die dabei gesammelten Daten (Standortdaten, Kommunikationsdaten, Tracking beim Surfen im Internet etc.) eine Vielzahl von sensiblen Informationen aus der Privatsphäre von individuellen Personen enthalten. Somit manifestiert sich hier der fundamentale Zielkonflikt zwischen dem Grundwert ("funda-

[483] Zur Regulierungsdiskussion vgl. PwC (2017, 225-243).

[484] Vgl. die neue Datenschutz-Grundverordnung (2016/679), die alte ePrivacy-Richtlinie (2002/58/EC) und den Kommissionsvorschlag für eine neue ePrivacy-Verordnung (EC 2017d).

mental value") Schutz der Privatsphäre und dem ökonomischen Verwertungsinteresse dieser Daten für die Datenökonomie in besonderer Weise. Insofern ist es nicht erstaunlich, dass im Kontext dieser Auseinandersetzungen der im Januar 2017 vorgelegte Vorschlag der EU-Kommission über eine neue ePrivacy-Verordnung besonders kontrovers diskutiert worden ist, mit – wie wir noch genauer sehen werden – einer klaren Frontstellung zwischen denjenigen, die möglichst stark die Privatsphäre schützen möchten, und denjenigen, die die wirtschaftlichen Vorteile einer möglichst weitgehenden Nutzung solcher Daten in den Mittelpunkt stellen. In Abschnitt 4 wird diese Regulierungsdiskussion, die sich zur Zeit noch im Trilog-Verfahren zwischen EU-Kommission, Europäischem Parlament und dem Europäischen Rat befindet, im Detail vorgestellt und die dabei von den jeweiligen Stakeholdern vorgebrachten Argumente und Positionen analysiert.

Rechte an nicht-personenbezogenen Daten: Während in der ePrivacy-Diskussion vor allem personenbezogene Daten und ihre Einwilligung zu deren Verarbeitung im Mittelpunkt stehen, bezieht sich der zweite im Detail analysierte Diskurs gerade auf nicht-personenbezogene Daten. Ausgangspunkt dieser erst in jüngster Zeit entstandenen Diskussion war die juristische Frage nach dem rechtlichen Schutz von maschinengenerierten Daten (insbes. Sensordaten), die in den neuen (oben bereits thematisierten) informationsmäßig integrierten Wertschöpfungsketten und IoT-Anwendungen eine besondere Rolle spielen. Diese Diskussion hat sich zunächst an den Fragen der Notwendigkeit eines Dateneigentums und wem die Daten (und ihre ökonomischen Vorteile) zugeordnet werden sollen, orientiert, bevor sie sich zunehmend auf Fragen des Zugangs zu Daten, insbesondere im Kontext von IoT-Anwendungen verschoben hat. Die von der EU-Kommission im Januar 2017 herausgegebene Mitteilung "Building a European data economy" und das sich daran anschließende Konsultationsverfahren hat in dieser Diskussion eine besondere Rolle gespielt.[485] Dies liegt zum einen daran, dass in dieser Mitteilung der in der wissenschaftlichen Diskussion vorgebrachte Vorschlag eines "Datenerzeugerrechts" als neues eigentumsähnliches Exklusivrecht für maschinengenerierte Daten aufgegriffen worden ist, zum anderen aber auch daran, dass diese Mitteilung die Diskussion über nicht-personenbezogene Daten in Richtung der Herstellung von adäquaten rechtlichen Rahmenbedingungen für eine florierende Datenökonomie gelenkt hat. Insbesondere ist damit die Aufmerksamkeit auf die Probleme und Hindernisse für eine möglichst weitgehende Teilung und Weiterverwendung von Daten (data-sharing and reuse of data) fokussiert worden. Insofern beziehen sich die Politikvorschläge vor allem darauf, wie insbesondere die vielen, von Unternehmen gehaltenen, Daten für die Datenökonomie besser zugänglich gemacht werden können. Hierzu zählen neben dem Datenerzeugerrecht vor allem auch Vorschläge für einen besseren vertragsrechtlichen Umgang mit Daten sowie verpflichtende Lösungen über den Zugang zu Daten. Ein zentraler Teil dieser Diskussion fokussiert sich dabei auf die Vielzahl der neuen IoT-Anwendungen. In Abschnitt 5 findet sich eine genauere Analyse der dabei diskutierten Politikvorschläge und von verschiedenen Stakeholdern in diesem Zusammenhang vorgebrachten Argumente.

[485] Vgl. die Mitteilung der EU-Kommission (EC 2017a) und der Synopsisreport der Konsultation (EC 2017c) sowie Zech (2015) für die Diskussion über ein neues Dateneigentumsrecht.

Daten im vernetzten Auto: Die dritte näher analysierte Diskussion bezieht sich auf den Umgang mit den vielfältigen Daten, die in vernetzten Fahrzeugen generiert werden. Vernetzte Autos stellen dabei einen wichtigen Anwendungsfall von IoT dar. Es ist unbestritten, dass die dabei generierten Daten über das Fahrzeug, den Verkehr, die Umwelt, aber auch das Fahrverhalten von Fahrern äußerst wertvolle Informationen liefern, die in vielfältiger Weise von verschiedenen Stakeholdern genutzt werden können. Besonders interessant ist dabei, dass hier sehr unterschiedliche Akteure Interessen an diesen Daten haben. Neben den Kfz-Haltern bzw. Fahrern, für die vor allem der Schutz ihrer Privatsphäre im Mittelpunkt steht, sind die Automobilhersteller sowie eine Fülle von Unternehmen, die entweder Reparatur- und Wartungsdienstleistungen oder vielfältige andere Serviceleistungen (Navigation, Entertainment etc.) an die Verbraucher im Fahrzeug offerieren möchten, sowie auch öffentliche Stellen (bspw. zur Verkehrssteuerung) an diesen Daten interessiert. Die Diskussion über die rechtliche Ausgestaltung bezieht sich dabei primär auf die Frage nach der Regelung des Zugangs zu diesen Daten des vernetzten Autos. In Bezug auf diese Frage hat die EU-Kommission bereits 2016 eine Diskussion zwischen allen relevanten Stakeholdern initiiert (C-ITS: Cooperative Intelligent Transport Systems), in der man sich auf Grundprinzipien für einen solchen Zugang geeinigt hat.[486] Hierbei hatte sich aber bereits ein grundlegender Konflikt zwischen den Automobilherstellern einerseits und den meisten anderen Stakeholdern andererseits angedeutet. Dieser Konflikt bezieht sich auf den Anspruch der Automobilhersteller, aufgrund von Sicherheitserwägungen eine exklusive Kontrolle über das vernetzte Auto und der in ihm generierten Daten auszuüben, was zu erheblichen Problemen für den Zugang anderer Stakeholder zu diesen Daten und damit zu negativen Wirkungen auf Wettbewerb und Innovation führen könnte. Trotz einer neuen umfangreichen, von der Kommission in Auftrag gegebenen, Studie zu dieser Problematik (TRL 2017) gibt es – jenseits von Forderungen von Stakeholdern nach regulatorischen Lösungen – bisher keine konkreten politischen Initiativen zu diesem Problem. Besonders interessant an dieser spezifischen Diskussion über Rechte an Daten ist, dass hier vor allem Konflikte über den Zugang zu Daten zwischen Unternehmen auftreten, gleichzeitig aber auch der Schutz der Privatsphäre von Autofahrern sowie öffentliche Interessen direkt betroffen sind. Diese Diskussion wird in Abschnitt 6 einer ausführlichen Analyse unterzogen.

3. ZUR DIFFERENZIERUNG VON VERSCHIEDENEN KLASSEN VON DATEN UND DAS PROBLEM VON ADÄQUATEN GRENZZIEHUNGEN

In diesem Abschnitt sollen mehrere grundlegende Klassifizierungen von Daten vorgestellt werden, die für die weitere Diskussion über Rechte an Daten besonders relevant sind. Eine

[486] Vgl. zum vernetzten und autonomen Fahren Johanning & Mildner (2015) und dem Problem des Zugangs zu den Daten des vernetzten Autos C-ITS (2016) und TRL (2017).

der grundlegenden Erkenntnisse aus den bisherigen Diskussionen über digitale Ökonomie und Daten besteht darin, dass es sehr unterschiedliche Arten von Daten gibt, bzgl. deren Produktion, Wert, Nutzung und Sensibilität in Bezug auf die Privatsphäre sehr unterschiedliche Bedingungen bestehen können. Insofern können die jeweils adäquaten Governance-Lösungen im Sinne eines Sets von Rechten und Regeln, die in Bezug auf die Sammlung, Produktion, Speicherung, Verarbeitung, Weiterverbreitung (Datenteilung, Verkauf) und Nutzung (für jeweils bestimmte Zwecke) für verschiedene Klassen von Daten sehr unterschiedlich sein.[487] Somit bezieht sich ein wichtiger Teil der Diskussion und der konkreten Politikdebatten darauf, welche Klassen von Daten in Bezug auf ihre rechtliche Ausgestaltung unterschieden werden sollten, wie diese Klassen dann im Detail rechtlich jeweils zu behandeln sind, und wo und wie die Grenzziehungen zwischen solchen unterschiedlich rechtlich geregelten Datenklassen verlaufen sollen. Ein Beispiel hierfür ist in der EU die Frage, welche Daten als personenbezogene Daten unter die neue Datenschutz-Grundverordnung (DS-GVO) oder die noch zu verabschiedende ePrivacy-Verordnung (mit ihren jeweils sehr weitgehenden rechtlichen Regulierungen zur Verarbeitung dieser Daten) fallen, und welche Daten ohne solche Beschränkungen frei verarbeitet werden können.

Welche Arten von Daten können grundsätzlich unterschieden werden? Zunächst kann zwischen freiwillig gegebenen Daten, durch Beobachtung bzw. Messung entstandenen Daten (bspw. durch Tracking des Surfverhaltens oder durch Sensoren in smarten IoT-Geräten) und Daten, die – bspw. durch Datenanalytik – aus anderen Daten abgeleitet werden (inferred data) differenziert werden. Weiterhin kann zwischen Rohdaten und (in unterschiedlichem Umfang) verarbeiteten Daten unterschieden werden. Auch die Differenzierung zwischen Daten als lediglich kodierte Information auf der syntaktischen Ebene und Daten als Information auf der semantischen Ebene kann eine wichtige Rolle spielen (wie bei der Diskussion um das Datenerzeugerrecht).[488] Daten können aber vor allem nach den Inhalten, auf die sie sich beziehen, d.h. ob es sich um technische Diagnosedaten bei Kraftfahrzeugen handelt, um Gesundheitsdaten, Finanzdaten, die Kaufhistorie von Personen auf bestimmten Plattformen, Energieverbrauchsdaten von Haushalten, Daten über das aktuelle Wetter oder Straßenverhältnisse, Kommunikations- und Standortdaten auf Smartphones etc. klassifiziert werden. In Bezug auf den Schutz der Privatsphäre können Daten danach differenziert werden, wie sensitiv sie in Bezug auf die mit ihrer Verarbeitung verbundenen Privacy-Risiken sind. Nach dem europäischen Datenschutzrecht (Art. 9 DS-GVO) gelten personenbezogene Daten bspw. über rassische und ethnische Herkunft, sexuelle Orientierung oder genetische und biometrische Daten als besonders sensitiv. Je nach den jeweiligen Problemen können insofern sehr unterschiedliche Klassen und Subklassen von Daten gebildet werden, für die jeweils eigene unterschiedliche Rechte und Regelungen bezüglich ihres Umgangs normiert werden können.

[487] Vgl. Frank & Kerber (2017, 5 ff.) für einen theoretischen Analyserahmen für die Untersuchung von Governance-Lösungen für Daten aus ökonomischer Sicht, der sich primär auf die Analyse von Marktversagensproblemen stützt.

[488] Vgl. Zech (2015) sowie Teil I des Gutachtens auf S. 66 ff.

In der EU besonders wichtig ist die Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten. Daten, die als nicht-personenbezogene Daten nicht dem Datenschutzrecht unterliegen, können jedoch einer Anzahl anderer rechtlicher Regelungen unterliegen. In Teil I des Gutachtens ist ausführlich untersucht worden, unter welchen Bedingungen solche Daten den Regelungsregimen des Immaterialgüterrechts (insbes. Urheberrecht), dem Geschäftsgeheimnisschutz (Trade Secrets), den rechtlichen Regeln zum Schutz von Datenbanken, dem Lauterkeitsrecht oder zivilrechtlichen Regeln wie Deliktsrecht oder Sachenrecht unterworfen sein können oder gar durch strafrechtliche Normen geschützt werden. In Abschnitt 5 werden wir uns näher die Diskussion ansehen, ob eine neue Klasse von Daten geschaffen werden soll, für die ein neues sui-generis-Exklusivrecht für den Datenerzeuger eingeführt werden soll oder – speziell in IoT-Kontexten – Rechte auf den Zugang zu einer bestimmten Klasse von Daten definiert und zugeordnet werden sollen. Allerdings ist schon die Frage der Grenzziehung zwischen den beiden Klassen personenbezogener und nicht-personenbezogener Daten schwierig. Wie bereits in Teil I dieses Gutachtens ausführlicher dargestellt,[489] sind personenbezogene Daten nach Art. 1 (1), Art. 4 Nr.1 DS-GVO "alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ... beziehen". Diese Abgrenzung ist aber deshalb schwierig, weil die Identifizierbarkeit von der jeweiligen Technologie, den dabei aufgewendeten Kosten, aber auch von den Kenntnissen der für die Datenverarbeitung Verantwortlichen und der Möglichkeit, auf Kenntnisse Dritter zuzugreifen, abhängig ist. Die bisherige juristische Diskussion hat gezeigt, dass diese so wichtige Grenzziehung zwischen der Klasse von Daten, die dem Datenschutzrecht unterworfen sind, und der Klasse von Daten, die dies nicht sind, alles andere als klar ist und über unterschiedliche Interpretationen der datenschutzrechtlichen Normen oder explizite rechtspolitische Entscheidungen in die eine oder andere Richtung verschoben werden kann.

Diese Problematik gilt auch für weitere Differenzierungen in Subklassen von personenbezogenen Daten, deren Verarbeitung und weitere Nutzung zwar immer dem Datenschutzrecht unterliegen, aber durch weitere rechtliche Differenzierung sehr unterschiedlich ausgestaltet sein kann. Auf die wichtigsten dieser Differenzierungen soll im Folgenden noch etwas näher eingegangen werden. Ausgehend vom Prinzip des informationellen Selbstbestimmungsrechts nimmt die Einwilligung des Datensubjekts eine Schlüsselrolle für die Zulässigkeit des Verarbeitens und Nutzens von personenbezogenen Daten ein (Art. 6 (1) S. 1 lit.a DS-GVO). Allerdings sind in der DS-GVO eine Anzahl von Regelungen enthalten, die eine Verarbeitung auch ohne Einwilligung erlauben. Dies ist bspw. der Fall, wenn es für die Durchführung des Vertrags erforderlich ist (Art. 6 (1) S. 1 lit. b DS-GVO), wenn es für andere aber mit dem ursprünglichen Zweck vereinbare Datenverarbeitungen geschieht (Art. 6 (4) DS-GVO) oder wenn die "berechtigten Interessen" eines datenverarbeitenden Unternehmens die Interessen an dem Schutz der personenbezogenen Daten der betroffenen Person überwiegen (Art. 6 (1) S. 1 lit. f DS-GVO). Es geht hier nicht um die Analyse dieser Legalausnahmen von dem

[489] Vgl. Teil I des Gutachtens auf S. 14 ff.

Prinzip der Einwilligung, sondern um die Einsicht, dass durch solche Regelungen jeweils Subklassen von Daten geschaffen werden, die nun – trotz Personenbezug – auch ohne spezifische Einwilligung unter bestimmten Bedingungen und für bestimmte Zwecke verarbeitet werden dürfen. Hiermit wird deutlich, dass die rechtliche Auslegung, was "vereinbare" Datenverarbeitungen sein können und insbesondere, wie die Interessenabwägung zwischen dem Schutzinteresse des Datensubjekts und den "berechtigten" Interessen von Unternehmen und anderen Akteuren an der Verarbeitung dieser Daten vorzunehmen ist, die konkreten Grenzziehungen zwischen diesen Subklassen von Daten stark beeinflusst. Je stärker die Interessen der datenverarbeitenden Unternehmen hierbei gewichtet werden, desto kleiner wird die Klasse von personenbezogenen Daten, gegen deren Verarbeitung individuelle Personen sich durch die Verweigerung der Einwilligung wehren können.

Solche relevanten Grenzziehungen liegen außerdem in anderer Hinsicht vor. Soweit Einwilligungen erforderlich sind, stellt sich vor allem die Frage nach den Anforderungen an die Gültigkeit von Einwilligungen. Wie explizit muss eine Einwilligung sein? Genügt auch ein konkludentes Tun, wie bspw. die weitere Nutzung einer Webseite, nachdem auf die Verwendung von Cookies hingewiesen worden ist? Wie stark müssen die Nutzer über die Sammlung von Daten und die Zwecke, für die sie genutzt werden, informiert werden? Wie spezifisch müssen diese Zwecke angegeben werden? Im letzten Abschnitt 2 haben wir bereits auf die schwierige Diskussion über das "privacy paradox" und die Kritik an "notice and consent"-Lösungen hingewiesen. Hier geht es nur darum, dass die konkrete Festlegung der Anforderungskriterien an eine gültige Einwilligung stark die Grenzziehung zwischen den Daten, die bei einem Einwilligungserfordernis tatsächlich den Unternehmen für die Verarbeitung zur Verfügung stehen, und den Daten, bei denen es ihnen nicht gelingt, eine solche Einwilligung zu erhalten, beeinflusst. Hierzu gehört auch die in verschiedenen Kontexten wichtige Frage, ob in Bezug auf die Einwilligung eine Opt-in oder eine Opt-out-Lösung normiert wird, d.h., dass entweder eine explizite Einwilligung erforderlich ist (Opt-in) oder dass die Personen "nur" ein Recht darauf haben, aus einer Verarbeitung ihrer Daten herauszuoptieren. Ausgehend von dem in Art. 25 (2) DS-GVO festgelegten Privacy-by-design-Grundsatz sollten eher Opt-in statt Opt-out-Lösungen für den Schutz der personenbezogenen Daten benutzt werden. Wir werden sehen, dass die Frage Opt-in oder Opt-out in der gegenwärtigen ePrivacy-Diskussion eine wichtige Rolle spielt.

Eine weitere wichtige Grenzziehung bezieht sich auf die Frage, was die Anforderungen an die Anonymisierung von personenbezogenen Daten sind, durch die ein datenverarbeitendes Unternehmen solche Daten dem Anwendungsbereich der Datenschutzregelungen entziehen kann, so dass über diese anonymisierten (aber ursprünglich personenbezogenen) Daten frei von datenschutzrechtlichen Beschränkungen verfügt werden kann. Allerdings zeigt die Diskussion über die Anonymisierung, dass auch diese Grenzziehung schwierig und umstritten ist, weil die Datenanalytik viele Möglichkeiten der Reidentifikation bei anonymisierten Datensätzen erlaubt, so dass sich auch hier die Frage nach dem adäquaten Grad an Anonymisierung stellt. Je höher die diesbezüglichen Anforderungen definiert werden (und je höher dann oft auch die Kosten der Anonymisierung sind), desto kleiner wird die Menge an ano-

nymisierten (personenbezogenen) Daten, die in der Datenökonomie verarbeitet werden können; allerdings ist umgekehrt der Schutz der Individuen vor den Privacy-Risiken solcher anonymisierten Datensätze entsprechend größer. Eine weitere Differenzierung liegt vor, wenn personenbezogene Daten nur pseudonymisiert statt anonymisiert werden, wie dies ebenfalls nach der DS-GVO möglich ist (Art. 6 (4) lit.e DS-GVO). Da bei pseudonymisierten Daten zwar die konkreten Personen nicht mehr identifiziert werden können, aber die Identifier bei den Datensätzen erhalten bleiben, erlauben pseudonymisierte Datensätze wesentlich größere Nutzungsmöglichkeiten, insbesondere in Bezug auf die Personalisierung von Angeboten und Diensten, allerdings sind die Privacy-Risiken auch höher als bei anonymisierten Datensätzen. Ob bestimmte personenbezogene Daten jenseits der Verarbeitung für den ursprünglichen Zweck anonymisiert werden müssen oder nur pseudonymisiert zu werden brauchen, um für andere Zwecke verwendet werden zu können, hat gravierende Auswirkungen auf das Ausmaß der weiteren Nutzbarkeit dieser Daten in der Datenökonomie und damit auch für ihren ökonomischen Wert.[490]

4. ÖFFENTLICHER DISKURS I: DIE DISKUSSION UM DIE EPRIVACY-VERORDNUNG

4.1 EINLEITUNG

Der Konflikt zwischen Datenschutz und den Interessen der Wirtschaft an Daten zeigt sich besonders deutlich in der Reformdiskussion über die neue ePrivacy-Verordnung. Nach der Verabschiedung und dem geplanten Inkrafttreten der DS-GVO im Mai 2018 war es notwendig, die alte ePrivacy-Richtlinie zu überarbeiten und an die neuen digitalen Entwicklungen anzupassen. Nach externen Evaluationsstudien und einem Konsultationsverfahren unterbreitete die Kommission am 10.1.2017 einen Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation, der eine Reihe von Neuerungen gegenüber der alten ePrivacy-Richtlinie umfasst.[491] Insbesondere erweitert der Vorschlag den Anwendungsbereich auch auf neue Kommunikationsformen wie die sog. Over-The-Top-Dienste (OTT), wie insbes. WhatsApp, Facebook, Skype, VoIP-Telefonie und webgestützte E-Mail-Dienste, sowie den Datenaustausch zwischen Maschinen (M2M). Weiterhin enthält der Vorschlag neue Regelungen bzgl.

[490] Vgl. zur Problematik Anonymisierung und Pseudonymisierung von Daten im europäischen Datenschutzrecht Esayas (2015) und Stalla-Bourdillon & Knight (2017).

[491] Vgl. den Vorschlag der Kommission (EC 2017d) sowie die begleitenden Staff Working Documents EC (2017e, 2017f, 2017g) mit "impact assessments" und der Ex-post REFIT Evaluation mit der ePrivacy-Richtlinie. Für eine ausführliche Synopse der Ergebnisse des öffentlichen Konsultationsverfahrens zur Überprüfung der ePrivacy-Richtlinie, die vom 12.4. - 5.7.2016 stattfand, vgl. EC (2016a). Die Ergebnisse einer begleitenden EU-weiten Eurobarometer-Umfrage über die Meinung von EU-Bürgern zum Thema Privatsphäre in der elektronischen Kommunikation finden sich in EC (2016b).

Kommunikationsdaten, der Verarbeitung von Daten aus Endgeräten, Cookies, Tracking, und (unerbetener) Direktwerbung durch elektronische Kommunikationsmittel, wobei die Kommission stark auf das Instrument der Einwilligung der Nutzer setzt. In den folgenden Monaten wurde dieser Kommissionsvorschlag von zahlreichen Institutionen und Interessengruppen kritisch diskutiert, wobei eine weitere Anzahl von Positionspapieren und Stellungnahmen entstand, deren Argumente dann in dem weiteren politischen Beratungsprozess, der zunächst vor allem im Europäischen Parlament (EP) stattfand, eingegangen sind. Nach kontroversen Diskussionen im federführenden LIBE-Ausschuss im EP sind dann Änderungen beschlossen worden, die allgemein als Stärkung des Datenschutzes und als Erschwerung für die datenverarbeitende Wirtschaft interpretiert wurden und die am 20.10.2017 vom EP als Verhandlungsposition für die Verhandlungen mit dem Rat und der EU-Kommission im Rahmen des weiteren Trilog-Prozesses verabschiedet worden sind.[492] Am 5.12.2017 hat die estnische Ratspräsidentschaft einen eigenen Kompromissvorschlag vorgelegt und einen Abstimmungsprozess zwischen den Mitgliedstaaten für die Erreichung einer gemeinsamen Position angestoßen.[493] Durch die vielen noch strittigen Fragen hat sich allerdings der ursprüngliche Zeitplan, nämlich eine neue ePrivacy-Verordnung gleichzeitig mit der DS-GVO im Mai 2018 in Kraft treten zu lassen, als nicht mehr realistisch erwiesen. Zum Zeitpunkt des Abschlusses dieser Studie ist noch keine Einigung über die endgültige Form der ePrivacy-Verordnung zustande gekommen.

Die Diskussion über die Ausgestaltung der ePrivacy-Verordnung ist äußerst komplex, da erstens viele unterschiedliche Stakeholder mit sehr verschiedenen Interessen beteiligt sind, zweitens schwierige technologische Fragen zu den Möglichkeiten und Wirkungen alternativer Regelungen auftreten, und drittens die ePrivacy-Regelungen in einem komplexen Zusammenhang zu einer Anzahl anderer rechtlicher Regelungen stehen, wie vor allem zur DS-GVO, aber auch teils zu nationalen Regelungen, die durch sie ersetzt werden.[494] Es kann hier nicht Schritt für Schritt der legislative Entstehungsprozess der ePrivacy-Verordnung mit den jeweilig vorgeschlagenen Änderungen, bspw. durch das EP, analysiert werden. Das Ziel dieses Abschnitts besteht vielmehr darin, die wesentlichen Interessen und Argumentationsmuster, die in diesem Diskussionsprozess eine wichtige Rolle spielen, herauszuarbeiten und zu analysieren. Hierbei stützen wir uns primär auf zentrale Positionspapiere, Stellungnahmen und Studien, die von Institutionen, Verbänden und Interessengruppen in diesem Prozess abgegeben worden sind. Da es sinnvoll ist, sich primär auf die besonders kontrovers diskutierten Fragen zu konzentrieren, weil hier gegensätzliche Interessen und Argumentationsmuster besonders klar aufeinander treffen, werden wir uns vor allem auf die Diskussion nach der Veröffentlichung des Vorschlags der Kommission konzentrieren. Insofern wird auch der

[492] Vgl. EP (2017) sowie die Stellungnahmen verschiedener Ausschüsse des Europäischen Parlaments LIBE (2017), JURI (2017) und ITRE (2017).

[493] Vgl. Europäischer Rat (2017, 2018a).

[494] Vgl. zur Beziehung mit anderen Regelungen bspw. Köhler (2017) in Bezug auf "unerbetene Kommunikation" und das deutsche UWG.

Kommissionsvorschlag das zentrale Referenzdokument sein, bzgl. dessen die Positionspapiere und Stellungnahmen analysiert werden, wobei auch einzelne wichtige spätere Modifikationen des Vorschlags, insbes. durch das EP, einbezogen werden. Es wird deshalb auch nicht eine detaillierte rechtliche Analyse im Mittelpunkt stehen,[495] sondern es wird primär von den Stakeholdern und ihren Interessen sowie den wichtigsten inhaltlichen Konfliktfeldern ausgegangen. Hierfür wurde folgende Vorgehensweise gewählt: Zunächst werden in Abschnitt 4.2 in knapper Form wichtige Regelungen des Kommissionsvorschlags vorgestellt und dabei die wichtigsten Konfliktfelder kurz herausgearbeitet. Anschließend folgt in Abschnitt 4.3 eine ausführliche Analyse der Positionen von Institutionen und Interessengruppen mit ihren jeweiligen Argumenten zu diesem Vorschlag, auf deren Basis dann im abschließenden Abschnitt 4.4 eine zusammenfassende Analyse der in dieser Diskussion um die ePrivacy-Verordnung auftretenden Konflikte und den in ihnen verwendeten Argumentationen durchgeführt wird, bei der auch ökonomische Analysen miteinfließen.

4.2 DER KOMMISSIONSENTWURF ZUR E-PRIVACY-VO UND DIE ZENTRALEN KONFLIKTFELDER

Mit ihrem Vorschlag einer ePrivacy-Verordnung hat die Kommission mehrere Grundsatzentscheidungen getroffen. So hat sie sich für eine unmittelbar in den Mitgliedstaaten anwendbare Verordnung statt der bisherigen Richtlinie entschieden. Dies ist auf breite Zustimmung gestoßen, da die Richtlinie zu unterschiedlichen Regelungen und einem unterschiedlichen Niveau der Durchsetzung in den Mitgliedstaaten sowie zu höheren Kosten für die Unternehmen geführt hat.[496] Wichtiger ist jedoch, dass – im Gegensatz zu Forderungen insbesondere aus der Wirtschaft – die Kommission weiter eigene zusätzliche Regeln für den Schutz der vertraulichen Kommunikation als lex specialis für notwendig erachtet. Bei dieser Grundsatzfrage, ob überhaupt eine eigene ePrivacy-Verordnung mit teilweise höherem Schutzniveau für die elektronische Kommunikation erforderlich ist, geht es vor allem darum, ob Kommunikationsdaten nach strengeren Maßstäben geschützt werden müssen. Dies zeigt sich konkret insbesondere daran, dass es im Vorschlag der ePrivacy-Verordnung keine Ausnahme von der Einwilligung zur Datenverarbeitung durch Abwägung zwischen den Interessen der Betroffenen an dem Schutz ihrer Kommunikationsdaten und den Interessen von Unternehmen an einer Datenverarbeitung gibt ("berechtigte Interessen"; Art. 6 Abs. 1 S.1, lit. f DS-GVO). Zu diesem grundsätzlichen Konfliktfeld gehört jedoch auch, dass umgekehrt im Kommissionsvorschlag der Grundsatz "privacy by design bzw. default" nicht konsequent umgesetzt ist, obwohl dies ein zentraler Grundsatz in der DS-GVO ist. Die dritte wichtige Grundentscheidung, die ePrivacy-Verordnung auch auf die neuen Kommunikationsformen (OTT-Dienste, wie WhatsApp, Facebook, Skype etc.) anzuwenden, die teilweise die klassi-

[495] Vgl. für erste rechtliche Analysen des Vorschlags der Kommission Herbrich (2017a, 2017b, 2017c), Engeler & Felber (2017), Voss (2017), Maier & Schaller (2017), Köhler (2017); vgl. auch Teil I dieses Gutachtens auf S. 71 ff.

[496] Vgl. bereits den Synopsisreport der Konsultation (EC 2016a, 2 ff.).

schen Kommunikationsformen ersetzen, ist auf breitere Zustimmung gestoßen (Art. 4 (2) e-Privacy-VO-E). Die Entscheidung für die Beibehaltung eines eigenen Regelungsregimes zusätzlich zur Datenschutz-Grundverordnung hat jedoch auch zu einer Fülle von Diskussionen und Klagen bezüglich der Klärung des Verhältnisses zwischen beiden rechtlichen Regelungen geführt.

Nach Art. 5 ePrivacy-VO-E gilt zunächst grundsätzlich ein Verbotsprinzip bzgl. Eingriffen in elektronische Kommunikationsdaten (wie Mit- und Abhören, Speichern, Beobachten oder andere Arten des Überwachens oder Verarbeitens elektronischer Kommunikationsdaten), soweit dies nicht ausdrücklich durch die ePrivacy-VO erlaubt wird.[497] Hintergrund ist hier Art. 7 der Charta der Grundrechte der EU, durch die das Privatleben und die Kommunikation aller Menschen geschützt werden. Bezüglich des Umfangs und der Bedingungen für die erlaubten Verarbeitungen von Kommunikationsdaten gibt es allerdings gravierende Meinungsverschiedenheiten und Konflikte. Dies bezieht sich zum einen auf die Fragen, für welche Verarbeitungen von welchen Daten keine Einwilligung erforderlich ist, wie eventuell notwendige Einwilligungsregelungen ausgestaltet werden sollen und wie und in welchem Umfang Daten für welche Zwecke verwendet werden dürfen, bzw. nach ihrer Verwendung gelöscht oder anonymisiert werden müssen (Art. 6 - 11). Zum anderen geht es um die Problematik der Regelung von unerbetener Direktwerbung (Art. 12 - 16).

Art. 6 ePrivacy-VO-E regelt zunächst Ausnahmen in Bezug auf die Bedingungen für die erlaubte Verarbeitung von elektronischen Kommunikationsdaten. Diese ist auch ohne Einwilligung erlaubt, wenn dies für die Kommunikation selbst oder die Sicherheit von Kommunikationsnetzwerken notwendig ist (Art. 6 (1)). Darüber hinaus unterscheidet die Kommission zwischen den Inhalten der Kommunikation und den Kommunikationsmetadaten (bspw. wer mit wem, wann, wo und wie lange kommuniziert). Letztere können auch ohne Einwilligung verarbeitet werden, wenn dies zur Einhaltung von Qualitätsanforderungen für die Dienste sowie zur notwendigen administrativen Abwicklung (Rechnungsstellung etc.) notwendig ist (Art. 6 (2) lit. a und b). Wesentlich umstrittener, insbesondere in Bezug auf die spezifischen Bedingungen, ist Art. 6 (2) lit. c, nach dem weitere Verarbeitungen der Metadaten möglich sind, wenn die Endnutzer zustimmen. In Bezug auf die Kommunikationsinhalte (Art. 6 (3)) besteht immer die Notwendigkeit einer Einwilligung, wobei die Verwendung von solchen Daten jenseits dessen, was für den spezifischen, vom Endnutzer gewünschten Dienst, erforderlich ist, trotz Einwilligung zusätzlichen Restriktionen unterliegt, wie bspw. eine Konsultation mit Aufsichtsbehörden. Die Konflikte beziehen sich dabei auf die Details der spezifischen Bedingungen für diese Regelungen, die mehr oder weniger restriktiv ausgestaltet sein können. Art. 7 ePrivacy-VO-E regelt dann die Frage der Speicherung und des Löschens von Kommunikationsdaten, wobei das Grundprinzip darin besteht, dass diese Daten nur solange gespeichert sein sollen, wie es für die Kommunikation notwendig ist und dann entweder gelöscht oder anonymisiert werden müssen.

[497] Vgl. zu den folgenden Regelungen im Detail auch Herbrich (2017b).

Art. 8 - 10 ePrivacy-VO-E enthalten Regelungen über die Nutzung von Informationen aus den Endgeräten von Endnutzern, d.h. es geht inhaltlich um Regelungen über Cookies und Tracking sowie die Ausgestaltung der Einwilligung zu solchen Praktiken. Nachdem Informationen aus den Endgeräten, insbesondere auch durch die Nutzerverfolgung im Internet, aber auch Offline-Tracking von Personen (bspw. in Supermärkten), wichtig sind für die Generierung vielfältiger wertvoller Informationen über Verbraucher, bspw. auch für personalisierte Dienste und Angebote sowie gezielte Werbung (targeted advertising), gleichzeitig diese Daten jedoch auch tiefe Einblicke in die Privatsphäre von Individuen geben können, ist es nicht verwunderlich, wenn es bei der Frage nach der genauen Ausgestaltung dieser Regelungen zu gravierenden Konflikten kommt. Zunächst soll nach dem Kommissionsentwurf nach Art. 8 (1) lit. a, c, und d ePrivacy-VO-E die Verarbeitung solcher Informationen erlaubt sein, wenn es für die Kommunikation oder den gewünschten Dienst erforderlich ist oder zur Messung des für die Werbung wichtigen Webpublikums (audience measurement). Für letzteres sind aber die konkreten Bedingungen sehr umstritten, insbesondere in Bezug auf die Möglichkeit, Dritte mit der Auswertung zu beauftragen. Von besonderer Bedeutung ist vor allem Art. 8 (1) lit. b, nach dem mit einer Einwilligung weitere Informationen aus den Endgeräten verarbeitet werden können. Hier ist allerdings sehr umstritten, ob statt einer Einwilligung auch die zusätzliche Option einer Abwägung mit "berechtigten Interessen" von datenverarbeitenden Unternehmen als Ausnahme eingeführt werden könnte (wie dies in der DS-GVO möglich ist). Dies findet sich aber weder im Kommissionsvorschlag wieder, noch konnte es sich im EP durchsetzen. Sehr umstritten ist auch die Frage nach dem Verbot von Tracking Walls, d.h. die Frage, ob der Zugang zu einer Webseite verwehrt werden kann, wenn der Nutzer keine Einwilligung in die Verarbeitung seiner Daten gibt. Diese auch ökonomisch sehr bedeutsame Regelung findet sich in den Abänderungen des EP (Art. 8 (1a)),[498] während der Kommissionsvorschlag kein solches Verbot enthält.

Besonders umstritten sind auch die Regeln über den Zugriff auf Informationen von Endgeräten über eine direkte Verbindung mit anderen Geräten (M2M-Kommunikation über Funkverbindung, WLAN oder Bluetooth; Art. 8 (2) ePrivacy-VO-E). Dies ist speziell relevant für das Offline-Tracking von mobilen Endgeräten (bspw. in Supermärkten und für Smart-City-Anwendungen).[499] Während im Kommissionsentwurf dies auch ohne vorherige Einwilligung möglich ist, falls es in hervorgehobener Weise mit einem deutlichen Hinweis über die konkreten Modalitäten und Möglichkeiten des Endnutzers, diese Erhebung zu beenden oder auf ein Minimum zu beschränken, angezeigt wird, ist in der Entschließung des EP diese Lösung durch eine Fülle weiterer Restriktionen stark eingeschränkt. Hierzu gehört insbesondere eine Zweckbeschränkung auf statistische Zählung, Beschränkung auf den strikt notwendigen Umfang, unverzügliche Datenlöschung oder Anonymisierung und eine wirksame Wider-

[498] Vgl. EP (2017, 58: Amendment 92). Eine solche Regelung würde dem in der DS-GVO verankerten Koppelungsverbot (Art. 7 (4) DS-GVO) entsprechen.

[499] Vgl. hierzu auch den Erwägungsgrund 25 des Kommissionsvorschlags (EC 2017d).

spruchsmöglichkeit, die nicht die Funktionalität des Endgeräts einschränkt.[500] Ein weiteres umstrittenes Konfliktfeld ist die Frage, wie Einwilligungen erteilt werden können (Art. 9 und 10 ePrivacy-VO-E). Hierbei kommt nach dem Kommissionsvorschlag den technischen Einstellungen von Webbrowsern oder Apps (insbes. bzgl. Cookies) eine zentrale Rolle zu.[501] Insbesondere müssen bei der Installation von solcher Software die Nutzer über die möglichen Privacy-Voreinstellungen informiert werden und diese müssen auch die Option bieten, den Zugriff von Dritten auszuschließen. Das EP ist dagegen wesentlich weiter gegangen und fordert zum einen die Möglichkeit von granularen Optionen der Einwilligung, um dem Nutzer die Möglichkeit zu geben, wesentlich spezifischer auszudifferenzieren, für welche Zwecke und für welche Daten eine Einwilligung gegeben werden soll. Zum anderen aber fordert das EP eine privacy-freundliche Voreinstellung von Software. Allerdings sollen die Nutzer immer auch spezifische Einwilligungen geben können.[502] Die Rolle von Webbrowsern und die dabei möglichen Voreinstellungen ist somit ein wichtiger Teil dieses Konfliktfeldes, da es hierbei um die Frage der Ausgestaltung von Einwilligungen über Opt-in- oder Opt-out-Lösungen geht. Art. 9 (3) klärt zusätzlich die genauen Bedingungen für das Widerrufsrecht bezüglich der gegebenen Einwilligungen.

Ein letztes großes Konfliktfeld, das aber in der Telekommunikationsregulierung bereits seit langem ein wichtiges Thema ist, ist die Frage der Zulässigkeit und Ausgestaltung von Direktwerbung bzw. "unerbetener Kommunikation". Bereits seit langem gibt es Regulierungen über die Begrenzung von unerwünschten Werbeanrufen und -emails und anderen Praktiken.[503] Zunächst bedarf die Direktwerbung über elektronische Kommunikationsdienste auch in Zukunft einer vorherigen Einwilligung (Art. 16 (1) ePrivacy-VO-E), wobei dies jetzt auch auf die durch die neue ePrivacy-Verordnung erfassten OTT-Dienste ausgeweitet wird. Direktwerbung wird dabei sehr weit verstanden. Allerdings gibt es auch weiterhin die Ausnahme vom Einwilligungserfordernis für Bestandskunden, wenn die Email-Adresse im Rahmen eines vorherigen Verkaufs erlangt wurde und auch jederzeit ein Widerspruch möglich ist. Wichtig ist, dass der Nutzer klar und einfach über den Werbecharakter informiert wird (z.B. über spezifische Codes oder Vorwahlnummern) sowie weitere Bedingungen, die es dem Nutzer erleichtern, mit unerbetener Direktwerbung umzugehen. Auch hier sind die Details der Regelungen umstritten. Andere wichtige Änderungen jenseits des Themas Direktwerbung beziehen sich zum einen auf die Frage, inwieweit Mitgliedstaaten im Detail von bestimmten Regelungen der ePrivacy-Verordnung abweichen dürfen (Art. 11 (1) und 16 (4) e-Privacy-VO-E), wozu es ebenfalls recht unterschiedliche Meinungen gibt. Zum anderen ändern sich – allerdings wenig umstritten – durch die ePrivacy-Verordnung die Regeln für die

[500] Vgl. EP (2017, 60: Amendment 99).

[501] Vgl. auch Erwägungsgrund 23 des Kommissionsvorschlags (EC 2017d), nach dem mehrere Stufen der Zulassung von Cookies angeboten werden sollen, wie bspw. "Cookies niemals annehmen", "Cookies von Drittanbietern zurückweisen" und "Cookies immer annehmen" als niedrigste Form des Schutzes.

[502] Vgl. EP (2017, 62 ff.).

[503] Vgl. auch Köhler (2017) und Herbrich (2017c).

Durchsetzung, da jetzt primär auf das Sanktionssystem der DS-GVO zurückgegriffen wird, was in vielen Bereichen zu einer wesentlichen Verschärfung der Sanktionen führt (Art. 18 - 24 ePrivacy-VO-E). Hierbei wird die Anwendung der ePrivacy-Verordnung den Datenschutzbehörden der Mitgliedstaaten übertragen und der Europäische Datenschutzausschuss ist für die einheitliche Anwendung dieser Verordnung zuständig. Lediglich die im Kommissionsvorschlag fehlende Klagebefugnis der Verbraucherschutzverbände ist umstritten und wurde dann in der Fassung des EP einbezogen.[504]

4.3 ANALYSE DER STAKEHOLDER-POSITIONEN UND IHRER INTERESSEN

In diesem Abschnitt sollen die wichtigsten Argumente aus den Positionspapieren von zentralen Stakeholdern in dieser Diskussion herausgearbeitet, in den Kontext ihrer spezifischen Interessen gestellt und mit ihren spezifischen Bedenken und Forderungen in Bezug auf die e-Privacy-Reform verbunden werden. Aufgrund der Vielzahl von Positionspapieren und Stellungnahmen werden die Stakeholder in Gruppen mit homogenen Interessen zusammengefasst und in einer solchen zusammengefassten Form analysiert. Dabei werden primär folgenden Stakeholder-Gruppen unterschieden: (1) Daten- und Verbraucherschutzorganisationen, (2) Telekommunikationsunternehmen, (3) Werbewirtschaft und (werbefinanzierte) Medienanbieter, (4) Industrie und Handel, (5) allgemeine Digitalwirtschaft, die sich aber heterogen aus verschiedenen Gruppen zusammensetzen kann, und (6) Staat, Behörden und Wissenschaft.

4.3.1 DATEN- UND VERBRAUCHERSCHUTZORGANISATIONEN

Daten- und Verbraucherschutzorganisationen[505] gehen von der normativen Position aus, dass die Privatsphäre von Individuen und insbesondere die vertrauliche Kommunikation unmittelbar als Grundrecht ("fundamental value") nach Art. 7 der Grundrechtecharta der EU einen besonderen Schutz genießt. In Bezug auf die ePrivacy-Diskussion können Daten- und Verbraucherschützer hierbei auch auf aktuelle Umfragen verweisen. In einer Umfrage des Eurobarometers, die im Auftrag der EU-Kommission im Juli 2016 stattfand (mit insgesamt 26.536 befragten Personen aus der gesamten EU), wurde festgestellt, dass die europäischen Bürgerinnen und Bürger sehr großen Wert auf den Schutz ihrer personenbezogenen Informationen und vertraulichen Kommunikation legen. So sind jeweils 92% der befragten Personen der Ansicht, dass personenbezogene Informationen auf ihrem Computer oder Smartphone nur mit ihrer Erlaubnis zugänglich sein sollen und die Vertraulichkeit von elektroni-

[504] Vgl. EP (2017, 83: Amendment 148).

[505] Vgl. zum folgenden die Positionspapiere und Stellungnahmen von EDRi (2017), Article 29 Data Protection Working Party (2017), European Data Protection Supervisor (2017), vzbv (2017), BEUC (2017), Digitale Gesellschaft (2017), und DVD (2017).

scher Kommunikation garantiert werden müsse. 82% finden es wichtig, dass der Einsatz von Mitteln zur Überwachung von Online-Aktivitäten nur mit ihrer Zustimmung stattfindet.[506] Hieraus ergibt sich für Daten- und Verbraucherschützer die starke Betonung der Notwendigkeit der Einwilligung in die Verarbeitung von Kommunikationsdaten sowie der Schutz der Integrität von Endeinrichtungen wie Smartphones, d.h. dass ohne Einwilligung nicht auf Kommunikationsdaten bzw. Informationen aus den Endgeräten zugegriffen werden darf, bzw. dass immer die Möglichkeit für Widerspruch gegen eine solche Verarbeitung, d.h. Opt-out-Lösungen, möglich sein muss. Hieraus leitet sich auch ab, dass Personen leicht die Möglichkeit haben sollten, keine Cookies akzeptieren zu müssen, sich nicht im Internet tracken lassen zu müssen und Endgeräte wie Smartphones benutzen zu können, ohne ein Offline-tracking (Standortdaten) akzeptieren zu müssen sowie auch die Verarbeitung ihrer Kommunikationsmetadaten verbieten zu können. Zwar wird akzeptiert, dass die Verarbeitung bestimmter Daten sowie Cookies etc. unter Umständen notwendig sein können, um bestimmte Dienste zu nutzen, aber dies sollte ohne zusätzliche Einwilligung immer nur soweit möglich sein, wie dies für die gewünschten Dienste und der Aufrechterhaltung von Sicherheit, Vermeidung von Betrug, Zwecke der Abrechnung etc. notwendig ist. Daten sollten zudem so bald wie möglich gelöscht oder zumindest anonymisiert werden. Aufgrund der vielfältigen Probleme bzgl. Einwilligungen und des Aufwandes für die Nutzer werden privacy-freundliche Voreinstellungen (privacy by default) als notwendig angesehen, bspw. durch die Nutzung von Voreinstellungen in Webbrowsern.[507] Hintergrund aller dieser Maßnahmen ist, dass nur so das Vertrauen der Nutzer in die elektronische Kommunikation sichergestellt werden kann.[508]

Auch wenn die Daten- und Verbraucherschützer mit einer ganzen Reihe von Regelungen im Kommissionsvorschlag einverstanden sind, gibt es bei einer Anzahl von Punkten teilweise große Bedenken, aus denen sich die folgenden spezifischen Forderungen ableiten: Das im Kommissionsvorschlag erlaubte Offline-Tracking von Endgeräten sollte nicht ohne explizite Einwilligung möglich sein oder nur insoweit, als gesammelte Daten anonymisiert und nur für statistische Zwecke benutzt werden und weitere restriktive Bedingungen gegeben sind, insbes. die Möglichkeit von wirksamen Opt-out-Möglichkeiten.[509] Eine weitere zentrale Forderung ist das Verbot von Tracking Walls, d.h. Nutzern sollte nicht der Zugang zu einem Dienst verwehrt werden, wenn sie die Einwilligung zu einem Tracking verweigern, das nicht strikt notwendig ist.[510] Als besonders wichtig wird von Daten- und Verbraucherschützern angese-

[506] Vgl. EC (2016b, 29).

[507] Vgl. BEUC (2017a, 10).

[508] Vgl. European Data Protection Supervisor (2017, 7).

[509] Vgl. Art. 29 Data Protection Working Party (2017, 11 f.).

[510] Vgl. BEUC (2017a, 9), Art. 29 Data Protection Working Party (2017, 4), European Data Protection Supervisor (2017, 16 f.); vgl. hierzu auch das Ergebnis des Eurobarometers (EC 2016b, 55), nach dem es 64% der Befragten für nicht akzeptabel finden, dass die Online-Aktivitäten überwacht werden im Tausch für den unbeschränkten Zugang zu einer bestimmten Webseite.

hen, dass es in der ePrivacy-Verordnung eine Verpflichtung zu privacy-freundlichen Voreinstellungen (privacy by design) gibt.[511] Insofern hat das EP mit seinen modifizierten Vorschlägen Bedenken von Verbraucher- und Datenschützern aufgegriffen. Besonders stark plädieren Daten- und Verbraucherschutzorganisationen dafür, dass – wie im Kommissionsvorschlag vorgesehen – die Abwägung mit "berechtigten Interessen" kein Rechtfertigungsgrund sein sollte und dass das Schutzniveau in der ePrivacy-Verordnung nicht unter das der DS-GVO fallen darf. Neben dem bereits angesprochenen Problem der fehlenden Umsetzung von "privacy-by-design" fordern diese Organisationen deshalb auch die Einführung der im Kommissionsvorschlag fehlenden Klagemöglichkeit von Verbraucherschutzverbänden, die ansonsten in der DS-GVO vorgesehen ist.[512] Darüber hinaus plädieren Daten- und Verbraucherschützer für eine weitere Präzisierung von Definitionen und Regeln, insbesondere um das Verhältnis zur DS-GVO weiter zu klären. In Bezug auf viele der angesprochenen Detailregelungen setzen sich Daten- und Verbraucherschützer meist für restriktivere Regelungsvarianten ein (bspw. auch bei Direktwerbung) bzw. möchten den Anwendungsbereich der e-Privacy-Verordnung eher breiter als enger definieren.

4.3.2 TELEKOMMUNIKATIONSUNTERNEHMEN

Für die Telekommunikationsindustrie[513] bedeutet die ePrivacy-Verordnung zunächst, dass in Bezug auf Regulierung ein stärkeres "levelling-the-playing-field" mit neuen elektronischen Kommunikationsformen geschaffen wird, die nun zum ersten Mal Regeln zum Schutz von Kommunikation beachten müssen, denen die traditionellen Telekommunikationsunternehmen aufgrund des Fernmeldegeheimnisses seit langem unterworfen waren. Trotz dieser Verringerung der asymmetrischen Regulierung würden aber auch die Telekommunikationsfirmen gerne die vielen ihnen zur Verfügung stehenden Daten, insbesondere Kommunikationsmetadaten, wesentlich stärker kommerziell nutzen. Insofern ist es nicht überraschend, dass die Verbände von Telekommunikationsfirmen die Vorteile von Kommunikationsmetadaten für Innovation und Wachstum betonen und diesbezüglich für weniger restriktive Lösungen eintreten als sie der Kommissionsvorschlag vorsieht. Insbesondere wird von der Telekommunikationsindustrie die Möglichkeit der Nutzung ohne Einwilligung aufgrund von "berechtigten Interessen" (mit einer Fall-zu-Fall-Bewertung und entsprechenden Sicherheitsvorkehrungen) gefordert, sowie die Möglichkeit, nur mit Pseudonymisierung (statt Anonymisierung) der Daten zu arbeiten (wie dies nach der DS-GVO grundsätzlich möglich wäre). Insbesondere Kommunikationsmetadaten sollten für Zwecke, die nicht privacy-sensitiv sind, ohne Einwilligung verarbeitet werden dürfen. Hierbei wird besonders auf das Problem der

[511] Vgl. BEUC (2017a, 11), Art. 29 Data Protection Working Party (2017, 4), European Data Protection Supervisor (2017, 18 f.)

[512] Vgl. zu "privacy by default" BEUC (2017a, 11 f.) und Art. 29 Data Protection Working Party (2017,4); zur Klagemöglichkeit von Verbraucherschutzverbänden BEUC (2017a, 12).

[513] Vgl. die Positionspapiere von GSMA/etno (2017) und VATM (2017).

Einwilligungsmüdigkeit ("consent fatigue") von Nutzern hingewiesen. Die Telekommunikationsunternehmen betonen, dass sie sich in besonderer Weise kompetent fühlen, in rechtlich einwandfreier Weise mit Kommunikationsdaten umzugehen.[514]

4.3.3 WERBEINDUSTRIE UND WERBEFINANZIERTE MEDIEN

Eine besondere Bedeutung kommt der Werbeindustrie, bzw. Geschäftsmodellen, die sich primär aus Werbeeinnahmen finanzieren, zu. Diese gehören größtenteils der digitalen Wirtschaft an, aber sollen hier zunächst als eine eigene Gruppe mit eigenen Interessen und Forderungen analysiert werden.[515] Eine spezielle Untergruppe sind dabei werbefinanzierte Medien wie insbesondere auch traditionelle Zeitungsverlage mit ihren Online-Ausgaben. In Bezug auf die ePrivacy-Verordnung stehen viele dieser Geschäftsmodelle vor dem Problem, dass es inzwischen Standard in der Online-Werbung ist, dass auf Daten von Nutzern, insbesondere durch Cookies und Tracking, zugegriffen wird, um die Wirksamkeit von Online-Werbung (durch Beobachtung der Reaktion der Werbeadressaten) direkt messen zu können ("online behavioral advertising"). Alle Regelungen, die folglich die Nutzung solcher Daten, insbesondere durch die Notwendigkeit einer Einwilligung, faktisch erschweren, bspw. auch durch explizite Opt-in-Lösungen und privacy-freundliche Voreinstellungen, würden es diesen Geschäftsmodellen sehr erschweren, Werbeaktivitäten anzubieten, die insbesondere mit denjenigen von Google und Facebook (als den bei der Online-Werbung führenden Anbietern) konkurrieren können. Diese großen Tech-Firmen haben solche Probleme in wesentlich geringerem Umfang, da sie die notwendigen Einwilligungen mit dem Einloggen ihrer Kunden – wie bei Facebook und Google – direkt erlangen können. Insofern ist es ein zentrales Argument der werbefinanzierten Medienunternehmen, dass hohe Anforderungen an die Einwilligung in Bezug auf Cookies und Tracking zu einem starken Wettbewerbsnachteil gegenüber den großen (und vornehmlich in den USA beheimateten) Tech-Firmen führt, so dass dadurch deren Marktmacht, insbesondere auf dem Werbemarkt, noch weiter gestärkt wird.[516] Die Medienunternehmen fordern deshalb, auch ohne Einwilligung Daten für die Reichweitenmessung (und "online behavioral advertising“) von Werbung verarbeiten zu dürfen, da dies notwendig ist für ihre Wettbewerbsfähigkeit auf dem Werbemarkt und damit für die finanzielle Basis ihrer Geschäftsmodelle. Sie würden dafür auch gerne die Rechtfertigung über die Abwägung mit "berechtigten Interessen" in Anspruch nehmen. Etablierte Zeitungsverlage verweisen dabei auf die Bedeutung der Aufrechterhaltung der wirtschaftlichen Basis für einen seriösen Qualitätsjournalismus.[517] Als besonders kritisch wird deshalb ein eventuel-

[514] Vgl. GSMA/etno (2017, 6).

[515] Vgl. die Positionspapiere und Stellungnahmen von FEDMA (2017), IAB (2017), Coalition for Audience Measurement (2017), News Media Europe (2017) und FAZ (2017).

[516] Folglich wird insbesondere von Medienunternehmen, die mit Werbung ihre journalistischen Angebote finanzieren, die Forderung nach der Herstellung gleicher Wettbewerbsbedingungen bzgl. des Angebots von Werbung gefordert (FAZ 2017).

[517] Vgl. dazu News Media Europe (2017) und FAZ (2017).

les Verbot von Tracking Walls gesehen, wie es das EP im Gegensatz zum Kommissionsvorschlag für die ePrivacy-Verordnung vorsieht. In jedem Fall würde aber jegliche Abschwächung der Voraussetzungen für Einwilligungen den werbetreibenden Medienunternehmen im Wettbewerb auf dem Werbemarkt sehr helfen.

Unabhängig von diesem spezifischen Problem für werbefinanzierte Angebote haben sich auch die Verbände von Unternehmen, die Direktmarketing betreiben (wie bspw. die "Federation for European Direct and Interactive Marketing (FEDMA)) sehr intensiv mit dem Kommissionsvorschlag auseinandergesetzt. Aus der Sicht des Direktmarketings geht es vor allem darum, mit einzelnen Kunden in einen direkten Kontakt bzw. Dialog treten zu können. Hierbei wird betont, dass der risikobasierte Ansatz der DS-GVO sowie die ebenfalls dort vorgesehene Möglichkeit der Pseudonymisierung statt Anonymisierung auch in der ePrivacy-Verordnung Anwendung finden sollte. Der Vorteil der Pseudonymisierung liegt darin, dass Werbetreibende dann immer noch bei ihrer gezielten Werbung Informationen über bestimmte Präferenzen verwenden können. Pseudonymisierung würde die Privacy-Risiken erheblich reduzieren, aber gleichzeitig wesentlich gezieltere Werbeaktivitäten erlauben.[518] Auch aus Sicht der Direktmarketingunternehmen sollte die Abwägung mit "berechtigten Interessen" in Art. 8 der ePrivacy-Verordnung möglich sein, insbesondere weil das primäre Abstellen auf die Einwilligung zu einer unangemessenen "one size fits all"-Lösung führt. Stattdessen sollten wesentlich flexiblere Lösungen, die sich an den tatsächlichen Privacy-Risiken orientieren, ermöglicht werden. Flexiblere Lösungen werden von Direktmarketingunternehmen auch in Bezug auf die Regeln bzgl. "unerbetener Kommunikation" (Art. 16 ePrivacy-VO-E) gefordert, wobei sie gerne mehr auf Opt-out-Lösungen setzen würden (wie bspw. Robinson-Listen, in die sich Verbraucher eintragen lassen können, um keine unerbetene Kommunikation zu erhalten).[519] Als ein besonders wichtiges Problem wird – auch von den werbefinanzierten Medienunternehmen – die Entscheidung der Kommission angesehen, den Webbrowsern eine Schlüsselstellung als "Gatekeeper" zuzuweisen.[520] Hier besteht die Gefahr darin, dass dritten Parteien über Voreinstellungen direkt der Zugang zu den Geräten und damit zu den Nutzern verwehrt wird und damit kein Dialog mehr möglich ist, um spezifische Einwilligungen von Nutzern einzuholen. Insbesondere würden damit die Informationen über die Nutzer in den Händen einer kleinen Anzahl von großen Browser-Unternehmen konzentriert werden, die den europäischen Markt dominieren. Vielmehr sollte nach anderen Lösungen für zentralisierte Privacy-Instrumente für Nutzer gesucht werden, die mehr Kommunikation und Interaktion erlauben und eine solche Konzentration von Daten von Nutzern bei wenigen Online-Unternehmen vermeiden.[521] [522]

[518] Vgl. FEDMA (2017, 2 f.).
[519] Vgl. FEDMA (2017, 9).
[520] Vgl. FEDMA (2017, 6 f.).
[521] Vgl. FEDMA (2017, 7).

4.3.4 INDUSTRIE UND HANDEL

Die Positionspapiere und Stellungnahmen von Verbänden der traditionellen Industrie (wie bspw. des BDI) sowie des stationären Einzelhandels (HDE) machen deutlich, dass die ePrivacy-Verordnung nur in relativ spezifischer Form für diese Sektoren relevant zu sein scheint.[523] Industrieverbände und Handelsverbände stellen generell die Sinnhaftigkeit einer eigenen ePrivacy-Verordnung in Frage und beklagen das Fehlen der Abwägung mit "berechtigten Interessen".[524] Obwohl die Ausweitung des Anwendungsbereichs auf neue Kommunikationsformen als Beitrag zum "levelling the playing field" positiv gesehen wird, ist der BDI sehr skeptisch bzgl. der Anwendung der ePrivacy-Verordnung auf Maschinen-zu-Maschinen-Kommunikation (M2M), weil dies auch eine Anwendung auf Industrie 4.0 und damit "Smart Manufacturing" beinhalten würde. ePrivacy-Regeln sollten nur in eng begründeten Grenzen für M2M-Kommunikation relevant sein.[525] Ansonsten betont der BDI nachdrücklich – wie auch viele andere Stellungnahmen – die Notwendigkeit, die vielen offenen Fragen zu klären, d.h. dass Gründlichkeit bei der Ausarbeitung der ePrivacy-Verordnung wichtiger sei als Schnelligkeit.[526] Für den traditionellen Handel ist die Möglichkeit von digitaler Werbung sowie Direktmarketing sehr wichtig, so dass aus dieser Sicht ähnliche Positionen vertreten werden wie von der werbetreibenden Wirtschaft, insbesondere in Bezug auf Cookies, Tracking sowie Direktwerbung einschließlich der Wichtigkeit der Beibehaltung der Ausnahme bzgl. Bestandskunden. Auch der Handel sieht das Problem einer möglichen Abhängigkeit von Webbrowser-Anbietern als Gatekeeper.[527] Ein besonders wichtiger spezifischer Punkt aus Sicht des Handels sind die Regelungen bzgl. der direkten Nutzung von Informationen aus den Endgeräten von Konsumenten (insbesondere Offline-Tracking mit WLAN). Hier werden möglichst geringe Anforderungen an die Einwilligung von Kunden gefordert, weil dadurch ganz neue Möglichkeiten der Digitalisierung in den Geschäften des Handels erleichtert würden.[528]

---

[522] Zu den unter Umständen negativen Auswirkungen der in dieser Form geplanten ePrivacy-Verordnung auf die Onlinewerbung und werbebasierte digitale Geschäftsmodelle vgl. auch die vom Bundeswirtschaftsministerium in Auftrag gegebene WIK-Studie (Hildebrandt/Arnold 2017).

[523] Vgl. hierzu BDI (2017a) und HDE (2017).

[524] Vgl. BDI (2017a, 5) und HDE (2017, 3).

[525] Vgl. BDI (2017a, 4 f.).

[526] Vgl. BDI (2017a, 6).

[527] Vgl. HDE (2017a, 3 f.).

[528] Vgl. HDE (2017a, 4 f.).

4.3.5 DIGITALWIRTSCHAFT

Die Verbände der Digitalwirtschaft haben sich in ihren Positionspapieren sehr ausführlich und detailliert geäußert.[529] Sie betonen am stärksten die generelle Gefahr, dass durch den Vorschlag der Kommission die Balance zwischen dem Schutz der Privatsphäre und neuen Technologien verloren geht: "The Commision's proposed privacy Regulation (e-PR) threatens to risk the balance between the protection of privacy and new technologies found during a long and arduous legislative process as it either completely prohibits many data processing operations, which are allowed under GDPR, or subjects them to a strict consent requirement. In addition, the proposal also covers cases where no personal data is involved and imposes strict rules for communication between companies and machines. This calls into question established practices in the European economy and narrows the scope for innovation in the area of Industry 4.0 and the Internet of Things. The competitiveness of the European economy is thus threatened in all sectors" (Bitkom 2017, 1). Diese grundsätzliche Position steht hinter vielen Stakeholder-Positionspapieren aus der Wirtschaft, auch wenn sie nicht immer in dieser Allgemeinheit formuliert wird. Das Positionspapier von Bitkom zeichnet sich auch dadurch aus, dass es stärker als andere auf die vielen konkreten technischen und rechtlichen Detailprobleme der konkreten Regeln des Kommissionsvorschlags eingeht und darauf, welche Leistungen dann hierdurch nicht mehr möglich wären.

In Bezug auf die grundsätzliche Ausrichtung der ePrivacy-Verordnung wird deshalb gefordert, dass nur das geregelt werden sollte, was nicht schon in der DS-GVO geregelt ist, so dass problematische Doppelregulierungen vermieden werden können, insbesondere weil oft schlecht abgegrenzt werden kann, welche Datenverarbeitungsprozesse unter die DS-GVO- oder ePrivacy-Regeln fallen würden. Die Unsicherheiten über Regelungen bzgl. M2M-Kommunikation würden neue Geschäftsmodelle im Bereich vom vernetzten Auto, Smart-Home-Lösungen etc. in Frage stellen, so dass M2M-Kommunikation nicht von den ePrivacy-Regeln erfasst werden sollten.[530] Bei der Verarbeitung von Kommunikationsmetadaten sollte die Abwägung mit "berechtigten Interessen" als zusätzliche Rechtfertigungslösung sowie Pseudonymisierungslösungen möglich sein, da Anonymisierung eine Fülle von wertvollen Diensten (wie geschäftliche Analysen, Verbesserung der Kundenservices und Big-Data-Anwendungen) nicht erlauben würde, da hierfür die "identifier" notwendig sind, die bei anonymisierten Daten verloren gehen.[531] Ebenso wichtig sei die Möglichkeit, Daten für Zwecke zu verwenden, die vereinbar mit dem ursprünglichen Datenzweck sind, wie dies auch die DS-GVO in Art. 6(4) DS-GVO erlaube. Die Verarbeitung von Kommunikationsmetadaten sollte in Art. 6 (2) ePrivacy-VO-E ohne Einwilligung auch zur Entdeckung von Spyware und Datenlecks sowie zur generellen Aufrechterhaltung des Netzwerks erlaubt sein.[532] In Bezug

[529] Vgl. die Positionspapiere von Bitkom (2017), BVDW (2017) sowie DigitalEurope (2016).
[530] Bitkom (2017, 3).
[531] Bitkom (2017, 7).
[532] Bitkom (2017, 8).

auf den Zugang zu Endgeräten von Endnutzern, Tracking und Cookies wird betont, dass wesentlich spezifischere und flexiblere Regelungen notwendig sind, weil es für die Nutzer sowohl nützliche als auch schädliche Cookies gibt und ein einheitlicher "One-size-fits-all"-Ansatz bei Einwilligungen nicht adäquat ist, so dass angesichts der ständigen Innovationen ein flexiblerer Ansatz notwendig ist.[533] Dies gilt gleichermaßen für Privacy-Voreinstellungen für Software sowie Browser, bei denen die Gefahr entsteht, dass privacy-freundliche Voreinstellungen Firmen faktisch vom Zugang zum Nutzer abschneiden. Als weiteres spezifisches Problem wird das Verbot der Nutzung von Drittanbietern für die Analyse von Daten angesehen, da dies insbesondere kleinere Unternehmen stark treffen würde. Wichtig ist auch, dass die Verbände der digitalen Wirtschaft in der ePrivacy-Verordnung stärker die Möglichkeit der Nutzung der Instrumente Selbstregulierung und Ko-Regulierung verankert sehen möchten, wie dies nach Art. 40-44 DS-GVO möglich ist.[534]

Allerdings sind nicht alle Firmen in der Digitalwirtschaft in gleicher Weise für eine Einschränkung des Datenschutzes. Sehr interessant ist in diesem Zusammenhang das Positionspapier von Mozilla (als Anbieter eines weit verbreiteten Webbrowsers).[535] Mozilla sieht sich selbst als ein Anbieter, der gerade den Internetnutzern helfen will, ihre Daten zu schützen, bspw. durch das Anbieten von Surfen im privaten Modus oder durch die Möglichkeit der Wahl von Webbrowsereinstellungen, die kein Tracking oder keine Cookies zulassen bzw. den Nutzern diesbezüglich sehr differenzierte Wahlmöglichkeiten einräumen. In Bezug auf den Vorschlag der ePrivacy-Verordnung hat Mozilla eine sehr differenzierte eigene Position entwickelt. Mozilla ist nicht der Meinung, dass die bisherigen Regeln die Privatsphäre von Nutzern wirksam geschützt haben, sodass es auch darum geht, Vertrauen wiederherzustellen "and to move together towards a more sustainable economic ecosytem where user control, transparency, and choice coexist with economic business models".[536] Mozilla unterstützt auf der einen Seite die Bemühungen der Kommission um den Schutz von Kommunikationsdaten, verweist jedoch auf der anderen Seite auf die Notwendigkeit, zu flexibleren Lösungen in Bezug auf bestimmte Zwecke der Datenverarbeitung zu kommen, die keine Privacy-Risiken bergen. Allerdings spricht sich Mozilla hierbei explizit gegen die Einführung einer Abwägung mit "berechtigten Interessen" aus, weil dies zu der Gefahr führt, dass Unternehmen dies benutzen könnten "as a loophole to collect and process sensitive data without users' knowledge or control".[537] In Bezug auf Tracking und Cookies unterstützt Mozilla die Datenschutzbemühungen der Kommission, warnt aber vor zu engen technisch definierten Regelungen, wie bspw. die Fokussierung auf "Third-Party Cookies", weil es auch viele andere Möglichkeiten des Trackings gibt (wie bspw. fingerprinting). Als besonders wichtig wird von Mozilla die

[533] Bitkom (2017, 11 f.).
[534] Bitkom (2017, 3).
[535] Vgl. Mozilla (2017). Es ist nicht klar, ob Mozilla wirklich der Digitalwirtschaft zugeordnet werden sollte, da es sich um eine Stiftung mit Non-profit-Charakter handelt.
[536] Mozilla (2017, 3).
[537] Mozilla (2017, 5).

Möglichkeit gesehen, den Nutzern explizit Wahlmöglichkeiten für Voreinstellungen zu geben. Dieser Ansatz sollte weiter ausgebaut werden.[538]

4.4 ZUSAMMENFASSENDE ANALYSE DER POSITIONEN UND ARGUMENTATIONEN IN DER DISKUSSION ÜBER DIE EPRIVACY-VERORDNUNG

Wie kann – auch unter Hinzunahme von ökonomischen Überlegungen – die Diskussion über die ePrivacy-Verordnung zusammenfassend charakterisiert werden und welche Interessen und zentrale Argumentationen spielen hierbei eine entscheidende Rolle? In einem ersten Schritt soll zunächst nochmals der sich in den Positionspapieren der verschiedenen Stakeholder zeigende Grundkonflikt verdeutlicht werden, bevor dann unter Zuhilfenahme von ökonomischen Überlegungen die spezifischen Konflikte und die jeweils verwendeten Argumentationen noch genauer analysiert, eingeordnet und bewertet werden.

4.4.1 DATENSCHUTZ VS. DATENÖKONOMIE: EIN KOMPLEXER KONFLIKT

Zunächst wird von den Verbraucher- und Datenschützern – gestützt durch Umfragen – das Argument in den Mittelpunkt gestellt, dass die Individuen ausgehend von Grundrechten ein Recht auf Schutz ihrer Privatsphäre haben, bzw. den Schutz "ihrer" Kommunikationsdaten als sehr wichtig ansehen. Dies geht argumentativ auf sehr alte rechtliche Grundprinzipien über den Schutz der Privatsphäre, wie die Unverletzlichkeit der privaten Wohnung, und des Post- und Fernmeldegeheimnisses zurück. Ausgehend von der Interpretation des Schutzes der Privatsphäre als informationelle Selbstbestimmung wird deshalb die Einwilligung der Individuen als zentraler Legitimationsgrund für die Verarbeitung von Kommunikationsdaten gesehen. Darüberhinaus wird direkt auf die Risiken abgestellt, die durch Offenlegung von sensiblen privaten Daten für die betroffenen Personen entstehen können. Als potentiell besonders problematisch kann dabei die Erstellung von umfassenden, psychologischen Nutzerprofilen gesehen werden, die für verschiedene Zwecke wie "behavioral targeting", Preisdiskriminierung und andere, möglicherweise problematische, Zwecke benutzt werden können.[539] Hieraus kann abgeleitet werden, weshalb zu irgendeinem (legitimen) Zweck erhobene Daten entweder möglichst schnell gelöscht oder sie möglichst sicher und zuverlässig anonymisiert werden sollten. Dabei gibt es eine Abstufung bzgl. der Risiken: Ein längeres Aufbewahren, evtl. auch bei einem (nur durch Verträge gebundenen) Drittanbieter, führt zu höheren Risiken, ebenso wie Pseudonymisierung einen geringeren Schutz im Vergleich zu Anonymisie-

[538] Vgl. Mozilla (2017, 9 f.).

[539] Vgl. zum Problem des consumer profiling und den daraus entstehenden Gefahren für Verbraucher aus verbraucher- und datenschutzrechtlicher Sicht Borgesius & Poort (2017), Petkova & Böhm (2017) sowie Hacker (2017), der auch auf einschlägige ökonomische Literatur zu sog. exploitative contracts verweist (Koszegi 2014).

rung bietet. Auch ist klar, dass jede Weitergabe von an sich harmlos erscheinenden Daten durch Kombination mit anderen Daten (Big Data) zu eventuell problematischen Informationen über Personen führen kann, sodass daraus die Empfehlung eines allgemeinen Vorsichtsprinzip abgeleitet werden kann, d.h. generell möglichst wenige Daten zur Verfügung zu stellen (Datensparsamkeit), gerade auch im Hinblick auf die Intransparenz und Ungewissheit bezüglich der zukünftigen Verwendung dieser Daten (speziell in Big-Data-Kontexten).[540] Aus dieser Position heraus wird verständlich, weshalb Verbraucher- und Datenschützer auch in der ePrivacy-Debatte gegenüber allen Regelungen skeptisch eingestellt sind, die anderen Akteuren ohne Zustimmung der Individuen die Verarbeitung von Daten erlauben, wie bspw. die diskutierten Vorschläge, dass auch "berechtigte Interessen" von wirtschaftlichen Akteuren als Legitimationsgrund (wie in der DS-GVO) anerkannt werden sollen oder dass Kommunikationsmetadaten ohne Einwilligung verarbeitet werden dürfen oder wenn sie nur pseudonymisiert statt anonymisiert werden. Hierzu gehört ebenfalls die Frage, ob wirtschaftliche Akteure auch ohne Einwilligung (oder mit einer schwachen Opt-out-Lösung wie im Kommissionsvorschlag) Zugang zu bestimmten Informationen (wie bspw. Standortdaten) in den Smartphones von Individuen bekommen können, um deren Bewegung in bestimmten Kontexten (wie bspw. Supermärkten) verfolgen zu können.[541] Die Gegenposition des weitaus größten Teils der Wirtschaft, insbesondere der digitalen Wirtschaft, der Werbeindustrie, werbefinanzierten Medien, aber auch traditionellen Unternehmen, die sich digitalisieren (Industrie 4.0), besteht darin, dass sie auf die vielfältigen Verwertungs- und Nutzungsmöglichkeiten der von den Regelungen der ePrivacy-Verordnung betroffenen Daten verweisen, die die Entwicklung von neuen Produkten und Dienstleistungen ermöglichen, insbesondere auch im Hinblick auf stärker personalisierte Angebote an Konsumenten. Gleichzeitig können hierdurch neue Geschäftsmodelle entstehen sowie Produktions- und Distributionsprozesse optimiert werden. Auch die Entwicklung und Ausbreitung von IoT-Anwendungen kann von den Regeln der ePrivacy-Verordnung mitbeeinflusst werden. Zum Teil ist der Zugang zu diesen Daten aber für Unternehmen wichtig, um ihre bestehenden Geschäftsmodelle aufrechtzuerhalten, insbesondere, wenn sie durch Werbung finanziert sind. Unternehmen sind an solchen Daten jedoch nicht nur zur unmittelbaren eigenen Verwendung interessiert, sondern auch, um daraus, bspw. durch Datenanalyse, weitere kommerziell verwertbare Erkenntnisse zu gewinnen. Insofern können die hierbei gewonnenen Daten (in pseudonymisierter oder anonymisierter Form) in die allgemeine Datenökonomie einfließen und von Unternehmen in ganz anderen Sektoren verwendet werden. Aufgrund des sich daraus ableitenden Wertes dieser Daten ist leicht verständlich, weshalb Unternehmen, die technisch Zugang zu diesen Daten gewinnen können (wie bspw. Telekommunikationsanbieter und andere Anbieter von Kommunikationsdiensten, Webseitenbetreiber mit Cookies- und Tracking-Technologien oder Supermärkte über ihre WLAN-Netze), daran interessiert sind, möglichst viele Daten zu möglichst geringen Kosten zu sammeln. Insbesondere in den allgemeiner gehaltenen Positi-

[540] Vgl. Solove (2013, 1889 f.), der auf das Aggregationsproblem hinweist, d.h. dass durch die Kombination von verschiedenen jeweils für sich unproblematischen Daten sehr sensitive Informationen aus der Privatsphäre offenbar werden können. Dies ist jedoch bei den jeweils einzelnen Einwilligungen aber nichtantizipierbar.

[541] Siehe weiter unten die Analyse zu Opt-in- und Opt-out-Lösungen.

onspapieren der Verbände der digitalen Wirtschaft wird deutlich, dass zu restriktive Regelungen in der ePrivacy-Verordnung deshalb den Prozess des Übergangs zu einer digitalen Wirtschaft mit ihrem großen innovativen Potential an sich gefährden können, da dadurch evtl. viele potentiell verwertbare Daten der Datenökonomie nicht zur Verfügung stehen. In diesem Zusammenhang wird auch auf die internationale Wettbewerbsfähigkeit der europäischen Wirtschaft verwiesen,[542] die im Vergleich zu den USA oder asiatischen Ländern zurückzufallen droht – mit möglicherweise erheblichen Konsequenzen für Arbeitsplätze und Wohlstand in Europa. Sowohl aus dieser allgemeinen als auch der spezifischen Perspektive einzelner Sektoren und Unternehmen wird deutlich, weshalb in Bezug auf die ePrivacy-Diskussion die Wirtschaft daran interessiert ist, möglichst viele Daten über gesetzliche Ausnahmen direkt ohne Einwilligung sammeln zu dürfen (bspw. durch Einführung der Abwägung mit "berechtigten Interessen") oder mit Opt-out-Lösungen bzgl. Einwilligungen zu arbeiten sowie die gesammelten Daten für möglichst viele Zwecke und möglichst in pseudonymisierter statt anonymisierter Form weiterverwerten zu können. Interessant ist, dass der überwiegende Teil der Wirtschaft deshalb die allgemeinen Regeln der DS-GVO gegenüber den aus ihrer Sicht restriktiveren Vorschlägen der ePrivacy-Verordnung bevorzugt. Obwohl bisher weitgehend unklar ist, wie die gesetzliche Ausnahme der Abwägung mit den "berechtigten Interessen" der datenverarbeitenden Unternehmen auszulegen ist, geht die Wirtschaft davon aus, dass ihnen dies mehr Spielraum für den Zugang und die Verwendung von diesen Daten erlauben würde. Gleichzeitig macht dies auch verständlich, dass sie den Anwendungsbereich der ePrivacy-Verordnung deshalb möglichst eng definieren möchte, bspw. in Bezug auf M2M-Kommunikation.

Diese beiden Grundpositionen zeigen sich dann auch in den politischen Konflikten, bspw. im Europäischen Parlament bzw. im laufenden Trilog-Verfahren. Dieser Grundkonflikt wird zunehmend auch mit Hilfe der Argumentationsfigur der Suche nach einer angemessenen Balance zwischen dem Grundwert Schutz der Privatsphäre und vertraulichen Kommunikation und den Vorteilen von datengetriebenen Innovationen für Wirtschaft und Gesellschaft diskutiert. Aus einer ökonomischen Perspektive könnte dies auch als ein Trade-off-Problem zwischen einem Grundwert ("fundamental value") und ökonomischer Effizienz und Wohlstand gesehen werden. Eine solche Abwägung von Werten ist aus wirtschaftspolitischer Sicht im Prinzip letztlich nur durch eine politische Entscheidung möglich, d.h. dass letztlich die Bürgerinnen und Bürger in der EU darüber demokratisch entscheiden müssen, in welcher Gesellschaft mit welchem Schutz an Privatsphäre und welchem Umfang des Zugangs zu privaten Daten sie leben möchten. Allerdings ist zu bedenken, dass eine genauere Analyse, gerade aus ökonomischer Sicht, ergeben würde, dass dieser Konflikt wesentlich komplexer und letztlich damit aber auch weniger zugespitzt ist, als er hier auf den ersten Blick erscheint.

[542] Vgl. hierzu bspw. Bitkom (2017, 1).

So hat die ökonomische Diskussion über den Schutz der Privatsphäre ("economics of privacy") gezeigt, dass Datenschutzregelungen auch ökonomisch positive Wirkungen, gerade im Hinblick auf eine Datenökonomie, haben können, d.h. der rechtliche Schutz personenbezogener Daten und der Schutz gegen missbräuchliche (die Datensubjekte selbst schädigende) Verwendungen solcher Daten auch ökonomisch positive Wirkungen haben kann. Insbesondere kann hierdurch auch das Vertrauen von Konsumenten in die Datenökonomie, mit der Folge einer größeren Akzeptanz digitaler Angebote, gestärkt werden. Insofern hat es auch immer Bestrebungen seitens der Wirtschaft gegeben, selbst für einen ausreichenden Schutz der Daten ihrer Kunden zu sorgen. Die in der ePrivacy-Diskussion immer wieder angeführten Forderungen, die Probleme durch Selbstregulierungen oder Ko-Regulierung zu lösen, passen in dieses Argumentationsmuster, auch wenn – auch aus ökonomischer Sicht – sehr unklar und auch zweifelhaft ist, dass dies ausreichen würde.[543] Aber auch aus der Perspektive der individuellen Personen, für deren Schutz der Privatsphäre sich Daten- und Verbraucherschützer einsetzen, ist der Konflikt wesentlich komplexer, weil viele dieser Unternehmen die dabei gewonnenen Daten für die Entwicklung neuer Produkte und Dienstleistungen verwenden, an denen wiederum auch die Individuen als Konsumenten ein Interesse haben können. Insofern sind die Interessen der Individuen mit der Betonung des Schutzes ihrer Privatsphäre nur teilweise umschrieben, denn sie sind auch an vielerlei Produkten und Dienstleistungen sowie privaten und beruflichen Aktivitäten interessiert, für die sie in unterschiedlichem Umfang auch in ihrem eigenen Interesse bereit sind, Informationen aus ihrer Privatsphäre zur Verfügung zu stellen (und unter Umständen auch ohne explizite spezifische Einwilligung). Allerdings lassen sich diesbezüglich verschiedene Fälle unterscheiden, die im Folgenden kurz ökonomisch charakterisiert und auf die konkreten spezifischen Konflikte in der aktuellen ePrivacy-Diskussion bezogen werden sollen.

Ein relativ einfacher Fall liegt vor, wenn Daten, die notwendig für die Erbringung einer von den Konsumenten gewünschten Dienstleistung sind, bspw. eines Kommunikationsdienstleisters, ohne zusätzliche Einwilligung verarbeitet werden können. Gleiches gilt für Daten, die für die Abrechnung der Dienstleistungen, Aufdeckens von Betrug oder Sicherheitsproblemen erforderlich sind. Hier geht es um die erforderlichen Daten für die direkte Gegenleistung des Nutzers (Erfordernisprinzip). Schwieriger ist es bereits, wenn es um Daten geht, die nicht für die direkte Gegenleistung erforderlich sind, aber generell die Qualität, Verlässlichkeit oder Sicherheit der Erbringung dieser Leistung des Dienstleisters erhöhen können. Hier muss es nicht mehr im Interesse des einzelnen Nutzers liegen, solche Daten zur Verfügung zu stellen und dabei die mit jeder Datenweitergabe evtl. verbundenen Risiken einzugehen. Dies sind die Fragen, um die es konkret in der Diskussion um Art. 6 (1) und (2) lit. a und b ePrivacy-VO-E in Bezug auf Kommunikationsdaten geht. Ein völlig anderer Fall liegt dagegen vor, wenn die Kommunikationsdienstleister wesentlich mehr oder andere Daten als direkt erforderlich für ihre Leistung sammeln. In diesen Fällen ist die Zurverfügungstellung von solchen Daten ökonomisch selbst eine eigenständige Gegenleistung, d.h. es handelt sich um die

[543] Zur Diskussion um Selbstregulierung vs. Regulierung vgl. die Diskussion in Acquisti et al (2016, 479 f. und 484).

bekannten und inzwischen viel diskutierten Fälle, in denen eine Leistung teilweise oder vollständig mit Daten bezahlt wird ("Daten als Gegenleistung"). Aus dieser Perspektive wird auch aus ökonomischer Sicht verständlich, weshalb hier eine explizite Einwilligung sowie eventuelle weitere Absicherungen, wie eine Prüfung der Privacy-Risiken durch eine Datenschutzbehörde, zweckmäßig sein könnten, um die Interessen der Nutzer zu schützen (Art. 6 (2) lit. c, Art. 6 (3) ePrivacy-VO-E). Die gleichen Überlegungen können auch in Bezug auf die Frage angestellt werden, ob und in welchem Umfang Informationen aus den Endgeräten der Verbraucher (einschließlich Cookies und Tracking) genutzt werden können. Art. 8 (1) lit a und c ePrivacy-VO-E) orientieren sich dabei wieder an der Erforderlichkeit für die gewünschte Leistung, während es bezüglich darüber hinausgehender Daten wiederum um eine Gegenleistung geht, für die nach dem Kommissionsvorschlag eine explizite Einwilligung notwendig ist (Art. 8 (1) lit. b ePrivacy-VO-E).

4.4.2 ZUR PROBLEMATIK UND ÖKONOMIK VON EINWILLIGUNGEN UND OPT-IN- UND OPT-OUT-LÖSUNGEN

Wie wir gesehen haben, unterstützen Daten- und Verbraucherschützer sehr das Einwilligungsprinzip im Kommissionsvorschlag, das sich wieder legitimationsmäßig direkt aus dem Prinzip der informationellen Selbstbestimmung ableitet. Allerdings ist die Wirksamkeit und damit die Zweckmäßigkeit dieses Instruments der Einwilligung seit langem stark umstritten, wobei es gleichzeitig von sehr unterschiedlichen Seiten kritisiert und angegriffen wird. Ein Hauptkritikpunkt bezieht sich auf das bereits angesprochene Problem, dass unklar ist, ob und inwiefern Nutzer rationale und wohlinformierte Entscheidungen über die Zurverfügungstellung ihrer Daten treffen können. "Informiert" bezieht sich dabei darauf, ob sie genügend Informationen über die Daten, die sie weitergeben, und welche evtl. problematischen Folgen diese Datenweitergabe für sie kurz- und längerfristig mit sich bringen kann, haben. "Rational" bezieht sich darauf, ob Nutzer – unabhängig von ihrem Informationsstand – tatsächlich rational entscheiden oder ob sie bestimmten Verhaltensanomalien unterliegen, wie sie bspw. in der Verhaltensökonomie ausführlich analysiert werden, und infolgedessen systematische Fehler machen und sich dabei selbst schädigen. Über beide Probleme gibt es inzwischen eine umfangreiche Literatur, die insgesamt in Frage stellt, ob es sich bei den im Rahmen der ePrivacy-Verordnung auftretenden Einwilligungen um das Ergebnis wohlinformierter rationaler Entscheidungen handelt.[544] Sobald man dies grundsätzlich in Frage stellt, wird auch die Argumentationsfigur "Daten als Gegenleistung" in einem bilateralen Vertrag zwischen Nutzer und Anbieter einer ansonsten "kostenlosen" Leistung problematisch.[545] Interessanterweise wird diese Problematik von Einwilligungen von keinem der Stakeholder wirklich explizit diskutiert. Zwar werden Informationsprobleme von den Daten- und Verbraucherschützern an-

[544] Vgl. die Literaturangaben in Fn. 479.

[545] Vgl. hierzu bspw. Schweitzer (2017, 277 ff.), die deshalb skeptisch ist, ob der Wettbewerb dann noch einen angemessenen "Datenpreis" für die kostenlose Leistung sicherstellen kann.

gesprochen (mit der daraus folgenden Forderung nach Transparenz und zusätzlichen restriktiven Bedingungen für solche Einwilligungslösungen), allerdings beharren gerade sie stark auf dem Kriterium der Einwilligung der Individuen als zentrales Legitimationskriterium für die Zulässigkeit der Verarbeitung von personenbezogenen Daten bzw. Kommunikationsdaten. Ob das Einwilligungsprinzip tatsächlich fähig ist, die Privatsphäre von Individuen und die Vertraulichkeit der Kommunikation wirksam zu schützen, ist jedoch auch aus anderen Gründen zweifelhaft. Besonders wichtig – und dies ist die zweite Hauptkritik, die besonders von Vertretern der Wirtschaft betont wird – ist dabei das Problem der Vielzahl von Einwilligungen, die konkret von den Nutzern gegeben werden müssen und die mit dem Inkrafttreten der DS-GVO und der geplanten ePrivacy-Verordnung noch weiter ansteigen werden. Hierauf kommen wir weiter unten nochmals ausführlich zurück.

Geht man jedoch davon aus, dass die Einwilligungen tatsächlich überwiegend wohlinformiert und rational gegeben werden, dann kann die Nutzung von Daten (jenseits der Erforderlichkeit) tatsächlich als Ausdruck eines normalen ökonomischen Tausches zwischen dem Nutzer und dem Anbieter einer Leistung interpretiert werden, sodass ökonomisch gesehen faktisch ein Datenhandel im Sinne der Einräumung eines faktischen Nutzungsrechts dieser personenbezogenen Daten für spezifische Zwecke vorliegt.[546] In der Diskussion um die Positionspapiere der Werbeindustrie bzw. der werbefinanzierten Medien haben wir gesehen, dass viele Dienste wie bspw. Online-Zeitungen oder andere Webseiten sich ganz oder teilweise aus Werbung finanzieren und es sich hierfür auf dem Online-Werbemarkt herausgebildet hat, dass mit Cookies und anderen Tracking-Technologien die Wirksamkeit von Werbung kontrolliert und gemessen werden kann. Während für eine reine Messung des Webpublikums im Kommissionsvorschlag keine Einwilligung erforderlich ist,[547] sondern dies unter gewissen Bedingungen erlaubt ist, ist für ein weitergehendes Tracking des Surfverhaltens der Nutzer eine Einwilligung erforderlich. Von besonderer ökonomischer Bedeutung ist dabei der von Daten- und Verbraucherschützern stark geforderte und dann auch vom EP aufgenommene Vorschlag eines Verbots von Tracking Walls, den es im Kommissionsvorschlag nicht gibt. Ein generelles Verbot von Tracking Walls, d.h. dass Nutzern der unbeschränkte Zugang zu einer Webseite nicht deshalb verwehrt werden darf, weil sie keine Einwilligung für die Nutzung ihrer Daten geben, ist aus ökonomischer Sicht ein sehr weitreichender Schritt mit unter Umständen erheblichen Konsequenzen für das Nutzern zur Verfügung stehende Webangebot. Wie in verschiedenen Stakeholder-Positionspapieren ausführlich erläutert, kann dies dazu führen, dass bestimmte Webseitenangebote mangels Finanzierung durch Werbung gar nicht mehr angeboten werden können oder hinter expliziten Bezahlschranken (mit Login-Lösungen) verschwinden. Allerdings stellt ein solches Verbot von Tracking Walls die an sich inzwischen mit dem Prinzip "Daten als Gegenleistung" breit akzeptierte Logik des Tausches einer Leistung gegen Daten nicht wirklich in Frage, da weiterhin Lo-

[546] Die Tatsache, dass nach dem Datenschutzrecht die Einwilligung jederzeit wieder zurückgenommen werden kann, ändert aus ökonomischer Sicht nichts an dem Tauschcharakter.

[547] Auch diesbezüglich gibt es unterschiedliche Auffassungen zwischen den Stakeholdern, wobei insbesondere die Frage umstritten ist, ob hierbei auch Dritte als Dienstleister eingeschaltet werden dürfen.

gin-Lösungen mit expliziter Einwilligung möglich sind, aber es macht solche Tauschgeschäfte wesentlich schwieriger. Aus ökonomischer Perspektive gibt es ernsthafte Zweifel, ob ein generelles Verbot von Tracking Walls tatsächlich im Interesse der Verbraucher ist, wobei dies nicht ausschließt, dass rechtliche Beschränkungen für Tracking Walls sinnvoll sein könnten.

Oben wurde bereits kurz das andere große Problem der Einwilligungslösung angesprochen, nämlich dass diese sehr oft gegeben werden muss. Insbesondere die Vertreter der digitalen Wirtschaft und anderer Sektoren, die an der Sammlung und Verwertung von Daten interessiert sind, betonen deshalb das Problem der "consent fatigue", d.h. der Einwilligungsmüdigkeit bei den Nutzern von Kommunikationsdienstleistungen. Sie ist deshalb für sie ein Hauptargument für ihre Forderungen nach Rechtfertigungen ohne Einwilligung bzw. zumindest nach Lösungen, die eine Verarbeitung von Daten erlauben, ohne eine explizite Zustimmung vorauszusetzen. Dies betrifft in der ePrivacy-Diskussion insbesondere Kommunikationsmetadaten, Offline-Tracking von Endgeräten, die Verwendung von Cookies und Tracking des Besuchs von Webseiten, wie es vor allem für "online behavioral advertising" erforderlich ist. Ökonomisch können solche Einwilligungen als (Transaktions-)Kosten interpretiert werden, die in unterschiedlichem Umfang sowohl bei den Serviceanbietern als auch den Nutzern auftreten können. Solche Kosten stellen auch dann ein Problem dar, wenn die Nutzer rational mit Einwilligungen umgehen. Um diese Kosten zu reduzieren, sind nun verschiedene Lösungen denkbar. Naheliegende Lösungen sind entweder die generelle Erlaubnis oder das generelle Verbot, bestimmte Daten zu verarbeiten. Allerdings können dadurch entweder nichtakzeptable Privacy-Risiken entstehen oder alternativ bestimmte Daten überhaupt nicht genutzt werden und es können individuell unterschiedliche Präferenzen über den Schutz der Privatsphäre oder die Bereitschaft Daten für einen "kostenlosen Dienst" zu tauschen, nicht mehr berücksichtigt werden.[548]

Aus der ökonomischen Analyse des Rechts ist bekannt, dass durch Einführung von geeigneten Default-Regeln solche Transaktionskosten wie Einwilligungskosten reduziert werden können. Dies bedeutet, dass entweder der Datenzugriff möglich ist, solange der Nutzer nicht widerspricht (Opt-out-Lösung), oder umgekehrt der Datenzugriff nicht erlaubt ist, wenn nicht eine explizite Einwilligung eingeholt wird (Opt-in-Lösung). Aus ökonomischer Sicht lassen sich die Kosten am stärksten vermindern, wenn die Default-Lösung gewählt wird, die von den meisten Nutzern gewählt würde, wenn sie explizit entscheiden würden. Allerdings kann in dem Zielkonflikt zwischen Schutz der Privatsphäre und ökonomischer Effizienz auch

[548] Ökonomisch würde dies bedeuten, dass die Kosten in Form von Privacy-Risiken bzw. Nichtverwendung von bestimmten Daten größer sind als die Transaktionskosten der notwendigen Einwilligungen.

bewusst eine Opt-in-Lösung gewählt werden.[549] Solche Opt-in Lösungen stellen die in der DS-GVO vorgesehenen privacy-freundlichen Lösungen dar (privacy by design),[550] die – wie von Daten- und Verbraucherschützern beklagt – nicht systematisch im Kommissionsvorschlag verankert wurden. Entscheidend ist, dass bei solchen Default-Lösungen nur Kosten für Einwilligung bzw. Widerspruch auftreten, wenn Individuen von der Default-Lösung abweichen wollen. Im Prinzip sind sich die Stakeholder in der ePrivacy-Diskussion über die große Bedeutung der Frage, ob der Gesetzgeber eine Opt-in oder eine Opt-out Lösung wählt, einig. Tatsächlich kann vermutet werden, dass bei einer Opt-in-Lösung für die Nutzung von Kommunikationsmetadaten im Vergleich zu einer Opt-out-Lösung wesentlich weniger Kommunikationsmetadaten verarbeitet werden können. Während für die Datenschützer dies gerade ein zentrales Argument für das Verlangen von expliziten Einwilligungen ist, ist es für die digitale Wirtschaft ein entscheidendes Argument für eine Opt-out-Lösung, da hierdurch wesentlich mehr Daten verarbeitet und genutzt werden können, mit den vermuteten positiven Wirkungen auf Innovationen und Wohlfahrt. Allerdings ist es in jedem Fall ein großer Vorteil von Default-Regeln, dass explizite spezifische Einwilligungen bzw. Widersprüche weiterhin möglich sind, und deshalb auch die Freiheit der Individuen, anders zu entscheiden, weiter besteht.

Wie wirkt sich die Entscheidung für eine Opt-in oder Opt-out-Regel aus ökonomischer Sicht auf die beteiligten Stakeholder direkt aus? Wenn eine Opt-in-Lösung vorliegt, müssen sich die Unternehmen aktiv bemühen und Kosten aufwenden, um von den Nutzern solche Einwilligungen zu erlangen. Bei einer Opt-out-Lösung sind es umgekehrt die Nutzer, die zur Verteidigung ihrer Privatsphäre aktiv werden und der Nutzung widersprechen müssen und hierfür auch die Kosten tragen müssen. Bezüglich der Profitabilität von Geschäftsmodellen, die auf der Verarbeitung von solchen Daten basieren, bedeutet dies, dass bei einer Opt-out-Lösung geringere Kosten für die Ressource Daten entstehen als bei einer Opt-in-Lösung. Dies bedeutet entweder, dass bestimmte Geschäftsmodelle bei einer Opt-in-Lösung nicht mehr rentabel sein werden (im Vergleich zu einer Opt-out-Lösung) oder dass zumindest die Produkte und Dienstleistungen, die auf Daten basieren, die im Rahmen einer Opt-in-Lösung gewonnen werden, kostenaufwendiger sind und damit zu einem höheren Preis verkauft werden als Produkte, die auf Daten basieren, die auf einer Opt-out-Basis gewonnen und verarbeitet werden können. Die Frage von Opt-in oder Opt-out und damit ob privacy-freundliche Default-Regeln implementiert werden, wirkt sich damit darauf aus, (1) wer Kos-

[549] Vgl. zur Ökonomie von Default-Lösungen sowie Opt-in- und Opt-out-Lösungen Ayres & Gertner (1989) und Cooter & Ulen (2011, 210-217). Die Lösung, dass diejenige Default-Regel zu empfehlen ist, die die Mehrheit bei expliziter Entscheidung wählen würde, wird als "majoritarian default rule" bezeichnet. Vgl. aber insbesondere auch Sunstein & Thaler (2003), die unter Verwendung von verhaltensökonomischen Erkenntnissen Default-Regeln dazu verwenden wollen, um Individuen zu einem für sie vorteilhaften Verhalten zu veranlassen (Nudging, "libertarian paternalism"). Wie aus empirischen Untersuchungen sehr gut bekannt ist, beeinflusst die Wahl der Default-Regel stark die Entscheidungen von Individuen, d.h. Default-Lösungen sind "sticky". In einem solchen Sinne kann auch die Entscheidung für "privacy-by-default" interpretiert werden; vgl. hierzu bspw. Borgesius (2015, 200f.).

[550] Vgl. generell zur Bedeutung von "privacy-by-design" Krebs (2013).

ten aufwenden muss, um entweder Daten nutzen zu dürfen oder umgekehrt seine Privatsphäre zu schützen, (2) ob und inwieweit bestimmte datenbasierte Geschäftsmodelle ökonomisch rentabel sind, und (3) wie viele Daten insgesamt der weiteren ökonomischen Verwertung zugänglich gemacht werden bzw. umgekehrt wie stark die Privatsphäre von Individuen geschützt wird. Insofern verschiebt der Übergang von einer Opt-in zu einer Opt-out-Regel (oder umgekehrt) auch die faktische Grenzziehung zwischen der Privatsphäre von Personen und der datenverarbeitenden Wirtschaft und damit der Datenökonomie.

In Bezug auf den konkreten ePrivacy-Verordnungvorschlag der Kommission sind diesbezüglich vor allem folgende Regelungsvorschläge hochumstritten: Erstens gilt dies für die schwache Opt-out-Lösung für das Offline-Tracking in Art. 8 (2) lit. b ePrivacy-VO-E. Das Offline-Tracking ist danach erlaubt, soweit in hervorgehobener Weise ein deutlicher Hinweis über die Modalitäten der Datenerhebung "sowie darüber, was der Endnutzer der Endeinrichtung tun kann, um die Erhebung zu beenden oder auf ein Minimum zu beschränken" gegeben wird. Insbesondere die letzte Alternative verdeutlicht, dass es sich hier nicht um eine wirkliche Opt-out-Lösung handelt. Diese Lösung ist von Daten- und Verbraucherschützern stark kritisiert worden und das EP hat in seiner Variante diese Opt-out-Lösung stark beschränkt und insbesondere ein explizites Widerspruchsrecht vorgesehen, ohne aber zu einer Opt-in-Lösung überzugehen.[551] Aus ökonomischer Sicht ist aber klar, dass eine Opt-out-Lösung die Nutzung von Offline-Tracking wesentlich erleichtert und umgekehrt den Individuen die Kosten für die Verhinderung des Offline-Trackings ihrer Endgeräte auferlegt. Zweitens wurde das Fehlen von privacy-freundlichen Voreinstellungen in Webbrowsern und Software in Art. 10 ePrivacy-VO-E des Kommissionsvorschlags beklagt, während nach der Fassung des EP solche privacy-schützenden Voreinstellungen aktiviert sein sollten, d.h. dass die Nutzer aktiv in andere Voreinstellungen optieren müssen. Nur in dem Vorschlag des EP wäre damit eine klare Opt-in-Lösung realisiert, wobei das EP auch Wert darauf legt, dass immer auch spezifische Einwilligungen möglich bleiben. Interessant an der Lösung der Kommission ist, dass die Software die Nutzer bei der Installation zu einer Entscheidung über eine Voreinstellung zwingen muss (Art. 10 (2) ePrivacy-VO-E).[552] Unabhängig davon, ob privacy-freundliche Voreinstellungen aktiviert werden, hat die Kommission in Art. 10 aber auch Webbrowsern durch die Verpflichtung der Möglichkeit der Wahl zwischen verschiedenen Voreinstellungen in Bezug auf die Akzeptanz von Cookies oder einer Do-not-track-Option auch eine Schlüsselrolle als Gatekeeper zugewiesen, da bei der Wahl bestimmter Voreinstellungen Einwilligungen automatisch abgelehnt oder angenommen werden können. Eine solche Gatekeeper-Funktion reduziert die Anzahl der Einwilligungen und gibt den Nutzern die Möglichkeit, ihre Präferenzen im Rahmen der angebotenen Voreinstellungsoptionen auszudrücken. Es wäre genauer zu untersuchen, ob und inwiefern eine kleine Anzahl von Webbrowseranbietern tatsächlich eine unter Umständen erhebliche Macht bezüglich des Zugangs zu Nutzern und

[551] Vgl. EP (2017, 59 ff.).

[552] Im Rahmen der Nudging-Literatur ist das Erzwingen einer aktiven Entscheidung ein weiteres Nudging-Instrument zusätzlich zu Default-Regeln. Vgl. Sunstein/Thaler (2003, 1194 f.).

ihren Daten zukommt, wie dies von der digitalen Wirtschaft befürchtet wird.[553] Eine andere Möglichkeit, die in jüngster Zeit verstärkt diskutiert wird, besteht darin, dass große unternehmensübergreifende Login-Lösungen entwickelt werden, durch die Nutzer sich direkt einloggen können und damit Zugang zu den Diensten vieler Unternehmen gewinnen. Dies könnte die Anzahl von unterschiedlichen Logins mit verschiedenen, schwer durchschaubaren AGB bzgl. Daten stark reduzieren und damit die Kosten der Einwilligung sowohl auf Nutzer- als auch Unternehmensseite erheblich vermindern.[554]

4.4.3 FAZIT

In diesem Abschnitt wurden die aktuellen Regulierungsvorschläge bezüglich einer neuen e-Privacy-Verordnung und die dabei von verschiedenen Stakeholder-Gruppen vorgebrachten Argumentationen analysiert. Hierbei zeigt sich in den konkret umstrittenen Regelungen, dass diese Diskussion dominiert wird von dem Grundkonflikt zwischen dem Schutz der Privatsphäre einerseits und den Interessen von unterschiedlichen Stakeholdern aus der Wirtschaft, die einen möglichst umfangreichen und kostengünstigen Zugang zu den Kommunikationsdaten von Nutzern sowie Informationen aus deren Endgeräten bekommen möchten. In den konkreten Auseinandersetzungen um einzelne Regelungen geht es dabei um die spezifischen Grenzziehungen zwischen der Klasse von Daten, die nur durch explizite Einwilligungen (Opt-in) verarbeitet werden dürfen, einer Klasse, bei denen auch Opt-out-Lösungen möglich sind, und einer weiteren Klasse von Daten, die direkt ohne Einwilligung und Widerspruchsmöglichkeit genutzt werden können. Letztere würde von weiten Teilen der Wirtschaft gerne durch die Einführung der aus der DS-GVO bekannten Abwägung mit "berechtigten Interessen" stark erweitert werden, was bisher aber nicht vorgesehen ist. Eine weitere wichtige Grenzziehung besteht darin, ob nur die für bestimmte Dienste erforderlichen Daten genutzt werden dürfen oder darüber hinaus Daten gesammelt werden können (Daten als Gegenleistung), bzw. ob personenbezogene Daten für die weitere Verwertung anonymisiert werden müssen oder ob aus Sicht des Datenschutzes auch eine Pseudonymisierung als ausreichend angesehen wird. Die politische Auseinandersetzung um die ePrivacy-Verordnung und die Suche nach Kompromisslösungen beziehen sich folglich auf Entscheidungen, welche Daten unter welchen Bedingungen in welche dieser Klassen zugeordnet werden, auch mit den oben andiskutierten Folgen für den Umfang des Schutzes der Privatsphäre, der Menge der von der Datenökonomie verwertbaren Daten (mit den sich daraus ergebenden Chancen auf zusätzliche Innovationen und Wohlstand einerseits und Privacy-Risiken für die betroffe-

[553] Vgl. FEDMA (2017, 7).

[554] Vgl. hierzu insbesondere Oetjen (2017, 30f.) sowie Spehr (2018) und FAZ (2018). Konkret geht es dabei um Identitätsmanagement mit der Idee eines Universalschlüssels für möglichst viele Dienste im Internet.
Aus einer anderen Perspektive, die stärker von den Interessen der Nutzer ausgeht, könnten auch die sog. Personal Information Management Systeme eine interessante Lösung darstellen, die als Intermediäre den Nutzern helfen, ihre personenbezogenen Daten zu managen und diese unter Umständen auch gegen Entgelt zur Verfügung zu stellen. Vgl. bspw. European Data Protection Supervisor (2016).

nen Individuen andererseits) sowie der Rentabilität von spezifischen digitalen Geschäftsmodellen. Mit allen diesen Entscheidungen wird auch beeinflusst, wer die faktische Verfügungsmacht über solche Daten besitzt.

5. ÖFFENTLICHER DISKURS II: RECHTE AN NICHT-PERSONENBEZOGENEN DATEN: EIGENTUMS- UND ZUGANGSRECHTE

5.1. EINLEITUNG

Die Diskussion über Dateneigentum bzw. "data ownership" hat sich in Europa vor allem als Diskussion über Rechte an nicht-personenbezogenen Daten manifestiert. Im Mittelpunkt stehen hierbei zunächst vor allem die Fülle von maschinengenerierten Rohdaten (Sensordaten), die im Rahmen von Industrie 4.0-Anwendungen ("Smart Manufacturing", "Smart Agriculture"), vernetzten Fahrzeugen oder in anderen IoT-Anwendungen generiert werden. Angesichts des potentiell hohen Wertes dieser Daten wurde die Frage nach dem rechtlichen Schutz dieser Daten mit der expliziten Thematisierung eines eigentumsrechtlichen Schutzes gestellt. Diese Diskussion ist insbesondere über den damaligen Digitalkommissar Oettinger schnell auf die europäische Ebene gelangt; dort aber ist die Anfang 2017 erschienene Mitteilung "Building a European data economy" direkt mit der viel allgemeineren Frage verknüpft worden, inwieweit es Probleme bzgl. der Entstehung einer funktionsfähigen Datenökonomie in Europa gibt, insbesondere in Bezug auf eine möglichst weitgehende Nutzung der großen vorhandenen Datenbestände.[555] Faktisch ist damit auch das Thema Datenhandel in den Blick gerückt. Als besondere Probleme werden dabei der ungenügende Zugang zu Daten, Data Sharing und Weiterverwendung („reuse“) von Daten gesehen, an die sich eine Diskussion anschließt, wie diese Probleme gelöst werden können. Der hierbei gemachte Vorschlag der Einführung eines "data producer right" ist deshalb vor allem auch im Kontext dieses Ziels zu sehen, eine weitgehendere Datennutzung zu ermöglichen. Stärker noch als die Frage nach einem eigentumsähnlichen Schutz von Daten ist deshalb in der Mitteilung die Frage nach Zugangsrechten zu Daten, insbesondere in IoT-Kontexten thematisiert worden. Insofern stellt diese Diskussion auch einen wichtigen Hintergrund für die im folgenden Abschnitt 6 stattfindende Debatte über den Zugang zu Daten im vernetzten Auto dar.

Die Diskussion über Rechte an nicht-personenbezogenen Daten unterscheidet sich nun in dreierlei Hinsicht wesentlich von der ePrivacy-Verordnung-Diskussion:
– Erstens bezieht sie sich gerade nicht auf personenbezogene Daten, sondern auf die Vielzahl von nicht-personenbezogenen Daten, die nicht unter die europäische DS-GVO fallen. Allerdings tritt insbesondere bei der Diskussion konkreter Anwendungen oft das Problem auf, dass in vielen Datensets beide Arten von Daten vorhanden sind, so dass die datenschutzrechtliche Perspektive miteinbezogen werden muss.

[555] Vgl. die Mitteilung der Kommission (EC 2017a) und das begleitende Staff Working Document (EC 2017b).

– Zweitens ist hier die Diskussion primär von einer theoretischen Ebene angestoßen worden, nämlich einer juristischen Diskussion bzgl. der Frage, ob und wie Daten als neue wertvolle Ressource der Datenökonomie rechtlich geschützt sind. Insofern waren es nicht bestimmte Industrien und Stakeholder, die diese Diskussion initiiert haben.
– Drittens spielen auch deshalb direkte Interessengegensätze zwischen verschiedenen Stakeholdern hier eine wesentlich geringere Rolle. Dies mag auch der Grund sein, weshalb diese Diskussion wesentlich weniger kontrovers und politisch brisant ist.
Für die folgende Analyse wird deshalb folgendermaßen vorgegangen: In Abschnitt 5.2 wird der Verlauf der akademischen Diskussion und die auch daraus entstandene Diskussion über Probleme und Politikoptionen in der Mitteilung "Building a European data economy" in einer knappen Zusammenfassung dargestellt. Anschließend werden in Abschnitt 5.3 die Positionspapiere und Stellungnahmen von Stakeholdern analysiert, wobei stark von der von der Kommission 2017 durchgeführten Konsultation und ihren Ergebnissen ausgegangen wird.[556] Hieran schließt sich wiederum eine zusammenfassende Analyse der dabei verwendeten Argumentationen in Abschnitt 5.4 an.

5.2 DER VERLAUF DER AKADEMISCHEN DISKUSSION UND DIE MITTEILUNG "BUILDING A EUROPEAN DATA ECONOMY" DER EU-KOMMISSION

Ausgangspunkt der Debatte war eine primär in Deutschland entstandene Diskussion über die Frage, ob es notwendig sei, ein (an IP-Rechten orientiertes) neues Exklusivrecht zum Schutz von nicht-personenbezogenen Daten, insbes. maschinengenerierten Daten, einzuführen. Hintergrund war die Erkenntnis, dass solche Daten weder von traditionellen IP-Rechten, vom Sacheigentum oder von anderen absolut wirkenden Rechten wie bspw. dem europäischen Datenbankschutzrecht geschützt sind. Zwar können sie unter bestimmten Bedingungen (ähnlich wie Knowhow) als Geschäftsgeheimnis geschützt sein und Gegenstand des Schutzes von Verträgen sein, aber hierdurch entsteht kein absolut wirkendes exklusives eigentumsähnliches Recht gegenüber Dritten.[557] Insofern wurde der Vorschlag gemacht, in Analogie zum Geistigen Eigentum ein temporäres exklusiv wirkendes Recht für den Datenerzeuger einzuführen, das demjenigen zukommen soll, der die wirtschaftliche Verantwortung für die Datenerzeugung trägt. Dieses Recht sollte sich aber nur auf den Schutz der Daten als kodierte Information auf der syntaktischen Ebene, nicht aber auf der semantischen Ebene, beziehen. Nachdem Daten im Kontext der digitalen Ökonomie als neue wichtige wertvolle Ressource verstanden werden, ist die Frage nach einem eigentumsähnlichen Schutz schnell aufgegriffen worden und hat intensive Diskussionen ausgelöst. In Bezug auf die Begründung ist dabei hervorzuheben, dass trotz der expliziten Analogiebildung zu IP-Rechten nicht auf

[556] Vgl. den Synopsisreport der Kommission (EC 2017c) einschließlich des Anhangs mit den detaillierten Ergebnissen (EC 2017h).
[557] Vgl. hierzu die ausführliche Darstellung in Teil I dieses Gutachtens (S. 17-39) mit weiterer Literatur.

die dort zentrale Argumentation der Notwendigkeit von Anreizen für die Produktion von Innovationen (hier: Daten) abgestellt wurde, sondern primär auf die Wichtigkeit von solchen Rechten für die Entstehung von Märkten für Daten sowie auf die Problematik, dass durch starke Machtungleichgewichte zwischen Unternehmen, gerade auch in digitalen Kontexten, in B2B-Verträgen Daten, insbesondere von kleinen und mittleren Unternehmen, unfair entgolten werden können, was durch die klare Zuordnung eines solchen Rechts an den Datenerzeuger gelöst werden könnte.[558]

Hierauf hat sich sehr schnell eine breite und lebhafte Diskussion entwickelt, die nicht nur auf der akademischen Ebene, sondern durch das Interesse der EU-Kommission auch auf der politischen Ebene mit Wirtschaftsverbänden und Interessenvertretern geführt wurde. Die Frage, ob solche nicht-personenbezogenen Daten ausreichend durch die bisherigen rechtlichen Regelungen geschützt sind oder ob ein zusätzlicher eigentumsähnlicher Schutz benötigt wird, ist innerhalb der rechtswissenschaftlichen Diskussion sehr detailliert und kontrovers diskutiert worden.[559] Allerdings kam eine deutliche Mehrzahl der juristischen Beiträge zu dem Schluss, dass (1) ein solches neues Recht mit großen Schwierigkeiten bzgl. seiner praktischen Ausgestaltung verbunden ist, was vor allem auch erhebliche Rechtsunsicherheit schaffen kann, und es (2) keine überzeugenden Gründe für die Notwendigkeit eines solchen Rechtes gäbe. Erste Stellungnahmen von Vertretern der Wirtschaft in dieser frühen Phase der Diskussion haben diese Einschätzung geteilt und auf die (aus ihrer Sicht) zufriedenstellenden vertraglichen Lösungen hingewiesen. Allerdings gab es in der rechtswissenschaftlichen Diskussion auch andere Auffassungen, wobei insbesondere die Bedenken über Machtungleichgewichte zwischen Vertragsparteien sowie die Notwendigkeit einer klaren rechtlichen Zuordnung von Daten eine besonders wichtige Rolle gespielt haben. Diese Diskussion über einen eigentumsähnlichen Schutz von Daten hat dann aber auch sehr schnell eine Diskussion ausgelöst über die umgekehrte Frage, ob nicht unter bestimmten Konstellationen auch Rechte auf Zugang zu privat gehaltenen Rohdaten bestehen sollten, bspw. um Wettbewerb zu ermöglichen oder in bestimmten IoT-Kontexten, in denen gleichzeitig verschiedene Stakeholder Zugang zu Daten benötigen würden. Auch hierbei konnte auf eine Analogie zum IP-Recht verwiesen werden, nämlich dass aus wettbewerbsrechtlicher Sicht die Verweigerung von Lizenzen einen Missbrauch einer marktbeherrschenden Stellung gemäß Art. 102 AEUV darstellen kann.

Die Frage, ob die Einführung eines Eigentumsrechts an Daten notwendig bzw. zu empfehlen sei, ist auch für die Ökonomie eine neue Frage.[560] Erste Analysen aus ökonomischer Sicht haben ergeben, dass es bisher keine Evidenz für ein diesbezügliches Marktversagen gibt und

[558] Vgl. zu diesem Vorschlag und seiner Begründung insbes. Zech (2012, 412-440, 2015, 2016).

[559] Vgl. Hoeren (2013), Dorner (2014), Hornung/Goeble (2015), Zdanowiecki (2015), Specht (2016). Wiebe (2016), Drexl (2016, 2017), Fezer (2017) und Schweitzer/Peitz (2017, 2018),

[560] Vgl. zum folgenden wesentlich ausführlich Kerber (2016, 2017); vgl. auch Schweitzer/Peitz (2017, 60ff.) sowie Jentzsch (2018) und zum breiteren ökonomischen Hintergrund Duch-Brown et al. (2017).

dass die damit verbundenen Nachteile im Hinblick auf Rechtsunsicherheit und den in der Datenökonomie so wichtigen Zugang zu vielen unterschiedlichen Daten gravierend sein können, gerade für datengetriebene Innovationen. Aus ökonomischer Sicht sind Daten nicht-rivale Güter, die möglichst viel genutzt werden sollten.[561] Im Gegensatz zu Innovationen können Daten aber üblicherweise gut geheim gehalten werden (insbes. auch durch technische Restriktionen), so dass bisher keine gravierenden Kopierprobleme aufgetreten sind, die ein exklusives gegenüber Dritten durchsetzbares Recht notwendig machen. Insofern gibt es bisher auch kein generelles Anreizproblem, was sich auch empirisch an dem exponentiellen Anstieg der produzierten Daten in der digitalen Ökonomie zeigt. Es gibt bisher auch keine empirische Evidenz dafür, dass die immer noch bestehenden Probleme des Datenhandels, der tatsächlich noch unterentwickelt ist, auf das Fehlen von Eigentumsrechten an Daten zurückzuführen sei. Weiterhin können die unter Umständen vorhandenen Probleme von unangemessenen Vergütungen für Daten durch ungleichgewichtige Verhandlungssituationen zwischen Unternehmen nicht durch die Kreation eines Exklusivrechtes an Daten gelöst werden, da dieses in asymmetrischen Machtkonstellationen wegverhandelt werden würde. Solche Machtungleichgewichtsprobleme müssten dagegen durch andere regulatorische Instrumente gelöst werden, wie insbesondere das Wettbewerbsrecht. Ansonsten kommt jedoch der Vertragsfreiheit für die Gestaltung von vertraglichen Vereinbarungen zwischen Unternehmen in Bezug auf Daten eine große Bedeutung zu, da hierdurch wesentlich flexiblere Lösungen für die Vielfalt unterschiedlichster Geschäftsmodelle möglich sind. Umgekehrt können aber aus ökonomischer Sicht unter bestimmten Umständen durchaus Zugangsrechte zu Daten gerechtfertigt sein. Aufgrund der Nichtrivalität von Daten kann es gerade in IoT-Kontexten, in denen oft mehrere Stakeholder die produzierten Daten entweder gemeinsam produzieren oder diese jeweils für ihre eigenen Zwecke nutzen können, nicht optimal sein, wenn ein (!) Akteur die exklusive Verfügung über diese Daten hat,[562] sei es über ein explizites Exklusivrecht oder über eine faktische Exklusivität des Datenhalters. Allerdings ist aus ökonomischer Sicht bei der Frage der Ausgestaltung von Zugangsrechten auch vorsichtig vorzugehen, da zu weitgehende und evtl. nicht ausreichend entgoltene Zugangsrechte die Anreize für die Generierung von Daten beeinträchtigen können. Insofern unterstützt die ökonomische Analyse bisher die in der rechtswissenschaftlichen Diskussion mehrheitlich vertretene Meinung, dass die Einführung eines solchen Exklusivrechts unter den gegebenen Bedingungen nicht zu empfehlen sei.

Auch vor dem Hintergrund dieser wissenschaftlichen Diskussion hat die EU-Kommission im Januar 2017 ihre Mitteilung "Building a European data economy" veröffentlicht, in der sie allerdings die Frage nach einer adäquaten Ausgestaltung eines rechtlichen Rahmens für die Datenökonomie wesentlich breiter angeht. Die Frage nach dem Zugang zu und der Nutzung

[561] Aus wohlfahrtsökonomischer Sicht sind die Grenzkosten zusätzlicher Nutzung null.

[562] Vgl. Kerber (2017, 127 ff.).

von Daten ist aber das wichtigste Thema in der Mitteilung.[563] Die Hauptsorge der Kommission besteht darin, dass die großen potentiellen Vorteile einer Datenökonomie nicht realisiert werden können, weil viele Unternehmen, die große Mengen an (insbesondere maschinengenerierten) Daten halten, diese nur intern nutzen und sie nicht anderen Nutzern zur Verfügung stellen. Empirische Studien zeigen, dass bisher nur eine begrenzte Menge von Daten geteilt und weiter genutzt wird, ebenso wie der Datenhandel sich erst langsam entwickelt.[564] Das zentrale Argument der Kommission ist, dass ein stärkerer Zugang zu Daten, auch zur Verwendung in anderen Sektoren, in der digitalen Ökonomie zu mehr Innovation und damit Wohlstand führen würde. Ein weiteres gravierendes Problem sieht die Kommission darin, dass oft der Hersteller eines gekauften datenproduzierenden Geräts (IoT) sich die de facto-Kontrolle über diese Daten vorbehält und die Käufer bzw. Nutzer keinen Zugang zu diesen Daten haben bzw. diese Daten nicht anderen zur Verfügung stellen können.[565] Die Kommission ist deshalb der Meinung, dass der Zugang zu und die Teilung von maschinengenerierten Daten erleichtert werden sollte.[566] Gleichzeitig sollten aber auch Investitionen, Vermögenswerte und vertrauliche Daten geschützt werden, sowie ein fairer Gewinn aus Investitionen in Innovationen gesichert werden. Weiterhin sollten aber auch die Vorteile der Daten in einer Wertschöpfungskette fair zwischen den Datenhaltern, den Verarbeitern von Daten und App-Anbietern geteilt werden, vor allem in machtungleichgewichtigen Situationen zwischen Firmen (aber auch im Verhältnis zu privaten Individuen). Besonders auffallend ist, dass in der Mitteilung der Kommission nicht nur ökonomische Argumente bezüglich einer möglichst weitgehenden Nutzung von Daten und Anreizen für "Data-Driven Innovation", sondern auch explizit Fairnessfragen hinsichtlich der Beteiligung an den Vorteilen der generierten Daten angesprochen werden.

Ausgehend von diesen identifizierten Problemen unterbreitet die Kommission in der Mitteilung eine breite Anzahl von unterschiedlichen Politikvorschlägen, um das Problem des Zugangs zu maschinengenerierten Daten besser zu lösen.[567] Insgesamt lassen sich die Vorschläge dabei in drei Gruppen einteilen. In einer ersten Gruppe finden sich Maßnahmen, die das Teilen und Handeln von Daten mit Hilfe von Verträgen erleichtern sollen. Hierzu gehören Leitlinien für die Behandlung von Datenkontrollrechten in Verträgen, technische Lösungen für verlässliche Identifikation und Austausch von Daten sowie Default-Regeln, die als Benchmarks für Verträge über Daten verwendet werden können. Letztere sollen auch dazu dienen, Fairness- und Verhandlungsungleichgewichtsprobleme in B2B-Vertragsbeziehungen zu lösen, d.h. es geht nicht nur um Maßnahmen zur Senkung von Transaktionskosten. Eine

[563] Die anderen Themen in dieser Mitteilung beziehen sich auf Anforderungen bzgl. Datenlokalisation, was den freien Datenverkehr innerhalb des Binnenmarktes beschränkt, auf Haftungsfragen sowie auf Fragen von Datenportabilität, Interoperablität und Standards.

[564] Vgl. EC (2017a, 8) und EC (2017b, 12 ff.).

[565] Vgl. EC (2017a, 10).

[566] Vgl. zu den folgenden Zielen der Kommission EC (2017a, 11 f.).

[567] Vgl. EC (2017a, 12 f.).

zweite Gruppe umfasst Maßnahmen, um Zugangsprobleme zu maschinengenerierten Daten von privaten Akteuren zu lösen. Solche Zugangsrechte könnten im "allgemeinen Interesse" handelnden öffentlichen Institutionen gewährt und für wissenschaftliche Zwecke etabliert werden. Weit darüber hinausgehend ist der Vorschlag, dass auch ein verpflichtender Zugang zu privat gehaltenen Daten für andere private Parteien (bspw. auf der Basis von FRAND-Bedingungen) möglich sein sollte, wobei allerdings "berechtigte Interessen" wie der Schutz von Geschäftsgeheimnissen einbezogen werden müssten. Dabei könnten auch die spezifischen Bedingungen von unterschiedlichen Sektoren und Geschäftsmodellen berücksichtigt werden. Wichtig ist, dass die Kommission bei diesen Lösungen auch explizit den Bereich maschinengenerierter, personenbezogener Daten miteinbezieht, die dann aber jeweils vorher anonymisiert werden müssten.

Die Einführung eines neu geschaffenen Datenerzeugerrechts ("data producer's right") stellt eine weitere ganz eigene Maßnahme dar, die sich gravierend von den ersten beiden Gruppen unterscheidet. An dieser Stelle fließt die oben ausführlich dargestellte Diskussion über ein neues Exklusivrecht für maschinengenerierte Daten ein. Im gleichzeitig mit der Mitteilung erschienenen zugehörigen Staff Working Document wird diese Diskussion in einer erstaunlichen Breite und Tiefe aufgearbeitet und verschiedene Varianten seiner Ausgestaltung diskutiert.[568] Insofern ist interessant, in welcher Form dieser Vorschlag eines Datenerzeugerrechts in die Mitteilung eingeflossen ist. Es geht nicht primär um die (im Sacheigentum und Immaterialgüterrecht im Vordergrund stehende) Ausschließungsfunktion eines solchen absoluten Rechts, sondern es soll die rechtliche Situation klären, um eine bessere Nutzung und Zugänglichmachung dieser Daten zu ermöglichen: "A right to use and authorise the use of non-personal data could be granted to the 'data producer', i.e. the owner or long-term user (i.e. the lessee) of the device. This approach would aim at clarifying the legal situation and giving more choice to the data producer … and thereby contribute to unlocking machine-generated data."[569] Diese klare Zuordnung des Datenerzeugerrechts zu dem Eigentümer bzw. Nutzer eines datenproduzierenden Geräts anstatt zum Hersteller ist mit Blick auf die ausführliche juristische Diskussion bezüglich der Zuordnung von maschinengenerierten Daten, welche primär das Kriterium der wirtschaftlichen Verantwortung in den Mittelpunkt stellt, durchaus überraschend. Es wird lediglich darauf hingewiesen, dass es auch Ausnahmen in Form eines nicht-exklusiven Zugangs zu diesen Daten für den Hersteller (oder öffentliche Institutionen, bspw. für Verkehrssteuerung oder Umweltfragen) geben kann. Der explizite Hinweis auf personenbezogene Daten macht deutlich, dass es auch hier nicht nur um maschinengenerierte Daten in B2B-Kontexten geht, sondern explizit auch um IoT-Anwendungen von privaten Personen.

[568] Vgl. EC (2017b, 33 ff.).
[569] EC (2017a, 13).

5.3 ANALYSE VON POSITIONSPAPIEREN UND STELLUNGNAHMEN VON STAKEHOLDERN

Obwohl diese Diskussion erst seit kurzem geführt wird, hat die Kommission inzwischen in einer Anzahl von Workshops und in einem im Frühjahr 2017 durchgeführten offiziellen Konsultationsverfahren eine Fülle von Meinungen und Stellungnahmen zu den Themen dieser Mitteilung und den zur Diskussion gestellten Lösungsvorschlägen eingeholt, die in diesem Abschnitt näher analysiert werden sollen.[570] Im Konsultationsverfahren selbst hat die Kommission in ihren Fragen die zur Diskussion gestellten Lösungsvorschläge im Vergleich zu ihrer Mitteilung teilweise noch weiter ausdifferenziert. Aufgrund der Innovativität der Fragestellung sowie des hohen Abstraktionsgrades der diskutierten sektorübergreifenden Lösungsansätze für Rechte an Daten hat sich die Diskussion wesentlich weniger an klarstrukturierten spezifischen Interessenkonflikten zwischen bestimmten Stakeholder-Gruppen – wie in der obigen ePrivacy-Diskussion oder der im folgenden Abschnitt analysierten Diskussion über Daten im vernetzten Auto – orientiert. Vielmehr werden wir sehen, dass die Diskussion mehr darum geht, inwieweit tatsächlich diesbezüglich Probleme im Markt existieren und ob und inwieweit deshalb in die Märkte mit solchen Politikmaßnahmen unterstützend oder regulatorisch eingegriffen werden soll. Insofern wird die folgende Analyse nicht nach Stakeholder-Gruppen strukturiert vorgestellt, sondern primär nach den von der Kommission angeführten Problemen und Lösungsoptionen.[571] [572]

Die als Online-Umfrage durchgeführte Konsultation bekam insgesamt 380 Antworten, wobei 322 von ihnen von Firmen und Organisationen kamen und von letzteren wiederum 22% kleine und mittlere Unternehmen (KMU) repräsentieren. Viele waren dabei aus den Bereichen IT-Services und dem Automobil- und Transportsektor.[573] In Bezug auf die Thematik Zugang und Weiterverwendung von nicht-personenbezogenen Daten hat die Kommission in einem ersten Schritt Fragen nach dem Ausmaß und den Problemen bei Zugang und Datenteilung gestellt, womit auch die bisher beschränkte empirische Faktenlage verbessert werden soll. Nicht wirklich überraschend ist, dass bei den Fragen nach den Quellen von Daten, dem Ausmaß der Abhängigkeit von externen Daten, ob Probleme beim Zugang zu Daten bestehen, ob diesbezüglich ungleichgewichtige Verhandlungspositionen auftreten und ob Daten mit anderen geteilt werden (und zu welchen Bedingungen) eine große Heterogenität zwischen den Befragten auftreten. Bspw. waren in Bezug auf Schwierigkeiten, Daten von externen Quellen zu bekommen, 53% der Meinung, dass sie keine Probleme haben, wäh-

[570] Vgl. den Synopsisreport der Kommission (EC 2017c) und die detailliertere Auswertung im Annex (EC 2017h).

[571] Insofern ist es auch zweckmäßig, stärker von der zusammenfassenden Auswertung der Kommission auszugehen und einzelne Positionspapiere von Stakeholdern nur ergänzend explizit heranzuziehen.

[572] In Bezug auf wissenschaftliche Beiträge zur Mitteilung der Kommission vgl. Wiebe (2017), Kerber (2017), Drexl (2017), Zech (2017) sowie weitere Beiträge aus dem Sammelband von Lohsse, Schulze & Staudenmayer (2017).

[573] Vgl. EC 2017h, 1 f.).

rend 47% andere Erfahrungen hatten.[574] Sehr unterschiedlich waren auch die Antworten in Bezug auf gleichgewichtige Verhandlungssituationen: Eine starke Minderheit von knapp 30% hat klar abgelehnt, dass sie sich in gleichgewichtigen Verhandlungssituationen befinden, knapp 20% haben dies bejaht, gut 30% sahen sich zwischen diesen Positionen. Knapp 20% sind der Meinung, dass sie bezüglich des Zugangs zu Daten oft einem missbräuchlichen Verhalten marktbeherrschender Unternehmen ausgesetzt sind.[575] In knapp 25% der Antworten waren die Unternehmen der Meinung, dass das Wettbewerbsrecht keine Wirksamkeit gegen möglicherweise wettbewerbswidrige Praktiken von Firmen entfaltet, die Daten halten oder nutzen, während nur gut 20% ihm einen hohen Grad an Wirksamkeit zuschreiben.[576] Für die Interpretation dieser Zahlen ist jedoch zu bedenken, dass die auftretenden Probleme sich eventuell auch sehr auf einzelne Sektoren konzentrieren können. Hierfür spricht, dass sowohl in der Konsultation als auch in begleitenden Workshops vor allem das Problem des Zugangs zu Daten im Automobilsektor für unabhängige Reparatur- und Wartungsservicebetriebe thematisiert worden ist. Die Schwierigkeiten des Zugangs zu den von den Automobilherstellern kontrollierten Daten ist in diesem Konsultationsprozess das am häufigsten genannte spezifische Problem, das wir im folgenden Abschnitt 6 noch vertieft analysieren werden.

Auch in Bezug auf die Bereitschaft, Daten zur Verfügung zu stellen, zeigte sich ebenfalls eine große Heterogenität.[577] Insbesondere die Halter von großen Datenmengen bevorzugen, die Daten nur intern zu analysieren oder sie nur an Firmen zu lizensieren, mit denen sie eine enge Geschäftsbeziehung unterhalten. Ca. 35% der Unternehmen teilen überhaupt keine Daten oder nur in einem geringen Umfang, knapp 20 % nur mit Subunternehmern und 13% nur innerhalb der gleichen Unternehmensgruppe. Allerdings gibt es auch Unternehmen, die einen Teil der Daten als Open Data zur Verfügung stellen (20%), an Kooperationspartner (insbes. in Innovationskontexten) weitergeben (11%) oder an einen größeren Kreis von Unternehmen gegen Entgelt verkaufen (13%). Auch die Frage der Teilung von Daten kann sektorspezifisch sehr unterschiedlich sein.[578] Insgesamt kam jedoch die Kommission zum Schluss, dass doch mehr Daten geteilt werden als in früheren Studien angenommen. Wenig aussagekräftig waren allerdings die Antworten, welche Daten geteilt werden. Von besonderer Bedeutung ist, dass 37% der Meinung sind, dass der existierende EU-Rechtsrahmen die Investitionen in die Sammlung von Daten durch Sensoren, die in Maschinen und Geräte ein-

[574] Vgl. EC (2017h, 13).
[575] Vgl. EC (2017h, 13).
[576] Vgl. EC (2017h, 14).
[577] Vgl. zum folgenden Kommission (2017h, 15 f.)
[578] Vgl. hierzu auch die Positionspapiere der Union Francaise de Electricité (UFE 2017) und der Community of European Railway and Infrastructure Companies (CER 2017), die jeweils auf bereits lange existierende sektorspezifische Regeln für die Offenlegung bestimmter Informationen im Energie- und Eisenbahnsektor (wie bspw. Fahrplaninformationen) hinweisen, gleichzeitig aber auch über viele Arten von Daten verfügen, die sie in unterschiedlichem Umfang und zu unterschiedlichen Bedingungen zugänglich machen möchten.

gebaut sind, genügend schützt; nur 16% widersprachen dieser Aussage. Allerdings war eine relative Mehrheit (knapp 40%) der Meinung, dass sie nicht wisse, ob der jetzige Rechtsrahmen solche Investitionen genügend schützt.[579] Hieraus ergibt sich die überaus wichtige Erkenntnis, dass eine große Unsicherheit über die Rechtslage und den Umgang bzgl. Daten besteht. Insgesamt zeigen die Antworten auf das Ausmaß von Datenzugang und Datenteilung, dass bzgl. beider Aspekte tatsächlich eine Fülle von Problemen existiert, die allerdings in sehr unterschiedlichem Ausmaß auftreten und selbst wieder sehr heterogen sein können. Letztlich unterstützen aber 2/3 der Antworten die Ansicht, dass das Teilen von Daten erleichtert und lock-in-Effekte (vor allem für KMU und Start-ups) vermindert werden sollten. Allerdings sind knapp 60% auch der Meinung, dass Investitionen in Daten geschützt werden sollten, insbesondere wenn es sich dabei um sensible und vertrauliche Geschäftsgeheimnisse handelt (knapp 80%).[580]

Eine zentrale Frage sowohl in der wissenschaftlichen Diskussion als auch in dem Konsultationsprozess mit der Wirtschaft bezieht sich darauf, in welchem Umfang die bisherigen rechtlichen Lösungen, die hauptsächlich auf vertraglichen Vereinbarungen zwischen den Unternehmen basieren, ausreichend sind. Diese Status-quo-Lösung impliziert, dass die Firmen selbst über die Weiterverwendung der Daten, die von Sensoren in Maschinen und Geräten gesammelt werden, und darüber im Rahmen der Vertragsfreiheit Vereinbarungen mit anderen schließen können, entscheiden können. Die Befürworter von vertraglichen Lösungen, zu denen vor allem die Unternehmensverbände, IT-Firmen, und Telekommunikationsfirmen gehören, argumentieren, dass nur durch freie vertragliche Gestaltung die Flexibilität gesichert werden kann, die für die Entwicklung der Datenökonomie und den damit verbundenen technischen Fortschritt notwendig ist, insbesondere aufgrund der sehr unterschiedlichen bereits bestehenden und zukünftigen Geschäftsmodelle. Die Sicherung der Vertragsfreiheit in Bezug auf den Umgang mit Daten wird deshalb von vielen Stakeholdern stark betont.[581] Allerdings ist die Meinung, ob dadurch mehr Daten zugänglich gemacht und weiterverwendet werden, in der Konsultation völlig geteilt. Je zur Hälfte wird davon ausgegangen, dass dies zu einer größeren oder geringeren Verfügung über Daten führen würde. Viele Befragte, insbesondere auch KMU, Start-ups und Verbraucherorganisationen halten es für unzureichend, sich nur auf vertragliche Vereinbarungen zu verlassen, da dies Hersteller in die Lage versetzen kann, eine dominante Stellung zu bekommen und den Wettbewerb auf "After-sale"-Märkten zu beschränken. In diesem Zusammenhang wird erneut auf die Automobilindustrie verwiesen. Auch besteht die Gefahr von unfairen Verteilungen der Vorteile aus Daten. Inso-

[579] Vgl. EC (2017h, 16).

[580] Vgl. EC 2017h, 17.

[581] Vgl. im Annex des Synopsisreports EC (2017h, 18). Dies wird insbesondere stark betont in einer Anzahl einzelner Positionspapiere von Unternehmensverbänden wie bspw. BDI (2017), BusinessEurope (2017, 6 ff.), TechUK (2017, 4), Ibec (2017), BDVA (2017); vgl. auch die Positionspapiere der britischen und der polnischen Regierung, die die gleiche Position vertreten (UK 2017, 9; Poland 2017, 1 f.).

fern plädierten einige Stakeholder für ein faires und flexibles Regime für den Zugang zu und die Weiterverwendung von Sensordaten.[582]

Von besonderem Interesse sind die Resultate bezüglich des in der Mitteilung gemachten Vorschlags eines "data producer rights". Bemerkenswert ist zunächst, dass die Kommission in der Konsultation bereits selbst ihren Vorschlag mit insgesamt vier Optionen weiter ausdifferenziert hat und hierbei jetzt von einem "data ownership right" spricht.[583] Die erste Alternative (1) bezieht sich auf eine Stärkung von zivilrechtlichen Abwehransprüchen gegen eine missbräuchliche Aneignung ("misappropriation") von Daten, ohne ein "full ownership right" einzuführen. Bei den anderen drei Alternativen würde ein exklusives Recht zur Lizenzierung des Gebrauchs dieser Daten als "sui generis intellectual property right on data" geschaffen, wobei dann zwischen den drei Varianten unterschieden wird, dass entweder (2) der Hersteller der Maschine oder des Geräts dieses Recht bekommt oder (3) der Nutzer (als "data producer") dieses Geräts oder (4) beide gemeinsam dieses Recht zugewiesen bekommen (wobei noch in der Mitteilung eindeutig der Nutzer derjenige sein sollte, dem dieses exklusive Recht zugeordnet wird). Ein besonders wichtiges Ergebnis der Umfrage ist, dass sowohl die Zuordnung eines solchen exklusiven Rechts nur an den Hersteller als auch nur an den Nutzer als Datenerzeuger eindeutig negativ eingeschätzt wurde in Bezug auf die Zurverfügungstellung von mehr Daten. Im Falle der Zuordnung zum Hersteller wurden von vielen Stakeholdern Bedenken geäußert, dass dies die gegenwärtig bereits bestehende de-facto-Kontrolle der Hersteller weiter verschärfen würde – mit der Gefahr von lock-in-Effekten und Datenmonopolisierung. Die umgekehrte alleinige Zuordnung des Rechts zum Nutzer wurde sehr kritisch von den Herstellern gesehen, die eine Gefahr für ihre internationale Wettbewerbsfähigkeit sehen und für Investitionen in die Fähigkeiten zur Datenproduktion. Als relativ beste Option wurde von den Befragten das exklusive "shared ownership right" eingeschätzt, von dem 1/3 der Meinung waren, dass es zu mehr Daten führen würde, während nur 27% der Auffassung waren, dass es sich diesbezüglich nicht positiv auswirken würde. Es wurde insgesamt auch besser eingeschätzt als die erste Option einer Stärkung zivilrechtlicher Abwehransprüche gegen eine "misappropriation" von Daten.[584] Besonders wichtig ist aber auch, dass viele generelle Vorbehalte gegenüber einem "data ownership right" geäußert wurden. Zum einen gibt es grundsätzliche Bedenken an einem solchen Eingriff in den Markt, der an sich besser geeignet sei, die richtige Allokation von Daten herbeizuführen als ein Regulierer. Zum anderen aber könnte die Einführung eines solchen neuen IP-Rechts Datenteilung gerade auch schwieriger machen, da es zu neuen rechtlichen Problemen und damit zusätzlichen Kosten für die Unternehmen führen kann.[585]

---

[582] Vgl. EC (2017h, 18) sowie speziell für die Probleme im Automobilsektor FIGIEFA (2016) und die ausführliche Diskussion im folgenden Abschnitt 6.

[583] Vgl. EC (2017h, 21 ff.).

[584] Vgl. EC (2017h, 23 f.).

[585] Vgl. EC (2017h, 23). Grundsätzliche Bedenken gegen das "data producer right" wurden auch in einer Anzahl von Positionspapieren geäußert wie bspw. BDI (2017), BusinessEurope (2017) und Ibec (2017).

An dieser Stelle ist es zweckmäßig, kurz aus ökonomischer Sicht die Ergebnisse der Konsultation bzgl. des Datenerzeugerrechts zu kommentieren. Die in der Konsultation aufgeworfene Frage, ob dem Hersteller, dem Nutzer oder beiden das exklusive Recht der Lizenzierung der Sensordaten eines Geräts zugewiesen werden soll, macht nochmals deutlich, dass wir uns in diesen IoT-Kontexten in Multi-Stakeholder-Situationen befinden, bei denen die exklusive Zuordnung der Daten zu einem (!) Stakeholder oft an sich nicht die ökonomisch optimale Lösung für die Spezifizierung der Rechte an diesen Daten ist.[586] Die exklusive Zuordnung und zwar gleichgültig ob sie – wie hier angedacht – durch ein exklusives Recht entsteht oder durch eine exklusive de-facto-Kontrolle über die Daten, schafft eine einseitige Machtposition, die gegenüber den anderen Stakeholdern ausgenutzt werden kann (Data Hold-up). Insofern ist auch nicht klar, ob dies zu einer größeren Datennutzung führen würde. Da Daten nicht-rivale Güter sind und gleichzeitig keine generellen Anreizprobleme ihrer Produktion bestehen, ist aus ökonomischer Sicht nicht von vorneherein klar, weshalb die exklusive Zuweisung zu einem Akteur effizient sein soll. Hinzu kommt, dass oftmals mehrere Akteure in solchen Situationen an der Produktion der Daten beteiligt sind. Insofern hat die (hier als relativ beste abgeschnittene) Lösung, Hersteller und Nutzer gemeinsam dieses Recht zuzuweisen, aus ökonomischer Sicht den Vorteil, dass beide Stakeholder die Daten nutzen können, ohne die Zustimmung des Anderen zu benötigen. Während dies die Nutzung durch diese beiden Stakeholder zweifellos erleichtert, ist es eine andere Frage, ob dies tatsächlich dazu führt, dass Dritten mehr Daten zur Verfügung gestellt werden. Entscheidend ist auch, ob sie sich beide hierfür einigen müssen, was bei "joint ownership" naheliegt, oder ob sie bezüglich der Nutzung dieser Daten auch unabhängig voneinander Lizenzen an Dritte einräumen können, was dann auch zu Wettbewerb zwischen beiden führen kann. Allerdings sollte angesichts dieser Ergebnisse auch bedacht werden, dass der Zugang von bestimmten Stakeholdern zu Daten in komplexen Multi-Stakeholder-Situationen auch ohne die Einführung eines exklusiven "data ownership rights" (mit einem exklusiven Lizenzierungsrecht) möglich ist, nämlich durch die direkte Zuweisung von spezifischen Zugangsrechten an bestimmte Stakeholder. Dieser vom Max-Planck-Institut für Innovation und Wettbewerb gemachte Vorschlag von "unwaivable access rights" war nicht als weitere Option im Konsultationsfragebogen enthalten.[587] Je nach der spezifischen Multi-Stakeholder-Situation können dabei sehr maßgeschneiderte Lösungen für sektorspezifische Problemkonstellationen entwickelt werden.

Die Ergebnisse der Stakeholder-Umfrage in Bezug auf "weiche" Maßnahmen, um Datenteilung und Zugang zu Daten zu erleichtern, ist generell auf eine positivere Resonanz gestoßen.[588] Hierzu gehört die Herausgabe eines Dokuments mit Leitlinien, wie Zugang, Nutzung und Weiterverwendung von Daten, die in Verträgen geregelt werden könnten, sowie Empfehlungen über die Ausgestaltung von AGB in Bezug auf solche Daten. Durch solche Maß-

[586] Vgl. zum Folgenden auch Kerber (2017, 127 ff.).
[587] Vgl. MPI (2017).
[588] Vgl. zum Folgenden EC (2017h, 19 ff.).

nahmen kann größere Klarheit geschaffen werden, was vor allem auch KMU helfen kann. Die jeweils starke Minderheit, die sich skeptisch äußerte, besteht aus zwei Gruppen: Eine Gruppe ist der Auffassung, dass die bisherigen vertraglichen Lösungen ausreichend sind, während eine zweite Gruppe den unverbindlichen Charakter dieser Lösungen als unzureichend ansieht, weil verhandlungsstarke Unternehmen diese nicht anwenden würden. Auf deutlich mehr Skepsis ist der eng damit verknüpfte Vorschlag einer gesetzlichen Regelung von (allgemeinen oder sektorspezifischen) nicht-verbindlichen Regeln in B2B-Verträgen in Bezug auf solche Sensordaten von Maschinen oder Geräten gestoßen (default rules). Dieser größere Widerstand ergibt sich jedoch primär durch die zusätzlich von der Kommission angedeutete Möglichkeit, dies mit einer Unfairness-Kontrolle in B2B-Verträgen zu verbinden (unfair commercial practices), woraus die Möglichkeit entsteht, dass diese Regeln über die Rechtsprechung faktisch verbindlich werden können. Dies würde aber wiederum der notwendigen Flexibilität in vertraglichen Lösungen entgegenstehen. Andere Stakeholder haben dies aber gerade als einen möglichen Vorteil dieser Lösung gesehen.[589] Auch bei der Stakeholder-Diskussion wurde damit sowohl auf die transaktionskostensenkenden Aspekte dieser Vorschläge abgestellt als auch auf ihre Geeignetheit, auf Verhandlungsmachtungleichgewichte basierende Probleme zu reduzieren.

Das wesentlich stärkere Instrument einer Verpflichtung zur Lizenzierung für die Weiterverwendung von Daten unter "FRAND"-Bedingungen ("fair, reasonable, and non-discriminatory") für Sensordaten von vernetzten Maschinen und Geräten wurde sehr unterschiedlich beurteilt.[590] 24% würden dies zu einem großen Teil unterstützen, während 35% sich strikt dagegen aussprachen. Ähnlich fiel das Urteil bzgl. Daten aus, die im Kontext von Plattformen erhoben werden. Diese sehr unterschiedliche Sichtweise ist nicht erstaunlich, da eine generelle Verpflichtung zur Lizenzierung unter FRAND-Bedingungen ohne weitere differenzierende Kriterien einen sehr weitgehenden Eingriff darstellt. Eine stärkere Zustimmung ergab sich bei der Frage, ob öffentliche Institutionen Zugang zu Daten erhalten sollten, wenn dies im öffentlichen Interesse ist. Dies ist insbesondere im Zusammenhang mit öffentlichen Gesundheitsrisiken, für öffentliche Statistiken und durch öffentliche Mittel geförderte, wissenschaftliche Forschung bejaht worden. Allerdings möchte auch hier 1/3 der Befragten keine Daten für solche Zwecke des öffentlichen Interesses zur Verfügung stellen. Besonders wichtig ist, dass hierbei bestimmte Bedingungen einzuhalten wären, insbesondere Sicherheit der IT-Systeme, Schutz der Privatsphäre (bspw. kein Tracking von Individuen durch Regierungsstellen), Schutz von Geschäftsgeheimnissen sowie die Frage einer fairen Kompensation für die Investitionen in die Generierung von Daten.[591]

Insgesamt wurde sowohl in der Konsultation als auch in der wissenschaftlichen Diskussion sehr deutlich, dass verpflichtende Lösungen, sei es ein exklusives Datenerzeugerrecht, obli-

[589] Vgl. EC (2017h, 21).
[590] Vgl. zum Folgenden EC (2017h, 24 ff.).
[591] Vgl. EC (2017h, 26).

gatorische Zugangslösungen oder verbindliche Vertragslösungen bzgl. Daten als generelle sektorübergreifende Lösungen sehr kritisch gesehen werden. Die konkreten Bedingungen, Probleme und Geschäftsmodelle sind hinsichtlich unterschiedlicher Arten von Daten so verschieden, dass allgemeine (in der europäischen Diktion: "horizontale") Regelungen kaum geeignet sind, die Probleme adäquat zu lösen, ohne möglicherweise eine Fülle neuer Probleme zu schaffen. Dies zeigt sich in der breiten Betonung, dass "one-size-fits-all"-Lösungen nicht als adäquat angesehen werden können.[592] Dies kann aus einer ökonomischen Perspektive unterstützt werden. Die konkreten Kosten und Nutzen unterschiedlicher rechtlicher Ausgestaltungen bzgl. Rechten an Daten und die adäquate Spezifizierung und Allokation dieser Daten dürfte für verschiedene IoT-Kontexte so unterschiedlich sein, dass in verschiedenen Sektoren vermutlich sehr verschiedene Datengovernance-Lösungen optimal sind. Hieraus ergibt sich die Empfehlung, zunächst eher für bestimmte Sektoren und Problembereiche, bei denen gutstrukturierte spezifische Probleme auftreten, wie bspw. bei den Daten des vernetzten Autos oder die im Rahmen von "Smart Agriculture" erhobenen Daten, nach geeigneten spezifischen Lösungen zu suchen und diese zu implementieren, evtl. auch durch sektorspezifische Regulierungen.[593] Dies hat sich auch in der (rechts-)wissenschaftlichen Diskussion als breite Meinung herausgebildet und geht ebenfalls konform mit der abschließenden Aussage der Kommission in der Mitteilung, dass das Experimentieren mit Lösungen ein wichtiger Teil des Suchprozesses für adäquate Regelungen ist. Dabei wird besonders auf den Automobilsektor mit dem vernetzten und automatisierten Fahren als naheliegendes Beispiel hingewiesen.[594]

5.4 DIE DISKUSSION ÜBER DEN RECHTLICHEN UMGANG MIT NICHT-PERSONENBEZOGENEN DATEN: EINE ZUSAMMENFASSENDE ANALYSE

In dieser Diskussion sind verschiedene einzelne Diskussionsstränge miteinander verknüpft worden. Dazu gehört erstens die primär aus der rechtswissenschaftlichen Diskussion thematisierte Frage nach dem rechtlichen Schutz von nicht-personenbezogenen Daten, insbesondere maschinengenerierten Sensordaten, zweitens – damit verknüpft – die neu auftretenden Probleme im Umgang mit Daten durch datenmäßig integrierte Wertschöpfungsketten und -netze im B2B-Bereich sowie die spezifischen Probleme in IoT-Kontexten (Hersteller/Nutzer etc.) und drittens die Frage nach Problemen für die möglichst weitgehende Nutzung von Daten in der Datenökonomie. Die beiden letzten Punkte sind direkt mit der Frage von Datenteilung und Zugang zu Daten verknüpft. Der Fokus auf nicht-personenbezogene Daten erlaubt in dieser Diskussion ein Ausblenden der Problematik des Schutzes der Privatsphäre, sodass die bei der ePrivacy-Diskussion so zentralen Konflikte zwischen dem Schutz perso-

[592] Vgl. EC (2017, 18).
[593] Vgl. Kerber (2017, 131 ff.).
[594] Vgl. EC (2017a, 17).

nenbezogener Daten und einer digitalen Ökonomie, die möglichst viele Daten zur Entwicklung neuer Produkte und Dienstleistungen (data-driven innovation) verwenden möchte, hier nicht aufzutreten scheinen. Allerdings wird auch in dieser Debatte immer wieder auf die Probleme der Abgrenzung von personen- und nicht-personenbezogenen Daten hingewiesen,[595] insbesondere auch in konkreten IoT-Kontexten (siehe auch die folgende Diskussion in Abschnitt 6 über Daten im vernetzten Auto). In der Debatte selbst führt dies aber dazu, dass ein sehr breiter Konsens darüber besteht, dass der Zugang zu und die (Weiter-)Verwendung von mehr Daten gefördert werden soll, weil dies zu mehr Innovation und Wohlstand führt. Insofern stehen hier ökonomische Vorteile (insbesondere auch für die Konsumenten) und damit ökonomische Argumentationen im Vordergrund. Die zentralen Auseinandersetzungen beziehen sich dabei primär auf die Frage, inwiefern es hierfür notwendig ist, durch neue rechtliche Regelungen Hindernisse für die Entwicklung einer solchen Datenökonomie zu beseitigen, oder ob die bisherigen rechtlichen Regelungen in Kombination mit vertraglichen Arrangements im Prinzip ausreichen, was ökonomisch dann als Frage nach einem möglichen Marktversagen zu interpretieren ist.

Besonders interessant in dieser Debatte ist die Diskussion um die Frage, ob ein neues exklusives eigentumsähnliches Recht für nicht-personenbezogene Daten eingeführt werden soll.[596] Obwohl es argumentativ auf den ersten Blick sehr einfach erscheint, die Notwendigkeit eines Eigentums an einer so wertvollen Ressource wie Daten aus der zentralen Bedeutung von Privateigentum und Vertragsfreiheit für die Funktionsfähigkeit einer marktwirtschaftlichen Ordnung abzuleiten, spielt dieses grundlegende Argumentationsmuster in dieser Debatte keine wirkliche Rolle. Vielmehr hat sich die Diskussion, insbesondere auch mit Wirtschaftsvertretern, sehr schnell auf die pragmatische Frage konzentriert, ob denn ein solches neues Exklusivrecht wirklich nötig sei oder ob nicht die bisherigen Lösungen (insbes. Schutz von Geschäftsgeheimnissen etc.) ausreichen. Die sich dabei ausdrückende Vorsicht hat sicherlich auch viel mit den vielfältigen Problemen bei den bisherigen traditionellen IP-Rechten zu tun, die teilweise zu Innovationshindernissen führen können. Wie oben bereits ausgeführt, kommt eine explizite ökonomische Analyse zu dem Schluss, dass ein solches neues IP-Recht nicht nötig sei und vielmehr gerade hinderlich für die digitale Ökonomie sein könnte. In dem Zusammenhang ist auch interessant, welche ökonomischen Argumente in dieser Debatte nicht verwendet werden: Anreizprobleme für die Produktion von Daten spielen in der Diskussion ebenso keine Rolle wie das Imitations-/Kopierproblem, was die zentralen Argumente für die Rechtfertigung von traditionellen IP-Rechten sind. Diese Auffassung

[595] Vgl. bspw. TechUK (2017, 3 f.): "It is difficult to imagine a situation in which a non-personal data set as described in the Commission's Communication might not contain a single piece of personal data as defined by GDPR".

[596] Theoretisch könnte die gleiche Frage auch für personenbezogene Daten gestellt werden, da diese aus ökonomischer Sicht die gleichen Eigenschaften aufweisen; allerdings wäre dies nicht vereinbar mit europäischem Datenschutzrecht. Zur Frage von Eigentumsrechten an personenbezogenen Daten vgl. Kilian (2015), Schwartmann & Hentsch (2015) und in der US-amerikanischen Diskussion bspw. Samuelson (2000) und Schwartz (2004).

spiegelt sich auch völlig in der von Anfang an kritischen Einstellung von weiten Teilen der Wirtschaft gegenüber einem solchen neuen Exklusivrecht wieder. Besonders bemerkenswert ist in diesem Zusammenhang, dass diejenigen Stakeholder, die über große Datenmengen verfügen, gerade nicht an der Einführung eines solchen Eigentumsrechts an diesen Daten interessiert sind. Dies könnte sich dadurch erklären, dass schon die jetzige Rechtslage und Technik genügend Möglichkeiten der Sicherung ihrer de-facto-Kontrolle über "ihre" Daten bietet, und sie solche eigentumsrechtlichen Lösungen eher als Hindernisse für den Zugang zu weiteren Datenbeständen sehen, die für ihre Big-Data-Analysen wichtig sind. Insofern hat schon die Mitteilung der Kommission diese Zurückhaltung geschickt aufgegriffen, indem sie die Diskussion dieses Vorschlags eines Datenerzeugerrechts primär aus der Perspektive diskutiert, ob (und in welcher Ausgestaltung) es zu einer größeren Zurverfügungstellung und Weiterverwendung von Daten führen und damit die europäische Datenökonomie mit ihren Vorteilen von mehr Innovationen und Wohlstand fördern würde.

Die zentrale Diskussion über Rechte an Daten macht sich vielmehr primär daran fest, ob die in den Märkten vorherrschenden vertraglichen Lösungen über die Produktion und Nutzung von und Zugang zu Daten ausreichend funktionieren oder ob diesbezüglich Marktversagen und andere Probleme auftreten, die zusätzliche rechtliche Regelungen erfordern. Eine wichtige Frage betrifft dabei die Anreize bezüglich der Zurverfügungstellung von Daten sowie – damit verknüpft – die dabei auftretenden Transaktionskosten und -probleme. Eine der ursprünglichen Begründungen für ein Datenerzeugerrecht war gerade die dadurch evtl. leichtere Entstehung von Märkten.[597] Auch wenn das Problem der immer noch unterentwickelten Märkte für Daten in der Mitteilung angesprochen wird, nimmt in der gesamten Diskussion die Frage nach der Funktionsfähigkeit von sekundären Datenmärkten und die dabei evtl. bestehenden Probleme eher eine Randposition ein. Obwohl die nicht-verbindlichen Instrumente bei den Politikoptionen in der Mitteilung wie Leitlinien, Empfehlungen und Default-Regeln in Verträgen über Daten als Maßnahmen zur Senkung von Transaktionskosten für das Teilen bzw. die Lizenzierung von Daten verstanden werden können, beziehen sich diese Optionen eher auf die Zurverfügungstellung von bisher nicht genutzten Daten, aber nicht primär auf den eigentlichen Datenhandel, bspw. auch über Plattformen oder Datenbroker. Insbesondere fehlen hier empirische Studien, die genauer klären, was die eigentlichen Transaktionsprobleme für den Handel mit Daten sind und wie man diese reduzieren könnte. Interessant sind in diesem Zusammenhang bspw. Informationsasymmetrieprobleme bezüglich der Qualität und der Herkunft von Daten.[598] Hier wären tiefere wissenschaftliche Analysen erforderlich, um eventuelle Marktversagensprobleme zu identifizieren und nach Lösungswe-

[597] Vgl. Zech (2015, 145).

[598] Vgl. zu den Problemen des Datenhandels aus empirischer Sicht Carnelley et al. (2016), Cattaneo et al. (2016) und EC (2017b, 12 ff.); aus stärker theoretischer Perspektive Koutroumpis et al. (2017) sowie aus einer breiteren Perspektive Schweitzer/Peitz (2017) und in knapper Form Kerber (2017, 120ff.); für das spezielle Problem Informationsasymmetrien und Qualitätsprobleme bei Daten vgl. Mattioli (2015); für ein vielversprechendes Konzept in Bezug auf Plattformen für den Datenhandel siehe Fraunhofer-Gesellschaft (2016).

gen zu suchen. Diese für eine wohlfunktionierende Datenökonomie wichtige Thematik ist in der bisherigen Diskussion noch zu kurz gekommen.

Viel mehr diskutiert wurde dagegen eine andere Frage. Sie bezieht sich darauf, ob aus einer Fairness- oder Verteilungsperspektive bei rein vertraglichen Lösungen in B2B-Zusammenhängen (insbes. in Wertschöpfungsketten oder in IoT-Kontexten mit mehreren Stakeholdern) die Marktergebnisse in Bezug auf die de-facto-Kontrolle von Daten, den Zugang zu Daten bzw. die Partizipation an den Vorteilen von Daten immer als gerechtfertigt angesehen werden können, oder ob es diesbezüglich Probleme durch Machtungleichgewichtssituationen zwischen den Vertragspartnern gibt. In der Diskussion besteht im Prinzip ein breiter Konsens darüber, dass solche ungleichgewichtigen Verhandlungsmachtkonstellationen auftreten und ein Problem sein können, so dass die Debatte sich in der Folge mehr darum dreht, ob bestehende Regelungen aus dem Wettbewerbs- und Unlauterkeitsrecht ausreichend geeignet sind, diese Probleme zufriedenstellend zu lösen.[599] Diese Diskussion ist allerdings von mindestens drei Problemen geprägt:[600] Erstens gibt es keinen klaren Konsens über die Kriterien, was ungleichgewichtige Verhandlungssituationen sind, wenn man über die Regelungen des Wettbewerbsrechts (Marktbeherrschung bzw. im deutschen GWB relative Marktmacht) hinausgehen möchte, bzw. was ein "unfaires" oder "unangemessenes" Ergebnis in solchen Verhandlungen ist. Zweitens ist festzustellen, dass die Frage, wer in welchem Umfang an dem Wert der produzierten Daten partizipiert, generell erstaunlich wenig in dieser Diskussion thematisiert wird. Dies betrifft nicht nur KMU und Start-ups in B2B-Kontexten, sondern vor allem auch die Frage der Beteiligung von privaten Nutzern (bei datenproduzierenden Geräten wie Smartphones und IoT-Geräten) an den nicht-personenbezogenen Daten, die diese Geräte produzieren. Diese Diskussion ist, wie wir auch in dem folgenden Abschnitt über Daten im vernetzten Auto sehen werden, immer noch sehr unterentwickelt. Da es aus ökonomischer Perspektive dabei auch um die distributive Frage geht, welche Gruppen wie an den vermuteten großen Vorteilen aus der Datenökonomie partizipieren (sollen), ist eine wesentlich ausführlichere Diskussion zur Lösung dieser Frage notwendig, unabhängig von dem Problem des Schutzes der Privatsphäre und des sich daraus ableitenden Datenschutzrechts.

Das dritte Problem dieser Diskussion über nicht akzeptabel erscheinende Marktergebnisse durch Verhandlungsmachtungleichgewichte ist, dass die dabei auftretenden Probleme evtl. wesentlich begrenzter sind, wenn eine spezifische Gruppe von Fallkonstellationen, nämlich Multi-Stakeholder-Situationen in IoT-Zusammenhängen, ausgeklammert werden würde. Wie oben bereits ausgeführt, haben im Grunde die Ergebnisse der Konsultation über die relativen Vor- und Nachteile von exklusiven Rechten für die Lizenzierung von nicht-personenbezogenen Daten (nur Hersteller, nur Nutzer oder beide) die theoretischen Überlegungen bestätigt, dass in bestimmten IoT-Konstellationen die Entstehung einer exklusiven

[599] Vgl. hierzu die Ergebnisse der Konsultation EC (2017h, 13 f.).

[600] Vgl. zum Folgenden Kerber (2017, 124 ff.).

Kontrolle über die dabei generierten nicht-personenbezogenen Daten durch einen einzigen Stakeholder, gleichgültig ob sie de facto entsteht oder durch rechtliche Zuweisung eines Exklusivrechts, an sich nicht die adäquate Lösung für die Governance dieser Daten ist, und zwar auch nicht aus einer ökonomischer Perspektive. Vielmehr schafft die entstehende exklusive Kontrolle über diese Daten gerade erst das Machtungleichgewicht für die dann folgenden Verhandlungen über den Zugang der anderen Stakeholder zu den generierten Daten, die der Datenhalter kontrolliert. Insofern kann gerade eine Fehlspezifikation von (Verfügungs-)Rechten an Daten die Ursache der beklagten Machtungleichgewichte bei Verhandlungen über den Datenzugang sein.

Solche Konstellationen treten bspw. im Bereich "Smart Agriculture" (Landwirte, Maschinenhersteller) oder im Bereich des vernetzten Autos auf, können aber auch in vielen IoT-Kontexten relevant werden. Im Bereich "Smart Agriculture" ist das Problem, dass sowohl die Hersteller der mit Sensoren ausgestatteten Landmaschinen als auch die Landwirte als Nutzer dieser Maschinen ein großes und gut begründbares Interesse an der Nutzung dieser Daten haben (für ihre jeweilig eigenen Zwecke der innovativen Verbesserung der Maschinen bzw. der Verbesserung der landwirtschaftlichen Produktion). Insofern erscheint es auch aus ökonomischer Sicht naheliegend, dass eine Governance-Lösung bzgl. dieser Daten, die beiden Stakeholdern die Nutzung dieser Daten erlaubt, zweckmäßiger ist, als eine exklusive Zuordnung der Kontrolle über diese Daten zu einem der beiden Stakeholder. Dies würde dann auch solche als ungleichgewichtig empfundenen Verhandlungssituationen bei dem Zugang zu Daten zwischen beiden Stakeholdern vermeiden. Wie im letzten Abschnitt bereits ausgeführt, ist es für solche Governance-Lösungen aber nicht notwendig, ein exklusives Lizenzierungsrecht zu schaffen, das man beiden zuordnet. Dies könnte leichter durch die Schaffung von einfachen nicht-exklusiven Zugangsrechten erfolgen.[601]

Es geht an dieser Stelle nicht darum, Lösungen für die spezifischen Governance-Probleme in IoT-Kontexten aufzuzeigen. Vielmehr soll lediglich darauf verwiesen werden, dass für Multi-Stakeholder-Situationen maßgeschneiderte komplexe Datengovernance-Lösungen (bestehend aus einem Set von Rechten und Regeln, insbesondere auch Zugangs- und Nutzungsrechten für eine bestimmte Gruppe von Stakeholdern) besonders geeignet sein können. Dabei kann es sinnvoll sein, für spezifische IoT-Anwendungen direkte Regulierungslösungen für die Ausgestaltung von geeigneten Datengovernance-Lösungen anustreben. Dies schließt aber nicht aus, dass auch dem Wettbewerbsrecht eine wichtige Rolle für die Lösung solcher Probleme des Zugangs zu Daten zukommen kann, bspw. über die Verweigerung des Zugangs zu Daten als Missbrauch einer marktbeherrschenden Stellung (Art. 102 AEUV) oder als unbillige Behinderung nach § 20 (1) GWB (relative Marktmacht). Das Wettbewerbsrecht könnte dabei einerseits selbst bestimmte Zugangsrechte begründen, andererseits aber auch in Kombination mit gesetzlich spezifizierten Zugangsrechten eingesetzt werden, bspw. um bei klar definierten Machtkonstellationen solche Zugangsrechte nicht-dispositiv (d.h. nicht-

[601] Vgl. MPI (2017).

abdingbar) auszugestalten, um ihr Wegverhandeln in ungleichgewichtigen Verhandlungssituationen zu verhindern.[602]

[602] Vgl. hierzu Drexl (2017), Kerber (2017, 125 ff.) und Peitz/Schweitzer (2018, 279 f.). Abschließend sei darauf hingewiesen, dass die EU-Kommission am 25.4.2018 nach Abschluss dieses Manuskripts ein "Datenpaket" veröffentlicht hat, das teilweise Vorschläge aus der Diskussion über die Mitteilung "Building a European Data Economy" aufgreift (wie Empfehlungen für "business-to-business“ (B2B) data sharing), teilweise aber auch Vorschläge wie ein "data ownership right" oder obligatorische Regelungen für den Zugang zu privat gehaltenen Daten nicht umsetzt. Vgl. hierzu EC (2018a, 2018b).

6. ÖFFENTLICHER DISKURS III: DATEN IM VERNETZTEN AUTO: EIN ANWENDUNGSBEISPIEL

6.1. EINLEITUNG

Nach der wichtigen Folgerung aus der Diskussion über "Rechte an Daten" (insbesondere bei IoT-Anwendungen), dass generelle rechtliche Lösungen bzgl. der Frage der Zuordnung von Rechten an Daten – seien es exklusive Rechte einerseits oder Zugangsrechte andererseits – schwierig sind, lag es nahe, dass sich die Diskussion in Richtung der Analyse von spezifischen Problembereichen mit der Idee der Suche nach spezifischen Lösungen für die Governance von Daten verlagert. Nach der Publikation der Mitteilung „Building a European Data economy" hat schon im Rahmen des Konsultationsprozesses dabei die Frage der Rechte an der Vielzahl von im vernetzten Auto erhobenen Daten eine erhebliche Rolle gespielt und ist von der EU-Kommission als ein wichtiges Anwendungsbeispiel identifiziert worden.[603] Unabhängig davon hat die EU-Kommission bereits 2016 im Rahmen ihrer C-ITS Initiative die sog. C-ITS Plattform (Cooperative Intelligent Transport Systems) ins Leben gerufen, in der alle Stakeholder, die für die Entwicklung des vernetzten bzw. autonomen Fahrens wichtig sind, zusammengebracht wurden, um gemeinsam die vielfältigen Probleme für die Entwicklung des autonomen Fahrens zu lösen.[604] Hierbei bezog sich eine zentrale Frage auf das Problem des Zugangs zu "in-vehicle data and resources" im vernetzten Auto für die unterschiedlichen Stakeholder, die an der Nutzung und Verwertung dieser Daten interessiert seien. In der C-ITS Plattformdiskussion hat sich dieses Multi-Stakeholder-Problem als eine besonders kontrovers diskutierte Problematik erwiesen. Auch hier geht es primär um die Frage, wer die de facto-Kontrolle über die erhobenen Daten ausübt und wie die Bedingungen für deren Nutzung und Verwertung bzw. den Zugang zu diesen Daten für andere Stakeholder sind. Da in Bezug auf das vernetzte Auto von Beginn an deutlich war, dass fast alle Daten auch einen Personenbezug aufweisen können, sind bezüglich dieser Daten auch die Regelungen der DS-GVO (und evtl. auch der zukünftigen ePrivacy-Verordnung) relevant.[605] Insofern treten bei dem hier behandelten Problem der Governance von Daten im vernetzten Auto auch Probleme aus den beiden obigen Abschnitten 4 und 5 auf. Die Frage der Notwendigkeit von regulatorischen Lösungen hinsichtlich des Zugangs zu Daten und Ressourcen des vernetzten Autos wurde systematisch in einer von der EU-Kommission in Auftrag gege-

[603] Vgl. EC (2017a, 17).

[604] Vgl. zur C-ITS Initiative DIRECTIVE 2010/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport, und insbesondere den C-ITS-Plattform-Report (C-ITS Platform 2016) sowie die sich in Bezug auf den Zugang zu Daten daran anschließende TRL-Studie (TRL 2017).

[605] Zum Personenbezug der Daten im vernetzten Auto vgl. Hornung/Goeble (2015) und Deutscher Bundestag (2016).

benen Studie untersucht (TRL 2017) und ist seitdem auf der politischen Agenda, ohne dass es bisher eine konkrete regulatorische Initiative gibt.[606]

6.2 ZUGANG ZU "IN-VEHICLE DATA": PROBLEMSTELLUNG UND BISHERIGE DISKUSSION

Für die Autoindustrie ist die Entwicklung zu vernetzten und später autonomen Autos eine potentiell revolutionäre Entwicklung, die das gesamte Geschäftsmodell der Autoindustrie mittel- und langfristig gravierend verändern kann. Die jetzt stattfindende Diskussion über den Zugang zu Daten bezieht sich jedoch nicht auf die zukünftig zu erwartenden autonomen Fahrzeuge, sondern auf die bereits jetzt existierenden und mittelfristig in der Anzahl stark zunehmenden Fahrzeuge, die mit einer erheblichen Anzahl von Sensoren große Mengen an Daten generieren und hierdurch die Fahrer mit verschiedenen Arten von intelligenten Fahr-Assistenzsystemen unterstützen können, während das Fahrzeug selbst immer noch unter der Kontrolle eines Fahrers bleibt und somit nicht autonom fährt. Entscheidend am vernetzten Auto ist, dass während des Fahrens permanent Daten über mobile Kommunikation zwischen dem Fahrzeug und anderen Akteuren übertragen werden können (Konnektivität). Die daraus erwarteten potentiellen Vorteile für die Insassen des Fahrzeugs und die Gesellschaft werden langfristig als sehr bedeutend eingeschätzt.[607] Die durch die Daten möglichen Fahrassistenzsysteme können zu einer spürbaren Entlastung der Fahrer führen und zu einer erheblichen Reduktion von Unfallzahlen (geringere Personen- und Sachschäden). Neben der Verbesserung der Verkehrssicherheit können die (Realzeit-)Daten auch zur Verkehrssteuerung (Reduktion von Stauproblemen) verwendet werden, was wiederum zu einer geringeren Umweltbelastung führt. Darüber hinaus kann ein großer Teil der gewonnenen technischen Daten ein wichtiger Input für innovative Verbesserungen des Autos sein (und der in ihm verwendeten Komponenten), aber auch zur Ferndiagnose und -prognose von Defekten genutzt werden. Daten über das Verhalten von Fahrern erlauben Versicherungen, neue risikoäquivalentere Versicherungsmodelle anzubieten und gleichzeitig Anreize für vorsichtigeres Fahrverhalten zu setzen. Insbesondere aber erlaubt die Konnektivität des Fahrzeugs den Fahrzeuginsassen die Möglichkeit der Nutzung einer Vielzahl von zusätzlichen Dienstleistungen wie bspw. von Navigation, Parkplatzsuche, Hotel- und Restaurantsuche, Entertainmentangeboten, Online-Shopping usw. Darüberhinaus ist es möglich, dass die dabei generierten Daten durch datenanalytische Verfahren in vielerlei Weise weiter ausgewertet und der Datenökonomie auch jenseits des Automobilsektors zur Verfügung gestellt werden. Bezieht

606 Allerdings hat das Europäische Parlament im Februar 2018 die Kommission aufgefordert, einen gesetzlichen Vorschlag über den Zugang zu "in-vehicle data and resources" vorzulegen, der ein "level playing field" und maximale Sichtérheit in Bezug auf die Speicherung von "in-vehicle data" und den Zugang für Dritte garantieren sollen. Vgl. EP (2018, 10) sowie vorher bereits Committee on Transport and Tourism (2017).

607 Für allgemeine Literatur zu vernetzten und autonomen Fahrzeugen und ihren vielfältigen Vorteilen vgl. bspw. McKinsey (2014), OECD/ITF (2015), PwC (2016), Andersen et al. (2016), Alonso Raposo et al. (2017); speziell zu den neuen kommerziellen Möglichkeiten aus der Perspektive der digitalen Wirtschaft vgl. BVDW (2015, 2016a, 2016b).

man zusätzlich noch das industriepolitische Argument der Sicherung der internationalen Wettbewerbsfähigkeit der europäischen Autoindustrie ein, ist es nicht erstaunlich, dass die Förderung des vernetzten und automatisierten Fahrens eine hohe Priorität auf der politischen Agenda der EU und vieler Mitgliedstaaten wie insbesondere auch Deutschland erhält.[608]

Aufgrund der Vielfalt der Verwendungsmöglichkeiten der Daten im vernetzten Auto und damit auch der Vielzahl der an diesen Daten interessierten Akteure ist in der C-ITS Plattformdiskussion bereits recht früh das Problem des Zugangs zu diesen Daten, bzw. wer die faktische bzw. rechtliche Verfügungsgewalt über diese Daten hat, thematisiert worden. Bereits im letzten Abschnitt 5 haben wir gesehen, dass die Frage, wer die de facto-Kontrolle über Daten hat, eine zentrale Rolle spielt, weil hierdurch auch bei Abwesenheit von exklusiven Rechten an Daten de facto-Exklusivitäten entstehen, die ökonomisch wie exklusive Rechte wirken können. Für die Frage, wer de facto (exklusiv) über diese Daten verfügt, ist vor allem aber die technologische Ausgestaltung der vernetzten Produkte von großer Bedeutung. Insofern ist es nicht überraschend, dass die Interessenskonflikte an den Daten des vernetzten Autos in der C-ITS Diskussion gerade in den technischen Lösungen für die Übertragung, Speicherung und möglichen Zugang zu diesen Daten besonders deutlich geworden sind.[609] Ohne an dieser Stelle zu sehr in die Details zu gehen, sind vor allem drei technische Lösungsmöglichkeiten diskutiert worden, wobei sich dann im Wesentlichen eine konkrete Diskussion zwischen zwei technische Lösungen (mit Varianten der konkreten Ausgestaltung) herauskristallisiert hat.[610] Im Mittelpunkt steht dabei zunächst das Modell der Automobilindustrie ("extended vehicle"). Demnach haben nur die Autohersteller einen direkten Zugang zum IT-System (und damit den Daten) des vernetzten Autos. Diese Daten werden auf einen externen Server des Autoherstellers übertragen und nur über diesen externen Server haben andere Stakeholder die Möglichkeit, Zugang zu diesen Daten zu erhalten. Eine wichtige Variante dieses technischen Konzepts des Zugangs über einen externen Server ist, dass dieser gemeinsam von allen relevanten Stakeholdern verwaltet wird, um damit einen diskriminierungsfreien Zugang zu gewährleisten ("shared server").[611] Neben der zweiten technischen Variante, dem "in-vehicle interface", das eine technische Weiterentwicklung des jetzt bereits existierenden "On-Board Diagnostic" (OBD) Adapters ist, mit dem Reparatur- und Wartungsdienstleister Diagnosedaten aus den Autos auslesen können, hat sich in der Diskussion insbesondere die "On-board application"-Plattform als vielversprechende mittel- und langfristige technische Lösung herausgebildet. Bei dieser technischen Lösung wäre das Auto

[608] Vgl. EC (2016c) und Bundesregierung (2015); von besonderer Bedeutung ist auch die Verordnung über die Einführung des "eCall in-vehicle system" (REGULATION (EU) 2015/758 (29 April 2015)), das die Autohersteller verpflichtet, neue PKWs mit einem Notfallsystem mit einer mobilen Kommunikation für Unfälle auszurüsten.

[609] Vgl. hierzu die kontroversen Diskussion in der Working Group 6 des C-ITS Reports (2016).

[610] Vgl. zu diesen technischen Lösungsmöglichkeiten und ihren Varianten ausführlich C-ITS Plattform (2016, 72-90) und TRL (2017, 32-49).

[611] Vgl. C-ITS (2016, 81 f.) und FIA (2015).

selbst die Plattform, auf der die Anwendungen laufen und Dienstleistungen über eine mobile Kommunikation angeboten werden können. Die Kfz-Fahrer (bzw. Kfz-Halter) können selbst über den Zugang zum Fahrzeug und den in diesem generierten Daten entscheiden, d.h. sie könnten auch Dritten direkten Zugang zum Fahrzeug und den Daten gewähren. Insofern kann das Problem auch anders formuliert werden. Bei dem "extended vehicle"-Konzept stellt das vernetzte Auto ein geschlossenes System dar, dessen Zugang von der Automobilherstellern vollständig kontrolliert wird, während die technische Lösung "On-board application"-Plattform die Möglichkeit bietet, offenere Varianten des vernetzten Autos zu verwirklichen.[612]

Entscheidend ist, dass diese unterschiedlichen technischen Lösungen das Ausmaß der de facto-Verfügungsmacht über die Daten des vernetzten Autos beeinflussen können. Im Falle des exklusiven Zugangs der Fahrzeughersteller zum vernetzten Auto und zu den darin generierten Daten gewinnen die Autohersteller technisch die exklusive de facto-Kontrolle über alle "in-vehicle"-Daten. Die "On-board application"-Plattform würde dagegen umgekehrt die Möglichkeit bieten, dass die Kfz-Eigentümer (oder der Fahrer) de facto über den Zugang zum Auto und seinen Daten entscheiden könnten. Allerdings wird die Kontrolle über diese Daten nicht nur von technologischen Bedingungen, sondern auch rechtlichen Regelungen beeinflusst.[613] Unbestritten ist, dass viele dieser Daten personenbezogen sein können und folglich unabhängig von der technischen Lösung dem Datenschutzrecht unterliegen.[614] Dies bedeutet, dass die Speicherung und Verarbeitung dieser Daten entweder unter eine gesetzliche Erlaubnis fällt ("erforderlich" für die Erfüllung des Vertrags oder aufgrund einer Abwägung mit den "berechtigten Interessen" der Autohersteller) oder eine explizite Zustimmung des Kfz-Halters (bzw. Fahrers) notwendig ist. In der einschlägigen rechtlichen Literatur wird davon ausgegangen, dass eine explizite Einwilligung erforderlich ist,[615] sodass es auf die Verträge zwischen den Autoherstellern und den Autokäufern ankommt, in denen sich die Autohersteller diese Einwilligung sichern können. Dies verweist erneut auf das Problem der konkreten Anforderungen an diese Einwilligung und damit auf die bereits mehrfach angesprochene Problematik von "notice and consent"-Lösungen. Aus ökonomischer Sicht ist jedoch auch zu berücksichtigen, dass sich auf dem Markt für neue (vernetzte) Kraftfahrzeuge unter Wettbewerbsbedingungen auch recht unterschiedliche vertragliche Lösungen über den Zu-

[612] Diese Diskussion kann auch aus der Perspektive, ob es sich bei vernetzten Autos um geschlossene oder offene Systeme handelt, geführt werden, d.h. dass der Zugang von dem Autohersteller vollständig kontrolliert wird oder ob über interoperable Schnittstellen auch ein direkter Zugang zum vernetzten Fahrzeug möglich ist. Vgl. aus dieser Perspektive in Bezug auf vernetzte Autos die Unterscheidung zwischen "open" und "closed cars" in Determann & Perens (2017). Begrifflich wird auch zwischen geschlossenen und offenen Telematiksystemen unterschieden.

[613] Vgl. zu den rechtlichen Bedingungen bzgl. der Daten im vernetzten Auto Hornung (2015), Hornung & Goeble (2015), TRL (2017, 179-199); vgl. auch die Studie BMVI (2017), in der noch breiter auf Rechte an Mobilitätsdaten (d.h. auch jenseits der direkt im vernetzten Auto generierten Daten) abgestellt wird.

[614] Allerdings können bestimmte technische Daten wiederum durch Immaterialgüterrechte geschützt sein.

[615] Vgl. Hornung (2015).

gang zum vernetzten Auto und die de facto-Verfügungsmacht über dessen Daten und deren Verwertungsmöglichkeiten herausbilden können. So schließt die technische Lösung eines geschlossenen Systems mit einem externen Server (wie im "extended vehicle"-Konzept) nicht aus, dass Autohersteller trotz exklusiver technischer Kontrolle sowohl den Zugang zum Auto als auch zu den Daten im Interesse ihrer Kunden sehr offen gestalten und ihnen hierüber breite Entscheidungsrechte einräumen. Umgekehrt kann die mögliche technische Offenheit bei der "On-board application"-Plattform auch durch Verträge zwischen Autoherstellern und Autokäufern so stark beschränkt werden, dass die Autohersteller trotzdem eine starke Exklusivität über den Zugang zum Auto und den Daten erhalten können. Dies ist – ökonomisch betrachtet – stark von den Präferenzen der Kunden und der Intensität des Wettbewerbs zwischen Autoherstellern abhängig. Die sich letztlich faktisch herausbildende Datengovernance-Lösung für "in-vehicle"-Daten und das Ausmaß der Offenheit oder Geschlossenheit des vernetzten Autos ist somit abhängig von (1) technischen Lösungen, (2) rechtlichen Regelungen und (3) dem Marktwettbewerb.[616]

In Bezug auf die Diskussion über den Zugang zu "in-vehicle data and resources" ist es bemerkenswert, dass sich die im Rahmen der C-ITS Plattform zusammengebrachten Stakeholder relativ früh in diesem Diskussionsprozess auf fünf Leitprinzipien geeinigt haben, die – wie wir sehen werden – bis heute den Argumentationsrahmen für die Diskussion über rechtliche und regulatorische Lösungen hinsichtlich des Zugangs zu diesen Daten bestimmt haben:

> "The five guiding principles that should apply when granting access to in-vehicle data and resources are the following:
> (a) Data provision conditions: Consent
> The data subject (owner of the vehicle and/or through the user of the vehicle or nomadic devices) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end customers and data subjects. This is without prejudice to requirements of regulatory applications.
> (b) Fair and undistorted competition
> Subject to prior consent of the data subject, all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the data subject.
> (c) Data privacy and data protection
> There is a need for the data subject to have its vehicle and movement data protected for privacy reasons, and in the case of companies, for competition and/or security reasons.
> (d) Tamper-proof access and liability
> Services making use of in-vehicle data and resources should not endanger the proper safe and secure functioning of the vehicles. In addition, the access to vehicle data and re-

[616] Vgl. für eine breitere Analyse, die auch die Märkte zwischen den Stakeholdern einbezieht, Frank & Kerber (2017, 25 ff.).

sources shall not impact the liability of vehicle manufacturers regarding the use of the vehicle.

(e) Data economy

With the caveat that data protection provisions or specific technologic prescriptions are respected, standardised access favours interoperability between different applications, notably regulatory key applications, and facilitates the common use of same vehicle data and resources."[617]

Diese fünf Prinzipien "Zustimmung des Kfz-Halters", "fairer und unverzerrter Wettbewerb", "Schutz der Privatsphäre", "Sicherheit und Haftung" sowie "Nutzung von Daten in der Datenökonomie durch standardisierten Zugang" haben sich in der Diskussion als die zentralen Ziele herausgebildet und die konkrete Diskussion kann zum großen Teil als Ausdruck ihrer spezifischen Interpretation bzw. der konfliktären Beziehungen zwischen diesen Zielen verstanden werden.

Schon im C-ITS Report haben sich die kontroversen Positionen, insbesondere zwischen der Automobilindustrie mit ihrem "extended vehicle"-Konzept und den unabhängigen Service-Providern, die an einem direkten Zugang zu (den Daten und) dem vernetzten Auto interessiert sind, an dem Ziel des "fairen und unverzerrten Wettbewerbs" und der Frage eines möglichen Konflikts zu dem Ziel "Sicherheit" festgemacht. Diese fünf Prinzipien und die zwischen ihnen evtl. bestehenden Spannungen standen dann auch im Mittelpunkt der von der EU-Kommission in Auftrag gegebenen Studie über "Access to in-vehicle data and resources", die die bisher umfassendste und systematische Analyse zu diesem Problem darstellt (TRL 2017). Das primäre Ziel dieser Studie besteht in einer qualitativen vergleichenden Analyse der obengenannten drei technischen Lösungen („data server platform"/„extended vehicle", „in-vehicle interface" und „On-board application"-Plattform) in Bezug auf das Ausmaß, mit dem durch sie diese fünf Leitprinzipien erfüllt werden können. Zentrale Ergebnisse dieser Studie sind: (1) Alle drei technischen Lösungen sind im Prinzip sowohl technisch als auch rechtlich machbar (auch in Bezug auf Sicherheit und Datenschutz). (2) Allerdings haben die verschiedenen Lösungen unterschiedliche Vor- und Nachteile bzgl. der fünf Prinzipien, wobei sich nicht eine Lösung als die nach allen Kriterien überlegene herausgebildet hat. (3) Trotzdem kommt die Studie letztendlich in der Abwägung, insbesondere aufgrund des Prinzips "fairer und unverzerrter Wettbewerb", zu dem Schluss, dass die "On-board application"-Plattform als die relativ beste technische Lösung zu bevorzugen sei.[618] Anschließend werden in der Studie verschiedene Szenarien hinsichtlich möglicher Politikmaßnahmen diskutiert und analysiert. Von zentraler Bedeutung ist hierbei, dass die Studie – wie auch viele Stakeholder und Beobachter – davon ausgehen, dass sich ohne Politikmaßnahmen wahrscheinlich das "extended vehicle"-Modell (evtl. kombiniert mit einer neutralen Serverlösung für den Datenzu-

[617] C-ITS Plattform (2016, 75 f.). Diese Leitprinzipien werden hier wörtlich zitiert, weil sie durchaus erheblichen Spielraum für unterschiedliche Interpretationen lassen.

[618] Aufgrund fehlender Informationen konnten aber die mit diesen technischen Lösungen jeweils verbundenen Kosten nur qualitativ abgeschätzt werden. Vgl. TRL (2017, 254 ff.).

gang) durchsetzt, da dies das von der europäischen Automobilindustrie angestrebte Modell ist, welches bei den bisherigen vernetzten Fahrzeugen bereits praktiziert wird.[619] In der Studie werden eine Anzahl von Politikmaßnahmen diskutiert, wobei insgesamt 4 Szenarien unterschieden werden. Neben einem Szenario 0 ohne Politikmassnahmen werden in einem weiteren Szenario 1 Maßnahmen diskutiert, die die auch von den Autoherstellern vorgeschlagene "neutrale Server-Lösung" in ihrer Wirksamkeit unterstützen und Risiken für Wettbewerbsverzerrungen vermindern sollen. Szenario 2 richtet sich auf die Implementierung der "Shared server"-Lösung statt des "extended vehicle"-Konzepts. Das langfristige Szenario 3 würde dagegen die "On-board application Plattform" in den Mittelpiunkt stellen, wofür die Autoren der Studie aber auch eine gesetzliche Regelung für nötig erachten würden. Allerdings geht die Studie nicht so weit, die Einführung einer solchen interoperablen Plattform verpflichtend zu machen.[620] Obwohl die EU-Kommission das Problem des Zugangs zum vernetzten Auto als ein wichtiges Problem ansieht, über das Workshops organisiert und Studien erstellt werden, scheint sie zur Zeit keine konkreten Pläne für Politikinitiativen in diesem Bereich zu haben.

Allerdings gibt es zurzeit eine andere eng mit dieser Problematik verknüpfte Reformdebatte. Das Prinzip des "fairen und unverzerrten Wettbewerbs" hat in der europäischen Automobilindustrie seit langem eine wichtige Rolle für den Wettbewerb in Bezug auf Reparatur- und Wartungsdienstleistungen sowie Ersatzteile gespielt. In der europäischen Wettbewerbspolitik wurde bereits vor langer Zeit eine klare Entscheidung getroffen, den Wettbewerb durch unabhängige Kfz-Reparatur- und Wartungsbetriebe gegen Versuche der Automobilhersteller zu schützen, diese potentiell sehr rentablen Aftermärkte für ihre eigenen Vertragswerkstätten (bzw. Original-Ersatzteile) durch unterschiedliche Ausschließungspraktiken vorzubehalten. Insofern sind teils in Gruppenfreistellungsverordnungen zum Kfz-Vertrieb bzw. vertikalen Vereinbarungen und teils in der Kfz-Typenzulassungs-VO (715/2007) Regelungen etabliert worden, die den Wettbewerb zwischen den Vertragswerkstätten und den unabhängigen Reparatur- und Wartungsbetrieben sicherstellen sollen. Ein zentrales regulatorisches Mittel ist dabei, dass diesen unabhängigen Unternehmen die gleichen für Reparatur und Wartung notwendigen, technischen Informationen zur Verfügung gestellt werden müssen wie den Vertragswerkstätten der Automobilhersteller. Ohne einen solchen regulierten Zugang zu technischen Informationen ("RMI: repair and maintenance service information"), der inzwischen auch den Zugang zu Fahrzeugdiagnosedaten über den "On-Board Diagnostic" (OBD) Adapter umfasst, könnten die unabhängigen Reparatur- und Wartungsservicebetriebe ihre Leistungen auf diesen Märkten nicht anbieten. Diese Lösung eines "regulierten Zugangs" zu notwendigen Informationen zur Sicherung des Wettbewerbs auf den Aftermärkten in der Automobilindustrie gilt seit langem als eine breit akzeptierte Regulierung mit einer klaren

[619] Wichtig ist in diesem Zusammenhang, dass die Autoindustrie bezüglich des "extended vehicles" auch eine ISO-Standardisierung vorantreibt. Vgl. hierzu TRL (2017, 58 ff.).

[620] Vgl. TRL (2017, 148-174).

wettbewerbspolitischen Zielsetzung,[621] auch wenn sie inzwischen rechtstechnisch in der Kfz-Typenzulassungs-VO verankert ist. Da diese Kfz-Typenzulassungs-VO von 2007 zur Zeit einer Revision unterzogen wird, die allerdings primär von der Diskussion über Emissionen (und dem Emissionsskandal) dominiert wird, ist die Frage, welche Informationen und Daten zukünftig über diese Regulierung den unabhängigen Kfz-Reparatur- und Wartungsdienstleistungsbetrieben in dieser regulatorischen Form zugänglich gemacht werden, auch in den Blickpunkt dieser Reform geraten.[622]

6.3 ANALYSE VON POSITIONSPAPIEREN VON STAKEHOLDERN BEZÜGLICH DATEN DES VERNETZTEN AUTOS

In diesem Abschnitt werden die Positionen und Argumente der wichtigsten Stakeholder in Bezug auf die Governance des Zugangs zum vernetzten Auto und der in ihm generierten Daten untersucht. Insgesamt lassen sich folgende Gruppen von Stakeholdern unterscheiden: (1) die Automobilhersteller, (2) die Verbraucher als Kfz-Eigentümer und Kfz-Nutzer (insbes. Fahrer), (3) die unabhängigen Kfz-Reparatur- und Wartungsdienstleistungsbetriebe und andere Service-Anbieter im automobilen Aftermarkt, (4) die Automobilkomponentenhersteller (Zulieferer), (5) die Kfz-Versicherungsunternehmen, (6) die Vielzahl weiterer Anbieter, die Dienstleistungen (Navigation, Online-Shopping, Entertainment etc.) an die Kfz-Halter und Kfz-Insassen anbieten möchten sowie Datenanalytikfirmen und Datenhändler, die an der weiteren Auswertung der Daten interessiert sind (Datenökonomie), und (7) öffentliche Institutionen, die im öffentlichen Interesse an Daten zur Verbesserung von Verkehrssicherheit und Verkehrssteuerung, Kriminalitätsbekämpfung sowie öffentlichen Statistiken und für Forschungszwecke interessiert sind. Bei der Analyse werden wir auf aktuelle Positionspapiere von einschlägigen Verbänden der wichtigsten dieser Stakeholder zurückgreifen und deren spezifische Argumentationen und die daraus abgeleiteten Forderungen untersuchen.[623]

6.3.1 AUTOMOBILHERSTELLER

Die folgende Analyse der Positionen und Argumente der Automobilhersteller (OEMs: Original equipment manufacturers) beruht primär auf den Positionspapieren des deutschen bzw. europäischen Verbandes der Automobilindustrie (VDA bzw. ACEA).[624] Im letzten Abschnitt

[621] Vgl. generell zu Wettbewerb auf Aftermärkten aus wettbewerbsrechtlicher Sicht Bauer (2007).

[622] Vgl. zu der bisherigen Regulierung Wegner (2010a, 2010b) und Becker/Simon (2015), und die Evaluationsstudie der Kommission (EC 2014). Die Reform der Kfz-Typenzulassungsverordnung ist zur Zeit im Trilog-Verfahren. In Bezug auf den regulierten Zugang zu Daten ist insbesondere die Frage interessant, inwieweit auch ein beschränkter mobiler Zugang möglich sein wird (remote access), damit unabhängige Serviceanbieter auch neue Dienstleistungen in Form von "remote maintenance" und "remote monitoring" anbieten können. Vgl. den Vorschlag der EU-Kommission zur Reform der Kfz-Typenzulassungsverordnung (EC 2016d) sowie den Kompromissvorschlag im Trilog-Verfahren vom 11. Januar 2018 (Europäischer Rat 2018b).

[623] Vgl. für eine Analyse von solchen Positionspapieren auch TRL (2017, 49-55).

[624] Vgl. VDA (2016) und ACEA (2016a, 2016b).

wurde das Grundprinzip des von den europäischen Automobilherstellern vertretenen "extended vehicle"-Konzepts bereits kurz dargestellt – mit der alleinigen Kontrolle der Hersteller über den Zugang zum vernetzten Auto und der Übertragung der Daten auf einen externen Server der Autohersteller, von dem aus dann Zugangsmöglichkeiten für Dritte geschaffen werden können. Das Hauptargument der Automobilhersteller für diese technologische Ausgestaltung besteht darin, dass nur so die hohen Standards für Sicherheit und Datenschutz gewährleistet werden können, die für das vernetzte Auto notwendig sind. Die besondere Bedeutung der Sicherheit beim vernetzten Auto ergibt sich allgemein durch die Gefahr von Unfällen, aber auch durch die besonderen Gefahren, die durch die Digitalisierung und Konnektivität entstehen, d.h. Cyber-Angriffe, Manipulation, Gefährdung der Integrität und Verfügbarkeit von Fahrzeugfunktionen etc. Insofern vertritt die Automobilindustrie die Auffassung, dass alle Lösungen, bei denen direkt von anderen Service-Providern auf das vernetzte Auto und seine Daten zugegriffen werden kann, bspw. durch Apps von externen Service-Providern, eine zu große Gefahr für die Funktionsfähigkeit und Sicherheit des vernetzten Autos darstellen: "Somit haben die Integrität und Sicherheit des Fahrzeugs und des Fahrers oberste Priorität und müssen jederzeit garantiert sein".[625] Damit verbindet sich auch der Anspruch der Automobilhersteller, die vollständige Verantwortung für die Sicherheit zu tragen, was unmittelbar mit der Frage der Haftung verknüpft ist. Auch wenn die Automobilhersteller damit die Sicherheit ganz in den Mittelpunkt stellen, so bekennen sie sich im Prinzip ebenfalls zu den anderen C-ITS Grundprinzipien, insbesondere Datenschutz, fairer und unverzerrter Wettbewerb und "consumer choice".

In Bezug auf den Zugang zu den Daten wird folgende konkrete Herangehensweise vorgeschlagen, wobei zwischen unterschiedlichen Datenkategorien differenziert wird:[626]
- Datenkategorie 1 umfasst anonymisierte Daten für die Verbesserung der Verkehrssicherheit, die "einer hoheitlichen Stelle vom Backend-Server des OEM diskriminierungsfrei basierend auf individuellen Vereinbarungen mit dem OEM zur Verfügung gestellt" werden.
- Datenkategorie 2: Dies ist ein definiertes OEM-übergreifendes Datenset, das aus anonymisierten Fahrzeugdaten (wie bspw. Umgebungstemperatur und Verkehrsfluss) besteht.
- Datenkategorie 3: Dies sind OEM-spezifische anonymisierte Daten für markenspezifische Services (3a) und Daten für die Komponentenanalyse und Produktoptimierung (3b), wie bspw. Leistungsdaten der Kraftstoffpumpe.[627]
- In der Datenkategorie 4 finden sich dann die Menge der persönlichen Daten, die "nur durch den Kunden autorisierten Drittanbietern zur Verarbeitung der Daten nach Gesetz, Vertrag oder Einwilligung zur Verfügung gestellt wird".
Die Daten der Kategorie 2 bis 4 können diskriminierungsfrei basierend auf individuellen B2B-Vereinbarungen Drittanbietern von Services zur Verfügung gestellt werden. Dies kann

[625] VDA (2016, 1).
[626] Vgl. zum folgenden VDA (2016, 6 ff.).
[627] Diese Daten würden nicht Drittparteien zugänglich gemacht, da sie Geschäftsgeheimnisse, Know-how oder durch IPRs geschützte Information enthalten können.

sowohl direkt durch spezielle Schnittstellen zwischen dem OEM-Server und den Drittanbietern geschehen als auch durch Einschaltung von neutralen (nicht von den OEMs betriebenen) Servern, die B2B-Vereinbarungen mit den OEMs über die Übertragung von Daten schließen können. Unberührt von diesem Modell wäre weiterhin der regulierte Zugang nach der Kfz-Typenzulassungs-VO für notwendige Informationen und Daten in Bezug auf Reparatur- und Wartungsdienstleistungen. Hierfür wäre es auch weiterhin möglich, im stationären Zustand des Fahrzeugs Daten aus dem OBD-Adapter auszulesen.[628] Insgesamt bedeutet dieses Modell, dass hinsichtlich einwilligungsbedürftiger, personenbezogener Daten die Kunden entscheiden können, ob und wem sie diese Daten zur Verfügung stellen. Für alle anderen Daten, insbesondere auch alle anonymisierten, personenbezogene Daten, gilt, dass die OEMs durch freie B2B-Vereinbarungen den Zugang für Drittanbieter ermöglichen können, wobei nach verschiedenen Datenkategorien differenziert werden kann und – neben des regulierten Zugangs zu RMI-Informationen – auch spezielle Regelungen für den Zugang zu Daten für öffentliche Institutionen bezüglich der Verkehrssicherheit getroffen werden können. Allerdings betont die Automobilindustrie die Notwendigkeit, dass die OEMs für alle Kosten kompensiert werden müssen, die ihnen bei der Generierung der Daten sowie der Organisation des Zugangs zu den Daten entstehen, ebenso wie für den Marktwert dieser Daten.[629]

Für die weitere Diskussion ist es zweckmäßig, bereits an dieser Stelle die ökonomischen Implikationen einer solchen Regelung der Governance von im vernetzten Auto generierten Daten näher zu analysieren. Hieraus folgt, dass zwar die Kunden die Möglichkeit behalten, darüber zu entscheiden, ob und wem personenbezogene Daten zugänglich gemacht werden können, aber über alle anderen Daten, sowie über die anonymisierten, personenbezogenen Daten, haben die OEMs die exklusive de facto-Kontrolle auf ihren OEM-Servern. Sie können den Zugang zu diesen Daten entweder direkt mit Drittparteien oder über neutrale Server frei zu Marktbedingungen über individuell ausgehandelte Verträge kommerziell verwerten. Kein anderer Akteur und auch nicht die Kunden haben die Möglichkeit, ohne Zustimmung der OEMs Zugang zu diesen Daten zu bekommen oder – im Falle der Kunden – diese Daten direkt anderen Drittparteien zur Verfügung zu stellen. Auch kann keine Drittpartei ohne Vereinbarung mit den OEMs direkt Dienstleistungen im vernetzten Auto anbieten. Hieraus ergibt sich auch, was die Autoindustrie unter "Auswahlfreiheit der Konsumenten" ("customer choice") versteht, nämlich dass diese in der Form gegeben ist, dass die Kunden frei zwischen den Service-Anbietern, die mit dem OEMs eine Vereinbarung geschlossen haben, wählen können. Auch "fair competition" ist bereits dann gegeben, wenn RMI-Informationen für Reparatur- und Wartungsdienstleistungen weiter nach den regulierten Zugangsregelungen gegeben werden, aber darüber hinaus andere Daten anhand frei vereinbarter Verträge zu Marktbedingungen zur Verfügung gestellt werden.[630] Das zentrale Argument der Automobil-

[628] Vgl. VDA (2016, 6).

[629] Vgl. VDA (2016, 9) und ACEA (2016a, 2).

[630] Vgl. ACEA (2016a, 1).

industrie für diese Governance-Lösung ist das bereits oben angeführte Sicherheitsargument, das allerdings von den anderen Stakeholdern bestritten wird.

Unabhängig davon stellt sich die Frage, wie begründet werden kann, weshalb die OEMs über die exklusive de facto-Kontrolle über die Daten des vernetzten Autos auch die faktische exklusive Möglichkeit der kommerziellen Verwertung dieser Daten erhalten sollen. Da diese Implikation des "extended vehicle"-Modells nicht explizit in den Positionspapieren angesprochen wird, kann nur indirekt auf zwei mögliche Argumentationen verwiesen werden, die im "Connectivity"-Positionspapier der ACEA (2016b) erwähnt werden. Zum einen wird auf die hohen Investitionen und Kosten für die Entwicklung und den Betrieb von vernetzten Autos verwiesen,[631] woraus sich die "usage fees" für kommerziell arbeitende Drittanbieter rechtfertigen würden. Zum anderen wird das industriepolitische Argument angeführt, dass durch die Digitalisierung der Automobilsektor in einem Wettbewerb mit neu entstehenden Wettbewerbern steht, bei dem zunehmend nicht Technologie oder Design der kritische Erfolgsfaktor ist, sondern Daten. Eine stärkere Orientierung an dem Prinzip "free flow of data", nach dem möglichst viele Daten so vielen Marktteilnehmern wie möglich zugänglich gemacht würden, würde nicht zwangsläufig zu mehr Wettbewerb, Innovation und zusätzlichen Arbeitsplätzen und Wertschöpfung in der EU führen. Vielmehr könnte auch das Gegenteil eintreten, nämlich dass "a very small number of companies based outside the European Union could rapidly acquire the same dominant position in the area of in-vehicle services as they already have in the field of data processing, search engines, online services or smartphones. Should this occur, vehicle manufacturers risk being left with stranded investments, a loss of company know-how, commercial secrets and industrial property rights. The consequences for the competitiveness of the autoindustry, service providers and for job and value creation in Europe would be significant".[632] Angesichts der unbestrittenen Marktmacht, die solche Firmen wie Google, Facebook, Amazon oder Microsoft haben, und dem disruptiven Charakter von vernetzten und später autonomen Fahrzeugen, ist das traditionelle Geschäftsmodell der Automobilunternehmen tatsächlich langfristig bedroht, sodass dem Problem der Verfügung über bzw. dem Zugang zu diesen Daten des vernetzten Autos zweifellos eine wichtige strategische Bedeutung zukommen kann.

6.3.2 VERBRAUCHERSCHÜTZER/AUTOMOBILVEREINIGUNGEN

Die zweite zentrale Gruppe von Stakeholdern sind die Kfz-Halter, Autofahrer (und andere Autoinsassen).[633] In Bezug auf ihre Positionen und Interessen kann auf Stellungnahmen von Verbraucherverbänden sowie – noch spezialisierter – von Automobilclubs zurückgegriffen

631 Vgl. ACEA (2016b, 7).

632 ACEA (2016b, 1).

633 Auf die spezifische Problematik der Unterscheidung zwischen Kfz-Halter, Autofahrer und andere Autoinsassen sowie die weitere Komplizierung durch Autoleasing und Car-sharing-Modelle wird hier nicht näher eingegangen.

werden, die sich teilweise wiederum auf Umfragen in Bezug auf Meinungen von Autofahrern stützen.[634] In der FIA Umfrage "What Europeans think about connected cars"[635] haben Autofahrer bezüglich folgender Gefahren Bedenken gegenüber Data Sharing in Bezug auf Daten im vernetzten Autos geäußert: (1) Disclosure of private information (88%), (2) Commercial use of your personal data (86%), (3) Hacking your vehicle to interfere with your driving (85%), (4) Car vehicle tracking (70%) .[636] 83% der Autofahrer denken, dass der Zugang zu den Fahrzeugdaten zeitlich beschränkt sein sollte. 90% der befragten Autofahrer sind der Meinung, dass die Daten, die im Auto generiert werden, dem Fahrer oder dem Eigentümer des Autos gehören sollten. 91% möchten die Möglichkeit der Abschaltung der Konnektivität ihres Autos haben.[637] In Bezug auf das Teilen von Daten bei einem Defekt des Fahrzeugs waren 92% der Meinung, dass sie auswählen können sollten, wer das Fahrzeug repariert. Weiterhin waren 95% der Befragten der Meinung, dass es einen Bedarf für eine spezifische gesetzliche Regelung gibt, um ihre Rechte in Bezug auf das Fahrzeug und ihre Daten zu schützen.[638]

Auch auf der Basis solcher Umfragen haben BEUC und FIA folgende Grundpositionen bezüglich Daten des vernetzten Autos formuliert:
(1) Der Datenschutz wird als besonders wichtig angesehen, wobei auch auf die Schwächen der DS-GVO (Gefahr des Missbrauchs der Abwägung mit "berechtigten Interessen") und der Vorschläge der ePrivacy-Verordnung hingewiesen werden, insbesondere die fehlende Verpflichtung zu "privacy by default" sowie dass "it must ensure that the tracking of the physical location and movements of consumers is not allowed without asking for their consent",[639] was auf die kontroverse Diskussion über die ePrivacy-Verordnung in Abschnitt 4 verweist.
(2) Unabhängig vom Schutz personenbezogener Daten ist das Problem zu klären, wem die Daten von vernetzten Fahrzeugen gehören bzw. wer sie kontrolliert. Dies bedeutet, dass es auch darum geht zu klären, welche Rechte die Autofahrer an den nicht-personenbezogenen Daten ihres vernetzten Fahrzeugs haben. Sowohl BEUC und FIA fordern deshalb eine Klärung der Frage der Kontrolle über Daten, wobei am Ende sicherzustellen ist, dass die Verbraucher die Kontrolle über personenbezogene und nichtpersonenenbezogene Daten ha-

[634] Die folgende Analyse stützt sich primär auf die Positionspapiere des europäischen Verbraucherschutzverbandes BEUC (2017b) als Dachverband nationaler Verbraucherschutzverbände (wie in D der Verbraucherzentrale Bundesverband (vzbv)) und der FIA (2016a) als Dachverband von nationalen Automobilclubs (wie in D dem ADAC) sowie des von der FIA durchgeführten Surveys "What Europeans Think about Connected Cars" (FIA 2016b); vgl. auch ADAC (2015).

[635] Hierbei handelte es sich um eine im Herbst 2015 durchgeführte Online-Befragung, in der jeweils 1000 ausgefüllten Online-Fragebögen in 12 europäischen Ländern.

[636] Vgl. FIA (2016b, 16).

[637] Vgl. FIA (2016b, 11).

[638] Vgl. FIA (2016b, 1).

[639] BEUC (2017, 7).

ben.[640] Damit verknüpft ist auch das in der neuen DS-GVO verankerte Recht auf Datenportabilität, d.h. dass Verbraucher leicht ihre Fahrzeugdaten von einem Serviceanbieter zu einem anderen übertragen können, um die Vorteile der neuen Technologie zu nutzen und um "lock-in"-Effekte zu vermeiden.[641]

(3) Ein weiterer zentraler Komplex bezieht sich auf das Recht von Verbrauchern, frei zwischen unterschiedlichen Service-Anbietern wählen zu können, sowie – damit verknüpft – die Sicherstellung des Wettbewerbs zwischen Service-Anbietern, auch durch innovative Entwicklung neuer Dienstleistungen. Dies bezieht sich unmittelbar auf unabhängige Reparatur- und Wartungsdienstleistungsbetriebe, die von Fahrzeugdaten abhängig werden. Bei der hierfür auch relevanten Reform der Kfz-Typenzulassungs-VO wäre es deshalb wichtig, dass auch die zunehmend bestehenden Möglichkeiten der Ferndiagnose auf der Basis von Realzeit-Zugang zu Fahrzeugdaten (und der Fernreparatur) berücksichtigt werden.[642] Dies würde die Auswahlfreiheit von Konsumenten, die nicht beschränkt sein sollte auf eine Liste von (von den OEMs ausgesuchten) Anbietern, und damit den Wettbewerb zwischen Service-Anbietern stärken.

(4) Alle diese Fragen sind eng mit der Frage der Ausgestaltung des Gesamtrahmens für den Zugang zu Fahrzeugdaten verknüpft. Insofern sieht die FIA den direkten, vollen und privilegierten Zugang zu Fahrzeugdaten durch die Automobilhersteller im "extended vehicle"-Konzept und ihren diskretionären Spielraum, ob unabhängige Firmen Zugang zu Realzeitdaten bekommen oder nicht, auch in Bezug auf Innovationen, sehr kritisch. Insofern fordert die FIA zunächst für eine Übergangsperiode eine weiterentwickelte "shared data server solution" mit einem Governance-Modell, das die Neutralität und den fairen und sicheren Zugang zu sensitiven Daten sichert.[643] Längerfristig aber sollte technisch zu einer „On-board application“-Plattform übergegangen werden. Dies würde zu einem hohen Grad an Innovation, Wettbewerb und größerer Auswahlfreiheit von Verbrauchern führen.[644] Insofern sollte die Kommission einen Gesetzesentwurf für eine "standardised, secure and open access platform" entwickeln, verknüpft mit einem neutralen Zertifizierungssystem bezüglich "safety, security and data integrity", um ein "level playing field" zwischen Autoherstellern und unabhängigen Anbietern herzustellen.

---

[640] Vgl. BEUC (2017, 8) und FIA (2016a, 7). Was allerdings nicht explizit angesprochen wird, ist die weitergehende Frage, ob Verbraucher an dem Wert der von ihren Autos produzierten Daten angemessen beteiligt werden sollten.

[641] Vgl. BEUC (2017, 8).

[642] Vgl. FIA (2016a, 2 und 4). "Adapt the type approval provisions on access to repair and maintenance information to include fair and non-discriminatory remote access to real-time vehicle data" (FIA 2016a, 4).

[643] Vgl. hierzu auch FIA (2015).

[644] Vgl. FIA (2016a, 6 f.).

6.3.3. UNABHÄNGIGE SERVICEANBIETER IM AUTOMOBILEN AFTERMARKT

Die vielfältigen unabhängigen Anbieter von Produkten und Service-Leistungen im automobilen Aftermarkt haben sich als die schärfsten Kritiker des "extended vehicle"-Konzepts der Automobilhersteller herausgebildet. Hierbei geht es um Kfz-Reparatur- und Wartungsbetriebe, um Hersteller von Ersatzteilen und Werkzeugen, aber auch andere Service-Dienstleister (wie bspw. die TÜV-Organisationen). Es sind vor allem diese Stakeholder, die bisher Anspruch auf einen regulierten Zugang zu Reparatur- und Wartungsinformationen nach der Kfz-Typenzulassungsverordnung hatten und darüber auch Diagnosedaten aus dem OBD-Adapter auslesen konnten. Die einschlägigen Verbände haben hierzu eine weitgehend einheitliche Position entwickelt, die viele Parallelen mit der obigen Position von Verbraucherschützern und Automobilclubs aufweist. Mit Hilfe des sehr detaillierten Positionspapiers von FIGIEFA (2016) soll diese Position im Folgenden kurz zusammenfassend charakterisiert werden.[645]

Es wird betont, dass im automobilen Aftermarkt die Fähigkeit zu Innovation und Wettbewerb im digitalen Zeitalter vom kontinuierlichen Zugang zu den im Auto generierten Daten ("in-vehicle data") und der Möglichkeit unabhängiger Unternehmen, ihr Knowhow auch direkt im Fahrzeug anzuwenden, abhängt. "Competition in the digital age starts already in the vehicle where the data quality determines the service quality".[646] "Especially timely data or data in real time around the clock brings about a wide variety of new products and services relating to the operation of vehicles. ... Foreseeable use cases are for example the proactive monitoring of safety-critical vehicle systems, the predictive and thus especially efficient maintenance in the workshop, remote monitoring of operations to prevent defects, remote maintenance through software updates or reconfiguration and automated services in case of a breakdown on the road".[647] Insofern ist der direkte Zugang zu Rohdaten, die nicht bereits von OEMs bearbeitet oder gefiltert sind oder (wegen des externen Servers) nur mit Zeitverzögerung übermittelt werden können, ebenso zentral wie die Möglichkeit, direkt mit dem Fahrzeug zu kommunizieren und Daten austauschen zu können. Das "extended vehicle"-Konzept der Automobilhersteller stellt dagegen ein geschlossenes Telematiksystem dar, dass das Anbieten vieler solcher innovativen Dienstleistungen durch unabhängige Service-Anbieter erschweren oder unmöglich machen würde. Dies liegt zum einen an der Zeitverzögerung des Zugangs zu Daten, die durch den Umweg über den "externen Server" entstehen, zum anderen aber auch an den vielerlei Möglichkeiten, die aus der privilegierten Stellung der Automobilhersteller in Bezug auf die Daten und den Zugang zu den Kunden folgen würden. So könnten bei der "externen Server"-Lösung die Automobilhersteller ein Monitoring sowohl der Datenflüsse zwischen unabhängigen Service-Anbietern und den Fahrzeugen als auch

[645] Vgl. FIGIEFA (2016) sowie AFCAR (2016) und Verband der TÜV (2018).

[646] FIGIEFA (2016,3; Hervorhebung im Original).

[647] FIGIEFA 2016, 3.

der Preise und des Kundenverhaltens in diesen Vertragsbeziehungen betreiben, um diese Informationen zur Gestaltung ihrer eigenen im Wettbewerb dazu angebotenen Leistungen zu nutzen.[648] Vor allem aber hätten die Automobilhersteller immer einen privilegierten sofortigen Zugang zu allen Daten, während den anderen Stakeholdern Daten nur in gefilterter oder aggregierter Form zugänglich gemacht würden.[649] Darüber hinaus könnten die Automobilhersteller über die neben dem Kaufvertrag notwendigen Telematikverträge, die für die Nutzung bestimmter Telematikfunktionen erforderlich sind, andere Service-Anbieter von bestimmten Dienstleistungen ausschließen (Bündelung), oder Exklusivvereinbarungen mit bestimmten Service-Anbietern abschließen.[650]

Welche Forderungen folgen hieraus für unabhängige Service-Anbieter im Automobilsektor? Um wirksamen Wettbewerb und Innovation im automobilen Aftermarkt zu sichern, sei ein robuster rechtlicher Rahmen für den faktischen Zugang zu "in-vehicle data" und für die digitale Interoperabilität der "in-vehicle telematics systems" notwendig. Hierzu gehört der direkte Zugang zu den im Auto generierten Daten in "Realzeit", die Möglichkeit über ein standardisiertes Interface ("interoperability by design"), eigene Apps und Knowhow direkt im Fahrzeug anzuwenden, und gleiche Bedingungen wie die Autohersteller in Bezug auf Zugang zu Daten und dem Dashboard (HMI: Human-Machine-Interface) des Fahrzeugs, um die Möglichkeit zu haben, den Fahrern Dienstleistungen zu gleichen Bedingungen anbieten zu können.[651] Besonders betont wird hierbei, dass es von kleinen und mittleren Unternehmen nicht erwartet werden kann, dies durch Wettbewerbsrecht auf dem Klagewege durchzusetzen. Vielmehr sei eine gesetzliche Lösung für den Automobilsektor notwendig, bei der verbindliche "key functionalities of the in-vehicle telematics system" vorgeschrieben werden sollen, um eine interoperable, sichere und offene Telematikplattform zu schaffen.[652]

6.3.4 KOMPONENTENHERSTELLER, VERSICHERUNGEN UND ANDERE SERVICEANBIETER

Jenseits der unabhängigen Kfz-Reparatur- und Wartungsbetriebe gibt es eine Vielzahl anderer Unternehmen, die Serviceleistungen an die Fahrer bzw. Insassen von vernetzten Autos anbieten möchten und hierfür einen direkten Zugang zum Fahrzeug und den Daten benötigen. Eine Gruppe sind die Hersteller von Komponenten für das Auto, bspw. Hersteller von Reifen, Bremsen, Autoelektrik, oder ganze Fahrassistenzsysteme, in die oft selbst Sensoren

[648] FIGIEFA (2016, 15). Diese Kritik ist bereits ausführlich in der Working Group 6 der C-ITS Plattform diskutiert worden und hat die Automobilhersteller dazu bewogen, zusätzlich die Möglichkeiten der oben bereits erwähnten "neutralen Server" zuzulassen, deren Datenflüsse die Hersteller nicht mehr beobachten können. Vgl. C-ITS (2016, 79 f.).

[649] Vgl. FIGIEFA (2016, 14).

[650] Vgl. FIGIEFA (2016, 15).

[651] Vgl. FIGIEFA (2016, 16).

[652] Vgl. FIGIEFA (2016, 17).

eingebaut sind. Da Komponentenhersteller Zulieferer von Automobilunternehmen sind, bestehen zwischen ihnen und den Automobilherstellern üblicherweise oft langfristige Lieferbeziehungen, die auch von manchmal problematischen bilateralen Macht-Abhängigkeits-Beziehungen gekennzeichnet sein können (Nachfragemacht in Zuliefer-Beziehungen), sodass Automobilzulieferer oft nur beschränkt unabhängig sind. Diese Komponentenhersteller können ein großes Interesse sowohl an den Daten in Bezug auf ihre eigenen Komponente haben (insbesondere für innovative Weiterentwicklungen ihrer Komponenten) als auch an einem direkten Kontakt mit den Kunden im Fahrzeug haben, wenn sie gleichzeitig Reparaturdienstleistungen und Ersatzteile anbieten.[653] Komponentenhersteller können die Frage des Zugangs zu Daten und dem Fahrzeug als Teil ihrer gesamten vertraglichen Vereinbarungen mit den Autoherstellern aushandeln. Probleme können hierbei aber durch asymmetrische Verhandlungsmacht entstehen.[654] Der europäische Verband der Automobilzulieferer CLEPA (2016) hat sich in ihrem Positionspapier ebenfalls für eine interoperable standardisierte und sichere "in-vehicle open telematics platform" ausgesprochen, um fairen Wettbewerb in Bezug auf die Service-Anbieter zu sichern, sowie das Recht der Verbraucher, selbst zu entscheiden, wem sie Zugang zu den Fahrzeugdaten für Diagnostik, Reparatur und Wartung sowie andere Zwecke geben möchten. Hierbei wird betont: "All relevant in-vehicle information should be accessible to third parties for service development and future business models".[655]

Eine andere wichtige Gruppe von Stakeholdern stellen die Versicherungen dar. Insbesondere Daten über das Fahrverhalten von Autofahrern eröffnen viele Möglichkeiten, neue Arten von Kfz-Versicherungen anzubieten (bspw. used-based insurance), wodurch einerseits bessere Klassifizierungen unterschiedlicher Risiken und damit stärker risikoäquivalente Prämiensysteme möglich sind, andererseits aber auch durch die stärkere Überwachung Anreize gesetzt werden, vorsichtiger zu fahren, wodurch Unfallzahlen vermindert und die Verkehrssicherheit erhöht werden kann.[656] Zusätzlich sind Versicherungen aber auch an vielfältigen anderen Daten über Strassenverhältnisse, aktuelle Wetterbedingungen etc. interessiert, um

[653] So verbindet das Bosch smartphone app "fun2drive" über Bluetooth direkt zum OBD Adapter des Fahrzeugs, so dass bestimmte Funktionen des Autos direkt über das Smartphone kontrolliert werden und Kunden über den nächsten Bosch Reparaturservice informiert werden können (vgl. McKinsey 2014, 216 ff., Bosch 2013).

[654] Vgl. zu diesem Verhältnis zwischen Komponentenherstellern und Automobilunternehmen ausführlicher Frank/Kerber (2017, 30 ff.)

[655] CLEPA (2016). In einer späteren gemeinsamen Stellungnahme des europäischen Automobilverbands (ACEA) mit CLEPA (ACEA/CLEPA 2016) hat sich CLEPA stärker an die Position der Automobilhersteller angeschlossen.

[656] Vgl. zum schwierigen Problem des Schutzes der Privatsphäre und einer empirischen (experimentellen) Studie, wie Verbraucher mit dem Zielkonflikt zwischen Schutz der Privatsphäre und niedrigeren Kfz-Versicherungsprämien umgehen, Derikx et al (2016).

den Autofahrern bspw. über Informationen zu helfen, Unfälle zu vermeiden.[657] Der europäische Verband von Versicherungsunternehmen (InsuranceEurope) hat sich ebenfalls der Koalition von Verbänden angeschlossen, die eine interoperable in-vehicle Telematik-Plattform unterstützen[658] und auch explizit die EU-Kommission aufgefordert, eine gesetzliche Regelung zu verabschieden "on access to in-vehicle data and resources before the end of 2018, enabling service providers to offer their products to drivers inside the vehicle, free from interference by vehicle manufactureres".[659] Insurance Europe unterstützt auch eine öffentliche Online-Petition "#Data4Drivers", die die europäische Politik auffordert, "to act to ensure that drivers - rather than vehicle manufacturers - control who can access their vehicle data and for what purpose".[660] Über die Versicherungen hinaus finden sich in der erwähnten Koalition von Verbänden, die sich für eine interoperable in-vehicle Telematik-Plattform aussprechen auch eine Anzahl weiterer Verbände, die zusätzliche Stakeholder umfassen wie bspw. Autoleasingunternehmen und TÜV-Organisationen.[661]

6.4 ZUSAMMENFASSENDE ANALYSE VON ARGUMENTATIONSMUSTERN UND INTERESSEN

Auch in diesem Abschnitt ist es nicht die Aufgabe, eine Analyse in Bezug auf die richtige regulatorische Lösung zu machen. Vielmehr geht es wiederum um eine Analyse der Argumentationen, die in dieser Diskussion von den beteiligten Stakeholdern mit ihren spezifischen Interessen vorgebracht werden. Schon in der Konsultation zur Mitteilung "Building a European data economy" ist der Automobilsektor mit besonders vielen Beschwerden über Probleme und ungleichgewichtige Verhandlungssituationen in Bezug auf den Zugang zu Daten aufgefallen. Die Konflikte zwischen Stakeholdern sind hier noch wesentlich klarer strukturiert als in der Diskussion über die ePrivacy-Verordnung. Auf der einen Seite stehen die Automobilhersteller, die mit ihrem "extended vehicle"-Konzept ein geschlossenes Telematiksystem entwickelt haben, durch das sie die exklusive Kontrolle über den Zugang zum Fahrzeug und den in ihm generierten Daten erhalten und (mit Ausnahme des regulierten Zugangs für Reparatur- und Wartungsinformationen nach der Kfz-Typenzulassungs-VO) Zugang zu diesen Daten nur nach frei ausgehandelten B2B-Vereinbarungen gewähren. Auf der anderen Seite stehen im Wesentlichen alle anderen wichtigen Stakeholder, von den Verbraucherschutzverbänden, den unabhängigen Aftermarkt-Service-Anbietern, Kfz-Versicherern, und anderen unabhängigen Service-Anbietern, die den Kfz-Insassen ihre Dienstleistungen im vernetzten Auto anbieten wollen und deshalb gerne direkten (nicht von den Autoherstellern kontrollierten) Zugang zum Fahrzeug, den in ihm generierten Daten und den Kfz-Insassen hätten, um

[657] Vgl. zu den Verwertungsmöglichkeiten der Daten des vernetzten Autos für Versicherungen HERE&ReSwiss (2016).
[658] Vgl. ADPA et al (2017).
[659] Vgl. Insurance Europe (2018).
[660] Vgl. die Webseite https://www.data4drivers.eu.
[661] Vgl. ADPA et al (2017).

mit ihnen Verträge schließen zu können. Auf der technischen Ebene geht es darum, ob die Telematiksysteme proprietäre und geschlossene Systeme der einzelnen Autohersteller sind oder ob – wie mit dem Konzept der „On-board application"-Plattform – interoperable offene Telematikplattformen entwickelt werden, die einen sicheren, direkten Zugang unter der Kontrolle der Kfz-Fahrer zulassen. Selbstverständlich sind auch kompromisshafte Zwischenlösungen (auch für eine Übergangszeit) denkbar, wie insbesondere geschlossene Systeme, bei dem die Daten auf einen (nicht vom Autohersteller kontrollierten) externen "shared server" übertragen werden, der Daten diskriminierungsfrei an alle Stakeholder zugänglich machen kann, oder die Kombination des "extended vehicle"-Konzepts mit weitreichenden Regulierungen zur Begrenzung der Missbrauchsmöglichkeiten, die evtl. aus der exklusiven Verfügung über die Daten folgen könnten. In diesem Zusammenhang könnte dann auch auf die Instrumente des Wettbewerbsrechts zurückgegriffen werden.[662]

Interessanterweise stützt sich die Automobilindustrie für die Verteidigung ihres Konzepts (fast) ausschließlich auf das Argument, dass nur mit ihrem geschlossenen Modell der im Grunde von allen als notwendig anerkannte hohe Standard im Hinblick auf die Sicherheit des Fahrzeugs und des Datenschutzes erreicht werden kann. Dieses technische Argument ist aber umstritten und auch die von der Kommission in Auftrag gegebene TRL-Studie kommt zu dem Schluss, dass die Sicherheit auch mit den anderen Lösungen gewährleistet werden kann. Die Automobilindustrie verteidigt ihre exklusive Verfügung über die Daten und die sich aus deren kommerziellem Wert ergebenden zusätzlichen Gewinne jedoch nicht direkt. Die Automobilhersteller argumentieren nicht, dass diese Daten ihnen zur weiteren exklusiven Verwertung aufgrund ihrer Verträge mit den Kunden zustehen, in denen sie sich die Zustimmung zur Nutzung der personenbezogenen Daten einholen, oder mit dem Argument einer – wie auch immer genau begründeten – Beteiligung an der Generierung dieser Daten.[663] Beispielsweise bestand eine der Varianten des "data ownership rights" in der Konsultation über die Mitteilung "Building a European data economy" darin, dass das exklusive Recht zur Lizenzierung dem Hersteller eines smarten Geräts zugeordnet werden kann. Solche oder ähnliche Begründungen finden sich in den Argumentationen der Automobilindustrie nicht. Es wird lediglich auf einer sehr allgemeinen Ebene der Argumentation darauf verwiesen, dass für den Übergang zu vernetzten und später autonomen Fahrzeugen sehr hohe Investitionen notwendig sind, insbesondere für die Entwicklung und die laufenden Kosten der IT-Systeme und der Kommunikationsinfrastruktur und dass sich diese Investitionen langfristig amortisieren müssen. Hierbei ist jedoch aus ökonomischer Sicht zu bedenken, dass diese Investitionen – wie auch sonst bei neuen innovativen Technologien im Auto – über den Verkaufspreis der vernetzten Fahrzeuge an die Verbraucher finanziert werden können und es

[662] Vgl. für erste Überlegungen zu einer expliziten ökonomischen Analyse der Beziehungen zwischen verschiedenen Stakeholdern und den dabei möglicherweise auftretenden Marktversagensproblemen Frank/Kerber (2017).

[663] Allerdings wird zu Recht darauf verwiesen, dass für bestimmte Arten von technischen Daten im Fahrzeug tatsächlich gut begründete Ansprüche aus IPR, dem Geschäftsgeheimnis- und Knowhow-Schutz bestehen können.

dann von der Wertschätzung der Verbraucher abhängig ist, ob diese bereit sind, für die zusätzlichen Vorteile einen entsprechend höheren Fahrzeugpreis zu zahlen.

Mehr Wettbewerb, mehr Innovationen und eine größere Auswahlfreiheit der Verbraucher sind dagegen die zentralen Argumente der vielen anderen Stakeholder, die entweder direkt im automobilen Aftermarkt tätig sind oder durch das Anbieten von zusätzlichen Dienstleistungen direkten Zugang zum vernetzten Auto und/oder den in ihm generierten Daten haben möchten. Auch wenn die dadurch in Zukunft möglichen Innovationen heute nur begrenzt abschätzbar sind, besteht ein breiter Konsens darin, dass das innovative Potential sehr hoch ist, was sich an vielen bereits sehr konkreten, zusätzlichen Dienstleistungen wie "remote maintenance" und "remote monitoring" zeigt, die einen solchen direkten Zugang benötigen. Interessanterweise ergeben sich aus ökonomischer Sicht dabei auch keine systematischen Unterschiede, ob es sich um direkte Aftermarktdienstleistungen wie Reparatur und Wartung handelt oder um andere Services, die ökonomisch als komplementäre Leistungen zum vernetzten Fahren zu verstehen sind, wie bspw. Navigationsleistungen oder Entertainmentangebote im Auto. Auch wenn hier keine systematische wettbewerbsökonomische Analyse durchgeführt werden kann, so ist doch festzustellen, dass die von den unabhängigen Serviceanbietern in Bezug auf einen fairen und unverzerrten Wettbewerb geäußerten Bedenken gerechtfertigt sein können, wenn die Automobilhersteller über das "extended vehicle"-Konzept eine solche exklusive Kontrolle über den Zugang zum Fahrzeug und den in ihm generierten Daten gewinnen. Die sich hieraus ergebende "Datenmacht"-Stellung könnte unter Umständen von ihnen tatsächlich dazu benutzt werden, um sich durch Verweigerung des Zugangs zu bestimmten Daten bestimmte Service-Leistungen selbst vorzubehalten und alle anderen Serviceanbieter auszuschließen, sich durch hohe Datenzugangspreise Vorteile im Wettbewerb auf den nachgelagerten Service-Märkten zu verschaffen oder auch Serviceanbieter auszuschließen, indem mit einzelnen Serviceanbietern Exklusivvereinbarungen abgeschlossen werden. Sehr zweifelhaft ist auch, ob die exklusive Verfügung über die Daten des vernetzten Autos durch die Autohersteller dazu führt, dass insgesamt mehr von diesen Daten der allgemeinen Datenökonomie für andere (außerhalb des Automobilsektors liegende) Zwecke zur Verfügung gestellt werden, als dies bei offeneren Systemen der Fall wäre.

Auf den ersten Blick erscheinen deshalb offene Systeme (wie es eine „On-board application"-Plattform erlauben würde), geeigneter zu sein, um mehr Wettbewerb, Innovation und Auswahlfreiheit für Verbraucher sicherzustellen. Allerdings ist dies aus ökonomischer Sicht nicht so eindeutig. Hierbei sind insbesondere zwei verschiedene Argumente zu bedenken. In der Ökonomie wird seit längerem die Diskussion geführt, ob Interoperabilität und offene Systeme generell proprietären geschlossenen Systemen vorzuziehen sind und folglich – insbesondere auch durch Standardisierung – Interoperabilität gefördert oder sogar obligatorisch gemacht werden sollte, gerade auch zur Ermöglichung von mehr Innovationen. Tatsächlich aber kann nicht allgemein gezeigt werden, dass offene interoperable Systeme immer geschlossenen proprietären System überlegen sind, insbesondere weil Unternehmen mit eigenen proprietären Systemen wesentlich differenziertere und evtl. auch qualitativ höherwertige Produkte oder Dienstleistungen entwickeln können, während Interoperabilität und

Standardisierung üblicherweise zu einer stärkeren Homogenität führt. Insofern können sowohl offene, als auch geschlossene Systeme unter Umständen vorteilhaft für Innovationen sein, so dass hierfür eine tiefere Analyse notwendig ist.[664] Es ist allerdings interessant festzustellen, dass die Automobilhersteller nicht damit argumentieren, dass durch ihre geschlossenen Telematiksysteme mehr oder bessere Innovationen im Aftermarkt oder bei komplementären Dienstleistungen entstehen würden. Das zweite gewichtige Argument besteht darin, dass die einzelnen Automobilhersteller keine marktbeherrschenden Unternehmen sind, sondern in Bezug auf ihr Angebot von vernetzten Autos im Wettbewerb zueinanderstehen. Insofern könnte argumentiert werden, dass die Kunden bei der Wahl eines Fahrzeugs auch die zukünftigen, mit dem Fahrzeug verknüpften Aftermarktservices und komplementären Serviceangebote einbeziehen, so dass ein Wettbewerb zwischen den Bündeln von Fahrzeugen und dazugehörigen Serviceangeboten stattfindet (Systemwettbewerb).[665] In diesem Fall hätten die Automobilhersteller Anreize, attraktive Bündel von Fahrzeugen und Serviceangeboten anzubieten. Insofern könnte ein intensiver Wettbewerb zwischen den Automobilherstellern um die Kunden mit möglichst attraktiven Bündeln von Leistungen auch zu sehr offenen Systemen mit viel Wettbewerb und Innovation von unabhängigen Serviceanbietern führen, ohne dass weitgehende regulatorische Lösungen hierfür erforderlich sind. Auch hier ist eine tiefere ökonomische Analyse erforderlich, ob solch ein wirksamer Wettbewerb vorliegen kann oder an welchen Marktversagensproblemen er scheitern könnte. Beide hier aufgeworfene Fragen, nämlich die Frage nach den Vor- und Nachteilen von offenen und geschlossenen Systemen für Innovation und die Frage nach der Wirksamkeit des Wettbewerbs zwischen Automobilherstellern wird in der bisherigen Diskussion über den Zugang zu Daten des vernetzten Autos zu wenig diskutiert.

Die zentrale Frage in der gegenwärtigen Diskussion ist aber, ob geschlossene, proprietäre Systeme mit der exklusiven Kontrolle durch die Automobilhersteller wie im "extended vehicle"-Konzept notwendig für die Sicherheit sind, sowohl in Bezug auf die Cybersicherheit als auch in Bezug auf die Fahrsicherheit. Auch wenn Verbraucherverbände auf die Wichtigkeit von Wettbewerb im Aftermarkt-Bereich und anderen Dienstleistungen hinweisen und diesbezüglich eine möglichst große Auswahlfreiheit für die Verbraucher fordern, so ist auch unbestritten, dass für die Autofahrer eine hohe Sicherheit von sehr großer Bedeutung bei dem Kauf von vernetzten Autos ist. Insofern ist in der Diskussion – zumindest implizit – relativ deutlich, dass bei einem echten Konflikt zwischen den Zielen Sicherheit und Wettbewerb und Innovation dem Ziel Sicherheit eine relativ größere Bedeutung zukommt. Die entscheidende und strittige Frage besteht deshalb nicht darin, wie beim Bestehen eines solchen Zielkonflikts entschieden werden sollte, sondern darin, ob überhaupt ein solcher Zielkonflikt besteht, d.h. ob die Behauptung der Automobilindustrie zutrifft, dass nur durch ein solches geschlossenes System unter der exklusiven Kontrolle des Herstellers der notwendige hohe

[664] Vgl. hierzu ausführlicher Kerber & Schweitzer (2017, 42 ff.) mit weiterer ökonomischer Literatur.

[665] Im Wettbewerbsrecht würde man dann den relevanten Markt anders abgrenzen. Vgl. hierzu Wegner (2010, 1805).

Grad an Sicherheit erreichbar ist. Dies ist allerdings umstritten und die von der Kommission in Auftrag gegebene TRL-Studie kam zu dem Schluss, dass die notwendige Sicherheit auch mit den anderen technischen Lösungen, insbesondere auch mit einer offenen "On-board application"-Plattform erreicht werden kann, wenn auch eventuell zu höheren Kosten.[666] Allerdings kann es hierfür erforderlich sein, dass Software und Apps, die von außen direkt auf das Fahrzeugen zugreifen, verbindliche Mindeststandards erfüllen und deshalb vom Automobilhersteller zertifiziert sein müssen und dass es notwendig sein kann, sicherheitskritische Funktionalitäten und Daten von anderen streng zu separieren, bspw. durch den Einsatz von Hypervisor-Technologien.[667] Aus solch einer für die Sicherheit notwendigen technologischen Kontrolle von Mindestsicherheitsstandards durch die Automobilhersteller folgt jedoch in keiner Weise, dass sie frei darüber entscheiden können sollen, wer Zugang zu dem vernetzten Fahrzeug und seinen Daten bekommt, und diesen Zugang kommerziell durch freie B2B-Vereinbarungen verwerten können. Die technische Kontrolle in Bezug auf die Sicherheit kann von der ökonomischen Kontrolle des Zugangs zum Fahrzeug und den in ihm generierten Daten getrennt werden. Dies wäre gerade mit dem Konzept der „On-board application"-Plattform verbunden. Darüber hinaus muss in Bezug auf Sicherheit berücksichtigt werden, dass für die langfristige Entwicklung von übergreifenden, intelligenten Mobilitätskonzepten des vernetzten und autonomen Fahrens herstellerübergreifende technische Standards, insbesondere in Bezug auf Sicherheit, entwickelt werden müssen, um die Kommunikation von Fahrzeugen zu Infrastruktur und zu anderen Fahrzeugen zu ermöglichen. Aus dieser Perspektive ist fraglich, ob das Konzept herstellerspezifischer, proprietärer Lösungen für Sicherheit überhaupt langfristig zukunftsfähig ist oder ob die Frage der Sicherheit (mit Standards und Zertifizierungen) aber auch der Governance der Daten des vernetzten und autonomen Fahrens nicht eher auf der Ebene des gesamten integrierten Mobilitätssystems gelöst werden muss. Auch bezüglich dieser Fragen steht die bisherige Diskussion erst am Anfang.

Eine weitere Diskussion, die in Bezug auf Daten des vernetzten Autos noch unterentwickelt ist, bezieht sich auf die Frage der konkreten Ausgestaltung des Datenschutzes von Autofahrern und deren Verfügungsmacht über Daten. Obwohl allgemein anerkannt wird, dass die meisten der im Fahrzeug erhobenen Daten (auch wegen der Verknüpfung mit der Fahrzeugidentifikationsnummer) personenbezogene Daten sind und auch in den C-ITS Prinzipien der Schutz der Privatsphäre eines der zentralen anerkannten Ziele ist, so hat sich bisher die Diskussion fast ausschließlich auf den Konflikt zwischen den Automobilherstellern und den anderen Unternehmen bezogen, während die Verbraucher mit ihrem Interesse an dem Schutz ihrer Privatsphäre und ihrem eventuellen Interesse, an dem Wert der im Fahrzeug generierten Daten beteiligt zu werden, wenig thematisiert worden sind. Dabei ist zunächst festzu-

[666] Vgl. TRL (2017, 8 f.); vgl. zur grundsätzlichen Diskussion von Cybersicherheit bei offenen und geschlossenen System Perens & Determann (2017).

[667] Vgl. ausführlicher TRL (2017, 77). "A hypervisor manages the separate execution of software tasks: in this contet allowing the management of messages to vehicle ECUs and the prevention of unauthorised access to safety-critical ECUs or to functions that are not authorised for the application" (TRL, 2017, 9).

stellen, dass der in der ePrivacy-Diskussion so massiv aufgetretene Konflikt zwischen der Privatsphäre der individuellen Personen und der datenverarbeitenden Wirtschaft in gleicher Weise auch hier auftritt. In dieser Beziehung haben die Automobilhersteller und die vielen anderen Serviceanbieter gleichgerichtete Interessen. Sie alle sind daran interessiert, Zugang zu möglichst vielen personenbezogenen Daten zu bekommen, um diese dann für personalisierte Dienste oder in pseudonymisierter oder anonymisierter Form weiterverarbeiten und nutzen zu können. Auffallend ist in der Diskussion, dass zwar in den C-ITS Prinzipien das Recht der Autofahrer betont wird, selbst darüber zu entscheiden, ob und wann sie welche Daten zur Verfügung stellen, aber dass die Frage der konkreten Ausgestaltung, insbesondere wie granular diese Entscheidungen getroffen werden können, und – damit verknüpft – wiederum die schwierige Problematik der Anforderungen an die Einwilligung und die generelle Funktionsfähigkeit von "notice and consent"-Lösungen (und ein eventuell daraus folgender weiterer Regulierungsbedarf) nicht systematisch thematisiert werden. Auch hier stellen sich Fragen der konkreten Ausgestaltung, zum einen ob und wenn ja, welche Daten ohne explizite Einwilligung der Verbraucher verarbeitet werden dürfen, wie spezifisch notwendige Einwilligungen sein müssen, wie lange sie gültig sind, und in welchem Umfang Opt-in oder Opt-out-Lösungen möglich sind oder sein sollen. In ähnlicher Weise wie in der ePrivacy-Diskussion wird die konkrete Ausgestaltung solcher Regeln die Menge der Daten des vernetzten Autos, die zur weiteren wirtschaftlichen Verwertung verfügbar sind, beeinflussen ebenso wie sie sich umgekehrt auf den Umfang des Schutzes der Privatsphäre von Autofahrern auswirken werden.[668]

Wenig explizit thematisiert wird auch die Frage, wem die nicht-personenbezogenen Daten (insbesondere auch die anonymisierten personenbezogenen Daten) "gehören" sollen bzw. wer die Verfügungsmacht über diese Daten haben soll. Der BEUC hat zwar die Frage nach den Rechten der Verbraucher an den nichtpersonenbezogenen Daten gestellt, aber trotz der kampagnenartigen Zuspitzungen wie "MyCarMyData"[669] wird diese Frage auch von den Verbraucherschutzverbänden noch vage und vorsichtig diskutiert.[670] Insbesondere die aus ökonomischer Sicht naheliegende Frage, ob und wie die Autofahrer an dem kommerziellen Wert der in ihren Fahrzeugen generierten Daten beteiligt werden, wird in dieser Diskussion nicht wirklich gestellt.[671] Auch wird in dieser Diskussion keine Beziehung zu dem im Kontext der Mitteilung "Building a European data economy" gemachten Vorschlag eines "Datenerzeugerrechts", das nach diesem Vorschlag eigentlich dem Eigentümer bzw. Nutzer des da-

[668] Vgl. zu dieser Problematik auch Akalu (2018).

[669] Vgl. FIA (2016a).

[670] Vgl. BEUC (2017b, 8).

[671] Dies gilt sowohl für die Diskussion auf der C-ITS Plattform als auch für die ansonsten sehr umfassende TRL-Studie (TRL 2017). Für eine ökonomische Überlegung, dass im Falle der Interpretation der Einwilligung in die Datenverarbeitung als "Daten als Gegenleistung" dies Auswirkungen auf den (monetären) Preis von vernetzten Autos, insbesondere bei Vorliegen von Wettbewerb, haben müsste (mit der Folge von niedrigeren Preisen) vgl. Frank/Kerber (2017, 27 ff.).

tensammelnden Geräts (hier: dem Auto) zugewiesen werden soll, hergestellt.[672] Die Frage, ob die Autohersteller oder die Verbraucher die faktische Verfügungsmacht über diese Daten erhalten sollen, verweist auch wieder zurück zur technologischen Grundentscheidung zwischen proprietären geschlossenen und offenen Systemen, da die technologische Lösung einer "On-board application"-Plattform zumindest die Möglichkeit einräumt, dass die Verbraucher die Kontrolle über die Daten und ihre Verwendung ausüben können. Besonders interessant ist in diesem Zusammenhang auch die Frage nach der Reichweite des neuen "Rechts der Datenportabilität" (Art. 20 DS-GVO) im Automobilsektor. Insofern die Verbraucher über dieses Recht Daten des vernetzten Autos an andere Unternehmen übertragen können, können sie auch die Kontrolle über diese Daten zumindest zum Teil gewinnen und gleichzeitig unter Umständen auch Zugangsprobleme anderer Stakeholder, deren Dienst sie in Anspruch nehmen möchten, lösen.[673] Die Frage, inwieweit dieses Instrument der Datenportabilität für solche Zwecke rechtlich und auch faktisch eingesetzt werden kann, ist ebenfalls ein wichtiger Bereich für stärkere Forschung und Diskussion in der Zukunft.

Fazit: Die Frage der adäquaten rechtlichen Regelungen bezüglich der Daten des vernetzten Autos ist sowohl aus Gründen des Schutzes der Privatsphäre als auch aufgrund des ökonomischen Gewichts des Automobilsektors von besonderer Brisanz. Gleichzeitig liegt hier eine besonders komplexe Problematik sowohl in Bezug auf technologische Fragen (einschl. Sicherheit) als auch in Bezug auf die Vielfalt der Interessen von Stakeholdern an diesen Daten (einschl. öffentlicher Interessen wie Verkehrsregelung und -sicherheit) vor, die es nahelegen, hier nach einer sektorspezifischen Lösung für die Governance dieser Daten zu suchen.[674] Auch wenn es hierzu noch wesentlich tieferer Analysen bedarf, so weisen doch die bisherigen Studien und ökonomischen Überlegungen darauf hin, dass das von den Autoherstellern favorisierte "extended vehicle"-Konzept mit einer exklusiven Kontrolle der Autohersteller über den Zugang zum vernetzten Auto und die in ihm generierten Daten mittel- und langfristig nicht zu einer adäquaten Lösung führt. Die Schwierigkeit jeglicher weitreichenderer Lösungen, wie die Etablierung von offenen Telematikplattformen, besteht jedoch darin, dass dies eine Regulierung auf der technologischen Ebene erfordern würde, die besondere Probleme in ihrer praktischen Umsetzung aufwirft. Allerdings ist abzusehen, dass der Übergang zu den angestrebten integrierten intelligenten Mobilitätssystemen der Zukunft die Einführung von herstellerübergreifenden, interoperablen Schnittstellen und Standards (insbesondere auch bezüglich Sicherheit) notwendig macht. Es ist jedoch auch zu prüfen, ob und inwieweit die Probleme durch bestehendes Wettbewerbsrecht gelöst werden könnten. Allerdings gilt zu berücksichtigen, dass bei der Suche nach geeigneten Datengovernance-Lösungen nicht nur auf die Konflikte zwischen den Automobilherstellern und den unabhängigen Ser-

[672] Aus dieser Sicht ist dann für diese Diskussion hier die in der Konsultation zu "Building a European data economy" gestellte Frage interessant, ob der Hersteller oder der Nutzer oder beide Rechte an diesen Daten haben sollten.

[673] Vgl. Schweitzer/Peitz (2017, 78 ff).

[674] Vgl. Frank/Kerber (2017) und Drexl (2017, 419).

vice-Anbietern abzustellen ist, sondern auch auf die auftretenden Probleme im Verhältnis zu den Verbrauchern. Dies betrifft sowohl die Frage der Ausgestaltung von Einwilligungslösungen als auch der Partizipation an den ökonomischen Vorteilen der produzierten Daten. Insofern könnten hierfür auch verbraucher- und datenschutzrechtliche Lösungen relevant werden.

7. ZUR DISKUSSION ÜBER RECHTE AN DATEN IN DEN USA

In Teil I dieses Gutachtens wurde bereits eine rechtsvergleichende Untersuchung in Bezug auf die rechtliche Regelung von Rechten an Daten in den USA vorgenommen. Hierbei zeigte sich, dass zum einen recht ähnliche Fragen und Lösungen auftreten, wie bspw. bei Abwehrrechten oder beim Schutz von Daten als Geschäftsgeheimnisse, zum anderen zeigten sich aber auch gravierende Unterschiede. Dies betrifft bspw. den in den USA nicht existierenden sui-generis-Datenbankschutz, aber vor allem auch die völlig unterschiedlichen Regelungen in Bezug auf den Schutz der Privatsphäre, da es keinen zum europäischen Datenschutzrecht vergleichbaren Rechtsrahmen für den Datenschutz in den USA gibt. Insofern stellen sich viele Fragen in Bezug auf die Verarbeitung von personenbezogenen Daten in den USA völlig anders. Allerdings gibt es dadurch nicht nur sehr unterschiedliche Diskussionen in Bezug auf den Umgang mit personenbezogenen Daten in der digitalen Ökonomie, sondern erhebliche Unterschiede ergeben sich auch in Bezug auf nichtpersonenbezogene Daten. So ist es vor dem Hintergrund der intensiven Diskussion in Europa über Dateneigentum und die Einführung eines Datenerzeugerrechts, wie dies insbesondere auch in der Mitteilung der Kommission "Building a European data economy" als Option vorgeschlagen wurde, überraschend, dass es in den USA keine vergleichbaren politischen Diskussionen gibt. Dies ist deshalb bemerkenswert, weil die USA in der Entwicklung der digitalen Ökonomie eine Vorreiterrolle haben, so dass solche Fragen eher früher als in Europa hätten diskutiert werden müssen, wenn sie tatsächlich ein großes Problem für eine wohlfunktionierende Datenökonomie darstellen würden. Insofern zeigt sich, dass zwischen Europa und den USA offensichtlich sowohl in Bezug auf personenbezogene als auch nichtpersonenbezogene Daten erhebliche Unterschiede in den Diskussionen über adäquate rechtliche Regeln für eine digitale Wirtschaft bestehen. Es war nicht Ziel dieses Teils des Gutachtens, die zu den Diskussionen in den Abschnitten 4 - 6 korrespondierenden Diskussionen in den USA mit ihren jeweiligen Politikvorschlägen, Stakeholdern und Argumentationen zu identifizieren und analysieren. Vielmehr soll in diesem kurzen Abschnitt nur herausgearbeitet werden, ob und inwiefern es vergleichbare Diskussionen gibt oder weshalb bestimmte Diskussionsprozesse ganz anders verlaufen.

Die sehr unterschiedliche grundsätzliche Herangehensweise an den Schutz der Privatsphäre zwischen Europa und den USA ist seit langem in der wissenschaftlichen Literatur ausführlich diskutiert worden, auch durch die Probleme des Austausches personenbezogener Daten zwischen Europa und USA. Wie bereits in Teil I dieses Gutachtens dargestellt, wird der Schutz der Privatsphäre mit dem Prinzip der informationellen Selbstbestimmung als ein

Grundwert (fundamental value) im Sinne der Grundrechtscharta der EU gesehen, woraus sich starke und weitreichende Rechte der Individuen in Bezug auf die Verarbeitung ihrer personenbezogenen Daten ableiten. Dies gibt es nicht in vergleichbarer Form in den USA.[675] Dort wiederum wird dagegen das Recht der Meinungsfreiheit (First Amendment der US-Verfassung) als zentrales Grundrecht gesehen, woraus sich starke Rechte in Bezug auf die Freiheit, Informationen zu sammeln und zu verbreiten, abgeleitet werden. Hieraus ergibt sich eine grundsätzlich unterschiedliche Einstellung zu einer (gerade auch auf der Nutzung personenbezogener Daten basierenden) digitalen Wirtschaft. Dies bedeutet allerdings nicht, dass in den USA dem Schutz der Privatsphäre keine Bedeutung zukommt. Tatsächlich gibt es in den USA eine Fülle von rechtlichen Regelungen zum Datenschutz. Allerdings sind diese nicht Teil eines konsistenten rechtlichen Gesamtrahmens, wie er in Europa entwickelt worden ist (und jetzt nochmals systematisch in der in Kraft tretenden Datenschutz-Grundverordnung neu verankert wurde). Vielmehr liegt in USA ein stark fragmentiertes System von Datenschutzregelungen vor, die oftmals sektorspezifisch sind und/oder in den einzelnen Bundesstaaten unterschiedlich sind oder sich in anderen Rechtsbereichen wie bspw. in der Verbraucherpolitik finden.[676] Umgekehrt haben wir auch gesehen, dass in der EU trotz der auf dem ersten Blick sehr weitgehenden Datenschutzrechten zugunsten von Individuen durch die Möglichkeiten der Einwilligung, sowie über Legalausnahmen wie die Abwägung mit "berechtigten Interessen" und die Anonymisierung (bzw. Pseudonymisierung) von Daten eine Weiterverarbeitung von Daten für die Zwecke der Datenökonomie möglich ist. Trotzdem kann kein Zweifel daran bestehen, dass die Möglichkeiten des Zugangs zu personenbezogenen Daten und deren Weiterverarbeitung in den USA wesentlich größer sind als in Europa,[677] insbesondere nach dem Inkrafttreten der neuen DS-GVO.[678]

Als Beispiel für die unterschiedlichen Möglichkeiten kann die Regulierungsdiskussion in den USA über Cookies und Tracking herangezogen werden. Zunächst wird die Frage der Zulässigkeit von Cookies und Tracking des Surfverhaltens in den USA von der Verbraucherpolitik thematisiert. Insbesondere die Federal Trade Commission hat sich als Verbraucherschutzbehörde in diversen Untersuchungen und Politikinitiativen mit der Frage beschäftigt, ob und inwieweit Regeln für Cookies und Tracking notwendig sind. Allerdings haben sich die USA primär auf die Herausgabe von Empfehlungen an Unternehmen beschränkt (pri-

[675] Vgl. zu den unterschiedlichen Ansätzen bzgl. Datenschutz in der EU und USA Tsesis (2014), Gautam (2015) und Zarsky (2017).

[676] Beispielsweise gibt es spezielle Privacy-Regelungen im Bereich von Kreditmärkten sowie im Gesundheitssektor. Auch haben die Bundesstaaten teilweise weitgehende Regelungen zum Schutz der Privatsphäre wie bspw. insbesondere Kalifornien. Vgl. zu sektorspezifischen Regelungen mit weiterer Literatur insbesondere Acquisti et al (2016, 469 ff.) sowie Teil I des Gutachtens auf S. 61 ff.

[677] Allerdings zeigt die öffentliche Diskussion in den USA über den aktuellen "Facebook-Skandal", dass der Schutz der Privatsphäre auch in den USA ein wichtiges Thema ist und Fragen über die Notwendigkeit von stärkeren Regulierungen zum Schutz von "Privacy" aufwirft.

[678] Zarsky (2017) stellt die Frage, ob die DS-GVO überhaupt mit einer Datenökonomie im Sinne von Big Data vereinbar ist.

vacy framework).[679] Diese beziehen sich auf "privacy by design", Transparenz (klarere "privacy notices", Information über gespeicherte Daten) und „Do Not Track"-Einstellungen. Darüber hinaus sollten Unternehmen nur in vernünftigem (reasonable) Umfang Daten sammeln, vernünftige Politiken bzgl. der Speicherung von Daten verfolgen und auch in vernünftiger Weise auf die Korrektheit von Konsumentendaten achten. Allerdings handelt es sich hierbei nur um Empfehlungen. Die FTC hat auch eine umfangreiche Untersuchung über die Aktivitäten von Data Brokern durchgeführt, die aufzeigt, in welchem großen Umfang in den USA Daten von Data Brokern über Konsumenten gesammelt werden.[680]

In Bezug auf nicht-personenbezogene Daten ist zunächst festzustellen, dass die Daten, die in den USA Regeln zum Schutz der Privatsphäre unterliegen, wesentlich enger definiert sind als in der EU mit der sehr weitgefassten Definition von personenbezogenen Daten im europäischen Datenschutzrecht. Insofern ist in den USA die Klasse von nicht Datenschutzregeln unterworfenen Daten wesentlich größer als in Europa. Trotzdem gibt es in den USA keine vergleichbare Diskussion über die Frage, ob Daten (wie bspw. maschinengenerierte Daten) einen Schutz durch Eigentumsrechte benötigen. Eine naheliegende Hypothese, weshalb kein solches exklusives Recht auf Daten diskutiert wird, besteht darin, dass vertragliche Lösungen als ausreichend angesehen werden, um die möglicherweise auftretenden Probleme zu lösen. Wie wir in Teil I gesehen haben, bedeutet das Fehlen eines Dateneigentumsrechts auch nicht, dass es nicht konkrete Abwehrrechte zum Schutz von Daten gegen Zerstörung, "misappropriation" (Trade Secret Law) oder direktes Kopieren geben kann, die allerdings teilweise sehr eng definiert und kontextspezifisch ausgestaltet sein können.[681] Die in Europa zusätzlich auftretende Begründung, ein Dateneigentumsrecht könnte dabei helfen, durch ungleichgewichtige Verhandlungsmachtsituationen verursachte unfaire Marktergebnisse in Bezug auf (die Verwertung von) Daten zu lösen, ist wesentlich schwerer mit dem in den USA viel stärkeren Prinzip vom Vorrang vertraglicher Lösungen zu vereinbaren. Eine andere wichtige Begründung, die in der Literatur über die Situation in den USA immer wieder angeführt wird, ist, dass Daten lediglich "facts" sind, auf die keine exklusiven Rechte vergeben werden können.[682] Auch wenn es somit keine Diskussion über die Einführung eines exklusiven Dateneigentumsrechts gibt,[683] so sind aber auch im US-amerikanischen Kontext konkrete rechtliche Fragen des Umgangs mit (und insbesondere auch in Bezug auf den Zugang zu) solchen Daten zu lösen. Insofern stellt sich die Frage, wie in den USA mit konkreten Problemen von "data ownership" und Zugangsrechten zu Daten umgegangen wird.

---

679 Vgl. hierzu ausführlich FTC (2012).

680 Vgl. FTC (2014).

681 Vgl. Teil I auf S. 23 ff. und 35 ff.

682 Vgl. Determann/Perens (2017, 46).

683 Vgl. aber Mattioli (2014) mit seinem sehr spezifischen Vorschlag, ein solches Recht zu vergeben, um die Herkunft von Daten und die Methodik ihrer Erhebung offenzulegen, was sich als ein Mittel zur Sicherung der Qualität von Daten interpretieren lässt.

Insofern ist es eine besonders interessante Frage, welche Regelungen in den USA bzgl. der Daten des vernetzten Autos diskutiert werden. Determann/Perens (2017) analysieren im Detail, welche rechtlichen Regelungen in den USA für die aus ihrer Sicht so wichtige Frage relevant sind, ob sich eher ein offenes oder geschlossenes Modell für vernetzte Autos durchsetzt. Hierbei kann sowohl nach dem Schutz der Privatsphäre als auch nach "data ownership" sowie dem Zugang zu Daten des vernetzten Autos für andere Serviceanbieter, insbesondere im automobilen Aftermarkt gefragt werden. In Bezug auf den Schutz von "privacy" ist in den USA noch weitgehend ungeklärt, in welchem Umfang Daten des vernetzten Autos von solchen Regeln erfasst werden können. In dem 2015 verabschiedeten "Driver Privacy Act" hat die US-amerikanische Bundesregierung entschieden, dass zu den Daten aus dem inzwischen weitverbreiteten "event data recorder" (EDR), die zur Aufklärung von Unfällen verwendet werden können, nur die Kfz-Eigentümer und -Nutzer Zugang haben sollen (und Dritte nur mit deren schriftlicher Zustimmung).[684] Ansonsten überlegt die Bundesregierung ein rechtliches System des Schutzes einzuführen, bspw. durch den im U.S. Congress eingebrachten Vorschlag eines "SPY Car Acts". Dieser würde die beiden Bundesbehörden NHTSA (National Highway Traffic Safety Administration) und die Verbraucherschutzbehörde FTC verpflichten, Regeln für den Schutz der Privatsphäre von Verbrauchern und für die Sicherheit für alle Fahrzeuge in den USA einzuführen. Dies würde auch den Umgang der Autohersteller mit solchen Daten des vernetzten Autos betreffen.[685]
Für den Zugang zu Daten des vernetzten Autos kann in den USA der "On-board Diagnostic port" (OBD) von zentraler Bedeutung sein. Dieses ursprünglich auch in den USA für die Abgasemissionskontrolle eingeführte OBD-System erlaubt den Zugang zu vielfältigen technischen Daten, insbesondere für diagnostische Zwecke. Auch wenn es in den USA bisher keinen vergleichbar gesetzlich regulierten Zugang zu notwendigen Informationen und Daten für Reparatur- und Wartungsdienstleister wie in der EU gibt, haben sich dort durch freiwillige und selbstregulatorische Lösungen der Automobilhersteller Regeln etabliert, den unabhängigen Reparaturwerkstätten Informationen im gleichen Umfang zur Verfügung zu stellen wie den Vertragshändlern. Einzelne Bundesstaaten wie insbesondere Massachusetts haben sog. Right to Repair-Gesetze verabschiedet. Daraufhin haben die Verbände der Automobilhersteller und die "Automotive Aftermarket Industry Association" ein Memorandum of Understanding unterzeichnet, die Regeln des Gesetzes von Massachusetts freiwillig in allen 50 Bundesstaaten anzuwenden und allen Autohersteller ihre diagnostischen Codes und Reparaturdaten in einem "common format" ab dem Modelljahr 2018 zur Verfügung stellen.[686] Allerdings sind diese Regelungen noch recht neu und bleiben inhaltlich hinter den bereits etablierten europäischen Regelungen zurück. Insgesamt

[684] Vgl. Determann/Perens (2017, 44).

[685] Vgl. Determann/Perens (2017, 44). Vgl. zur ungeklärten Situation bzgl. "data privacy" und "data ownership" in vernetzten Fahrzeugen in den USA und der Notwendigkeit, hierfür weitere gesetzliche Regelungen zu schaffen insbesondere Fagnant/Kockelman (2015, 178 ff.) und Anderson et al. (2016, 94 f. und 146 ff.).

[686] Vgl. Determann/Perens (2017, 29 f.).

scheint die US-amerikanische Diskussion über den Zugang zu den Daten des vernetzten Autos noch sehr am Anfang zu stehen. Dies gilt sowohl für die Fragen "data ownership" und Zugang durch andere Serviceanbieter als auch insbesondere für den Schutz der Privatsphäre. Allerdings gibt es in den USA eine stärkere Tendenz, solche Fragen über Selbstregulierung statt gesetzliche Regelungen zu lösen.

Abschließend soll in knapper Form auf eine neue Diskussion über Rechte an Daten aufmerksam gemacht werden, die in den USA im Anschluss an das Supreme Court-Urteil im Fall "Ass'n for Molecular Pathology v. Myriad Genetics, Inc" entstand.[687] Für lange Zeit war das Unternehmen Myriad Genetics der alleinige Anbieter von genetischen Tests in den USA für BRCA1- und BRCA2- Gene, die genetische "Marker" für ein Brustkrebsrisiko sind. Diese Monopolstellung basierte im Wesentlichen auf Patentrechten in Bezug auf die genetischen Tests, die aber dann der Supreme Court in seinem Urteil für ungültig erklärte. Vor dieser Entscheidung aber hatte Myriad über mehr als 10 Jahre die exklusive Möglichkeit, mit ihrem Test eine große Sammlung von genetischen Daten über Patientinnen zu sammeln, die Myriad einen großen Wettbewerbsvorsprung gegenüber anderen Wettbewerbern in Bezug auf die Diagnose von Brustkrebsrisiken von Frauen verschafft haben. Wichtig ist dabei, dass je größer der Patientinnendatenpool an genetischen Informationen ist, desto besser kann das spezifische Brustkrebsrisiko bei einzelnen Frauen diagnostiziert werden. Ein Teil dieser Diskussion bezieht sich auf das Problem, dass durch Patente eine exklusive Möglichkeit entsteht, eine bestimmte Art von Daten zu generieren, die Wettbewerber oft nicht replizieren können. Die Folge ist, dass durch solche Patente ein faktisch exklusives Datenset entsteht, das dann auch noch zusätzlich durch "Trade Secret Law" geschützt wird. Simon/Sichelman (2017) sehen solche "data-generating patents" sehr kritisch und diskutieren, ob diese Möglichkeit der Gewinnung einer monopolistischen Stellung aufgrund von Daten durch Änderungen im Patentrecht oder durch Antitrustrecht eingeschränkt werden sollte. Burk (2015) weist dagegen auf einen anderen wichtigen und möglicherweise positiven Effekt von solchen Patenten hin. Wenn es so ist, dass die Qualität der Diagnose von Brustkrebsrisiken um so größer ist, je größer der verfügbare Datenset ist, dann würde der Schutz der Methode der Datengenerierung durch das Patent die Möglichkeit eröffnen, dass ein Anbieter alle Testdaten bei sich aggregieren könnte und damit eine wesentlich größere Diagnosequalität erreichen kann als wenn es mehrere Diagnosefirmen gibt, die dann mit jeweils kleineren Datensets Diagnosen vornehmen müssen. Aus dieser Perspektive sieht Burk das Urteil des Supreme Courts auch kritisch und diskutiert, welche anderen Möglichkeiten es geben könnte, trotz Wettbewerb bei der Diagnose zu möglichst großen Datensätzen zu kommen. Aus ökonomischer Sicht ist diese Diskussion insofern interessant, weil im Bereich von Datenanalysen tatsächlich ein solches Aggregationsproblem in dem Sinne auftreten kann, dass die Erkenntnisse, die man aus einem Datenset gewinnen

[687] Ass'n for Molecular Pathology v. Myriad Genetics, Inc", 133 S. Ct. 2107 (2013). Vgl. zum Folgenden ausführlich Burk (2015) und Simon/Sichelman (2017).

kann, mit wachsender Größe zunehmen.[688] Wichtig an dieser Diskussion ist, dass durch Patente auf die Methoden der Gewinnung von Daten unter Umständen indirekt faktische Datenmonopole entstehen können, die dann - je nach den Umständen - Vor- und Nachteile mit sich bringen können.

8. DISKUSSIONEN UM RECHTE AN DATEN: ZUSAMMENFASSUNG UND FOLGERUNGEN

Das Ziel dieses zweiten Teils der vorliegenden Studie war eine Analyse von Diskussionsprozessen in Bezug auf Rechte an Daten, die im Prozess der digitalen Transformation stattfinden. Hierbei ging es insbesondere darum, für ausgewählte aktuelle Problembereiche wie die ePrivacy-Reform, die Diskussion um Eigentums- und Zugangsrechte an nichtpersonenbezogenen Daten sowie dem Zugang zu Daten im vernetzten Auto jeweils die Interessen und Argumentationen der relevanten Stakeholder und gesellschaftlich relevanten Gruppen zu analysieren. Auch wenn es nicht die Aufgabe war, eine Analyse im Hinblick auf die jeweils besten rechtlichen und regulatorischen Lösungen vorzunehmen, so war jedoch - zumindest in einem beschränkten Umfang - eine Analyse der zu regelnden Probleme und möglicher Wirkungen alternativer Lösungsmöglichkeiten notwendig für ein adäquates Verständnis dieser Diskussionen. Empirische Basis dieser Untersuchung der Diskussionsprozesse waren vor allem Positionspapiere und Stellungnahmen der Stakeholder sowie Studien und offizielle Dokumente von Regierungsinstitutionen, wie insbesondere der EU-Kommission. Wir haben uns dabei auf möglichst aktuelle Diskussionen aus den letzten zwei Jahren unter Einbeziehung der jeweils aktuellen rechtlichen und regulatorischen Vorschläge konzentriert. In diesem letzten Abschnitt sollen die wichtigsten Ergebnisse kurz zusammengefasst und einer stärker integrierten Analyse unterzogen werden. Im Mittelpunkt werden dabei die jeweiligen Argumentationen und Konflikte zwischen den Interessen der Stakeholder stehen. Hierbei soll auch auf die Frage der Verteilung der faktischen Verfügungsmacht über Daten eingegangen werden.

In der Debatte um die neue ePrivacy-Verordnung hat sich der Grundkonflikt zwischen dem Schutz der Privatsphäre von Individuen und der Datenökonomie am deutlichsten gezeigt. Anhand der konkreten Auseinandersetzungen um die spezifischen rechtlichen Regelungen bzgl. der Verarbeitung von Kommunikationsmetadaten, der Zulässigkeit von Cookies und Tracking des Surfverhaltens sowie des Offline-Trackings von vernetzten Endgeräten von Individuen wurde deutlich, dass je nach der genauen Ausgestaltung der Regelungen über die Notwendigkeit von Einwilligungen, Opt-in- oder Opt-out-Regelungen sowie Anforderungen in Bezug auf Anonymisierung oder Pseudonymisierung von Daten den jeweiligen, an der Nutzung dieser Daten interessierten, Stakeholdern eine größere oder kleinere Menge von Daten zur Verfügung steht. Die Argumentationen der verschiedenen datenverar-

[688] Vgl. generell aus ökonomischer Sicht zu diesem Aggregationsproblem auch Duch-Brown et al (2017, 29 ff.).

beitenden Stakeholder beziehen sich auf die ökonomischen Vorteile, insbesondere im Hinblick auf die Entwicklung neuer Produkte und Dienstleistungen (data-driven innovation), die Optimierung von Prozessen und einer gezielteren Ausrichtung der Angebote auf die Verbraucher. Eine besondere Untergruppe stellen dabei Unternehmen dar, die ihre Serviceangebote durch den Verkauf von Werbeaktivitäten finanzieren und hierfür Daten bzgl. der Wirksamkeit ihrer Werbeangebote benötigen, sodass Einschränkungen des Zugangs zu solchen Daten das Angebot ihrer Serviceangebote in Frage stellt. Umgekehrt verweisen Daten- und Verbraucherschützer auf die Sensibilität dieser personenbezogenen Daten in Bezug auf den Schutz der Privatsphäre und die Wichtigkeit der Vertraulichkeit von Kommunikation, die durch Grundrechte geschützt sind und beharren deshalb auf der Notwendigkeit der Einwilligung zur Verarbeitung solcher Daten. Aus ökonomischer Sicht liegt hier auf der einen Seite ein tatsächlicher Grundkonflikt vor, weil je nachdem, ob eine explizite Einwilligung (Opt-in) einzuholen ist oder auch Opt-out-Lösungen (wie beim Offline-Tracking) oder gar eine Abwägung mit "berechtigten Interessen" der datenverarbeitenden Unternehmen möglich sind, es entweder die Unternehmen sind, die die Kosten für die Einholung von Einwilligungen tragen müssen, oder umgekehrt die individuellen Personen Kosten aufwenden müssen, um ihre Privatsphäre zu schützen. Auf der anderen Seite aber ist die Interessenlage wiederum wesentlich komplexer, da auch die Individuen an neuen Produkten und Serviceleistungen sowie personalisierten Angeboten interessiert sein können. Gleichzeitig haben auch alle Beteiligten ein Interesse daran, die Probleme und Kosten einer zu großen Zahl von notwendigen Einwilligungen zu lösen. Insofern stellen die konkrete Ausgestaltung von neuen Instrumenten wie Voreinstellungen von Webbrowsern als Gatekeeper und andere Ansätze zur Entwicklung von zentralen Logins interessante neue Lösungsansätze dar, die zum Vorteil von beiden Seiten sein können. Dies ändert jedoch nichts daran, dass je nach der konkreten Ausgestaltung der Regeln in der ePrivacy-Verordnung entweder die individuellen Personen oder die Unternehmen der Datenökonomie eine größere faktische Verfügungsmacht über die Kommunikationsdaten und Informationen aus Endgeräten der Nutzer gewinnen können.

Während sich die ePrivacy-Debatte auf die Grenzziehung zwischen der Privatsphäre individueller Personen und der Datenökonomie bezieht, geht es bei den Diskussionen über Rechte an nichtpersonenbezogenen Daten gerade um Fragen des rechtlichen Umgangs mit Daten außerhalb der Reichweite des Datenschutzrechts, d.h. um die Ausgestaltung rechtlicher Rahmenbedingungen innerhalb der Datenökonomie. Insofern geht es in dieser Diskussion auch in erster Linie um den Umgang mit Daten in Beziehungen zwischen Unternehmen (B2B). Da Daten nicht-rivale Güter sind und sie deshalb möglichst viel genutzt werden sollten, hat die EU-Kommission in ihrer Mitteilung "Building a European data economy" zu Recht die Frage des Data Sharing und der Weiternutzung von Daten als wichtiges Problem für die Entstehung einer florierenden Datenökonomie thematisiert. Obwohl Daten wertvolle ökonomische Güter und ihre Nutzung durch andere auch Gegenstand von Verträgen sein können, haben sich Vorschläge, IP-ähnliche Eigentumsrechte an maschinengenerierten Daten (Datenerzeugerrecht) einzuführen, in der Diskussion als nicht weiterführend erwiesen, da sie weder aus Anreizgründen noch für die Kreation von Daten-

märkten notwendig zu sein scheinen. Allerdings war in den Positionspapieren von Stakeholdern umstritten, ob die bisher dominierenden vertraglichen Lösungen zwischen Unternehmen über Daten gerade wegen ihrer Flexibilität gut funktionieren oder ob es aufgrund von ungleichgewichtigen Verhandlungsmachtsituationen zu unfairen Marktergebnissen für "schwächere" Unternehmen wie bspw. KMU kommt. Insbesondere in IoT-Kontexten und in Bezug auf Aftermärkte scheint es unter Umständen besonders große Probleme bezüglich des Zugangs zu Daten zu geben. Während die Vorschläge der Kommission über freiwillige, unterstützende Lösungen wie Empfehlungen und Default-Regeln für Verträge über Daten als überwiegend positiv beurteilt wurden, sind andere Vorschläge mit obligatorischen Regelungen wie allgemeine verpflichtende Zugangsregelungen (bspw. unter FRAND-Bedingungen) sowie das Datenerzeugerrecht eher kritisch gesehen worden. Eine besondere - und gerade in IoT-Kontexten besonders häufig auftretende - Problematik liegt vor, wenn für bestimmte maschinengenerierte Daten mehrere Stakeholder legitime Interessen an der Nutzung der gleichen Daten haben. Da in solchen Fällen die exklusive Zuordnung zu einem einzigen Stakeholder - sei es durch ein exklusives Recht oder eine exklusive de-facto-Kontrolle - (auch ökonomisch) nicht die adäquate Lösung sein muss, kann es zweckmäßig sein, wesentlich komplexere (und auf den jeweiligen Problembereich zugeschnittene) Governance-Lösungen für solche Daten zu entwickeln, die bspw. auch spezifische Zugangsrechte für bestimmte Stakeholder beinhalten können. Hieraus läßt sich folgern, dass aus der exklusiven de-facto-Kontrolle über Daten eine faktische Verfügungsmacht entstehen kann, die unter Umständen sowohl ökonomisch ineffizient sein als auch zu unfairen Marktergebnissen durch Daten-Hold up-Situationen führen kann. Beidem könnte durch geeignete Datengovernance-Lösungen begegnet werden. Diese Problemstellungen werden in dem sich entwickelnden "Internet der Dinge" eine zunehmend größere Bedeutung gewinnen.

Die dritte Diskussion über Daten im vernetzten Auto zeichnet sich dadurch aus, dass hier ein besonders wichtiges Anwendungsbeispiel im "Internet der Dinge" vorliegt, bei dem mehrere Probleme in Kombination auftreten. Zunächst ist unbestritten, dass das vernetzte Auto mit seinen vielen generierten Daten und Fahrassistenzsystemen ein sehr großes innovatorisches Potential besitzt, insbesondere für viele neue Dienstleistungen, die im vernetzten Auto angeboten werden können, aber auch für Verbesserungen von Verkehrssicherheit und Verkehrsregelung. Gerade die Vielfalt möglicher Anbieter von neuen Dienstleistungen, die Zugang zu den Daten bzw. dem vernetzten Auto benötigen, hat die Frage, wer die faktische Verfügungsmacht über die Daten und den Zugang zum Fahrzeug inne hat und haben soll, zur zentralen Streitfrage in der bisherigen Diskussion gemacht. Hierbei hat sich bereits klar herausgestellt, dass das von der Autoindustrie favorisierte Modell des "extended vehicle", in dem alle Daten direkt auf von den Autoherstellern kontrollierte Server übertragen werden, zu einer technologisch bedingten exklusiven faktischen Verfügungsmacht der Autohersteller über die Daten des vernetzten Autos führt, die sie dann (unter Beachtung der datenschutzrechtlichen Grenzen über B2B-Vereinbarungen und des eng definierten regulierten Zugangs zu Daten über die Kfz-Typenzulassungs-VO) mit interessierten Stakeholdern frei kommerziell verwerten können. Diese Implikationen des "ex-

tended vehicle"-Konzepts haben deshalb schon in der C-ITS-Plattformdiskussion zu einem direkten Konflikt mit anderen unabhängigen Serviceanbietern geführt, die ohne Zustimmung der Automobilhersteller keinen Zugang zu dem Markt für Aftermarktleistungen und komplementäre Dienstleistungen für vernetzte Autos haben und deshalb fürchten, von diesen Märkten ausgeschlossen zu werden. Insofern hat sich fast die gesamte Diskussion über Daten im vernetzten Auto auf diesen Konflikt zwischen den Automobilherstellern und den anderen unabhängigen Serviceanbietern bezogen, die sich weitgehend einig sind in ihrer Forderung nach einer gesetzlichen Regelung zur Sicherung eines gleichen Zugangs zum Fahrzeug und seinen Daten wie die Automobilhersteller, insbesondere durch die Etablierung einer interoperablen offenen Telematikplattform (On-board application-Plattform) als alternative technische Lösung. Insgesamt fällt in dieser Diskussion auf, dass die Interessen der Autofahrer in Bezug auf den Schutz ihrer Privatsphäre zwar im Prinzip anerkannt werden, aber die Diskussion darüber, wie die konkrete Ausgestaltung dieses Schutzes, insbesondere in Bezug auf die Einwilligung zur Datenverarbeitung und deren spezifische Probleme, aussehen soll (und ob hierfür regulatorische Lösungen notwendig sind), bisher recht vage und unterentwickelt bleibt. Gleiches gilt für die Frage, ob die Verbraucher auch eine faktische Verfügungsmacht über die nicht-personenbezogenen Daten des vernetzten Autos haben sollten, mit der Möglichkeit, über deren Zugang an Dritte eigenständig ohne die Automobilhersteller zu entscheiden und hierüber auch an dem Wert dieser Daten beteiligt zu werden. Durch die von den unabhängigen Serviceanbietern geforderte Etablierung einer interoperablen offenen Telematikplattform könnten die Verbraucher auch eine solche faktische Verfügungsmacht über die Daten des vernetzten Autos erhalten. Diese Lösung wurde als langfristig überzeugendste Lösung auch von der (von der Kommission in Auftrag gegebenen) TRL-Studie nahegelegt. In Bezug auf diese technische Lösung haben somit Verbraucher und unabhängige Serviceanbieter gleichgerichtete Interessen. Allerdings stellt die Durchsetzung einer solchen technischen Lösung eine große regulatorische Herausforderung dar. Eine andere wichtige Möglichkeit der Durchsetzung einer stärkeren faktischen Vefügungsmacht für die Verbraucher, die gleichzeitig Chancen des Zugangs zu Daten für unabhängige Serviceanbieter ereöffnet, stellt das Instrument der Datenportabilität dar. Während es für personenbezogene Daten durch die DS-GVO rechtlich bereits etabliert ist, sich allerdings viele Frage seiner praktischen Umsetzung stellen, ist die Frage der Datenportabilität für nicht-personenbezogene Daten in Bezug auf die Daten des vernetzten Autos bisher kaum diskutiert worden.

Welche Grundargumentationen, Datenklassen und Grenzziehungen spielen somit generell eine wichtige Rolle in diesen Diskussionen? Die überragende Bedeutung des Schutzes der Privatsphäre als Grundwert und damit die Grenzziehung zwischen Daten, die privat bleiben, und denjenigen, die in unterschiedlicher Form der Verwertung durch Wirtschaft und Gesellschaft zur Verfügung gestellt werden, zeigt sich in der ePrivacy-Debatte, während sie in der Diskussion über vernetzte Autos bisher - trotz gleicher Relevanz - vergleichsweise wenig thematisiert worden ist. Zentraler Teil dieser Grenzziehung sind dabei immer die konkreten Regeln über die Notwendigkeit von Einwilligungen bzw. die Details der Regelungen bzgl. der Frage, wie und unter welchen Bedingungen Einwilligungen in die Verarbei-

tung personenbezogener Daten gegeben werden müssen. Es wird besonders interessant sein, wie bei der Anwendung der DS-GVO mit dem Kriterium der "Vereinbarkeit" der Nutzung für andere Zwecke sowie mit der Legalausnahme der Abwägung mit "berechtigten Interessen" von datenverarbeitenden Unternehmen konkret umgegangen wird. Gleichermaßen stellt sich die Frage der Grenzziehung auch bei der Frage nach den Anforderungen an eine Anonymisierung von Daten, durch die ursprünglich personenbezogene Daten in eine Klasse von Daten überführt werden können, die nicht mehr den Restriktionen des europäischen Datenschutzes unterliegt. Eine weitere besondere Klasse von Daten mit besonderen rechtlichen Regelungen stellt die Menge der pseudonymisierten Daten dar. Die grundlegenden Argumente der Datenwirtschaft für einen möglichst weitgehenden Zugang zu personenbezogenen Daten beziehen sich auf die Möglichkeit, aus diesen Daten neue innovative Produkte und Dienstleistungen entwickeln zu können, Produktions- und Distributionsprozesse besser optimieren zu können und damit Kosten und Ressourcen einzusparen, aber auch dem Staat helfen zu können, seine öffentlichen Aufgaben besser und kostengünstiger erstellen zu können. Insofern geht es größtenteils um wirtschaftliche Vorteile, aber teils auch um allgemeine gesellschaftliche Vorteile wie weniger Verkehrsstaus und Verkehrsunfälle, weniger Umweltverschmutzung, bessere Energieeffizienz und größere Sicherheit. Eine auch ökonomisch spannende (hier nicht weiter diskutierte) Frage ist, ob bei diesen Grenzziehungen auch industriepolitische Argumente eine Rolle spielen sollen, wie zum Beispiel die internationale Wettbewerbsfähigkeit von europäischen Unternehmen auf den Weltmärkten, die evtl. durch einen leichteren Zugang zu Daten gefördert werden könnte. Es wird eine der großen Fragen der nächsten Jahre sein, wesentlich klarer und tiefer über diese Konflikte zwischen Schutz der Privatsphäre von Individuen und den wirtschaftlichen und gesellschaftlichen Vorteilen der Verarbeitung und Analyse von mehr Daten zu diskutieren und nach adäquaten Lösungen zu suchen. Hierzu wird vor allem aber auch gehören, die möglichen Gefahren und Risiken stärker zu untersuchen, die aus der wesentlich umfangreicheren Verfügung von Informationen privater Unternehmen und des Staates über individuelle Personen resultieren. Insbesondere werden hierbei auch normative und ethische Fragen vertieft zu diskutieren sein.

Wie wir gesehen haben, spielt aber nicht nur die Grenzziehung zwischen der Privatsphäre von Individuen und der Datenwirtschaft eine zentrale Rolle, sondern auch die Frage des Umgangs mit Daten zwischen Unternehmen. Hierbei zeigte sich, dass auch zwischen Unternehmen erhebliche Konflikte über die faktische Verfügung und den Zugang zu Daten entstehen können. Hier ist die Frage, welche rechtlichen Rahmenbedingungen besonders gut geeignet sind, die Entstehung und Nutzung von Daten innerhalb der Datenökonomie zu regeln. Eine relevante Frage bezieht sich dabei auf den Handel mit Daten auf dem sekundären Datenmarkt. Eine andere wichtige Frage bezieht sich darauf, ob es bestimmte Problembereiche gibt, wie bspw. in Multi-St akeholder-Situationen in IoT-Kontexten, in denen die exklusive de-facto-Kontrolle über Daten durch einen Akteur Machtpositionen schafft, die zum einen zu unfairen Marktergebnissen aufgrund von ungleichgewichtiger Verhandlungsmacht führen können und zum anderen sich negativ auf Wettbewerb und Innovation auf Aftermärkten und Märkten mit komplementären Dienstleistungen auswirken können. Folglich ist auch systematisch darüber nachzudenken, in welchen Problemkonstel-

lationen spezielle Klassen von Daten definiert und geschaffen werden sollen, für die spezielle Governance-Lösungen, bspw. auch durch sektorspezifische gesetzliche Regelungen, eingeführt werden sollten oder ob solche Probleme sich auch durch Anwendung allgemeiner rechtlicher Regeln wie bspw. des Wettbewerbsrechts lösen lassen. Insofern geht es innerhalb der Wirtschaft auch darum, welche Governance-Lösungen in Bezug auf Daten insgesamt zu mehr Wettbewerb und Innovation führen, wobei - wie beim vernetzten Auto - immer auch andere wichtige Ziele (wie bspw. Sicherheit) eine wichtige Rolle spielen können.

LITERATURVERZEICHNIS TEIL II

ACEA (2016a). Access to vehicle data for third-party services. ACEA Position Paper. Brüssel. December 2016.

ACEA (2016b). ACEA Strategy Paper on Connectivity. Brüssel. April 2016.

ACEA & CLEPA. (2016). Automotive industry joins forces on access to vehicle data. Brüssel.

Acquisti, A., Wagman, L., & Taylor, C. R. (2016). The Economics of Privacy. *Journal of Economic Literature 54(2)*. 442-492.

Acquisti, A., & Grossklag, J. (2007). What can behavioural economics teach us about privacy? In: Acquisti, A., & Vimercati, S. (Hrsg.), *Digital Privacy: Theory, Technologies and Practices. Boca Raton: Auerbach Publications*. 363-380.

ADAC (2015). Daten im Fahrzeug. München. Juni 2015.

ADPA et al. (2017). Insurance, leasing, dealers, vehicle inspection, automotive aftermarket and consumers coalition: Keeping the principles of the Treaty of Rome alive in the automotived digital age. Press Release. Brüssel. 23 March 2017.

AFCAR (2016). Fair and Equal Access to Vehicles in a Digital Single Market. Brüssel. 2016.

Alonso Raposo, M., Ciuffo, B., Makridis, M., & Thiel, C. (2017). The r-evolution of driving: from Connected Vehicles to Coordinated Automated Road Transport (C-ART). European Commission. JRC Science for Policy Report, Part I: Framework for a safe & efficient Coordinated Automated Road Transport (C-ART) system. doi:10.2760/225671.

Akalu, R. (2018). Privacy, consent and vehicular ad hoc networks (VANETs). *Computer Law & Security Review 34*, 37-46.

Anderson, J., Kalra, N., Stanley, K. D., Sorensen, P., Samaras, C., & Oluwatola, O. A. (2016). Autonomous Vehicle Technology – A Guide for Policymakers. Santa Monica. Calif.: RAND.

Article 29 Data Protection Working Party (2017). Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC). 4 April 2017.

Autorité de la Concurrence & Bundeskartellamt (2016). Competition Law and Data. Gemeinsames Papier der Autorité de la concurrence und des Bundeskartellamtes zu Daten und Auswirkungen auf das Wettbewerbsrecht. 10.05.2016.

Ayres, I., & Gertner, R. (1989). Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules. *Yale Law Journal 99*, 87-130.

BDI (2017a). Entwurf einer ePrivacy-Verordnung -Stellungnahme der deutschen Industrie.

BDI (2017b). Positionspapier Datenwirtschaft. Berlin. 8. Juni 2017.

BDVA (2017). BDVA's response to the European Commission's Communication and Consultation "Building a European Data Economy". Brüssel. April 2017.

Becker, R., & Simon, S. (2015). GVO Nr. 461/2010 (Kfz-GVO) Vertriebs- und Kundendienstvereinbarungen im Kfz-Sektor. In: Bornkamm, J./Montag, F./Säcker, F. J. (Hrsg.), *Münchner Kommentar Europäisches und Deutsches Wettbewerbsrecht (Kartellrecht)*. 2. Auflage. München: C.H. Beck. 1173-1214.

Bernhart, W., Olschewski, I., Burkard, C., & Galander, S. (2016). Automated Vehicle Index. Q3 2016. https://www.fka.de/consulting/studien/index-automated-vehicle-2016-07-q3-e.pdf (2nd October 2017).
BEUC (2017a). Proposal for a Regulation on Privacy and Electronic Communications (e-Privacy). BEUC Positionspapier. Brüssel. 09.06.2017
BEUC (2017b). Protecting European Consumers with connected and automated cars. Positionsapier. Brüssel.11.12.2017
Bitkom (2017). EU Commission proposal Regulation on Privacy and Electronic Communication (COM(2017) 10 final). Positionspapier. 30.Mai 2017.
BMVI (2017). Eigentumsordnung für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive. 02.08.2017.
BMWi (2017). Weissbuch Digitale Plattformen: Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe.
Borgesius, Z. (2015). Behavioural Sciences and the Regulation of Privacy on the Internet, in: Alemanno/Sibony (Hrsg.), *Nudging and the Law - What can EU Law learn from Behavioural Sciences?*, Oxford: Hart Publishing 2015. 179-207.
Borgesius, F. Z., & Poort, J. (2017). Online Price discrimination and EU Data privacy law. *Journal of Consumer Policy 40 (3), 347–366.*
Bosch (2013). Neue fun2drive-App von Bosch bringt Fahrzeugdiagnose und Bordcomputer auf das Smartphone. http://www.bosch-presse.de/pressportal/de/de/neue-fun2drive-app-von-bosch-bringt-fahrzeugdiagnose-und-bordcomputer-auf-das-smartphone-34707.html. Zugegriffen: 26.09.2017.
BVDW (2015). Connected Cars – ein Diskussionspapier zum Thema Services.
BVDW (2016a). Connected Cars – Geschäftsmodelle. Diskussionspapier. 23.05.2016.
BVDW (2016b). Connected Cars – Chancen und Risiken für die künftigen Anbieter im Automobilmarkt.
BVDW (2017). Stellungnahme des Bundesverbandes Digitale Wirtschaft (BVDW) e.V. zum Entwurf einer Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation. Berlin (3. März 2017).
Bundesregierung (2015). Strategy for Automated and Connected Driving.
Burk, D. L. (2015). Patents as Data Aggregators in Personalized Medicine. *B. U. J SCI. & TECH. L.*21. 233 - 255.
BusinessEurope (2017). Building a European Data Economy. Position Paper (26 April 2017).
Carnelley, P. et al. (2016). Europe's Data Marketplaces. Current Status and Future Perspectives (European Data Market SMART 2013/0063 D 3.9). IDC/Open Evidence.
Cattaneo, G. et al. (2016). D8 Second Interim Report (European Data Market SMART 2013/0063), 52-58.
CER (2017). CER Position. European Data Economy (26 April 2017).
C-ITS Platform (2016). Final Report.
CLEPA (2015). CLEPA position paper. Open Telematics Platform (22 July 2015).

Coalition for Audience Measurement (2017). Position Statement on ePrivacy Regulation (21.9.2017).

Committee on Transport and Tourism (2017). Draft Report on a European strategy on Cooperative Intelligent Transport Systems (2017/2067(INI)) (16.10.2017).

Cooter, R., & Ulen, T. (2011). *Law and Economics*. 6. Aufl., Boston: Pearson.

De Streel, A., & Larouche, P. (2015). Disruptive Innovation and Competition Policy Enforcement. OECD Background Note. 20 October 2015.

Derikx, S., de Reuver, M., & Kroesen, M. (2015). Can privacy concerns for insurance of connected cars be compensated? *Electronic Markets 26(1)* 1-9, doi:10.1007/s12525-015-0211-0

Determann, L., & Perens, B. (2017). Open Cars. UC Hastings Research Paper No. 213. Available at SSRN: https://ssrn.com/abstract=283759; publiziert in: Berkeley Technology Law Journal 32(2), 915-988.

Deutscher Bundestag (2016). Fragen zum Datenschutz im vernetzten Auto. Wissenschaftlicher Dienst: Ausarbeitung WD 3 - 3000-168/16.

Digitale Gesellschaft (2017). Stellungnahme der Digitalen Gesellschaft e.V. zum Vorschlag der Europäischen Kommission für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektromischen Kommunikation. Berlin (21.März 2017).

DIGITALEUROPE (2016). DIGITALEUROPE views on the review of the ePrivacy Directive. Brüssel, 31 Oktober 2016.

DIRECTIVE 2010/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

Dorner, M. (2014). Big Data und "Dateneigentum", Grundfragen des modernen Daten- und Informationshandels. *Computer und Recht*, 617-628.

Drexl, J. (2016). Designing competitive markets for industrial data: Between propertisation and access, Max Planck Institute for Innovation and Competition Research Paper No. 16-13.

Drexl, J. (2017). Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz, NZKart, 339-343 (Teil 1) und 415-421 (Teil 2).

Duch-Brown, N., Martens, B. & Mueller-Langer, F. (2017). The economics of ownership, access and trade in digital data. EC JRC Technical Reports Working Paper 2017-01.

DVD (Deutsche Vereinigung für Datenschutz) (2017). Presseerklärung. Bonn, 31. Mai 2017.

EC (2014). Study on the operation of the system of access to vehicle repair and maintenance information. Final report.

EC (2016a). Synopsis report of the public consultation on the evaluation and review of the ePrivacy Directive.

EC (2016b). Report e-Privacy (Flash Eurobarometer 443, December 2016).

EC (2016c). Communication “A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility”. COM (2016) 766 final, 30.11.2016.

EC (2016d). Proposal for a Regulation of the European Parliament and of the Council on the Approval and Market Surveillance of Motor Vehicles and Their Trailers, and of Systems, Components and separate technical units intended for such vehicles. COM(2016) 31 final (27.1.2016).
EC (2017a). Communication "Building a European data economy", COM(2017) 9 final (10.1.2017).
EC (2017b). Commission Staff Working Document on the free flow of data and emerging issues of the European data economy accompanying the Communication "Building a European data economy". SWD(2017) 2 final (10.1.2017). Brussels.
EC (2017c). Synopsis report. Consultation on the "Buildung a European data economy" Initiative.
EC (2017d). Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation). COM (2017) 10 final. Brüssel (10.01.2017).
EC (2017e). Commission Staff Working Document. Impact Assessment. SWD(2017) 3 final. (Brussels, 10.1.2017).
EC (2017f). Commission Staff Working Document. Executive Summary of the Impact Assessment. SWD(2017) 4 final. (Brussels, 10.1.2017).
EC (2017g). Commission Staff Working Document. Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC, SWD(2017) .5 final. (Brussels, 10.1.2017).
EC (2017h). Annex to the Synopsis report. Detailed analysis of the public online consultations results on "Building a European data economy".
EC (2018a). Communication "Towards a common European data space", COM(2018) 232 final (25.4.2018).
EC (2018b). Guidance on sharing private sector data in the European data economy. Commission Staff Working Document, SWD(2018) 125 final (25.4.2018).
EDRi (2017). EDRi's position on The Proposal of an e-Privacy Regulation. Brussels: European Digital Rights.
Engeler, M., & Felber, W. (2017). Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis. Reguliert der Entwurf an der technischen Realität vorbei?. *Zeitschrift für Datenschutz 7*, 251-257.
Engeler, M. (2017). Die ePrivacy-Verordnung zwischen Trilog und Ungewissheit. *Zeitschrift für Datenschutz 7*, 549-550.
EP (2017). Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017)0010 – C8-0009/2017 – 2017/0003(COD), 23.10.2017.
EP (2018). Report on a European strategy on Cooperative Intelligent Transport Systems (2017/2067(INI)). Committee on Transport and Tourism (PE610.712v02-00).

Esayas, S. Y. (2015). The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. *European Journal of Law and Teachnology 6(2)*, 1-20.

European Data Protection Supervisor (2014). Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy. Preliminary Opinion.

European Data Protection Supervisor (2016). EDPS Opinion on Personal Information Management Systems. Opinion 9/2016.

European Data Protection Supervisor (2017). EDPS Opinion on the proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation). Opinion 6/2017, 24 April 2017.

Europäischer Rat (2017).Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text. (15333/17). Brüssel. 05.12.2017.

Europäischer Rat (2018a).Opinion on the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency discussion paper. (5165/18). Brüssel (11.01.2018).

Europäischer Rat (2018b). Proposal for a regulation of the European Parliament and of the Council on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles. 2016/0014 (COD) Analysis of the final compromise text with a view to agreement (11.1.2018).

Evans, David, & Schmalensee, Richard. (2007). The Industrial Organization of Markets with Two-Sided Platforms. *Competition Policy International Journal 3*, 151-179.

Fagnant, D. J., & Kockelman, K. (2015). Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. Transport Research Part A 77 (2015)167-181.

FAZ (2017). Offener Brief an das Europäische Parlament (29.05.2017).

FAZ (2018). Universalschlüssel für das Internet. FAZ, 11.April 2018, 18.

FEDMA (2017). Position paper. ePrivacy Regulation proposal, Brussels (20.02.2017).

Fezer, Karl-Heinz (2017), Dateneigentum – Theorie des immaterialgüterrechtlichen Eigentums an verhaltensgenerierten Personendaten der Nutzer als Datenproduzent, MMR, 3-5

FIGIEFA (2010). Right to Repair. The new competition law framework for the automotive aftermarket. Brussels.

FIGIEFA (2016). Commission Communication on "Free Flow of Data". Input from the Independent Automotive Aftermarket (23 December 2016).

FIA (2015). FIA - interim solution Date Server Platform. Shared Server. (Powerpoint Presentation) (C-ITS WG6 - A2D - ANNEX 4).

FIA (2016a): Policy Position on Car Connectivity. Brüssel.
FIA (2016b). "What Europeans think about connected cars". Brüssel. Januar 2016.
Frank, S. & Kerber, W. (2017). Data Governance Regimes in the Digital Economy: The Example of Connected Cars, available at: https://ssrn.com/abstract=3064794.
Fraunhofer-Gesellschaft (2016). Industrial Data Space White Paper.
FTC (2012). Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers. FTC Report.
FTC (2014). Data Brokers. A Call for Transparency and Accountability: A Report of the Federal Trade Commission (May 2014). Washington D.C.
Fudenberg, D., & Villas-Boas, J.M. (2012). Price Discrimination in the Digital Economy. In: Peitz, M. & Waldfogel, J. (Hrsg.), *Oxford Handbook of the Digital Economy, 254-272*. DOI: 10.1093/oxfordhb/9780195397840.013.0010
Gautam, S. (2015). 21st century problems: Will the European Union data reform properly balance its citizens' business interests and privacy?, Southwestern Journal of International Law, 195-216.
Gilbert, F., & Zallone, R. (2016). Connected Cars. Recent Legal Developments. mimeo.
Graef, I. (2015). Market Definition and Market Power in Data: The Case of Online Platforms. *World Competition 38*, 473-506.
GSMA/etno (2017). The Proposed European ePrivacy Regulation. GSMA and ETNO Joint Position (June 2017).
Hacker, P. (2017). Personal Data, Exploitative Contracts. and Algorthmic Fairness: Autonomous Vehicles meet the Internet of Things, forthcoming in: International Data Privacy Law.
HDE (2017). Stellungnahme zum Vorschlag für eine Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation. Berlin (26.04.2017).
HERE/Swiss Re (2016). The future of motor insurance. A joint white paper.
Herbrich, T. (2017a). Der Vorschlag für eine ePrivacy-Verordnung-EU (Teil 1): Anwendungsbereich und Verhältnis zur DS-GVO und Zum nationalen Recht. jurisPR-ITR 18/2017 Anm. 2, 1-8.
Herbrich, T. (2017b). Der Vorschlag für eine ePrivacy-Verordnung-EU (Teil 2): Fernmeldegeheimnis, Zulässigkeit der Datenverarbeitung, Privacy by Default. jurisPR-ITR 23/2017 Anm. 2, 1-8.
Herbrich, T. (2017c). Der Vorschlag für eine ePrivacy-Verordnung-EU (Teil 3): Kontrolle über elektronische Kommunikation, insbesondere Direktwerbung, unabhängige Aufsichtsbehörden, Rechtsbehelfe, Haftung und Sanktionen. jurisPR-ITR 25/2017 Anm. 2, 1-8.
Hermstrüwer, Y. (2016). *Informationelle Selbstgefährdung*. Tübingen: Mohr-Siebeck.
Hermstrüwer, Y. (2017). Contracting around privacy: The (Behavioral) Law and Economics of Consent and Big Data. *Jipitec 8*, 9-26.
Hildebrandt, C., & Arnold, R. (2017). Economic Impact of the ePrivacy Regulation on Online Advertising and Ad-based Digital Business Models. WIK report: Study for the Bundeministerium für Wirtschaft und Energie. Bad Honnef.

Hoeren, T. (2013). Dateneigentum: Versuch einer Anwendung von § 303a StGB im Zivilrecht. *MultiMedia und Recht 16*, 486-491.

Hoffmann, F., Inderst, R., & Ottaviani, M. (2013). Hypertargeting, Limited Attention, and Privacy: Implications for Marketing and Campaigning. Working Paper.

Hornung, G. (2015). Verfügungsrechte an fahrzeugbezogenen Daten. Das vernetzte Automobil zwischen Wertschöpfung und Persönlichkeitsschutz. *Datenschutz und Datensicherheit 38*, 359-366.

Hornung, G., & Goeble, T. (2015). "Data Ownership" im vernetzten Automobil. *Computer und Recht 31*, 265-273.

IAB Europe (2017). Position on the proposal for an ePrivacy Regulation (28 March 2017).

Ibec (2017). Ibec's view on the European Commission's Communication "Building a European Data Economy" (April 2017).

ICDP (2017). ICDP statement on "Building a European Data Economy" Communication & Consultation. Brussels (26 April 2017).

Insurance Europe (2018). European Parliament approach on access to in-vehicle data welcomed (Press statement, 21 February 2018).

ITRE (2017). Draft Opionion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications. 22.05.2017

Jentzsch, N. (2018). Dateneigentum - Eine gute Idee für die Datenökonomie? Berlin: Stiftung Neue Verantwortung.

Johanning, V. & Mildner, R. (2015). *Car IT kompakt – Das Auto der Zukunft – Vernetzt und autonom fahren*. Wiesbaden: Springer Vieweg.

Joint Industry Statement (2016). Empowering trust and innovation by repealing the e-Privacy Directive (05.07.2016).

JURI (2017). Entwurf einer Stellungnahme des Rechtsausschusses für den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation). 06.06.2017

LIBE (2017). ENTWURF EINES BERICHTS über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8-0009/2017 – 2017/0003(COD)). 09.06.2017

Kerber, W. (2016a). Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection. *GRURInt 11*, 639-647.

Kerber, W. (2016b). A new (intellectual) property right for non-personal data? An economic analysis. *GRURInt 11*, 989–998.

Kerber, W. (2017). Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective, forthcoming in: Lohsse, S., Schulze, R., Staudenmayer, D. (Hrsg.), Trading Data in the Digital Economy: Legal Concepts and Tools, Baden-Baden: Nomos, 109-133.

Kerber, W., & Schweitzer, H. (2017). Interoperability in the Digital Economy, in: Journal of Intellectual Property, Information Technology and Electronic Commerce Law *(JIPITEC) 8(1)*. 2017, 39 - 58.

Kilian, W. (2015). Property Rights und Datenschutz. Strukturwandel der Privatheit durch elektronische Märkte, in: Kaal/Schwarzte/Schmidt (Hrsg.). Festschrift zu Ehren von Christian Kirchner. Mohr Siebeck, 901-916.

Köhler, H. (2017). Die Regelung der "unerbetenen Kommunikation" in der ePrivacy-Verordnung und ihre Folgen für das UWG. *Wettbewerb in Recht und Praxis*, 1291-1297.

Kokolakis, S. (2015). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security 64*, 122-134.

Koszegi, B. (2014). Behavioral Contract Theory, Journal of Economic Literature (52), 1075-1118.

Koutroumpis, P., Leiponen, A., & Thomas, L. D. W. (2017). The (Unfulfilled) Potential Of Data Marketplaces. ETLA Working Papers No 53. http://pub.etla.fi/ETLA-Working-Papers-53.pdf.

KPMG (2017). The Chaotic middle. The autonomous vehicle and disruption in automobile insurance. White Paper (June 2017).

Krebs, D. (2013). "Privacy by Design": Nice-to-have or a necessary principle of data protection law? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law 2*. 2-20.

Lohsse, S., Schulze, R. & Staudenmayer, D. (Hrsg.) (2017). Trading Data in the Digital Economy: Legal Concepts and Tools. Baden-Baden: Nomos.

Lüdemann, V. (2015). Connected Cars - Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück. *Zeitschrift für Datenschutz 5*, 247-254.

Luzak, J. (2014). Privacy Notice for Dummies? Towards European Guidelines on How to Give “Clear and Comprehensive Information” on the Cookies’ Use in Order to Protect the Internet Users’ Right to Online Privacy. *Journal of Consumer Policy 37*, 547-559.

Maier, N., & Schaller, F. (2017). ePrivacy-VO - alle Risiken der elektronischen Kommunikation gebannt? Entwurf ohne datenschutzrechtliche Regelungen für P2P-Kommunikationsdienste. *Zeitschrift für Datenschutz 7*, 373-377.

Mattioli, M. (2014). Disclosing Big Data. *Minnesota Law Review* 99, 535-583.

McKinsey (2014). Connected car, automotive value chain unbound. Advanced Industries Report.

McKinsey (2016). Monetizing car data. New service business opportunities to create customer benefits.

Monopolkommission (2015). Competition policy: The challenge of digital markets. Special Report No. 68.

Mozilla (2017). Mozilla position paper on the European Commission's draft e-Privacy Regulation.

MPI (2017). Position Statement on the European Commission's "Public Consultation on Building the European Data Economy" (MPI for Innovation and Competition, 26 April 2017).

News Media Europe (2017). Position paper ePrivacy (March 2017).

Norberg, P., Horne, D., & Horne, D. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs 41*. 100-126.

OECD (2015). Data-driven innovation: Big data for growth and well-being. OECD, Paris.

OECD/ITF (2015). Automated and Autonomous Driving. Regulation under uncertainty. Corporate Partnership Report.

Oetjen, J. (2017). Wie die EU-Verordnungen den Umgang mit Daten verändern werden. OVK-Report für digitale Werbung 2017/02. 29-31.

Petkova, B., & Boehm, F. (2017). Profiling and the essence of the right to data protection. In: Poletsky, J., Tene, O., & Selinger, E. (Hrsg.). *Cambridge Handbook of Consumer Privacy*. Cambridge University Press. 285-300

Petrovic et al. (2015). Self-Driving Cars: Disruptive or Incremental? *Innovation Review. Issue 1*. June 2015, 3-21.

Poland (2017). Poland's non-paper on the European Commission's public consultation: "Building the European data economy".

PwC (2016). Connected car report 2016 – Opportunities, risk, and turmoil on the road to autonomous vehicles.

PwC (2017). Cross-cutting Business Models für IoT. Final report (SMART number 2017/0027), Brussels.

REGULATION (EC) No 715/2007 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information.

REGULATION (EU) No 461/2010 of 27 May 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices in the motor vehicle sector.

REGULATION (EU) No 758/2015 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC.

Urquhart, L., Sailaja, N., & McAuley, D. (2017). Realising the right to data portability for the domestic Internet of Things. Personal and Ubiquitous Computing. Springer. DOI: 10.1007/s00779-017-1069-2

Samuelson, P. (2000). Privacy as intellectual property. *Stanford Law Review 1996*, 1125-1173.

Schwartmann, R. & Hentsch, C.-H. (2015). Eigentum an Daten - Das Urheberrecht als Pate für ein Datenverwertungsrecht. *RDV (5)*, 221-230.

Schwartz, P. M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review 117*, 2055-2128.

Schweitzer, H. (2017). Neue Machtlagen in der digitalen Welt? Das Beispiel unentgeltlicher Leistungen, in: Kühling, J., T. Körber (Hrsg.), *Regulierung, Wettbewerb, Innovation*. Baden-Baden. Nomos. 269-305.

Schweitzer, H., & Peitz, M. (2017). Datenmärkte: Funktionsweise und Regelungsbedarf. Diskussionspapier 17-043. Mannheim: ZEW.

Schweitzer, H., & Peitz, M. (2018). Ein neuer Ordnungsrahmen für Datenmärkte? *Neue Juristische Wochenschrift 71*, 275-280.

Solove, D. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review 126*, 1880-1903.

Specht, L. (2016). Ausschließlichkeitsrechte an Daten - Notwendigkeit, Schutzbereich, Alternativen. *Computer und Recht*, 288 - 296.

Specht, L. (2017). Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus? *Juristenzeitung 72*, 763-770.

Spehr, M. (2018), Ein Universalschlüssel für alle Dienste im Internet, FAZ, 27.Februar 2018, T4

Stalla-Bourdillon, S., & Knight, A. (2017). Anonymous data v. personal data - A false debate: An EU perspectvie on anonymization, pseudonymisation and personal data. Wisconsin International Law Journal. 284-322.

Stucke, M.E. & Grunes, A.P. (2016). Big Data and Competition Policy. Oxford University Press.

Sunstein, C. R., & Thaler, R.H. (2003). Libertarian Paternalism is not an Oxymoron. *The University of Chicago Law Review* 70, 1159-1202.

TechUK (2017). TechUK response to the European Commission's Building the European Data Economy Communication. London. April 2017.

TRL (2017). Access to In-Vehicle Data and Resources – Final Report (18.05.2017).

Tsesis, A. (2014). The right to erasure: Privacy, data brokers, and the indefiniteretention of data. *Wake Forest Law Review*, 433-484.

UFE (2017). Building a European Data Economy. https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy.

UK (2017). UK Government response to the European Commission's Consultation on Building the European Data Economy.

VATM (2017). Eckpunktepapier des VATM zum Vorschlag der Kommission für eine ePrivacy-Verordnung. Köln (12.06.2017).

VDA (2016). Position. Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten. Berlin.

Verband der TÜV (2018). Position. Data Protection, IT Security & Compliance as a Basis for New Business models in a digital connected mobility. Berlin (15.01.2018).

vzbv (2017). Gewährleistung der Privatsphäre und Vertraulichkeit in der elektronischen Kommunikation. Stellungnahme der Verbraucherzentrale Bundesverbands e.V. zum Vorschlag der Kommission für eine Verordnung über Privatsphäre und elektronische Kommunikation. Berlin (15.März 2017).

Voss, W. G. (2017). First the GDPR, now the proposed ePrivacy Regulation. *Journal of Internet Law 21*, 3-11.

Wegner, A. (2010a). Neue Kfz-GVO (VO 461/2010) - des Kaisers neue Kleider? Teil 1: die Anschlussmärkte. *Betriebs-Berater*, 1803-1809.

Wegner, A. (2010b). Neue Kfz-GVO (VO 461/2010) - Teil 2: Individuelle Beurteilung von Verträgen außerhalb der GVO auf den Anschlussmärkten, Betriebs-Berater, 1867-1874.

Weidert, S., & Klar, M. (2017). Datenschutz und Werbung - gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung. *Betriebs-Berater*, 1858-1864.

Wiebe, A. (2016). Protection of industrial data - a new property right for the digital economy? *GRURInt*. 2016, 877-884.

Wiebe, A. (2017). Von Datenrechten zu Datenzugang - Ein rechtlicher Rahmen für die europäische Datenwirtschaft. *Computer und Recht 33(2)*, 87-93.

Zarsky, T. Z. (2017). Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review 47*. 995-1020.

Zdanowiecki , K. (2015). Recht an den Daten, in: Bräutigam & Klindt (Hrsg.). *Digitalisierte Wirtschaft/Industrie 4.0*. Ein Gutachten der Noerr LLP im Auftrag des BDI. Berlin: Noerr. 19-28.

Zech, H. (2012). *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck.

Zech, H. (2015). Daten als Wirtschaftsgut - Überlegungen zu einem "Recht des Datenerzeugers". *Computer und Recht 31*, 137-146.

Zech, H. (2016). A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data. *Journal of Intellectual Property Law & Practice 11*, 460-470.

Zech, H. (2017). Building a European data economy - The proposal of the European Commission for a data producer's right. *Intellectual Property Journal 9(3)*, 317-330.

TEIL III: THESEN

These 1: Daten und Informationen sind im Grundsatz verschiedene Größen. Während Daten begrifflich die auf einem Datenträger festgehaltenen Zeichen oder Zeichenfolgen beschreiben und damit allein die syntaktische Zeichenebene betreffen, definiert die Informationen eine semantische Bedeutung dieser Zeichen. Funktional aber bedingen sich syntaktische und semantische Ebene: Ein Datum zeichnet sich funktional dadurch aus, dass ihm zwar nicht eine einzige und stets gleichbleibende Bedeutung innewohnt, es aber als Kodierung mehrerer Bedeutungsmöglichkeiten dient, von denen der Rezipient im Rahmen eines Verständnisvorgangs eine dieser Bedeutungsmöglichkeiten selektiert. Aufgrund dieser Funktion von Daten als Informationsgrundlage trifft eine Regulierung von Daten auch die aus ihnen ableitbaren Informationen. Ebenso kann sich eine Regulierung auf der semantischen Ebene reflexartig auf die syntaktische Ebene auswirken.

These 2: Verschiedene Kategorien von Daten werden rechtlich in unterschiedlicher Art und Weise adressiert. Zu unterschieden ist v.a.

a) zwischen personenbezogenen und nicht-personenbezogenen Daten, wobei die Reichweite des Personenbezugs einerseits sehr weit ist, zu den nicht-personenbezogenen Daten andererseits aber auch anonymisierte Daten gehören

- innerhalb der Kategorie der personenbezogenen Daten zwischen sensiblen und nicht-sensiblen Daten, wobei sensible Daten sehr viel restriktiver verarbeitet werden dürfen, als nicht-sensible Daten

- innerhalb der Kategorie der personenbezogenen Daten zwischen pseudonymisierten und nicht-pseudonymisierten Daten, wobei eine Pseudonymisierung nicht per se eine Verarbeitung rechtfertigt, jedenfalls aber in einer Interessenabwägung z.B. im Rahmen der Durchbrechung des Zweckbindungsgrundsatzes zu berücksichtigen ist.

b) zwischen Kommunikationsdaten und anderen Daten, wobei die Kommunikationsdaten unabhängig von ihrem Personenbezug in den Anwendungsbereich der vorgeschlagenen E-Privacy-Verordnung fallen

- innerhalb der Kommunikationsdaten zwischen Kommunikationsmetadaten und Kommunikationsinhalten, deren Verarbeitung jeweils unterschiedlichen Erlaubnistatbeständen unterliegt

c) Zwischen „Rohdaten“ und angereicherten Daten, d.h. solchen Daten, die bereits mit anderen Daten zusammengeführt wurden, wobei eine Zusammenführung personenbezogener Daten zu einer stärkeren Gefährdung des informationellen Selbstbestimmungsrechtes

und damit zu erhöhten datenschutzrechtlichen Voraussetzungen der Verarbeitung führen kann.

These 3: Weder im deutschen, noch im US-amerikanischen Recht existiert de lege lata eine eigentumsrechtlich oder eigentumsähnlich ausgestaltete Rechtsposition an Daten. Sprechen sektorspezifische Regelungen in der Rechtsordnung der USA insbesondere im Zusammenhang mit Connected Cars von einem „Ownership" an Daten, ist nicht ersichtlich, ob hierdurch tatsächlich eigentumsähnliche Befugnisse an den betroffenen Daten zugewiesen werden sollen, insbesondere, ob an diesen ausschließliche Nutzungsrechte eingeräumt und die eingeräumten Nutzungsrechte auch nach erstmaliger Entäußerung in den Rechtsverkehr dinglich ausgestaltet sein sollen. Tendenziell erscheint eine solche Auslegung als zu weitreichend.

These 4: Sowohl im europäischen, als auch im US-amerikanischen Recht können Datenbestände vom Geschäftsgeheimnisschutz erfasst sein, wenn die spezifischen Voraussetzungen der jeweiligen gesetzlichen Grundlage vorliegen. Dies gilt gleichermaßen für personenbezogene, wie für nicht-personenbezogene Daten. Der Geschäftsgeheimnisschutz ist aber als reines Abwehrrecht ausgestaltet. In den USA lässt sich eine kosten-, und zeitintensive Zusammenstellung von Daten darüber hinaus nach der sogenannten Misappropriation-Doktrin vor unbefugter Übernahme schützen. Sowohl die Voraussetzungen, als auch Schutzumfang und -dauer sind allerdings sehr eng. Erfasst ist daher nur eine sehr geringe Anzahl von Fällen. Es existiert kein generelles Common Law Tort of Misappropriation.

These 5: Einzeldaten sind mangels Werkcharakter weder im deutschen und europäischen noch im US-amerikanischen Recht urheberrechtlich geschützt. Einen Schutz schöpferischer Datenbankwerke kennen beide Rechtsordnungen, das US-amerikanische Recht enthält aber im Unterschied zum deutschen und europäischen Recht keinen Schutz nichtschöpferischer Datenbanken.

These 6: Deliktsrechtlich kommt im deutschen Recht ein Schutz vor der Löschung oder anderweitigen Beeinträchtigung von Daten gem. § 823 Abs. 2 BGB i.V.m. §§ 202a ff., 303a StGB in Betracht,[689] sofern die spezifischen Voraussetzungen der Schutzgesetze vorliegen. Auch die Verbotsvorschriften des Datenschutzrechts lassen sich als Schutzgesetze begreifen, ebenso wie der strafrechtliche Schutz gegen den Geheimnisverrat in besonderen Vertrauensverhältnissen, § 203 StGB. Im Falle einer sittenwidrigen Schädigung kommen Ansprüche gem. § 826 BGB in Betracht. Bei Betriebsbezogenheit des Eingriffs kann eine Löschung oder anderweitige Beeinträchtigung von Daten einen Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb begründen. Im Rahmen des § 823 Abs. 1 BGB wird ein Schutz vor Löschung und Beeinträchtigung von Daten aber im Wesentlichen über den Schutz des Eigentums am Trägermedium erreicht (Beeinträchtigung und Löschung von Daten als Beeinträchtigung des Rechts, den Datenträger auf beliebige Art und Weise und

689 Zu Letzterem vgl. hierzu: *Faust*, 71. DJT 2016, S. A50; *Hieke*, InTeR 2017, 10, 14 ff.

damit auch zum Abruf der konkreten Daten verwenden zu können). Diskutiert wird auch ein Recht am eigenen Datenbestand, das aber de lege lata noch nicht abschließend anerkannt ist. Im US-amerikanischen Recht ergibt sich ein Schutz von Daten im Wesentlichen über die Privacy Torts, aber auch über den Breach of Confidenciality sowie über die Torts of Trespass to Chattels und Conversion.

These 7: Eine vertragliche Disposition über Daten kann sowohl im deutschen, als auch im US-amerikanischen Recht selbst dann erfolgen, wenn keinerlei ausschließlichkeitsrechtliche Rechtspositionen an ihnen existieren. Wird vertraglich das „Eigentum" an Daten geregelt, ist freilich nicht die vertragliche Verschaffung einer ausschließlichkeitsrechtlichen Rechtsposition gemeint, sondern die Bestimmung desjenigen, der im Vertragsverhältnis bestimmen dürfen soll, wie mit den betreffenden Daten umzugehen ist. Nachteil des Vertragsrechtes ist es, dass es Abwehr- und Regressmöglichkeiten allein gegenüber dem Vertragspartner, nicht aber auch gegenüber Dritten begründet. Dies ist nach US-amerikanischem Recht nicht anders als nach deutschem Recht.

These 8: Der Datenhandel mit nicht-personenbezogenen Daten lässt sich im deutschen Recht weitgehend problemlos mit den de lege lata bereitstehenden Vertragstypen erfassen. Schwieriger ist die Erfassung einer vertraglichen Disposition über personenbezogene Daten. Aufgrund der datenschutzrechtlichen Beschränkung einer Verarbeitung personenbezogener Daten ergeben sich spezifische Probleme aus der erforderlichen Verzahnung von Datenschutz- und Vertragsrecht. Insbesondere die jederzeitige Widerruflichkeit der datenschutzrechtlichen Einwilligung stellt das Vertragsrecht vor erhebliche Herausforderungen. Im US-amerikanischen Rechtsraum können Daten sowohl im Kontext vertraglicher Leistungspflichten, als auch als Gegenleistung geschuldet sein, sofern den grundsätzlichen Anforderungen des Vertragsrechts genügt wird (insbesondere sind „past-consideration", und eine „pre-existig-duty" als Gegenleistung nicht ausreichend). Die Anforderungen des Datenschutzrechts begrenzen den Datenhandel hier sehr viel weniger weitreichend, als dies im deutschen und europäischen Recht der Fall ist. Insbesondere kennt das US-amerikanische Datenschutzrecht kein allgemeines Verbotsprinzip.

These 9: Möchte man Verträge über die Überlassung und Verwertung von Daten de lege lata im deutschen Recht erfassen, ist zwischen primärem und sekundärem Datenmarkt zu differenzieren. Während der primäre Datenmarkt das Vertragsverhältnis zwischen dem Betroffenen und der datenerhebenden Stelle (Datenerhebungsvertrag) erfasst, bezeichnet der sekundäre Datenmarkt das Vertragsverhältnis zwischen der datenerhebenden Stelle und dem Datenerwerber (Datenüberlassungsvertrag/Datenverwertungsvertrag, sekundärer Datenmarkt). Auf dem primären Datenmarkt werden Daten als Gegenleistung hingegeben. Handelt es sich um personenbezogene Daten, ist die Erklärung der datenschutzrechtlichen Einwilligung Teil der Gegenleistung, wenn die Auslegung der Willenserklärungen der Vertragsparteien dies ergibt. Auf dem sekundären Datenmarkt werden bereits erhobene Daten an Drittunternehmen weitergereicht.

These 10: Neben der Begrenzung des rechtlichen Umgangs mit Daten durch das Datenschutzrecht, erfolgt eine Begrenzung auch durch bereits de lege lata existente Zugangsrechte, die sich z.B. über das Kartellrecht oder sektorspezifisch durch unionsrechtliche Regulierung etwa im Automotive-Bereich ergeben.

These 11: Es existieren eine Mehrzahl von Regulierungsansätzen sowohl im deutschen und US-amerikanischen Recht zur Ausgestaltung des rechtlichen Umgangs mit Daten, die teils jedoch sehr heteronome Ziele verfolgen. Insbesondere über die Einräumung ausschließlichkeitsrechtlicher Rechtspositionen und eine Ausgestaltung des vertragsrechtlichen Umgangs mit Daten sollen nach Vorstellung der EU-Kommission Rechtssicherheit hergestellt und auf diese Weise Transaktionskosten im Umgang mit Daten verringert werden. Im US-amerikanischen Recht indes ist mit Blick auf diese Zielsetzung allenfalls eine Randdiskussion zu verzeichnen. Auf eine Beteiligung des datenschutzrechtlich Betroffenen zielen Ansätze, die eine Lizenzierungsmöglichkeit personenbezogener Daten entsprechend dem Urhebervertragsrecht vorschlagen und damit an Überlegungen zur kommerziellen Ausgestaltung des Persönlichkeitsrechts anknüpfen. Eine Diskussion über die vertragsrechtliche Stellung des datenschutzrechtlich Betroffenen wird in den USA schon seit mehreren Jahrzehnten geführt. Hierbei wird zwar auch die Terminologie „data property" verwendet, sie ist aber vor dem Hintergrund gewählt, dass das US-amerikanische Datenschutzrecht keinen dem europäischen Datenschutzrechtrecht entsprechenden starken Datenschutz des Betroffenen kennt und der Terminus „data property" daher gewissermaßen als gegenüber dem de lege lata bestehenden US-amerikanischen Datenschutzrecht stärkeres Kontrollrecht des Betroffenen verstanden wird. Daneben existiert in den USA die Idee eines „datarights", das ein ausschließliches Nutzungsrecht an Daten einräumt, wenn die Methode ihrer Erhebung offengelegt wird. Ziel dieses Ansatzes ist es, die Datenqualität und die Qualität ihrer Auswertung zu erhöhen.

These 12: Im Rahmen möglicher Regulierungsansätze ist zu berücksichtigen, dass der datenschutzrechtliche Begriff des Personenbezugs sehr weit ist, sodass eine Vielzahl von Daten personenbezogen sind. Selbst nicht-personenbezogene Daten können durch Hinzufügung weiterer Daten zu personenbezogenen Daten werden. Letztlich wird ein Datenbestand in der Regel sowohl aus personenbezogenen, als auch aus nicht-personenbezogenen Daten bestehen. Hieraus können eine Vielzahl von Problemen entstehen, sodass es sinnvoll erscheint, wenn mögliche Rechtspositionen an Daten oder auch Zugangsrechte entweder sowohl personenbezogene als auch nicht-personenbezogene Daten adressieren oder aber rechtssichere Möglichkeiten einer Beseitigung des Personenbezugs etabliert werden (z.B. Standards zur Anonymisierung).

These 13: Ausschließlichkeitsrechte können in einer freiheitlich angelegten Rechtsordnung stets nur die Ausnahme sein. Es bedarf daher eines (rechtlichen oder ökonomischen) Problems, das zu lösen die Ausgestaltung von Ausschließlichkeitsrechten erfordert. Ein solches Problem ist jedenfalls de lege lata nicht generell zu erkennen. Die betroffenen Beteiligteninteressen unterscheiden sich in den vielen verschiedenen datengetriebenen Geschäfts-

modellen so erheblich, dass es gewinnbringend scheint, die Diskussion auf spezifische Sektoren zu verlagern und dort nach spezifisch passenden Lösungsoptionen zu suchen. Keine Lösungsoption sollte dabei per se ausgeschlossen werden. In Betracht kommende Ausschließlichkeitsrechte müssen auch nicht zwingend so umfassend gestaltet sein, wie das Eigentumsrecht gem. § 903 BGB, sondern können durchaus nur einzelne Nutzungs- und Abwehrbefugnisse umfassen oder mehreren Beteiligten zugewiesen werden. Ebenso wie die Reichweite ihres Schutzes ließe sich auch die Schutzdauer und eine mögliche Erschöpfung sehr flexibel gestalten.

These 14: Auch die Diskussion über Zugriffsrechte an Daten sollte vermehrt auf die sektorspezifische Ebene verlagert werden. Zugangsrechte zu Daten könnten sich hier insbesondere für komplexe Multi-Player-Sachverhalte als gewinnbringend erweisen, sofern sich eine (rechtliche oder ökonomische) Notwendigkeit ergibt. Auch hier müssen die Voraussetzungen derartiger Rechte aber ausreichend bedacht und in ihren Auswirkungen hinreichend untersucht sein.

These 15: Auch über einen möglichen Regulierungsbedarf im Vertragsrecht lässt sich nicht generalisierend entscheiden. Zwischen primärem und sekundärem Datenmarkt bestehen erhebliche Unterschiede, denen Rechnung zu tragen ist. Ein möglicher Regulierungsbedarf im Vertragsrecht lässt sich dabei mit drei Zielrichtungen erörtern: Erstens könnten angemessene gesetzliche Rahmenbedingungen den Datenverkehr erleichtern, indem sie ihn auf rechtssichere Grundlage stellen und so Transaktionskosten verringern. Zweitens könnten Regelungen zur Klauselkontrolle jedenfalls in gewissem Maße Machtungleichgewichte zwischen den Vertragsparteien ausgleichen. Allerdings fehlen zu beiden Aspekten bislang tiefergehende empirische Studien, die genauer analysieren, ob sich der bisherige vertragsrechtliche Rahmen tatsächlich als Hemmnis für den Handel mit Daten erweist. Drittens aber ergibt sich regulatorischer Handlungsbedarf v.a. zum Schutz des Betroffenen: Verträge, in denen wir personenbezogene Daten hingeben und die Einwilligung in die Datenverarbeitung erklären, um hierdurch einen Dienst in Anspruch nehmen zu können, z.B. die Nutzung eines sozialen Netzwerkes, können nach §§ 133, 157 BGB nicht anders ausgelegt werden, als dass die Erklärung der Einwilligung und die Hingabe der Daten als Gegenleistung geschuldet sind. Hier bedarf es einer regulatorischen Entscheidung darüber, wie die datenschutzrechtlichen Vorgaben in das nach den Grundsätzen der Privatautonomie ausgestaltete Vertragsrecht hineingetragen werden können, insbesondere, wie die jederzeitige Widerruflichkeit der Einwilligung zivilrechtlich abgebildet werden kann. Regulatorischer Handlungsbedarf ergibt sich danach v.a. auf dem primären Datenmarkt.

These 16: Im Rahmen der Diskussion um den rechtlichen Umgang mit Daten darf der Schutz des informationellen Selbstbestimmungsrechtes nicht geschwächt werden. Der Datenschutz sollte insofern weiterhin jeden rechtlichen Umgang mit personenbezogenen Daten – ob nun auf vertragsrechtlicher-, ausschließlichkeitsrechtlicher oder zugangsrechtlicher Ebene – begrenzen.

These 17: Die Diskussion über Rechte in Bezug auf Daten ist auch aufgrund der rasch fortschreitenden digitalen Transformation (Internet der Dinge) sehr komplex, unübersichtlich und in vielerlei Hinsicht unterentwickelt. Allerdings schält sich für konkrete Problembereiche immer klarer der grundlegende Konflikt zwischen dem Schutz der Privatsphäre von Individuen und den Datenbedürfnissen der Datenökonomie heraus. Dieser Konflikt zeigt sich bei konkreten regulatorischen Diskussionen in Auseinandersetzungen über Fragen der Definition von Datenklassen (und den für sie bestehenden rechtlichen Regelungen) und den zwischen ihnen bestehenden Grenzziehungen. Gleichzeitig wird damit auch die Verteilung der faktischen Verfügungsmacht über Daten beeinflusst.

These 18: In der Diskussion über die ePrivacy-Verordnung über den Schutz der Vertraulichkeit von Kommunikation wird dieser Konflikt besonders deutlich. Auf der einen Seite würde ein weitreichender Zugriff auf Kommunikationsmetadaten sowie Informationen aus den Endgeräten (insbes. Smartphones) von Personen (insbes. Cookies, Tracking bzgl. Surfverhalten, sowie Offline-Tracking) viele wertvolle Daten für die Datenwirtschaft zugänglich machen, die bspw. für personalisierte Dienste und gezielte Werbung genutzt werden können, auf der anderen Seite aber können gerade diese Daten einen besonders tiefen Einblick in die Privatsphäre von individuellen Personen bieten und damit für sie mit erheblichen schwer abschätzbaren Risiken verknüpft sein.

These 19: Während Daten- und Verbraucherschutzverbände in der ePrivacy-Diskussion aus dem Grundwert Schutz der Privatsphäre das Recht der Individuen ableiten, dass Kommunikationsdaten (einschl. Kommunikationsmetadaten), Informationen aus den Endgeräten sowie die Zulassung von Cookies und Tracking (einschl. Offline-Tracking) nur mit Zustimmung der Individuen möglich sein soll, verweisen die Stakeholder aus der Wirtschaft auf die Bedeutung eines leichten und kostengünstigen Zugriffs auf solche Daten für Innovationen, gezielte Werbung und für die generelle Entwicklung der Datenökonomie, auch in Bezug auf die internationale Wettbewerbsfähigkeit. Eine besondere ökonomische Bedeutung hat diese Frage für alle primär werbefinanzierte Serviceangebote, wie bspw. auch Medienangebote.

These 20: In Bezug auf die konkreten Diskussionen über den Vorschlag der EU-Kommission für eine ePrivacy-Verordnung zeigt sich dieser Konflikt darin, dass die an Daten interessierten Stakeholder der Wirtschaft die Notwendigkeit und Anforderungen an explizite Einwilligungen bzgl. Kommunikationsmetadaten, Informationen aus den Endgeräten (Cookies, Tracking) möglichst reduzieren möchten, bspw. auch durch Zulassung der Abwägung mit "berechtigten Interessen" oder weitreichenden Opt-out-Regelungen, während Daten- und Verbraucherschützer stark die Notwendigkeit von Einwilligungen (Opt-in) und zusätzlichen Sicherungen zum Schutz der Privatsphäre betonen und diesbezüglich den Kommissionsvorschlag eher weiter verschärfen möchten, bspw. auch durch konsequente Umsetzung des Prinzips von "Privacy-by-design" und eines generellen Verbots von Tracking Walls.

These 21: Aus ökonomischer Sicht können alternative Regelungen in der ePrivacy-Verordnung, d.h. ob auf Daten mit oder ohne Einwilligung zugegriffen werden darf, ob bei Einwilligungen Opt-in oder Opt-out-Lösungen etabliert werden, und ob solche Daten für die weitere Verarbeitung anonymisiert oder nur pseudonymisiert werden müssen, sowohl das Ausmaß des Schutzes der Privatsphäre als auch die Menge der faktisch der Datenwirtschaft zur Verfügung stehenden Daten in erheblicher Weise beeinflussen. Denn je nach der gewählten Regelung können die Kosten entweder für die Individuen für den Schutz ihrer Privatsphäre oder für die Unternehmen für das Einholen von Einwilligungen stark steigen. Sowohl die Grundsatzfrage, ob durch das Setzen auf Einwilligungen die Privatsphäre überhaupt in effektiver Weise geschützt werden kann, als auch die praktische Frage, wie solche Einwilligungslösungen (auch angesichts ihrer Vielzahl) zweckmäßiger organisiert werden können, bedürfen einer wesentlich intensiveren Diskussion.

These 22: Die Diskussion über Rechte an nicht-personenbezogenen, maschinengenerierten Daten hat zwar zunächst eine kontroverse Diskussion über Eigentumsrechte an Daten ausgelöst, sich dann aber recht schnell in eine allgemeinere Diskussion über Rechte an Daten entwickelt, die sich primär auf die Frage des Zugangs zu Daten und den adäquaten Rahmenbedingungen für eine wohlfunktionierende Datenökonomie fokussiert hat, in der die Förderung der Teilung und Weiterverwendung von Daten im Mittelpunkt steht. Die Mitteilung "Building a European data economy" der EU-Kommission und die dort gemachten Vorschläge spiegeln diese Diskussion gut wieder.

These 23: Die Ergebnisse der sich an diese Mitteilung anschliessenden öffentlichen Konsultation der EU-Kommission zeigten, dass teilweise erhebliche Probleme bgzl. der Datenteilung und Weiterverwendung von Daten existieren. Insbesondere werden bezüglich des Zugangs zu Daten auch ungleichgewichtige Verhandlungsmachtsituationen beklagt, wobei sehr unterschiedliche Auffassungen darüber geäussert wurden, ob und inwieweit diesbezüglich tatsächlich Marktversagensprobleme vorliegen oder ob doch vertragliche Arrangements über Daten ausreichend sind und wegen ihrer Flexibilität regulatorischen Eingriffen vorzuziehen sind. In der Konsultation deutete sich aber auch an, dass die auftretenden Probleme unter Umständen sehr sektorspezifische Ursachen haben könnten.

These 24: Die Vorschläge der Kommission in Bezug auf nicht-personenbezogene Daten haben in der Konsultation eine sehr gemischte Reaktion erhalten, von überwiegend eher positiven Reaktionen in Bezug auf transaktionskostensenkende, unverbindliche Instrumente wie Leitlinien, Empfehlungen und Default-Regeln für Verträge über den Umgang mit Daten, bis hin zu wesentlich kritischeren Reaktionen in Bezug auf verbindliche regulatorische Eingriffe wie das Datenerzeugerrecht oder Regelungen über den obligatorischen Zugang zu privat gehaltenen Daten (bspw. mit FRAND-Bedingungen) für andere private Akteure, während dies für Zwecke im öffentlichen Interesse und für wissenschaftliche Forschung positiver beurteilt wurde.

These 25: Während es aus ökonomischer Sicht keine guten Gründe für die allgemeinen Einführung eines Datenerzeugerrechts für maschinengenerierte Daten gibt, zeigt sich allerdings insbesondere in Internet der Dinge-Kontexten, in denen es oft mehrere Stakeholder (wie den Hersteller und den Nutzer) gibt, die Zugang zu den gleichen Daten benötigen, dass eine exklusive Kontrolle durch einen Akteur (sei es durch de-facto-Kontrolle oder ein exklusives Recht) nicht zu einer ökonomisch adäquaten Governance-Lösung für solche Daten führen muss. Insofern kann es zweckmäßig sein, nach spezifisch zugeschneiderten Governance-Lösungen zu suchen, die auch ein Bündel von Zugangsrechten auf diese Daten enthalten können. Für die zukünftige Ausbreitung des Internet der Dinge wird die Suche nach geeigneten Lösungen für solche Datengovernance-Probleme von zentraler Bedeutung sein.

These 26: Der Umgang mit Daten im vernetzten Auto stellt eine besondere Herausforderung für regulatorische Lösungen dar. Die Probleme des Zugangs zu den für viele Unternehmen wertvollen Daten im vernetzten Auto, die gleichzeitig sehr sensibel in Bezug auf die Privatsphäre von Autofahrern sind, ist ein besonders wichtiges Beispiel für die Komplexität der Suche nach einer geeigneten Governance-Lösung. Es geht bei diesem Zugang zu Daten und zum vernetzten Fahrzeug dabei nicht nur um die Interessen der Automobilhersteller und unabhängigen Serviceanbieter, sondern auch um die Interessen der Verbraucher und öffentliche Interessen (wie bspw. Verkehrsregelung und Verkehrssicherheit).

These 27: Die bisherige Diskussion hat sich hauptsächlich an dem Konflikt zwischen Autoherstellern und unabhängigen Serviceanbietern orientiert, der dadurch entsteht, dass die Autohersteller mit ihrem "extended vehicle"-Konzept eine technische Lösung für das vernetzte Auto favorisieren (und auch praktisch bereits umsetzen), das ihnen (unter Beachtung der datenschutzrechtlichen Vorgaben und des eng definierten regulierten Zugangs zu Daten für Reparatur- und Wartungszwecke) die exklusive Kontrolle (und damit die Verfügungsmacht) über die im Fahrzeug generierten Daten und damit auch die exklusive Möglichkeit ihrer kommerziellen Verwertung sichert. Die unabhängigen Serviceanbieter sehen daher - nicht zu Unrecht - die Gefahr, dass sie dadurch vom Wettbewerb und der Möglichkeit, den Autofahrern neue innovative Serviceleistungen anbieten zu können, ausgeschlossen werden, was sich negativ auf Innovation und Wettbewerb bei automobilen Aftermarktdienstleistungen und anderen Serviceangeboten im Umfeld des vernetzten Fahrens auswirken würde.

These 28: Eine breite Koalition unabhängiger Serviceanbieter fordert deshalb eine gesetzliche Regulierung für den Zugang zu den Daten des vernetzten Autos, die ihnen die gleichen Zugangsbedingungen sichert wie den Automobilherstellern. Dies könnte als Zwischenlösung eine "shared server"-Lösung sein, bei der die Daten auf einen gemeinsam verwalteten externen Server (mit diskriminierungsfreiem Zugang) übertragen werden. Besonders interessant aber wäre insbesondere mittel- und langfristig der Übergang zu einer anderen technischen Lösung, nämlich interoperablen offenen Telematiksystemen ("On-board application-Plattform“), bei der die Autofahrer die faktische Kontrolle über den Zugang zum

vernetzten Fahrzeug und seinen Daten ausüben könnten. Dies könnte einen direkten Zugang zu Daten unabhängig von der Zustimmung der Autohersteller ermöglichen und somit zu mehr Wettbewerb und Innovation bei diesen Serviceangeboten führen. Die Argumentation der Automobilhersteller, dass ihre exklusive Kontrolle notwendig sei für die Aufrechterhaltung der Sicherheit vernetzter Fahrzeuge ist sehr umstritten.

These 29: Auch wenn diese Diskussion über den Zugang zu Daten für unabhängige Serviceanbieter gerade auch aus ökonomischer Sicht wegen ihrer Bedeutung für Wettbewerb und Innovation sehr wichtig ist, sollten für die Frage einer adäquaten Governance-Lösung für die Daten im vernetzten Auto zwei weitere Fragen wesentlich stärker als bisher diskutiert werden. Zum einen ist die Frage nach der konkreten Ausgestaltung des Schutzes der Privatsphäre von Autofahrern zu stellen (insbesondere in Bezug auf die Spezifizität von Einwilligungen zur Verarbeitung von Daten) ebenso wie die Frage nach der Kontrolle und Beteiligung am Wert der nicht-personenbezogenen Daten des vernetzten Autos. Diese Diskussion ist bisher sehr unterentwickelt. Zum anderen sollte die Frage der angemessenen technischen Lösung für die Governance von Daten in und die Kommunikation mit vernetzten Fahrzeugen auch im Hinblick auf die Anforderungen eines zukünftigen integrierten Mobilitätssystems gesehen werden, in dem Fahrzeuge auch mit der Verkehrsinfrastruktur und anderen Fahrzeugen direkt kommunizieren müssen.

These 30: Insgesamt zeigt sich bei allen diesen Diskussionen, dass die grundlegenden Konflikte sich zwar teilweise bereits in klaren gegensätzlichen Positionen zwischen verschiedenen Stakeholdern niederschlagen, aber dass die Wirkungen der verschiedenen Regelungsoptionen in Bezug auf den Schutz der Privatsphäre und die Wirkungen in Bezug auf Innovationen und Wettbewerb noch wenig verlässlich untersucht sind. In gleicher Weise bleiben bisher in diesen Diskussionen die notwendigen normativen Abwägungen zwischen dem Schutz der Privatsphäre von Individuen als Grundwert und den ökonomischen Vorteilen einer größeren Verwertung von Daten noch sehr unklar und werden wenig explizit diskutiert. Insofern ist zum einen mehr Forschung über die Wirkungen alternativer rechtlicher Regelungen notwendig und zum anderen eine intensivere öffentliche Diskussion um die Chancen und Gefahren der weiteren Digitalisierung von Wirtschaft und Gesellschaft. Dies wirft auch zentrale Fragen in Bezug auf den zukünftigen Stellenwert des Schutzes der Privatsphäre von Individuen in einer mehr und mehr digitalisierten Wirtschaft und Gesellschaft, ebenso wie umgekehrt auch stärker über eventuell notwendige Grenzen einer weiteren Digitalisierung nachzudenken ist.