

Betriebs Berater

22 | 2019

Recht ... Wirtschaft ... Steuern ... **Dateneigentum** ... **Digitalsteuer** ... **BetrVG** ... Recht ... 27.5.2019 | 74. Jg. Seiten 1217–1280

DIE ERSTE SEITE

Prof. Dr. Felix Buchmann, RA/FAIT-Recht/FAUrheber- und Medienrecht

Neue Regeln für Verbraucher beim Online-Handel – Few Deals statt New Deals for Consumers

WIRTSCHAFTSRECHT

Dr. Udo Kornmeier, RA, und **Anne Baranowski**, LL.M., RAin

Das Eigentum an Daten – Zugang statt Zuordnung | 1219

STEUERRECHT

Dipl.-Finw. **Georg Eder**, RA, und **Dr. Jörg Dehn**, RA

Sind Verrechnungspreisanpassungen zollwertrechtlich relevant? –

Eine kritische Bestandsaufnahme anlässlich des EuGH-Grundsatzurteils Hamamatsu (C-529/16) | 1238

Prof. DDr. Gunter Mayr

Neue Digitalkonzernsteuer auf Onlinewerbung in Österreich | 1245

Prof. Dr. Dieter Dziadkowski

Zum Einkommensteuertarif 2019: Berücksichtigung des Grundfreibetrags | 1248

BILANZRECHT UND BETRIEBSWIRTSCHAFT

Prof. Dr. Michael Hommel, StB, **Tessa Kunkel**, M.Sc., und **Theresa Zick**, M.Sc.

Passive Rechnungsabgrenzungsposten – Statische Interpretation durch die neuere Rechtsprechung? | 1259

ARBEITSRECHT

Bernd Weller, RA/FAArbR, und **Johannes Reuther**

BB-Rechtsprechungsreport zur Arbeitnehmermitbestimmung nach dem BetrVG – Teil III: Organisationsrechte des Betriebsrats | 1268

Dr. Udo Kornmeier, RA, und Anne Baranowski, LL.M., RAin

Das Eigentum an Daten – Zugang statt Zuordnung

Die ökonomische Betrachtung von Daten als einem zentralen Wirtschaftsgut im Kontext von Big Data, Industrie 4.0 oder des Internets der Dinge stellt die Rechtsordnung vor große Herausforderungen. Seit einigen Jahren wird intensiv zur Schaffung einer europäischen Datenökonomie diskutiert, ob es ein eigentumsähnliches Recht an Daten geben soll oder ob diese grundsätzlich frei verfügbar sein sollen, solange nicht das Datenschutzrecht, Urheberrechte bzw. der Schutz der Datenbankhersteller sui generis, der Schutz als Betriebs- oder Geschäftsgeheimnis oder Strafrechtsnormen einem freien Zugang entgegenstehen. Die Kontroverse beruht auf dem Befund, dass derzeit de lege lata keine eigentumsähnliche Zuordnung des einzelnen Datums besteht. Wie nachstehend ausgeführt, ist auch ein Bedarf nicht zwingend erkennbar. Demgegenüber scheint es sinnvoller, über ein Recht des Zugangs zu Daten nachzudenken. Im Folgenden werden Ansätze zur Ermittlung eines Datenberechtigten (I.) sowie die Möglichkeit, Zugang zu Daten statt Zuordnung zu schaffen (II.), dargestellt.

I. Eigentum an Daten – Zuordnung

Zunächst werden die Vorteile und Merkmale eines etwaigen Ausschließlichkeitsrechts an Daten dargestellt (1.). Anschließend wird auf Basis bestehender gesetzlicher Regelungen untersucht, inwieweit eine Zuordnung von Daten zu einem Datenberechtigten in Betracht kommt als Sacheigentum (2.), als Nutzung einer Sache (3.), bei Daten mit Personenbezug – Datenschutz (4.), bei Daten ohne Personenbezug (5.), als Datenverwertungsrecht für personenbezogene Daten in Anlehnung an das Urheberrecht (6.), in Anlehnung an das Datenbankherstellerrecht (7.), durch Abstellen auf den Skripturakt (8.), als Geschäftsgeheimnis (9.) und durch Integritätsschutz durch das Deliktrecht (10.).

1. Vorteile und Merkmale eines Ausschließlichkeitsrechts

Der wirtschaftliche Wert der Daten berechtigt zur Frage, ob es zivilrechtliches Dateneigentum geben soll. Wenn von Eigentum an Daten gesprochen wird, ist ein absolutes, dingliches Recht gemeint, das dem Eigentümer ein Ausschließlichkeitsrecht gewährt. Als Grund für die Schaffung von Eigentums- bzw. eigentumsähnlichen Ausschließlichkeitsrechten an Daten werden von Teilen der Literatur vor allem zusätzliche Anreize für Unternehmen genannt, um Daten zu erheben, zu teilen und so einen eigenen Datenmarkt zu schaffen. Ohne eine klare rechtliche Zuweisung sei ein solcher Markt wenig attraktiv, weil Daten ihren Wert verlören, sobald sie einem Dritten bekannt werden.¹ So liegt der Diskussion um das Dateneigentum die Frage nach einer Zuordnung und Nutzungsberechtigung von Daten zugrunde. Im Folgenden wird untersucht, ob tatsächlich ein Ausschließlichkeitsrecht an Daten notwendig ist.

Ausschließlichkeitsrechte gewähren dem Eigentümer gegenüber jedermann (erga omnes) wirkende Befugnisse an seinem Gut. Diese Befugnisse bestehen in der Möglichkeit, nach freiem Belieben mit dem Gegenstand zu verfahren (Nutzungsfunktion) und andere von der Nutzung auszuschließen (Ausschlussfunktion), § 903 BGB. Dritte dürfen grundsätzlich auf den zugewiesenen Bereich weder einwirken noch diesen positiv nutzen. Das Recht des Eigentümers ist verkehrsfähig, um einen Handel mit Gütern zu ermöglichen. Solche Ausschließlichkeitsrechte gewähren zum Beispiel Sacheigentum und Immaterialgüterrechte.²

Daten sind unkörperlich und zeichnen sich jedoch durch Nicht-Rivalität, Nicht-Exklusivität und Nicht-Abnutzbarkeit aus, sodass ihnen kein ausschließlicher Vermögenswert inne ist.³ Dies gilt für personenbezogene Daten sowie für Daten ohne Personenbezug. Daten können von einer Vielzahl von Nutzern verwendet werden, ohne dass die Nutzung des jeweils anderen dadurch beeinträchtigt wird. Darüber hinaus sind Daten beliebig kopierbar und unterliegen keiner Abnutzung oder Alterung. All dies ist bei körperlichen Gegenständen anders und rechtfertigt zumindest in Teilen die Schaffung eines absoluten Rechts, wie es das Sacheigentum vorsieht.⁴

Aufgrund der Vielzahl von Akteuren, die Interesse an Daten geltend macht, und der diversen bereichsspezifischen Regelungen sind vertragliche Absprachen zwischen den Parteien zunehmend ungeeignet, eine valide Rechtsposition für ein Rechtssubjekt zu schaffen. Da vertragliche Absprachen stets nur zwischen den beteiligten Parteien Geltung beanspruchen, besteht stets das Risiko, dass Dritte Daten in unerwünschter, ggf. beeinträchtigender Weise nutzen und dies rechtlich nicht unterbunden werden kann. Daher wird diskutiert, ob Daten eine dingliche, eigentumsähnliche Rechtsposition zukommen sollte.⁵

2. Zuordnung wie bei Sacheigentum

Einige Autoren möchten ein Eigentumsrecht an Daten unmittelbar aus den Regelungen zum Sacheigentum begründen (§§ 903 Satz 1, 90 BGB).⁶ Ein solches Eigentumsrecht knüpfe an die Erzeugung von Daten durch Aufnahme bzw. Codierung an und solle daher dem Daten-

1 Daten als Wirtschaftsgut, Smart-Data-Begleitforschung, FZI Forschungszentrum Informatik, S. 19, https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_datens_wirtschaftsgut.pdf?__blob=publicationFile&v=3 (Abruf: 25.4.2019).

2 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 89, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

3 Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister des Länder, Bericht vom 15.5.2017, S. 30, https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf (Abruf: 25.5.2019).

4 Hoeren, MMR 2019, 6.

5 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 89, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

6 Z. B. Zech, CR 2015, 144.

erzeuger als originär Berechtigtem zustehen. Wer Datenerzeuger ist, bestimme sich nach wirtschaftlichen Gesichtspunkten, sodass beispielsweise in Auftragsverhältnissen der Auftraggeber als Datenerzeuger gelte.⁷

Eigentum kann im deutschen Recht jedoch nur an beweglichen und unbeweglichen Sachen nach § 90 BGB bestehen. Nach der Legaldefinition des § 90 BGB sind Sachen sind körperliche Gegenstände. Unkörperliche Gegenstände können grundsätzlich nicht Gegenstand des Eigentums sein. Daten sind jedoch unkörperlich.⁸ Ihnen fehlt es an der körperlichen Sacheigenschaft. Daraus folgt, dass ein Eigentum an Daten nach § 903 BGB nicht besteht. Die Notwendigkeit von Sacheigentum an Daten ist auch nicht ersichtlich, wenn das Nutzungsrecht von Daten nicht-rival ist, sich also nicht durch den Gebrauch mehrerer abnutzt oder an Wert verliert.

Im Ergebnis ist festzuhalten, dass Eigentum am Gegenstand und Eigentum an einem Datenträger und an einem Datum getrennt zu betrachten sind. Regelungen zu zivilrechtlichem Eigentum lassen sich mangels Körperlichkeit von Daten nicht übertragen.

3. Nutzungen einer Sache

Andere Autoren möchten die Daten als Nutzungen des Datenträgers anerkennen (§ 100 BGB).⁹ Dabei wird auf die Sachherrschaft bzw. das Eigentum an dem Datenträger, auf dem sich die Einzeldaten befinden, abgestellt. Daraus soll sich das ausschließliche Recht an den Nutzungen, nämlich den auf dem Datenträger verkörperten Daten, ableiten.¹⁰ Nach diesem Ansatz sollen also Daten als Nutzungen einer Sache einen eigenständigen Rechtsschutz genießen, der jedoch nicht einem absoluten Vollrecht entspricht.

Dieser Ansatz erinnert an das Softwarerecht, bei dem das Recht an der Software in enger Beziehung zu dem Eigentumsrecht an dem die Software verkörpernden Datenträger gesehen wurde. Beim Softwarerecht hat sich jedoch das Recht an der Software von der Existenz eines Datenträgers zur Begründung der eigenständigen Rechte an der Software gelöst. Daher kommt hier ein Umweg über die Hardware zur Begründung etwaiger Rechte an Daten nicht in Betracht.¹¹

Zudem kann dieser Ansatz zu einer unterschiedlichen Zuordnung von Inhalt und Datenmedium führen. Er kann bei Datentransfer und erneuten Speichervorgängen fraglich werden. In gewissen Leistungsmodellen, zum Beispiel beim Cloud Computing, fallen Datennutzer und Eigentümer des Datenmediums auseinander. Dann wäre die Verfügungsgewalt in der Hand des Akteurs, der gerade nicht das wirtschaftliche Interesse an den Daten hat. Daher ist eine Zuordnung eines Ausschließlichkeitsrechts nach dem Datenmedium nicht förderlich.¹²

4. Zuordnung von Daten mit Personenbezug – Datenschutz

a) Schutzgegenstand

Die Erhebung und Verarbeitung personenbezogener Daten ist vor allem durch die Datenschutz-Grundverordnung geregelt. Das Datenschutzrecht basiert auf dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 GG), das eine Ausprägung des allgemeinen Persönlichkeitsrechts darstellt. Zweck des Datenschutzrechtes ist es, den Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht durch Datenverarbeitung zu schützen.¹³ Im Fokus steht also primär der Schutz immaterieller Güter des Betroffenen.

b) Rechtsposition des Betroffenen

Eine Verarbeitung von personenbezogenen Daten ist lediglich mit Einwilligung des Betroffenen oder im Fall eines gesetzlichen Erlaubnistatbestandes möglich. Der Betroffene kann gegen eine nicht legitimierte Datenverarbeitung Abwehrrechte geltend machen. So ermöglicht das Datenschutzrecht der betroffenen Person, über das Ob und Wie der Verarbeitung ihrer personenbezogenen Daten zu entscheiden, z. B. durch Einwilligung und der Betroffenenrechte wie Auskunft, Einschränkung der Verarbeitung, Löschung.¹⁴ Dadurch erlangt er eine starke Rechtsposition.¹⁵ Zur Stärkung der Betroffenenrechte scheint es derzeit keines Ausschließlichkeitsrechts zu bedürfen, da die datenschutzrechtlichen Mechanismen ausreichen.¹⁶

c) Datenschutzrecht versus Eigentumsrecht

Zudem gewährt das Datenschutzrecht unter anderem dem Betroffenen ein Recht auf Widerruf seiner Einwilligung sowie einen Lösungsanspruch. Diese Rechte widersprechen dem Charakter des Eigentums. Ein Wesensmerkmal des Eigentums ist seine zeitlich unbefristete Geltung. Durch die „schwebende Entziehbarkeit“ durch beliebige Dritte wäre das Eigentum im Kern entwertet.¹⁷ Betroffene könnten so Verträge Dritter inhaltslos machen. Es stellt sich die Frage nach dem Wert eines verfassungsrechtlich nach Art. 14 GG geschützten Eigentumsrechts an personenbezogenen Daten, wenn dieses Recht jederzeit und durch gewillkürte einseitige Erklärung eines beliebigen Dritten entzogen und zunichte gemacht werden kann.¹⁸

d) Eigenleistung beim Datenschutz?

Konstituierend für die Zuweisung von Herrschaftsrechten wie z. B. im Immaterialgüterrecht ist eine erbrachte Eigenleistung.¹⁹ Im Datenschutzrecht ist es fraglich, ob die betroffene Person stets einen erheblichen Anteil an der Entstehung eines auf ihn bezogenen Datums hat.²⁰ Das Persönlichkeitsrecht und die damit verbundenen Rechte in Bezug auf personenbezogene Daten stehen dem Betroffenen nicht aufgrund von Leistung, sondern kraft seiner Existenz zu. Bei bekannten Persönlichkeiten könnte eine Leistung im Aufbau ihre Images und der damit verbundenen Steigerung des Marktwertes der auf sie bezogenen Daten vorliegen, bei einem Großteil der betroffenen Personen ist dies jedoch nicht der Fall. So erbringt der Betroffene grundsätzlich keine ausreichende Eigenleistung im Rahmen der Datener-

7 Daten als Wirtschaftsgut, S. 19, https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_datens_wirtschaftsgut.pdf?__blob=publicationFile&v=3 (Abruf: 25.4.2019).

8 Stresemann, in: MüKoBGB, 8. Aufl. 2018, BGB, § 90, Rn. 8.

9 Z. B. Heun/Assion, CR 2015, 814.

10 Heun/Assion, CR 2015, 818.

11 Daten als Wirtschaftsgut, S. 21, https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_datens_wirtschaftsgut.pdf?__blob=publicationFile&v=3 (Abruf: 25.4.2019).

12 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 97, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

13 BVerfG, 15.12.1983 – 1 BvR 209/83.

14 BVerfG, 13.6.2007 – 1 BvR 1550/03; Roßnagel/Pfützmann/Garstka, DuD 2001, 258.

15 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 97, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

16 Stender-Vorwachs/Steeger, NJOZ 2018, 1363.

17 Härting, CR 2016, 648f.

18 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 23, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

19 Specht/Rohmer, PinG 2016, 127 (Anfangsseite).

20 Zech, GRUR 2015, 1051; Specht/Rohmer, PinG 2016, 127 (Anfangsseite).

stellung, sodass daran keine Rechtsposition zugeordnet werden kann.²¹

e) Verfassungsrechtlicher Rahmen

Der Normierung eines Ausschließlichkeitsrechts an (personenbezogenen) Daten stehen auch verfassungsrechtliche Gründe entgegen. Zwar gewährt das Recht auf informationelle Selbstbestimmung dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Zugleich wurde jedoch betont, dass dieses Recht keine absolute, uneingeschränkte Herrschaft über Daten vermittelt.²² Das Bundesverfassungsgericht betrachtet Informationen, auch personenbezogene, als ein Abbild sozialer Realität, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann.²³

f) Anonymität eines Datums

Ein besonderes rechtliches Problem besteht auch in der Zuordnung von Daten in personenbezogene oder nicht-personenbezogene. Selbst vormals nicht-personenbezogene Daten können mittels Verknüpfung anderer Informationen aus diversen Quellen einer bestimmten Person zugeordnet werden. Die Schutzbedürftigkeit eines Datums ist in der Praxis dadurch erschwert, dass jede Einzelangabe im Kontext einer Vielzahl weiterer Daten betrachtet werden muss.²⁴ Es ist unklar, ab welchem Grad der Aufwand zur Herstellung eines Personenbezuges als unverhältnismäßig und damit die Daten als anonym zu werten sind. Um den Personenbezug als taugliches Zuweisungskriterium für ein Ausschließlichkeitsrecht anzukennen, bedürfte es einer klaren Definition. Fraglich ist darüber hinaus auch, wie ein vormals personenbezogenes Datum bei einer nachträglichen Anonymisierung zu behandeln ist. Möglich wäre, dass das „Dateneigentum“ des Betroffenen in diesen Fällen erlischt.²⁵ Zu dieser Problematik fehlt bisher ein Ansatz zur Zuweisung eines Ausschließlichkeitsrechts.

g) Mehrrelationalität von Daten

Ein weiteres Problem ist auch die Mehrrelationalität von Daten. Daten beziehen sich häufig auf mehrere Personen.²⁶ Eine eindeutige Zuordnung zu einem Berechtigten ist aufgrund der Mannigfaltigkeit der Aussagemöglichkeit eines Datums nicht stets gewährleistet.²⁷ Am Beispiel eines Autos werden die mehreren Zuordnungsmöglichkeiten der beim Fahren erhobenen Daten gut erkennbar: Die Daten könnten dem Automobilhersteller, dem Händler, dem Serviceprovider, dem Fahrer, dem Eigentümer des Fahrzeugs und/oder dem Halter (insbesondere beim Leasing) zugeordnet werden.²⁸ Diese Problematik könnte durch einen Rückgriff auf das Gemeinschaftseigentum (vgl. §§ 741 ff. BGB) gelöst werden (s. Ziff. II. 4.a). Die Betroffenen könnten dann gemeinschaftlich über das Datum disponieren.²⁹ Dies kann aber in der Praxis unter Umständen schwer handhabbar sein.

h) Fazit

Als Fazit ist festzuhalten, dass Datenschutzrecht kein Ausschließlichkeitsrecht an den personenbezogenen Daten gewährt. Das Datenschutzrecht hat vielmehr primär immaterielle Schutzgüter wie das Recht auf informationelle Selbstbestimmung zum Gegenstand.

5. Zuordnung von Daten ohne Personenbezug

Für Daten ohne Personenbezug ist das Datenschutzrecht nicht anwendbar. Daher stellt sich die Frage nach einer Zuordnung umso

mehr. Derzeit erfolgt eine Zuordnung von Daten meist durch vertragliche Vereinbarung. In einer solchen Vereinbarung können auch Daten geschützt werden. Zudem kann ein unbefugter Zugriff durch technische Schutzmaßnahmen gewährleistet werden. Da Daten grundsätzlich uneingeschränkt reproduzierbar sind, kann eine echte Kontrolle der Verwendung bereitgestellter Daten nur mit technischen Lösungen zur Nachvollziehbarkeit, Rückverfolgbarkeit und Identifizierung der Datenquellen ermöglicht werden. Dies führt zu einer faktischen Herrschaft über die Daten.³⁰

Die Lösung über das Vertragsrecht birgt jedoch auch Nachteile. Ein Vertrag gilt nicht gegenüber jedermann (erga omnes), sondern nur zwischen den Vertragsparteien (inter partes). Zwar kann vereinbart werden, dass eine Partei die Datenherrschaft einer anderen Partei als Dateneigentümer anerkennt. Dies führt jedoch nicht dazu, dass an Daten Eigentumsrechte entstehen. Fehlt es am Eigentum, hat die Datenberechtigung nur eine schuldrechtliche, aber keine dingliche Wirkung.³¹ So ist die Frage der Zuordnung losgelöst von vertraglichen Gestaltungsmöglichkeiten zu beantworten.

Trotz der Schwäche der Drittabwehr, bieten Datennutzungsverträge eine Flexibilität, um den Anforderungen des Einzelfalls gerecht zu werden.³² Geht es um den Schutz von Daten, können diese auch durch Vertraulichkeitsvereinbarungen, welche zum Beispiel eine Vertragsstrafe beinhalten, geschützt werden. Die Übermittlung von Daten funktioniert somit grundsätzlich auch ohne ein Eigentum an Daten, sodass im Handel mit Daten nicht unbedingt eine gesetzliche Zuweisung an Daten erforderlich ist.³³

Für Daten ohne Personenbezug ist zudem die Verordnung für den freien Verkehr von nicht-personenbezogenen Daten (COM/2017/495) anwendbar. Sie trifft jedoch keine Aussage über Eigentum an nicht-personenbezogenen Daten.³⁴

Im Ergebnis besteht derzeit keine Möglichkeit, nicht-personenbezogenen Daten Eigentumsrechte zuzuordnen. Da Daten oft in Kombination von personen- und nicht-personenbezogenen Daten entstehen und eine Abgrenzung oft nicht gelingt, ist auch hier keine eindeutige Zuordnung von Ausschließlichkeitsrechten möglich.

6. Datenverwertungsrecht für personenbezogene Daten in Anlehnung an das Urheberrecht

Daten sind grundsätzlich nicht urheberrechtlich geschützt. Werke im Sinne des Urheberrechts sind nur persönliche geistige Schöpfungen. Auch bei kleinsten Textausschnitten kann der Werkcharakter vorlie-

21 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 92, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

22 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 92, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

23 BVerfGE 65, 43.

24 Schwartmann/Hentsch, PinG 2016, 117, 121.

25 5.1.2.3.1, 93.

26 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 93, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

27 Specht/Rohmer, PinG 2016, 127 (Anfangsseite).

28 Stender-Vorwachs/Steeger, NJOZ 2018, 1361.

29 Specht/Rohmer, CR 2016, 295; Ensthaler, NJW 2016, 3477.

30 Stender-Vorwachs/Steeger, NJOZ 2018, 1360.

31 Stender-Vorwachs/Steeger, NJOZ 2018, 1363.

32 Sahl, PinG 04.16, 150.

33 Stender-Vorwachs/Steeger, NJOZ 2018, 1365.

34 Daten als Wirtschaftsgut, S. 27, https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_daten_wirtschaftsgut.pdf?__blob=publicationFile&v=3 (Abruf: 25.4.2019).

gen.³⁵ Einfache Beschreibungen oder die Wiedergabe rein sachlicher Informationen in Alltagssprache sollen für diesen hingegen nicht ausreichen, sodass gerade in Bezug auf user generated content eine Einzelfallprüfung der Gestaltungshöhe erforderlich ist.³⁶

a) Daten – kein Werkschutz

Urheber und damit Inhaber eines urheberrechtlich geschützten Werkes ist derjenige, der ein Werk, also eine persönliche geistige Schöpfung (§ 2 Abs. 2 UrhG), geschaffen hat (§ 7 UrhG). Ein solches Werk setzt eine menschliche Tätigkeit voraus, die über Individualität verfügt. Der Urheber kann zwar technische Hilfsmittel einsetzen, so dass auch digitale Zeichnungen und Fotografien Werkschutz genießen können. Keine menschliche Tätigkeit liegt dagegen vor, wenn Maschinen ungesteuert vollautomatisch Informationen generieren.³⁷ Zudem erreichen einzelne Worte kaum die nötige Gestaltungshöhe, um hinreichend individuell zu sein. So weisen der Inhalt eines Datums und dessen Entstehung in der Regel wie z. B. bei Kontaktinformationen einzelner Fahrer oder deren PIN keine Schöpfungshöhe in diesem Sinne auf und stammen auch meist nicht von einer Person als Urheber. Mangels persönlicher geistiger Schöpfung bei Daten kann hier nicht auf den Schöpfer abgestellt werden.³⁸ Daher erhält der Betroffene auch kein Ausschließlichkeitsrecht an seinen Daten durch das Urheberrecht.

b) Datenverwertungsrecht nach dem Urheberrecht

Es wird jedoch überlegt, ob unabhängig von der Tatsache, dass ein Datum keinen Urheberrechtsschutz genießt, gleichwohl ein Datenverwertungsrecht für personenbezogene Daten in Anlehnung an das Urheberrecht zu schaffen. Das Eigentum an Daten wäre im Rahmen eines Datenverwertungsrechts jedoch nicht exklusiv. Ein und dasselbe Datum könnte öfter übertragen werden. Daher erfahren Daten eine Nähe zu Lizenzen. An ein und demselben Datum könnten mehrere Lizenzen vergeben werden. Die datenschutzrechtliche Einwilligung könnte beispielsweise durch Lizenzierungen ersetzt werden. Es könnten einfache oder ausschließliche Rechte an den Daten eingeräumt, übertragen und zeitlich, räumlich oder inhaltlich beschränkt werden. Dies würde eine flexiblere Gestaltung als eine datenschutzrechtliche Einwilligung zulassen und die Verkehrsfähigkeit dieser Rechte durch die Übertragbarkeit sichern.³⁹ Bei diesem Ansatz handelt es sich jedoch nicht um eine Zuweisung eines eigentumsähnlichen Ausschließlichkeitsrechts, sondern um eine Ausgestaltung zur Datenverwertung.⁴⁰

7. Zuordnung in Anlehnung an das Datenbankherstellerrecht

Auch das Datenbankherstellerrecht (§ 87a UrhG) bietet keine Eigentumsrechte an Daten. Schutzgegenstand des Datenbankherstellerrechts sind nicht die einzelnen in der Datenbank aufgenommenen Informationen, sondern die Datenbank als Gesamtheit des unter wesentlichem Investitionsaufwand gesammelten, geordneten und einzeln zugänglich gemachten Inhalt als immaterielles Gut. Der Datenbankhersteller kann nur die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Datenbank insgesamt oder nach Art und Umfang wesentlicher Teile untersagen. Dem steht die wiederholte und systematische Nutzung unwesentlicher Teile gleich, sofern diese Handlungen einer normalen Auswertung der Datenbank zuwiderlaufen oder die berechtigten Interessen des Datenbankherstellers unzumutbar beeinträchtigen.

Auch wenn sich aus dem Datenbankherstellerrecht kein Eigentumschutz für einzelne Daten ergibt, könnte sich eine Zuordnung von Daten am Recht des Datenbankherstellers orientieren. Bei der Einführung des Datenbankherstellerrechts ging es um den Schutz der Investition in die Beschaffung, Prüfung und Darstellung der Daten. Inhaber des Datenbankherstellerrechts ist also Datenbankhersteller, der die Herstellung organisatorisch betreut und mit der Investition das wirtschaftliche Risiko trägt. Die getätigte Investition in die Datenerzeugung als Zuweisungskriterium entspricht dem Grundprinzip von Leistungsschutzrechten, wonach demjenigen der Wert des Gutes zugewiesen wird, der für dessen Erzeugung in wirtschaftlicher Sicht verantwortlich ist.⁴¹ Die Kopplung von Investition mit der Verfügungsgewalt an Daten ist grundsätzlich auch bei Daten sachgerecht.

Allerdings kann die Investition nicht als alleiniges Kriterium zur Bestimmung des Inhabers eines Ausschließlichkeitsrechts an Daten dienen. Die Investitionstätigkeit ist ein unbestimmtes Kriterium im Bereich der Daten. Getätigte Investitionen verteilen sich meist auf mehrere Akteure und das Gewicht der einzelnen Beiträge lässt sich häufig schwerlich ermitteln. Beispielsweise verkaufen Autohersteller eventuell ihre Fahrzeuge günstiger, wenn der Käufer in die kontinuierliche Übermittlung von Sensordaten aus dem Fahrzeug einwilligt.⁴² Im Ergebnis erscheint das Abstellen auf die Investition allenfalls als ein Kriterium von mehreren zur Bestimmung des Datenberechtigten geeignet. Zudem ist zu beachten, dass der Investor nicht immer eindeutig erkennbar ist und dies zu Rechtsunsicherheit im Rechtsverkehr führt.

8. Abstellen auf den Skripturakt

Einige Autoren vertreten ein Eigentumsrecht in Analogie zum Strafrechtsschutz. Wer Daten aufzeichnet, soll sie behalten dürfen und andere von der Nutzung ausschließen bzw. die Nutzung von seiner Zustimmung abhängig machen.⁴³ Anknüpfungspunkt für die Verfügungsbefugnis über die Daten im Sinne eines Dateneigentums soll dabei der Skripturakt, der aus dem Strafrecht (§ 202a StGB) stammt, sein. Der Skripturakt ist der Akt des Erschaffens, mit dem das jeweilige Datum erzeugt wird.⁴⁴ Formell Verfügungsberechtigter ist in der Regel die speichernde Stelle, der Ersteller.⁴⁵ Soweit es sich um maschinengenerierte Daten handelt, ist der Ersteller derjenige, der die Maschine bedient. Demzufolge ist grundsätzlich der Ersteller der Berechtigte an diesen Daten. Der Ersteller dürfte regelmäßig auch der Speichernde und Zugreifende sein.⁴⁶

Bei der Übermittlung von Daten ist zunächst der Übermittler Berechtigter, jedoch kann die Verfügungsberechtigung auf den Empfänger

35 EuGH, 16.7.2009 – C-5/08, K&R 2009, 707; OLG München, 14.7.2016 – 29 U 953/16, K&R 2016, 752, WRP 2016, 1557.

36 Bullinger, in: Wandtke/Bullinger, UrhG, 4. Aufl. 2014, § 2, Rn. 156, 159.

37 Bullinger, in: Wandtke/Bullinger, UrhG, 4. Aufl. 2014, § 2, Rn. 16.

38 Vgl. „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 51, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

39 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 95, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

40 Schwartmann/Hentsch, PinG, 2016, 117, 122.

41 Specht/Rohmer, PinG 2016, 127 (Anfangsseite).

42 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 98, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

43 Hoeren, MMR 2013, 486.

44 Kilian/Heussen, ComputerR-HdB, 34. EL, Mai 2018, 20,5 Rechte an Daten, Rn. 21.

45 Eisele, in: Schönke/Schröder, StGB, 30. Aufl. 2019, StGB § 202a, Rn. 8.

46 Markendorf, ZD 2018, 409.

übergehen.⁴⁷ Sind die Daten also für den Empfänger bestimmt, werden sie also z. B. auf einem Server zum Abruf bereitgehalten, wird der Empfänger erst zum Berechtigten, wenn er von seinem Abrufrecht Gebrauch macht.⁴⁸ Geschäftliche E-Mails sind dabei regelmäßig für den Arbeitgeber, private E-Mails hingegen für den Arbeitnehmer bestimmt. Ohne Bedeutung im Strafrecht ist, ob der Täter Eigentümer des Datenträgers ist oder sich die Daten inhaltlich auf ihn beziehen; er wird dadurch weder zum Berechtigten, noch sind sie deshalb schon für ihn bestimmt. Eine solche Bestimmung ist auch noch nicht darin zu sehen, dass Daten unter gewissen Voraussetzungen allgemein zugänglich sind, z. B. der (entgeltliche) Abruf aus einer Datenbank nach ordnungsgemäßem Anschluss.⁴⁹

Der Ansatz des Skripturaktes bedarf daher der Weiterentwicklung: Einerseits muss zwischen den unterschiedlichen Datenarten unterschieden werden. Andererseits muss genau ermittelt werden können, wer für den jeweiligen Skripturakt verantwortlich ist. Eine passende Idee könnte sein, den Skripturakt mit dem Ansatz der Zuweisung entsprechend dem Investitionsanteil zu verbinden.⁵⁰

9. Zuordnung nach Geschäftsgeheimnis

Ein ausschließliches Recht an Daten kann nicht nur im Wege des Eigentums, sondern auch durch faktische Exklusivität erreicht werden. Zum Beispiel durch Geheimhaltung von Daten. Wird das Geheimnis jedoch offenbart, dann endet diese Exklusivität und es besteht – anders als bei einem echten Ausschließlichkeitsrecht – keine (rechtlich gewährte) Exklusivität mehr.⁵¹ Ähnlich wie eine Geheimhaltungsvereinbarung können Datenbanklizenzverträge, Übertragungen von Rechten an Datenbanken etc. wirken.

Auch die gesetzliche Regelung von Betriebs- und Geschäftsgeheimnissen kann einen Schutz von Daten gewähren. Geschäftsgeheimnisse sind nunmehr insbesondere nach dem Gesetz zum Schutz von Geschäftsgeheimnissen („GeschGehG“) geschützt, das am 26.4.2019 in Kraft getreten ist. Dieses Gesetz enthält – erstmalig im deutschen Recht – eine Definition des Begriffs des Geschäftsgeheimnisses. Demnach ist ein Geschäftsgeheimnis eine Information, die nicht allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und die Gegenstand von den Umständen angemessenen Geheimhaltungsmaßnahmen ist (§ 2 Satz 1 Nr. 1 GeschGehG).⁵² Durch das neue Geschäftsgeheimnisgesetz wird ein quasi-proprietäres Recht geschaffen, das nunmehr auch Unterlassungs-, Auskunft-, Rückruf-, Vernichtungs- und Schadensersatzansprüche des Geheimnisinhabers umfasst.⁵³

10. Integritätsschutz durchs Deliktrecht

Außerhalb von Vertragsbeziehungen schützt das Deliktrecht die Integrität von Daten nicht ausreichend. Das Deliktrecht schützt Daten nur lückenhaft. Eine Verletzung des nach § 823 Abs. 1 BGB geschützten Eigentums allgemein beim Datenverlust wird mangels Körperlichkeit der Daten abgelehnt.⁵⁴ Eine Eigentumsverletzung wird jedoch bei Veränderung eines Datenträgers sowie bei Löschen oder Verändern von Daten auf einem Datenträger angenommen. Über das Deliktrecht wird somit mittelbar die Integrität der verkörperten Daten geschützt.⁵⁵

Allerdings sind weder die einzelnen elektronischen Daten als solche noch der Datenbestand einer Person als sonstiges Recht nach § 823 Abs. 1 BGB einzustufen. Solche Daten sind nicht nach dem Deliktrecht geschützt, sodass der mittelbare Integritätsschutz von Daten

heute nicht (mehr) ausreicht.⁵⁶ Schutzlücken bestehen insbesondere bei Datenverarbeitungsstrukturen in der Cloud. Löscht oder beeinträchtigt ein Dritter auf andere Weise fahrlässig die Integrität von Daten, stehen dem Dateninhaber meist keine Ansprüche nach § 823 Abs. 1 BGB zu, da er kein Eigentümer des als Cloud-Service bezogenen Speicherplatzes ist und ihm auch keine Besitzposition zugewiesen werden kann.⁵⁷

Im Ergebnis ist festzuhalten, dass der Integritätsschutz von Daten aufgrund deliktischer Bestimmungen derzeit unzureichend ist, da das Deliktsrecht nicht ausreichend vor einer fahrlässigen Beeinträchtigung durch Dritte schützt. Ein verbesserter Integritätsschutz für Daten, die nicht auf eigenen Datenträgern gespeichert sind, führt zu mehr Rechtssicherheit. Zudem stärkt es das Vertrauen von Unternehmen, künftig mehr Datenverarbeitungsvorgänge in die Cloud auszulagern. Es könnte z. B. die Einführung einer eigenen Haftungsnorm erwogen werden.⁵⁸

11. Fazit zu Eigentum an Daten – Zuordnung

Es wurden die verschiedenen Ansätze zur Ermittlung eines Datenberechtigten dargestellt, insbesondere Daten mit und ohne Personenbezug, sachenrechtlicher Eigentumsbegriff, Zuordnung nach Speichermedium, Investitionsschutz und der Skripturakt. Im Ergebnis wird deutlich, dass kein Ansatz vollständig überzeugen kann. Allerdings sind einige Indizien für eine sachgerechte Zuordnung erkennbar. Insbesondere der Gedanke des Investitionsschutzes und die Bestimmung des Datenerzeugers mittels Abstellens auf den Skripturakt können als Grundlage zur Ermittlung des Berechtigten dienen.

An Daten besteht nach bisheriger Rechtslage kein Eigentum. Daten werden partiell durch Gesetze wie die Datenschutz-Grundverordnung, das Geschäftsgeheimnisgesetz, das Wettbewerbs- und Strafrecht geschützt. Daneben besteht ein Schutz der Daten durch faktische Zugriffsbeschränkungen. Derzeit besteht nach überwiegendem Diskussionsstand allerdings keine Notwendigkeit, ein neues exklusives dingliches Datenrecht zu schaffen. Sollte sich zeigen, dass ein Zugang zu Daten reguliert werden muss, setzt dies kein Eigentum an Daten voraus. Ein Zugewinn ist durch die Schaffung eines Eigentums an Daten auch nicht ersichtlich. Vertragliche Regelungen und technische Schutzmaßnahmen tragen im Übrigen dazu bei, dass in der Praxis kein Bedarf nach einer neuen gesetzlichen Regelung zur eigentumsrechtlichen Zuordnung von Daten besteht. Dies führt nun automa-

47 Eisele, in: Schönke/Schröder, StGB, 30. Aufl. 2019, StGB § 202a, Rn. 10.

48 BT-Drs. 16/3656, 9.

49 BT-Drs. 16/3656, 9.

50 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 102, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

51 Daten als Wirtschaftsgut, S. 25, https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_datens_wirtschaftsgut.pdf?__blob=publicationFile&v=3 (Abruf: 25.4.2019).

52 Daten als Wirtschaftsgut, S. 26, https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/2017-11-22_smartdata_datens_wirtschaftsgut.pdf?__blob=publicationFile&v=3 (Abruf: 25.4.2019).

53 S. dazu auch den BB-Online-Standpunkt von *Brammsen/Apel*, <https://betriebs-berater.ruw.de/bb-standpunkte/standpunkte/Das-Geschäftsgeheimnisgesetz-GeschGehG-ist-in-Kraft-getreten-38143> (Abruf: 9.5.2019).

54 Z. B. LG Konstanz, 10.5.1996 – 1 S 292/95.

55 Härting, CR 2016, 647.

56 Spindler, JZ 2016, 812; Wendehorst, NJW 2016, 2612.

57 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 115, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

58 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 122, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

tisch zu der Frage, ob in der Datenpraxis Bedarf danach besteht, gesetzliche Regelungen über einen *Zugang von Daten* zu fordern.

II. Zugang statt Zuordnung

1. Ausgangslage

Fakt ist, dass eine datengetriebene Wirtschaft bzw. die Schaffung und Förderung digitaler Geschäftsmodelle nicht nur mit der Erhebung und Verarbeitung von Daten steht und fällt, sondern auch damit, dass (Start-up-)Unternehmen Zugang zu Daten ermöglicht wird. Hier geht es einerseits um Daten der öffentlichen Hand, andererseits aber auch um Zugang zu den von Datenkraken gehorteten Datensätzen. Denn im Interesse übergeordneter gesellschaftlicher Ziele ist es hinderlich, den (weiteren) Ausbau von Marktmacht dadurch zuzulassen, dass faktische Monopole entstehen. Die Entwicklung von künstlicher Intelligenz, Big Data Analysen etc. sind nur dann möglich, wenn Zugang zu Daten besteht. Grundsätzlich unterschieden werden sollte hierbei zwischen den Bereichen der öffentlichen Daseinsvorsorge und rein kommerziellen Nutzungen.

2. Öffentliche Daseinsvorsorge

Zur öffentlichen Daseinsvorsorge gehören beispielsweise die Bereiche Sicherheit, Verkehr, Gesundheit, Energiebewirtschaftung, Landwirtschaft/Ernteerträge, die Strafverfolgung bzw. die Bereiche Mieten und Wohnen. Die öffentliche Hand, die in diesen Bereichen ihren Aufgaben nachkommen will, ist im Zuge einer zunehmenden Digitalisierung darauf angewiesen, Zugang zu Daten zu haben, die von Unternehmen in diesen Bereichen erhoben werden. So kann es im Bereich der Gesundheitsvorsorge oder bei Katastrophenfällen sinnvoll sein, staatlichen Stellen Zugang zu Standortdaten von Mobiltelefonen zu verschaffen. Seitens der Versicherungswirtschaft wird vorgeschlagen, dass z. B. Kfz-Hersteller anonymisierte Daten im Interesse von Schadensregulierungen über einen neutralen „Datentreuhänder“ zur Verfügung stellen. Gerade mit Hinblick auf autonom fahrende Kraftfahrzeuge wird es in Zukunft kaum noch möglich sein, Schadensfälle zu rekonstruieren oder Schadensursachen festzustellen, ohne dass Zugriff auf die bei der Kfz-Industrie vorhandenen Daten gewährt wird. Dass hierbei Sicherheitsrisiken, Cyberattacken etc. Rechnung getragen werden muss, ist selbsterklärend.

Anstöße für eine mögliche Regelung bietet zum Beispiel die EU-Verordnung zum freien Datenverkehr vom 13.9.2017 (COM/2017/495) – „Free Flow Verordnung“. Gemäß Art. 1 dieser Verordnung soll der freie Verkehr nicht-personenbezogener Daten in der Union gewährleistet werden. Ziel der Verordnung ist es, neue digitale Techniken, Big Data, künstliche Intelligenz und dem sogenannten Internet der Dinge eine maximale Effizienzsteigerung zu verschaffen. Die Verordnung will dies dadurch bewirken, dass grenzüberschreitende Mobilität nicht-personenbezogener Daten im Binnenmarkt verbessert wird, zuständige Behörden im Rahmen ordnungspolitischer Kontrollzwecke Zugang zu Daten auch in anderen EU-Staaten erhalten. Art. 5 Abs. 1 der Verordnung regelt daher, dass der Zugang zuständiger Behörden zu Daten nicht mit der Begründung verweigert werden darf, dass die Daten in einem anderen Mitgliedstaat gespeichert werden. Behörden eines anderen Mitgliedstaates sind gemäß Art. 5 Abs. 2 der Verordnung verpflichtet, insoweit Amtshilfe zu leisten.

Einen weiteren Denkansatz zum Datenzugang zugunsten von Behörden im Rahmen der öffentlichen Daseinsvorsorge bietet die Novellie-

rung der Public Sector Information Richtlinie (PSI Richtlinie) vom 25.4.2018 (2013/37/EU). Mit der Novellierung der PSI-Richtlinie wird zwar das wirtschaftspolitisch motivierte Anliegen verfolgt, privaten Unternehmen Informationen, die bei öffentlichen Stellen vorhanden sind, kostengünstig oder kostenfrei elektronisch zur Verfügung zu stellen; dies gerade zu dem Zweck, neue Geschäftsmodelle zu ermöglichen. Art. 10 Abs. 2 der Novellierung sieht die generelle Verpflichtung vor, die gewerbliche bzw. nicht-gewerbliche Weiterverwendbarkeit von öffentlich zugänglichen Forschungsdaten für Dritte zu ermöglichen. Unabhängig von der an der Novellierung der PSI-Richtlinie unter anderem von öffentlichen Verkehrsunternehmen geäußerten Kritik, steht die Novellierung der PSI-Richtlinie stellvertretend für den Bedarf, Zugang zu Daten zu verschaffen. Die Kritik richtet sich dagegen, dass Verkehrsunternehmen der öffentlichen Hand (Nahverkehr, Flughäfen, Binnenhäfen etc.) künftig verpflichtet sein sollen, in Echtzeit Daten der Industrie zur Verfügung zu stellen. Die Kritik wird in erster Linie mit Bezug auf Datenkraken geäußert, die mit derartigen Daten weitere Geschäftsmodelle gerade zu Lasten eines Wettbewerbs nutzen können. Auch wenn die PSI-Richtlinie Datenzugang zugunsten der Privatwirtschaft ermöglichen soll, bietet sie einen Denkansatz dafür, über eine Regelung auf EU-Ebene nachzudenken, aufgrund derer *umgekehrt* dem Staat im Rahmen öffentlicher Daseinsvorsorge analog den Regelungen der PSI-Richtlinie Zugriff auf Daten von Unternehmen verschafft wird.

3. Kommerzielle Nutzungen

Schwieriger ist der Bereich eines Zugangs von Daten auf privatwirtschaftlich-unternehmerischer Ebene. Denn jedes Unternehmen, das im Rahmen seiner geschäftlichen Aktivitäten Daten sammelt, um diese (zu eigenen Zwecken) zu verarbeiten und kommerziell zu nutzen, wird sich zu Recht die Frage stellen, warum anderen Unternehmen zu deren kommerzieller Nutzung Daten zur Verfügung gestellt werden sollen. Andererseits mehrten sich in der Wirtschaft in letzter Zeit Fälle, in denen Unternehmen kooperieren und über gemeinsame Plattformen wechselseitig Zugang zu Daten schaffen; dies im beidseitigen Interesse zur Optimierung bestehender Produkte oder Dienstleistungen sowie zur Förderung neuer Geschäftsmodelle. So gibt es beispielsweise die industrielle digitale Plattform Mindsphere von Siemens, ein offenes IoT-Betriebssystem, das es ermöglicht, Systeme, Maschinen, Anlagen und Produkte zu verbinden, Daten zu analysieren und für Prozesse der Industrie 4.0 zu nutzen. Oder das von Disney und Audi gegründete Gemeinschaftsunternehmen Holoride, dessen Ziel Virtual-Reality-Anwendungen bei Autofahrten sind. Das Unternehmen bietet auch Dritten eine Schnittstelle zu Fahrzeugdaten, um diese in eigene Inhalte einzubauen.

4. Open Data Plattform

Bei der Frage, ob, in welchem Umfang und ob ohne oder gegen Zahlung einer Vergütung Schnittstellen zur Überlassung von Daten einzuräumen sind, wird es selbstredend noch eine Fülle von Vertrags- und lizenzrechtlichen Fragen zu klären geben. Nachfolgend einige Anregungen:

a) Joint Ownership

Wie vorstehend beschrieben (Ziff. I. 4) sind an der Datenerzeugung häufig mehrere Unternehmen bzw. Personen beteiligt. In Fällen einer

„Joint Ownership“ könnte daran gedacht werden, die Regelungen aus §§ 741 ff. BGB anzuwenden. Gemäß § 743 Abs. 2 BGB ist jeder Teilhaber einer Bruchteilsgemeinschaft zum Gebrauch des gemeinschaftlichen Gegenstandes insoweit befugt, als nicht der Mitgebrauch der übrigen Teilhaber beeinträchtigt wird. Auf Grundlage dieser Bestimmung erscheint es möglich, mehreren an einer Datenerzeugung Beteiligten wechselseitig Zugang zu Daten der jeweils anderen Joint Owner zu verschaffen.

b) Missbrauch einer marktbeherrschenden Stellung

Das Horten von Daten bzw. die Verweigerung des Zugangs durch marktbeherrschende Unternehmen kann den Missbrauch einer marktbeherrschenden Stellung bedeuten. So hat der Europäische Gerichtshof in seiner Entscheidung „Lizenzverweigerung/Essential Facilities“⁵⁹ entschieden, dass ein marktbeherrschendes Unternehmen, das sich weigert, eine Lizenz an einem gemäß § 4 UrhG geschützten Datenbankwerk zu erteilen, missbräuchlich nach Art. 82 EG Vertrag (heute: Art. 102 AUEV) handeln kann; dies u. a. dann, wenn die Weigerung geeignet ist, dem Inhaber des betroffenen Rechts einen bestimmten Markt vorzubehalten, indem jegliche Wettbewerber auf diesem Markt ausgeschlossen werden. Analog zu der Begründung des Europäischen Gerichtshofs im vorgenannten Fall könnte die Verweigerung eines marktbeherrschenden Unternehmens, Zugang zu Daten zu gewähren, ebenfalls einen Missbrauch darstellen. Auch die Europäische Kommission erwägt aktuell, als milderes Mittel gegenüber einer Zerschlagung von marktbeherrschenden Unternehmen der Digitalwirtschaft oder Verboten, eigene Produkte auf monopolartigen Plattformen anzubieten, Dritten Zugang zu Daten von Datenkraken zu ermöglichen.⁶⁰

c) Auskunftsrechte

Der Zugang zu Daten kann durch Auskunftsrechte geregelt werden. In Bezug auf staatliche Daten existiert mit dem Informationsfreiheitsgesetz und diversen bereichsspezifischen Regelungen wie z. B. dem Umweltinformationsgesetz und dem Geodatenzugangsgesetz bereits ein im Grundsatz voraussetzungsloser Zugang zu den in Daten verkörperten Informationen.

d) Rechtliche Lösungsansätze

Neben gesetzlichen Ansprüchen auf Datenzugang und einem kommerziellem Austausch von Daten wird ein Anreizsystem durch offene Daten-Plattformen für einen Austausch diskutiert: Daten als Allgemeingüter bzw. als Datenallmende.⁶¹ Durch einheitliche Standards und rechtliche Marktbedingungen können Voraussetzungen und Bedingungen für eine freiwillige Zurverfügungstellung und Nutzung der Daten geschaffen werden. Dies könnte auch eine unentgeltliche Nutzung und insbesondere Verarbeitung und Aggregation der Daten ermöglichen.⁶² Eine solche Plattform könnte auch als Open-Data-System gestaltet werden. So wie Softwareanwendungen einen Open-Source-Ansatz verfolgen, ist auch ein open bzw. shared Ansatz zur Datenökonomie vorstellbar.

5. Fazit zu Zugang statt Zuordnung

Statt einer neuen gesetzlichen Regelung einer eigentumsähnlichen Zuordnung von Daten erscheint es sinnvoller, über eine gesetzliche Lösung hinsichtlich des Zugangs von Daten nachzudenken. Zur Erfüllung staatlicher Aufgaben, wie Ausbau und Erhalt der öffentlichen

Infrastruktur, könnte eine Pflicht eingeführt werden, dem Staat an Daten im Rahmen der vorstehend beschriebenen hoheitlichen Aufgaben zu gewähren. Diese Verpflichtung von Privaten kann alle Daten erfassen, die der reinen Verkehrssicherheit und dem sonstigen Gemeinwohl, wie z. B. Informationen über den Straßenzustand, dienen.⁶³

Zunehmen dürfte auch der kommerzielle Austausch von Daten zwischen Unternehmen. Es bleibt abzuwarten, wie und ob sich ein Open-Data-System etablieren wird. Sofern ein solches Open-Data-System durch gesetzliche Regelungen unterstützt werden sollte, sollten entsprechende Regelungen hinsichtlich des Zugangs zu Daten nicht national, sondern auf europäischer Ebene, bestenfalls international gestaltet werden.

III. Ausblick

„Eigentum an Daten – Zugang statt Zuordnung“ lautet die Ausgangsthese dieses Beitrages. Nach momentanem Stand der Diskussion ist festzuhalten, dass kein (neues) Recht der Datenerzeugung mit der Folge der Schaffung einer absoluten Rechtsstellung erforderlich ist. Sinnvoll ist vielmehr, die Verhältnisse mehrerer an einer Datenerzeugung Beteiligter zu klären, wobei die Regelungen der §§ 741 BGBff. einen Ansatz bieten. Des Weiteren ist es sinnvoll, neue Regelungen zu schaffen, die den Zugang Dritter zu Daten regeln, ggf. gegen Zahlung einer angemessenen Vergütung. Dabei ist zu unterscheiden zwischen der Ebene staatlichen Zugriffs auf Daten von Privatunternehmen im Rahmen der öffentlichen Daseinsvorsorge und auf wechselseitigen Zugriff von Unternehmen im Bereich der Privatwirtschaft untereinander.

Dr. Udo Kornmeier, RA, ist Partner bei Schalast Rechtsanwälte Notare und betreut Mandanten insbesondere im Urheber- und Medienrecht sowie im Bereich International Litigation.



Anne Baranowski, LL.M., RAin, ist Council bei Schalast Rechtsanwälte Notare und betreut Mandanten insbesondere im IT-, Datenschutz- und Urheberrecht mit einem Schwerpunkt auf der Technologie- und Medienbranche.



59 EuGH, 29.4.2004 – Az. C-418/01, EWS 2004, 310 m. EWS-Komm. *Welser*, WRP 2004, 717, BeckRS 2004, 77143.

60 So Wettbewerbskommissarin *Vestager*, FAZ vom 15.4.2019.

61 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 116, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

62 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 4, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).

63 „Eigentumsordnung“ für Mobilitätsdaten?, BMVI, S. 117, https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (Abruf: 25.4.2019).