Smart Data

Daten als Wirtschaftsgut

Europäische Datenökonomie oder Rechte an Daten?

Impressum

Herausgeber
Smart-Data-Begleitforschung
FZI Forschungszentrum Informatik
Außenstelle Berlin
Friedrichstr. 60, 10117 Berlin
www.smart-data-programm.de

Redaktion und Konzeption
Fachgruppe Rechtsrahmen der Smart-Data-Begleitforschung

Schlussredaktion und Gestaltung
LoeschHundLiepold Kommunikation GmbH

Stand
September 2017

Druck
WIRmachenDRUCK, Backnang

Bildnachweis
sdecoret – Fotolia.com (Titel), Nataliya Hora – Fotolia.com (S. 9), xiaoliangge – Fotolia.com (S. 10), 75tiks – Fotolia.com (S. 11), Gorodenkoff – Fotolia.com, (S. 12), nd3000 – Fotolia.com (S. 17), alphaspirit – Fotolia.com (S. 22), Björn Wylezich – Fotolia.com (S. 40), Olivier Le Moal – Fotolia.com (S. 41), by-studio – Fotolia.com (S. 42)

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

Inhalt

Vorwort

Eine ökonomische Betrachtung von Daten als einem der zentralen Wirtschaftsgüter im Kontext von Big Data, Industrie 4.0 oder des Internets der Dinge stellt die Rechtsordnung vor große Herausforderungen, die mit der Einleitung eines Konsultationsprozesses zur Schaffung einer „europäischen Datenökonomie“ durch die EU-Kommission nun zunehmend auch in der europäischen Dimension an Bedeutung gewinnt. Sollten Informationen grundsätzlich frei verfügbares Gemeingut sein – zumindest solange nicht das Datenschutzrecht, Urheberrechte bzw. der Schutz der Datenbankhersteller sui generis, der Schutz als Betriebs- oder Geschäftsgeheimnis oder Strafrechtsnormen einem freien Zugang entgegenstehen? Kann die Schaffung eines über die bereits bestehenden Rechte hinausgehenden allgemeinen „Rechts am Datum“ Impulse für die zukünftige Ausgestaltung der Datenökonomie generieren? Oder werden sich vielmehr die typischen Rechtsfolgen von Ausschließlichkeitsrechten als wenig zielführend erweisen? Wie könnten – aus unserer Perspektive vorzugswürdig – die Ausgestaltung von wettbewerblichen Zugangsansprüchen zu Daten und Plattformen sowie diese ergänzenden vertraglichen Regelungen ein kohärentes gesetzliches Gesamtbild unter Einbeziehung von Datenschutzaspekten bilden?

In der Fachgruppe Rechtsrahmen wurde diese Thematik intensiv diskutiert. Als Zwischenfazit präsentieren wir fünf Thesen, die in der Fachgruppe abgestimmt wurden.

Wir bedanken uns ganz herzlich bei unseren Autoren Herrn Dr. Alexander Duisberg und Herrn Bunk, die diese Publikation mit fundierten wissenschaftlichen Inhalten und wertvollen Erfahrungen unterstützt haben.
Im ersten Beitrag wird der aktuelle Meinungsstand der juristischen Diskussion aufbereitet und der bestehende Schutzrahmen von Datensammlungen im Urheber- und Wettbewerbsrecht skizziert. Der zweite Beitrag widmet sich der im Kontext von Smart Data relevanten Technik des Text und Data Minings und deren Konflikt mit dem Urheberrecht.

Im Abspann finden Sie Kurzerläuterungen zu den wesentlichen Begrifflichkeiten und Aspekten des Rechtsrahmens in Bezug auf „Daten als Wirtschaftsgut“. Nicht personenbezogene Daten befinden sich keinesfalls in einem rechtsfreien Raum. Auch abseits des im Rahmen des Entstehungsprozesses der kommenden Datenschutz-Grundverordnung viel diskutierten Datenschutzrechts finden sich wichtige Rechtsfragen, die die Nutzung von Daten beeinflussen können. So können Daten als Bestandteil einer schutzfähigen Datenbank, eines Text- oder Bildwerkes sowie eines Presseerzeugnisses nur mit Zustimmung des jeweiligen Urhebers bzw. Herstellers nutzbar sein. Daneben können Daten als Betriebs- und Geschäftsgeheimnis rechtlich geschützt sein. Erwähnung finden sollte ebenfalls die Strafbarkeit des Abfangens und Ausspähens von Daten.

PD Dr. Oliver Raabe und Manuela Wagner
Begleitforschung des Technologieprogramms
„Smart Data – Innovation aus Daten“

Fünf Forderungen zur europäischen Datenökonomie

Die Fachgruppe Rechtsrahmen der Begleitforschung des Technologieprogramms „Smart Data – Innovationen aus Daten“ besteht aus Vertretern der 16 Leuchtturmprojekte des Technologieprogramms sowie Expertinnen und Experten aus Politik, Wirtschaft und Wissenschaft. Im Rahmen von regelmäßigen Fachgruppenworkshops diskutierten die Expertinnen und Experten über die Schaffung einer europäischen Datenökonomie und formulierten fünf zentrale Forderungen.

Forderung 1: Der Zugang zu anonymen, von Maschinen erzeugten Daten sollte verbessert werden

Die EU-Kommission startete dieses Jahr den Konsultationsprozess zu der Frage, wie eine europäische Datenökonomie geschaffen werden kann.[1] Zentrales Thema ist die Verbesserung des grenzüberschreitenden Datenaustauschs. Auf Basis der in den Pilotprojekten gewonnenen Erkenntnisse stimmt die Mehrheit der Teilnehmer der Fachgruppe Rechtsrahmen in der Smart-Data-Begleitforschung dem von der EU-Kommission postulierten Ziel zu, dass eine Verbesserung des Zugangs zu anonymen Daten sinnvoll ist:

> „Indem von Maschinen generierte Daten geteilt, wiederverwendet und aggregiert werden, können sie Wertschöpfung begründen, werden zu Innovationsquellen und ermöglichen unterschiedlichste Geschäftsmodelle."

Die EU-Kommission definiert dabei von Maschinen generierte Daten folgendermaßen:

> „Daten werden von Maschinen ohne den unmittelbaren Eingriff eines Menschen im Rahmen von Computerprozessen, Anwendungen oder Diensten oder auch durch Sensoren erzeugt, die Informationen von virtuellen oder realen Geräten oder Maschinen oder von einer Software erhalten."

Als potenzielle Lösungsmöglichkeiten zur Schaffung von Anreizen, Daten zu teilen und damit den Zugang zu anonymen, von Maschinen erzeugten Daten zu verbessern, schlägt die Kommission folgende Ansätze vor:

- Erstellung von EU-Leitfäden zur Rechtslage in den Mitgliedstaaten
- Förderung der Entwicklung technischer Lösungen für die zuverlässige Identifizierung und den Austausch von Daten
- Standardvertragsklauseln für den (rechtssicheren) Austausch von Daten
- Schaffung eines Rechts auf Zugang zu nicht personenbezogenen Daten im öffentlichen Interesse oder für wissenschaftliche Zwecke
- Schaffung eines Rechts des „Datenerzeugers": Der Eigentümer oder Besitzer des Gerätes hätte dadurch das Recht, nicht personenbezogene Daten zu nutzen und anderen deren Nutzung zu gestatten oder sie von der Nutzung auszuschließen
- Schaffung von Zugangsrechten gegen Entgelt

Die Mehrheit der Teilnehmer der Fachgruppe Rechtsrahmen sieht Potenzial in der Förderung technischer Lösungen und der Schaffung von Zugangsrechten im öffentlichen Interesse und für Forschungszwecke. Dem Konzept eines Eigentumsrechts an Daten stehen die Mitglieder der Fachgruppe eher ablehnend gegenüber. Es sollte kritisch hinterfragt werden, ob der Datenzugang durch eine eigentümerähnliche Rechtsstellung des „Datenproduzenten" tatsächlich befördert werden kann oder ob diese nicht vielmehr die Gefahr steigender Transaktionskosten und einer Verstärkung von Lock-in-Effekten in sich birgt. Ein (ausschließliches) Dateneigentum wäre auch mit Blick auf die Meinungs- und Informationsfreiheit problematisch und könnte zu ungewollten Informationsmonopolen führen. Zudem sind diverse Abgrenzungsfragen zu befürchten. Da Daten in der Regel durch Interaktion von Maschinen mit Menschen, anderen Maschinen oder ihrer Umwelt entstehen, dürften sich Herausforderungen bei der Zuordnung zu einem einzigen „Erzeuger" ergeben. Personenbezug könnte gegeben sein, sobald Daten auch Rückschlüsse auf identifizierbare natürliche Personen zulassen, sodass Überschneidungen mit dem Datenschutzrecht absehbar sind.

Die größte Herausforderung dürfte daher darin liegen, eine rechtliche Basis für Datenzugang unter nicht diskriminierenden Konditionen zu gewährleisten. Insoweit könnten wettbewerbsrechtliche Mechanismen erforderlich sein, um Anreize für einen unternehmens- und grenzüberschreitenden Datenaustausch zu schaffen. Die Standardisierung und Herstellung von Interoperabilität dürften technische Grundvoraussetzungen für einen funktionierenden Datenaustausch bilden.

Einige Smart-Data-Projekte verfolgen das Ziel, offene Plattformen für den unternehmensübergreifenden Datenaustausch zu realisieren. Herausforderungen, die sich u. a. dabei stellen, sind die Interessen der Unternehmen, ihre Betriebs- und Geschäftsgeheimnisse zu schützen und keine personenbezogenen Daten ohne Legitimationsgrundlage herauszugeben. Die Entwicklung intelligenter Filtermechanismen, Anonymisierungswerkzeuge sowie Konzepte der Datennutzungskontrolle könnten Lösungen bieten.

Die Smart-Data-Begleitforschung engagiert sich in der Förderung eines kulturellen Wandels hin zur Open-Data-Ökonomie für eine smarte Gesellschaft.[2] Der Begriff „Open Data“ steht für technische und rechtliche Offenheit, d. h., Datensätze müssen in einem maschinenlesbaren und standardisierten Format vorliegen und frei von rechtlichen Beschränkungen nutzbar sein (d. h. allgemein zugänglichen bzw. nicht unverhältnismäßig einschränkenden Lizenzbestimmungen unterliegen).

Forderung 2: Entwicklung technischer Lösungen für zuverlässige Identifizierung und Datenaustausch fördern

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. Sowohl Lizenzmodelle als auch Open-Data-Konzepte erfordern zunächst standardisierte, genormte Protokolle, Schnittstellen und Datenformate. Oft sind Daten nicht frei von Lizenzbestimmungen oder technischen Einschränkungen verfügbar. Wenn Daten in unterschiedlicher Granularität und verschiedenen Formaten vorliegen oder bereits vorinterpretiert sind, erschwert gerade die Fragmentierung deutschlandweite Analysen. Die Entwicklung von Datentreuhänder-Konzepten sowie die Standardisierung maschinenlesbarer, freier Formate, insbesondere bei Daten der öffentlichen Hand, wären hier Lösungsoptionen. Um Vertrauen in das System zu schaffen und Aussagen über die Datenqualität zu gestatten, kann es auch notwendig werden, zuverlässige und möglichst genormte Protokolle für die durchgehende Identifizierung von Datenquellen festzulegen.

Offene, genormte und gut dokumentierte Programmierschnittstellen (API) können den Aufbau eines Ökosystems der Anwendungs- und Algorithmenentwicklung fördern und so den Zugang zu Daten, die sich in der Hand von Unternehmen oder Behörden befinden, vermitteln. Um sicherzustellen, dass der Zugang datenschutzkonform ist, sollte die Entwicklung von Anonymisierungswerkzeugen und -prüfverfahren unterstützt durch technische Leitfäden parallel gefördert werden.

Forderung 3: Künftige Lösungen sollten Lock-in-Effekte minimieren

Ein Lock-in-Effekt kann vorliegen, wenn die Höhe der zu erwartenden Wechselkosten einem Anbieterwechsel entgegenstehen. Derartige Wechselbarrieren können einerseits bewusst zur Kundenbindung eingesetzt werden, andererseits Markteintrittshemmnisse für kleinere neue Mitbewerber schaffen.

Bei der Etablierung einer europäischen Datenökonomie sollten die divergierenden Verhandlungspositionen von marktmächtigen und weniger marktmächtigen Unternehmen sowie Privatpersonenberücksichtigt werden. Vor allem für kleine und mittelständische Unternehmen, Start-ups und Privatpersonen sollten Lock-in-Effekte vermieden werden.

Sowohl das europäische als auch das deutsche Wettbewerbsrecht sind derzeit grundsätzlich erst dann einschlägig, wenn der Missbrauch einer marktbeherrschenden bzw. marktmächtigen Stellung feststellbar ist. Die hierbei relevanten Fragen der Marktabgrenzung, der Marktkonzentration und der Missbrauchsschwellen müssen dem Wandel hin zu mehrseitigen, datenbasierten Märkten angepasst werden.

Die 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen, die am 9. Juni 2017 in Kraft getreten ist, verfolgt das Ziel, ein modernes Wettbewerbsrecht im Zeitalter der Digitalisierung zu erreichen. Die Reform soll vor allem auf Daten basierende Netzwerk- und Skaleneffekte adressieren, die zu Marktkonzentration führen können, sowie den Zugang zu wettbewerbsrelevanten Daten besser berücksichtigen. Dadurch sollen die Kartellbehörden im Rahmen ihrer Missbrauchsaufsicht die Marktstellung eines Unternehmens besser, da nicht nur auf Basis von Geldflüssen, beurteilen können und damit den sich verändernden internetbasierten Angeboten Rechnung tragen.

Einen weiteren Diskussionspunkt bildet die Frage, ob es ein allgemeines Recht auf Datenportabilität, vergleichbar mit Art. 20 der Datenschutz-Grundverordnung („Recht auf Datenübertragbarkeit“), geben sollte.

Forderung 4: Recht auf Zugang zu Daten im öffentlichen Interesse oder für wissenschaftliche Zwecke

Forschung im Bereich „Smart Data“ basiert häufig auf nicht personenbezogenen Daten aus dem Unternehmenskontext, zu denen Forscher Zugang benötigen, um datenbasiert innovationssteigernde neue Erkenntnisse zu generieren. Ebenso kann die Funktionsfähigkeit des öffentlichen Sektors durch die Analyse statistischer Daten verbessert werden. Würde beispielsweise Statistikämtern Zugang zu Geschäftsdaten gewährt, könnte der Aufwand für Wirtschaftsteilnehmer verringert werden, gegebenenfalls bestehenden Berichtspflichten nachzukommen. Die dadurch ermöglichte Infrastrukturoptimierung könnte sich wiederum insgesamt positiv auf den Wirtschaftsstandort auswirken.

Bei der Schaffung eines Zugangsrechts muss selbstverständlich der Problematik Rechnung getragen werden, dass die Abgrenzung zwischen personenbezogenen und anonymen Daten oft fließend ist und sich im Laufe der Zeit durch hinzutretendes Zusatzwissen oder die Verbesserung von Analysemethoden verändern kann. Ein (wettbewerbsrechtliches) Zugangsrecht sollte daher die widerstreitenden Interessen in Ausgleich bringen und dabei den Fokus auf einen nicht diskriminierenden Zugang sowie Interoperabilität richten. Dies sollte kohärent mit der kommenden Datenschutz-Grundverordnung etabliert werden.

Daneben muss das Interesse der Unternehmen, ihre Betriebs- und Geschäftsgeheimnisse zu bewahren, berücksichtigt werden. Anonymisierungsmethoden könnten hier z. B. neben dem Schutz personenbezogener Daten auch dazu eingesetzt werden, um den Unternehmensbezug aus einem Datensatz zu entfernen.

Forderung 5: Schaffung eines diskriminierungsfreien Rechtsrahmens für Text und Data Mining sowie Webcrawling

Im Vorschlag für eine Richtlinie über das Urheberrecht im digitalen Binnenmarkt[3] definiert die EU-Kommission Text und Data Mining als

> „eine Technik für die automatisierte Auswertung von Texten und Daten in digitaler Form, mit deren Hilfe beispielsweise Erkenntnisse über Muster, Trends und Korrelationen gewonnen werden können".

Der Begriff „Webcrawling" steht für die automatisierte Auswertung von Onlinequellen des World Wide Web, wobei in der Regel Text- und Data-Mining-Technologien zum Einsatz kommen.

Aufgrund von Urheberrecht, Datenbankschutz sui generis, Lichtbild- und Presseverlegerleistungsschutzrecht dürfen Rechteinhaber Webcrawlern das Text und Data Mining auf geschützten Daten ausschließen oder eine Lizenzgebühr verlangen, soweit das Text/Data Mining technisch eine (permanente) Zwischenkopie und damit eine Vervielfältigungshandlung oder Veröffentlichung von Originaldaten (z. B. Snippets) erfordert. Da die Lizenzerteilung grundsätzlich der Dispositionsfreiheit privatautonomer Marktteilnehmer unterliegt, besteht unterhalb der wettbewerbs- und kartellrechtlichen Missbrauchstatbestände kein Kontrahierungszwang. Große Marktteilnehmer (wie die Suchmaschine „Google") erhalten insofern oft bessere Konditionen (unter Umständen Gratislizenzen), da z. B. Verlage auf die Indexierung angewiesen sind, wodurch weniger marktmächtige Anbieter diskriminiert werden. Daneben besteht die Gefahr, dass Verlage Exklusivverträge einfordern (bzw. die Garantie, dass mit bestimmten Konkurrenten keine vergleichbaren Lizenzvereinbarungen getroffen werden) und damit zum Nachteil der Webcrawler Konkurrenzverhältnisse auf Sekundärmärkte verlagern.

Umstritten ist, ob die reine Informationsextraktion durch Text und Data Mining überhaupt eine lizenzpflichtige Nutzungshandlung darstellen sollte. Die Erschließung von neuem Wissen auf Grundlage verfügbarer Daten im World Wide Web kann als ein neues Geschäftsmodell der Datenveredelung verstanden werden. Hierbei stellt sich die grundsätzliche Frage, ob Urheber bzw. Informationsaggregatoren wie Presseverlage an der Wertschöpfung durch sogenannte Datenveredler beteiligt werden sollten. Auf der einen Seite steht die Vorstellung von Datenwertschöpfungsketten, die auf lizenzbasierten Geschäftsmodellen basieren. Auf der anderen Seite besteht die Gefahr, dass ein exklusiver Schutz den gesellschaftlichen Austausch und Fortschritt behindern und zur Monopolisierung von Informationen führen könnte. Die Frage, ob Informationen als solche daher gemeinfrei bleiben sollten, stellt sich somit auch in diesem Zusammenhang, wie auch in der Debatte um die Relevanz eines „Dateneigentums".

Die zentrale Schlüsselfrage ist daher, wie die rechtliche Regulierung im Bereich „Smart Data" effektiv Diskriminierungsfreiheit herstellen kann. Diese Problematik würde sich nicht stellen, wenn eine generelle Erlaubnis für Text und Data Mining (eine sogenannte Schranke) ausschließlich zur Informationsextraktion erfolgende Vervielfältigungen zustimmungsfrei ermöglichen würde. Alternativ müssten wettbewerbsrechtliche Mechanismen etabliert werden, um die Gewährung des Zugangs zu Informationen unter diskriminierungsfreien Konditionen festzuschreiben.

Analyse der aktuellen Diskussion um das „Recht an Daten“

Entscheidend für die Schaffung einer europäischen Datenökonomie ist der Zugang zu und die Nutzbarkeit von nicht-personenbezogenen Daten. Die aktuelle juristische Debatte dreht sich diesbezüglich um die Schaffung eines „Dateneigentums“ mit dem Ziel, die Verkehrsfähigkeit von Daten zu erhöhen. Zu bedenken sind jedoch, dass ein Dateneigentum eine eindeutige Zuordnung eines Datums zu einem Eigentümer bzw. einer Eigentümerin sowie eine klare Abgrenzung zwischen Daten mit und ohne Personenbezug impliziert. Die Schaffung eines Ausschließlichkeitsrechts könnte somit einige Abgrenzungsschwierigkeiten und unbedachte Rechtsfolgen mit sich bringen.

Der folgende Beitrag befasst sich mit der juristischen Herleitung eines solchen Rechts am Einzeldatum und den damit einhergehenden Konsequenzen. Daneben setzt er dieses Konzept in Bezug zu bereits bestehenden Rechten an Datensammlungen, nämlich dem Recht des Datenbankherstellers. Das Ergebnis dieser Betrachtung zeigt, dass durch die Schaffung eines Rechts am Einzeldatum keine sachgerechte Lösung zu erwarten ist.

„Datenhoheit und Recht des Datenbankherstellers“ – Recht am Einzeldatum vs. Rechte an Datensammlungen

*Dr. Alexander Duisberg, Bird & Bird LLP**

I. Zielsetzung und Kontext

Mit diesem Arbeitspapier sollen die rechtlichen Voraussetzungen und Parameter zur transaktionalen Handhabe von Daten als Wirtschaftsgut de lege lata und de lege ferenda beschrieben werden. Die Thematik spielt sich auf zwei Betrachtungsebenen ab: Die eine betrifft die Frage einer rechtlichen Zuordnung und Verfügungsbefugnis in Bezug auf das Einzeldatum, die andere betrifft Verfügungsbefugnisse über, Zugang zu und den Umgang mit Datensammlungen. Hierzu wird in einem ersten Schritt der Stand der Diskussion um die Frage der „Datenhoheit“ als solcher (der häufig anzutreffende Begriff „Dateneigentum“ soll als juristisch irreführend bewusst vermieden werden) dargestellt (unter II.). Im Anschluss folgen Überlegungen zum Recht des Datenbankherstellers („RBD“) als derzeit maßgebliches Rechtsinstitut im Zentrum der Betrachtung (unter III.).

II. Datenhoheit – Diskussionsstand

1. Vorüberlegungen: „open“ und „shared“ vs. proprietäre Datendomänen

Die Diskussion um „Dateneigentum“ oder anderweitige proprietäre „Rechte an Daten“ beflügelt die Fantasie der Juristen. Dazu ist festzustellen, dass unsere Rechtsordnung – wie auch derzeit praktisch alle anderen Jurisdiktionen – kein sachenrechtlich oder in anderer Form als absolutes, mit Ausschließlichkeitsbefugnissen definiertes „Eigentum“ an Daten- oder Datensätzen als solchen anerkennt (§§ 903 S. 1, 90 BGB). Entsprechend bilden sämtliche Stellungnahmen gegenwärtig eine Diskussion de lege ferenda darüber, ob es ein zivilrechtliches „Dateneigentum“ geben sollte.

1.1 Sozio-ökonomische Gesichtspunkte

Eine solche Frage ist – weit über die Frage hinaus, ob und wie sich ein solches absolutes Datenrecht begründen ließe – in ganz erheblichem Maße sozio-ökonomischer Natur und kann nicht durch eine rein juristische Betrachtung abschließend geklärt werden. Vorrangig gilt es dabei, die Weichen in Richtung einer möglichst offenen, innovationsorientierten Rechtskultur zu stellen und zu fragen, ob mögliche Ausschließlichkeitsrechte an Daten hier innovationshindernd wirken würden.[4] So, wie in der Welt der Softwareentwicklung und -anwendungen der Open-Source-Ansatz eine entscheidende Rolle für die Innovationskraft, die Skalierung und das Wachstum ganzer Ökosysteme spielt (siehe etwa den Siegeszug der App-Ökonomie), kann man sich – zumindest theoretisch – ebenso gut vorstellen, dass ein „open“- bzw. „shared“-Ansatz den maßgeblichen Schlüssel zum Erfolg bestimmter Modelle in der sich aufbauenden Datenökonomie darstellt. Nicht zuletzt die Begründungserwägungen zur Reform der Public Sector Directive („PSI-Richtlinie“) unterstreichen genau diesen Punkt.[5]

1.2 Wettbewerbs- und kartellrechtliche Gesichtspunkte

Die damit verbundenen Fragen hinsichtlich technischer Standards, offener Plattformen, geregelter, nicht diskriminierender Zugänge und Interoperabilität[6] berühren in Teilen Fragen des Wettbewerbs- und des Kartellrechts de lege lata und de lege ferenda (dazu separate Betrachtungen der AG Recht). Sie sind zugleich Ausdruck und Reflex der faktischen Realität, dass es eine Vielzahl von Datendomänen gibt, die einzelne Unternehmen oder Gruppen von Unternehmen – bis hin zu Datenmonopolen und -oligopolen – innehaben und kontrollieren. Die rechtlichen Antworten hierauf sind bislang unvollkommen, aber im vorliegenden Rahmen nicht im Einzelnen zu diskutieren. Sie werden in Zukunft erheblich an Bedeutung gewinnen.

1.3 Lineare Wertschöpfungskette vs. digitales Eco-System

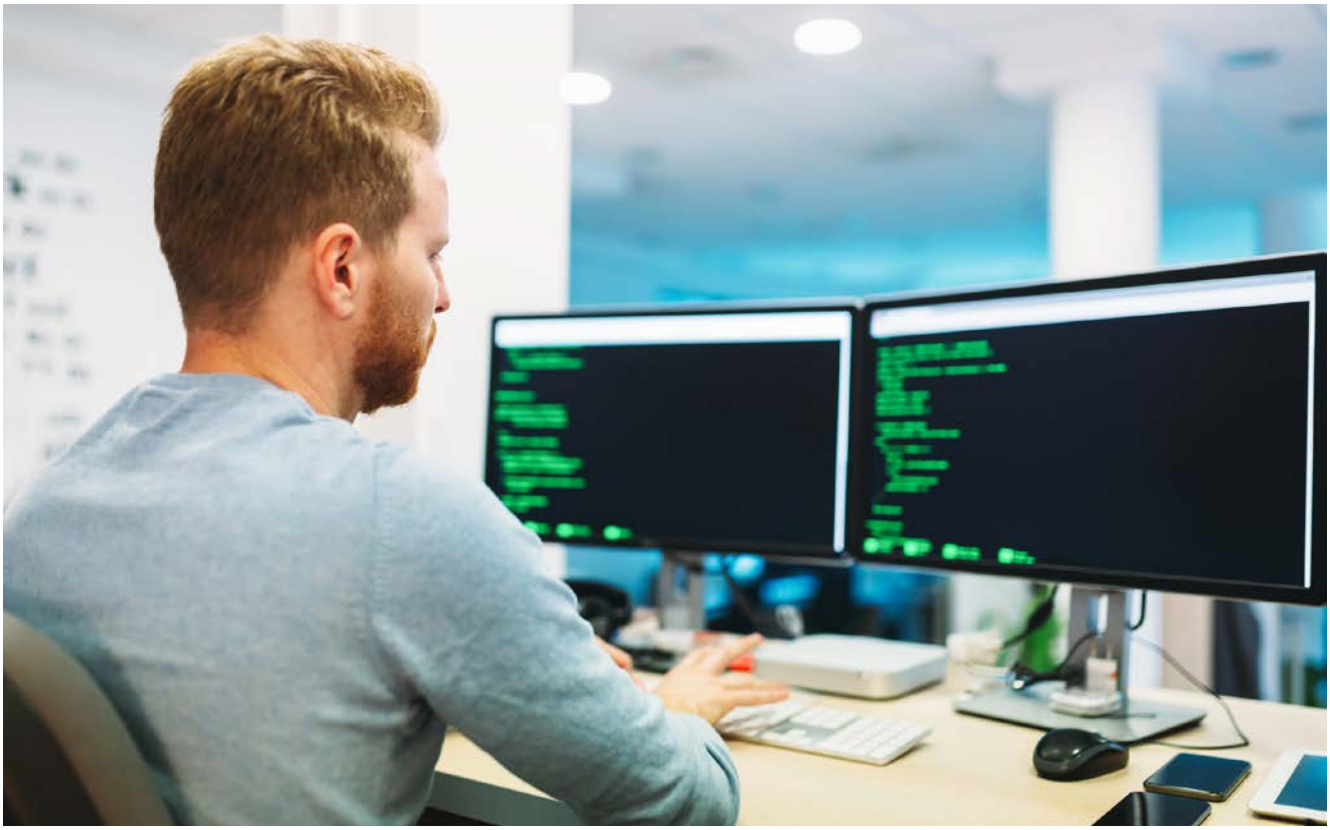
Zugleich gibt es Aussagen dahingehend, dass die „Herrschaft über die Daten“ und der „Kampf um die Datenhoheit“ einen, wenn nicht sogar den entschei-

denden Faktor für die Entwicklung und Begründung von Wertschöpfungsketten in der digitalisierten Wirtschaft darstellen. Diese Wertschöpfung ist nicht mehr überwiegend linear ausgestaltet, sondern entwickelt sich in der Digitalisierung zu einer – zuweilen wirtschaftlich schwer realisierbaren – Wertschöpfung in Eco-Systemen, in denen sich der Einzelne nach dem Grad seiner Vernetzung definiert – und ebenso durch andere Teilnehmer danach bewertet wird.

Wer „die Daten hat", bestimmt auch die Spielregeln, nach denen sich die übrigen Nutzer und Verwerter von Daten zu richten haben. Das Streben nach „Datenhoheit" ist hier am ehesten als Wettbewerb um Metadaten[7] zu verstehen. Deren Sammlung, Zugriff und Auswertung ermöglicht zum einen den zeitlichen Vorsprung bzw. den Erstzugriff auf Informationen, um eigene Wertschöpfungsketten und Geschäftsmodelle zu begründen, und zum anderen die in den Metadaten liegenden eigenen Betriebs- und Geschäftsgeheimnisse vor Zugriffen Dritter zu schützen. Aus alledem könnte man einen – immerhin in der Industrie artikulierten – Bedarf an (i) angemessenen Schutzmechanismen für „proprietäre" Datenbeständen und (ii) Rechtsklarheit hinsichtlich der Mittel zur Gestaltung von Wertschöpfungsketten ableiten.[8]

1.4 Schutzgut „Information"

Hier wird zunächst der begriffliche und materielle Unterschied zwischen „Daten" und „Information" relevant. Der einfache Datenpunkt hat keine informationelle Aussagekraft (Beispiel: „Sensordatum 19"). Der Informationsgehalt eines Datenpunkts wird erst durch die ihm zugeordneten Bestimmungsmerkmale (Metadaten) und den Kontext bestimmt, in dem dieser Datensatz im Verhältnis zu anderen Datensät-



zen steht bzw. betrachtet werden kann. Vor diesem Hintergrund kann man überlegen, ob der angesprochene Schutz- und Regelungsbedarf im Kern eher die Daten als solche oder eher das Potenzial der in ihnen verkörperten bzw. aus ihrer Auswertung beziehbaren Informationen bezwecken sollte. Letzteres mag eine Indikation dafür sein, dass rechtlicher Schutz auf der „passenden Ebene" – weniger auf der Ebene des Einzeldatums oder des einzelnen Datensatzes als vielmehr auf der Ebene der Kontextualität von Daten – angesiedelt werden sollte. Mit anderen Worten, es steht die Frage im Raum, weswegen auf den Schutz von Einzeldaten (sozusagen den „nackten Rohdaten") abgestellt werden sollte, wenn die Schutzqualität sich möglicherweise erst aus der Kontextualität (insbesondere Metadaten und/oder der Verbindung mit anderen Datensätzen) und der sich daraus ableitenden Inhaltsebene ableitet.[7]

Daraus könnte schließen, dass ein nicht die Proprietät von Einzeldaten definierender bzw. auf Proprietät bewusst verzichtender Ansatz, der einen generellen freien – dabei nicht notwendigerweise auch zur offenen Teilhabe oder dem „sharing" verpflichtenden – Ansatz einschließt, durchaus vereinbar ist mit Schutzmechanismen, die (erst) auf der Kontextebene bzw. der potenziellen Informationsebene – mithin einschließlich der die Einzeldaten qualitativ beschreibenden Metadaten – ansetzen.

Als Folge böten Regelungsansätze, die nicht (zwangsläufig) schon auf der Datenebene ansetzen, höhere Flexibilität, um (auch) durch „shared"- oder „open"-Ansätze die Vorteile von Innovation, Skalierung und multilateraler Wertschöpfung zu heben. Die in Kapitel II kurz zusammengefassten Ansichten befassen sich im Kern nicht mit diesen Überlegungen. Entsprechend sind die nachfolgenden Ausführungen – ohne diesen Querbezug – lediglich immanent zusammengefasst und kurz bewertet.

1.5 Geltung von Sonderrechten

Selbstverständlich gilt dabei für sämtliche diskutierten Ansätze, dass Sonderrechte an Daten, wie sie sich aufgrund ihrer inhaltlichen Beschaffenheit gegebenenfalls ergeben (Beispiel: Urheber- und Leistungsschutzrechte an Musikdateien), hiervon unberührt bleiben. Kommt man zur Annahme proprietärer Rechte an „Daten als solchen", sollen damit die bestehenden Sonderrechte an dem Inhalt der Daten selbstverständlich nicht außer Kraft gesetzt werden. Am deutlichsten wird dies, wenn man sich im Folgenden mithin „reine Rohdaten" vorstellt, wie sie etwa von Sensoren im industriellen Umfeld erhoben werden (Beispiel: Maschinenmessdaten).[9]

Im Gegenteil sollten jene Sonderrechte und die vorliegende Fragestellung gänzlich unabhängig voneinander behandelt werden. Wie das Beispiel des Urheberrechts zeigt, lassen sich die hinter den Sonderrechten steckenden Zielsetzungen nicht – jedenfalls nicht ohne Weiteres – auf die Frage der „Datenhoheit" übertragen. Nach der klassischen Lehre des „Copyright" setzt das Urheberrecht an dem Schutz vor nicht autorisierter Vervielfältigung an. Da der Urheber/Autor typischerweise nicht über das Kapital und die unternehmerischen Mittel verfügt, sein Werk selbst zu verlegen und zu vervielfältigen, will ihm das Urheberrecht eine wirtschaftliche Teilhabe an seinem Werk sichern. Wertschöpfungsketten bauen sich hier linear auf (Autor–Verleger–Buchhändler; Komponist–Musikverlag–Plattenfirma–Sender/Konzertveranstalter etc.). Demgegenüber sind im Zeitalter der Digitalisierung die direkten Kosten für Vervielfältigungen sowie den Vertrieb von Daten und digitalen Inhalten auf Grenzwertkosten von praktisch null reduziert.[10] Das dem Urheberrecht zugrundeliegende Leitbild ist daher nur begrenzt – oder gar nicht – geeignet, (nicht-lineare) Wertschöpfungsketten im Zeitalter der Digitalisierung zu begründen, abzubilden oder zu schützen.

1.6 Datenschutzrechtliche Gesichtspunkte

Aus datenschutzrechtlicher Sicht tritt ein weiteres Pro-

blem hinzu, soweit Einzeldaten zugleich inhaltlich die Qualität personenbezogener Daten haben oder diese im Sinne der Big-Data-Wirkmechanismen erlangen können. Nach § 35 Abs. 2 S. 2 BDSG besteht der jederzeitige, grundrechtlich im allgemeinen Persönlichkeitsrecht und im Recht auf informationelle Selbstbestimmung verankerte Löschungsanspruch des Betroffenen. Es stellt sich die Frage nach dem Wert eines – an sich durch Art. 14 GG im Grundrechtschutz verankerten – Eigentumsrechtes an Einzeldaten, wenn dieses jederzeit und durch gewillkürte einseitige Erklärung eines beliebigen Dritten entzogen und zunichte gemacht werden kann.

2. Proprietärer Ansatz

Teile der Literatur plädieren für die Schaffung eines Eigentums- bzw. eigentumsartigen Ausschließlichkeitsrechts an Daten, verfolgen dabei aber unterschiedliche dogmatische Ansätze und Begründungen. Als Gründe für ein solches Recht werden insbesondere zusätzliche Anreize für Unternehmen genannt, Daten zu erheben, zu speichern und zu teilen und so einen eigenen Datenmarkt zu entwickeln.[11] Ohne eine klare rechtliche Zuweisung sei ein solcher Markt wenig attraktiv, weil Daten ihren Wert verlören, sobald sie einem Dritten bekannt seien.

2.1 Eigentumsrecht in Analogie zum Sacheigentum

2.1.1 „Datenerzeuger“

Einige Autoren, insbesondere Zech, wollen ein Eigentumsrecht an den Daten unmittelbar aus den Regelungen zum Sacheigentum (§§ 903 S. 1, 90 BGB) herleiten.[12] Ein solches Eigentumsrecht knüpfe an die Erzeugung von Daten durch Aufnahme bzw. Codierung an und solle daher dem Datenerzeuger als originär Berechtigtem zustehen. Wer Datenerzeuger ist, bestimme sich nach wirtschaftlichen Gesichtspunkten, sodass etwa in Auftragsverhältnissen der Auftraggeber als Datenerzeuger gelte.

Begründet wird die Schaffung eines (übertragbaren) Ausschließlichkeitsrechts vorrangig vor dem Hintergrund, eine klare Zuordnung des Datennutzens zu ermöglichen und Ersatzansprüche (z. B. Schadensersatz oder Eingriffskondiktion) eindeutig zuweisen zu können. Obgleich abweichende vertragliche Regelungen vorgenommen werden können, diene das Eigentumsrecht zumindest als Ausgangspunkt für vertragliche Regelungen und als grundsätzliche Entscheidung bei einem Fehlen vertraglicher Regelungen.[13]

Dieser aus praktischen Gründen nachvollziehbare Ansatz wirft allerdings die Frage auf, ob die für eine Analogie erforderliche planwidrige Regelungslücke und vergleichbare Interessenlage gegeben sind. Die Verfasser des BGB konnten zweifellos nicht einmal ahnen, dass über 100 Jahre später die Existenz digitalisierter Daten rechtlich diskutiert werden würde. Gleichwohl dürfte angesichts inzwischen zahlreicher anderer Spezialvorschriften für Daten eine Planwidrigkeit zu verneinen sein.[14] Auch die Interessenlage scheint hier eine andere zu sein, denn während das Eigentumsrecht ein ausschließliches Zuweisungsrecht ist, betont das Bundesverfassungsgericht, dass der Einzelne gerade kein Recht im Sinne einer absoluten, uneingeschränkten Herrschaft über „seine“ Daten habe, sondern er vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit sei.[15]

2.1.2 § 950 BGB

Auch Ensthaler befürwortet eine Übernahme von Regelungen des Sacheigentums. Ein Eigentumsrecht im Sinne einer allumfassenden Berechtigung gemäß § 903 S. 1 BGB bestehe allerdings nicht.[16] Vielmehr lasse sich die Eigentumsfrage über § 950 BGB lösen: Der Bearbeiter von Informationen als „Rohmaterialien“ erwerbe das Eigentum, soweit nicht der Wert der Bearbeitung geringer als der des Stoffes ist. Parallel zum Leistungsschutzrecht wird dem Bearbeiter somit kein bloßer schuldrechtlicher Ausgleichsanspruch gegen den Eigentümer eingeräumt, sondern er wird selbst Eigentümer. Dies

sei sachgerecht, weil die Rohdaten üblicherweise erst durch die vorbereitende Bearbeitung wertvoll werden. Als Bearbeiter soll das Unternehmen gelten, das die technischen Vorrichtungen zur Erfassung und Übermittlung der Daten am jeweiligen Gerät anbringt.[17]

2.2 Eigentumsrecht in Analogie zum Strafrechtsschutz

Hoeren hat in einem vielbeachteten Aufsatz den Versuch unternommen, zumindest de lege ferenda ein Eigentumsrecht entsprechend den Wertungen der §§ 303a, b StGB zu begründen.[18] Er vertritt dabei die Ansicht, dass die Schutzregelung der §§ 303a, b StGB an dem Besitz von Aufzeichnungsgeräten und -verfahren ansetzt. Entsprechend soll sich aus dem „Skripturakt" ein Eigentumsrecht ableiten, das ausschließlich dem „Skribenten" zusteht. Verkürzt gesagt: Wer Daten aufzeichnet, darf sie behalten und andere von der Nutzung ausschließen bzw. die Nutzung von seiner Zustimmung abhängig machen.

In diesem Zusammenhang stellt sich die Frage, ob die Schutzziele des Strafrechts tatsächlich mit denen eines zivilrechtlichen Eigentumsbegriffs, der ins Zentrum proprietärer Nutzung und der Begründung entsprechender Wertschöpfung gesetzt werden können. Heymann sieht hier zudem – nicht ganz zu Unrecht – das Risiko eines hermeneutischen Zirkelschlusses. Auch in praktischer Hinsicht scheint der Ansatz des Skripturakts eher Fragen aufzuwerfen, als Antworten zu bieten: Nimmt man die in vielen Anwendungen vollständige Virtualisierung von Datenkontrolle und Datenaufzeichnung – einschließlich entsprechender Vervielfältigungen durch Dienstleister und Subunternehmer –, wäre zunächst jede autochthone Aufzeichnung ein „Skripturakt", der proprietäre Rechte begründet – die dann möglicherweise erst im Wege vertraglicher Vereinbarungen zugunsten des eigentlichen „Erst-Skribenten" bzw. Anwenders einer Cloud-Lösung wieder an diesen übertragen bzw. abgetreten werden müssten –, obwohl es sich um dieselben bzw. inhaltlich voll-identische Datensätze handelt.

Boesche/Rataj[19] sehen eine Lösung jenseits der vertraglichen Regelung vor, um in solchen Fällen das Dateneigentum zuzuordnen. Dies erfolgt in zwei Stufen: Zunächst sollen die Daten nach ihrer Art und ihrem Nutzungszweck unterschieden werden. Handelt es sich um reine Daten über den Zustand des Endgerätes, sind die Daten eher dem Hersteller zuzuordnen. Handelt es sich jedoch um Daten zum Nutzungsverhalten, so sind diese eher dem Dritten (beispielsweise dem Dienstleister) zuzuordnen. Dann soll ermittelt werden, wo der Schwerpunkt des Skripturaktes liegt und wer die Verantwortung für die maßgebliche Handlung im Sinne des Skripturaktes hat.

2.3 Nutzungen einer Sache (§ 100 BGB)

Im Unterschied zu den vorgenannten Ansichten halten Heun/Assion Einzeldaten zwar für rechtlich nicht eigentumsfähig. Sie wollen aber den durch die faktische Verfügbarkeit der Einzeldaten bestehenden Vermögensvorteil als „proprietär" zuweisen, indem sie die Daten als Nutzungen des Datenträgers anerkennen. Anders als beim „Skripturakt" stellen sie nicht auf den eigentlichen Akt der Erstellung oder Erhebung der Daten, sondern auf die Sachherrschaft bzw. das Eigentum an dem Datenträger ab, auf dem sich die Einzeldaten befinden.[20] Daraus soll sich dann – entsprechend dem Grundgedanken des § 100 BGB – das ausschließliche Recht an den „Nutzungen", nämlich den auf dem Datenträger verkörperten Daten, ableiten. Allerdings betonen Heun/Assion in diesem Zusammenhang, dass es hierbei keine einheitliche, sondern stets nur einzelfallbezogene Antworten auf die Frage geben könne, wem die Daten letztlich „gehörten".[21]

Dieser Ansatz ist interessant und lässt doch zugleich an die Anfänge des Softwarerechts zurückdenken, als das Recht an der Software ebenfalls in enger Beziehung zu dem Eigentumsrecht an dem die Software verkörpernden Datenträger gesehen wurde – bis hin zur Begründung der Sacheigenschaft von Software für die Zwecke des AGB-Rechts und der Regeln des allgemeinen und besonderen Schuldrechts.

Folgt man der Logik der Virtualisierung und sieht, wie sich die Rechtspraxis beim Softwarerecht von der Existenz eines Datenträgers zur Begründung eigenständiger Rechte an der Software gelöst hat (natürlich auch infolge der Umsetzung der EU-Richtlinie 2009/24/EG zum urheberrechtlichen Schutz von Computerprogrammen), so sollte man sich diesen „Umweg über die Hardware“ zur Begründung etwaiger Rechte an Daten sparen. Die Allmacht der Virtualisierung und verteilter Rechenprozesse (Cloud & Co.) rückt den „Hardware-Bezug“ eher in das 20. als in das 21. Jahrhundert.

Gleichwohl ist der Gedanke, dass Daten als Nutzungen einer Sache einen eigenständigen Rechtsschutz genießen sollen – der nicht dieselbe Rechtsqualität wie ein absolutes Vollrecht an Daten als solchen erreicht –, immerhin ein interessanter und weiter zu bedenkender Ansatz.

2.4 Früchte einer Sache (§ 99 BGB)

Ähnlich zu Heun/Assion vertritt Grosskopf[22] die Ansicht, dass Daten die Früchte der sie herstellenden Sache seien und sie mithin dem Eigentümer der Sache gehören (§ 953 BGB). Damit folge das Recht an den Früchten dem Eigentum an der Sache, aus der die Früchte entstehen.

Diesem Ansatz wird entgegengehalten, dass Früchte nur körperliche Gegenstände sein können und Daten daher als Früchte ausscheiden.[23] Andere Autoren sehen die Daten nicht als Erzeugnis der Sache, die die Daten generiert, sondern als Erzeugnis der Sache oder Person, auf die sich die Daten beziehen.[24] Die Daten gehörten daher nicht notwendigerweise dem Eigentümer der Sache. Selbst wenn man die Daten als Früchte der datenerzeugenden Sache ansähe, folgt daraus nicht zugleich die Sacheigenschaft von bzw. ein Recht an Daten.

2.5 Eigentumsrecht des Betroffenen

Weitere Autoren befürworten ein Eigentums- oder jedenfalls eigentumsähnliches Recht des Betroffenen, jedoch losgelöst von den §§ 903 ff. BGB. Die Existenz eines solchen Rechts wird unterschiedlich hergeleitet: Einige knüpfen an das Persönlichkeitsrecht als Ausformung des informationellen Selbstbestimmungsrechts an, andere leiten das Eigentumsrecht implizit aus den umfassenden datenschutzrechtlichen Rechten und Befugnissen des Betroffenen ab.[25] In beiden Fällen erhalte der Betroffene eine absolute Rechtsposition gegenüber jedem Dritten, wie sie für das Eigentumsrecht typisch sei.

2.6 Gesetzesinitiative zum „Datengesetz“

Einen im Grundsatz proprietären Ansatz für den spezifischen Bereich der Fahrzeugdaten verfolgt womöglich auch das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI). Ein im März 2017 vorgestelltes Strategiepapier des BMVI[26] stellt zwar fest, dass Daten im Rechtssinn keine Sachen und dadurch nicht eigentumsfähig seien[27] Daten sollen aber im Ergebnis mit Sachen gleichgestellt und dadurch eindeutig natürlichen oder juristischen Personen als „Eigentum“ zuordenbar sein.[28] Die betreffenden Verfügungsrechte sollen künftig demjenigen zugewiesen werden, „auf den die Erstellung der Daten zurückgeht.“[29]

Praktische Bedeutung erlangt das Strategiepapier insbesondere im Bereich der Mobilität, namentlich für Fahrzeugdaten. Ein modernes Serienfahrzeug produziert schon heute Daten von bis zu 25 Gigabyte pro Stunde, etwa zum Wetter sowie zu Routen, Staus und Risikosituationen.[30] Diese Daten sollen grundsätzlich dem Halter „gehören“, der das Fahrzeug erworben hat. Ohne (widerrufliche) Einwilligung des Betroffenen in die Verwendung seiner personenbezogenen Daten darf laut BMVI eine Verarbeitung und Vernetzung der Daten ausschließlich anonymisiert und pseudonymisiert erfolgen.

3. Open-Data-Ansatz

Überwiegend wird die Eigentumsfähigkeit von Einzeldaten abgelehnt und ein dem Freihaltebedürfnis ent-

sprechender Ansatz verfolgt. Vertreter dieser Auffassung sehen derzeit keine regulatorische Notwendigkeit für ein solches Recht, vielmehr seien die gegenwärtigen Instrumentarien sowohl aus rechtlicher [31] als auch aus ökonomischer Sicht[32] ausreichend. Insbesondere könne im Wege vertraglicher Vereinbarung ein hinreichender Schutz gewährleistet werden. Auch seien die wirtschaftlichen Auswirkungen eines Eigentumsrechts am Einzeldatum unsicher: Eine generalisierte Datenzuweisung ohne Zugangs- und Teilhaberecht wirke innovationshemmend, weil insbesondere Big-Data-Anwendungen von großen Datenmengen abhingen.[33] Diese Auffassung folgt im Ergebnis der Einschätzung des Bundesverfassungsgerichts: Es betrachtet Informationen, auch soweit sie personenbezogen sind, seit dem Volkszählungsurteil aus dem Jahr 1983 als ein „ein Abbild sozialer Realität […], das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann.“[34]

Das zentrale Argument für ein Ausschließlichkeitsrechts, wonach ohne ihn die Datenverarbeitung und Entwicklung eines Datenmarkts unattraktiv sei,[35] kann wegen anderer Geheimhaltungsmöglichkeiten seitens der Unternehmen nicht verfangen.[36] Ein Ausschließlichkeitsrecht ist vielmehr überflüssig, wo das Nutzungsrecht (wie bei Daten) nicht-rival ist.[37]

Um dabei dem Interesse an einem wirksamen Schutz von Daten gerecht zu werden (sei es etwa aus persönlichkeitsrechtlichen oder wirtschaftlichen Gründen), werden Rechte an Daten in unterschiedlichen Intensitätsstufen anerkannt.

3.1 Schutz der in Daten repräsentierten Information

Hoppen lehnt ein Eigentumsrecht an Daten schon aus dem Grund ab, dass dessen Sicherung aufgrund der fehlenden Verkörperung von Daten technisch prinzipbedingt nicht umsetzbar sei.[38] Im Kern gehe es dem „Eigentümer“ von Daten ohnehin nicht um den Schutz der Daten als solcher, sondern um den Schutz der abstrakt durch die Daten repräsentierten Informationen bzw. des durch diese Informationen repräsentierten Wissens.[39] Daten können demnach frei zugänglich übertragen und kopiert werden, sofern ihr Inhalt nicht erkennbar, also verschlüsselt ist. Hoppen schlägt vor, dass eine gesetzliche Regelung auf unverschlüsselte Datenbestände bzw. auf den Schutz der Eigentumsrechte an Informationen und Wissen abstellen sollte.[40]

3.2 Schutz mittels Schutzzielen

Einen im Ergebnis vergleichbaren Ansatz verfolgt Heymann. Er vertritt die Auffassung, dass ein eigentumsrechtlicher Schutzgehalt an Einzeldaten ausdrücklich weder wünschenswert ist noch die Zuordnungs- und Kontrollfragen überhaupt lösen könne.[41] Dagegen stellt er überzeugend heraus, dass es kein Eigentums-

recht an Daten geben darf. Vielmehr solle ein an Schutzzielen orientiertes Konzept der ordnungsgemäßen Datenverarbeitung angestrebt werden, um u. a. die Vertraulichkeit, Integrität, „Intervenierbarkeit“ und Portabilität von Daten zu sichern.[42] Im Ergebnis lehnt er angesichts der Diversität der betroffenen Daten eine generalisierende Lösung ab.[43]

3.3 Schutz durch Flexibilität der Privatautonomie

Eine generalisierende „statisch“ zuordnende Lösung lehnt Sahl ebenfalls ab.[44] Er empfiehlt stattdessen den Abschluss individueller Datennutzungsverträge. Diese enthielten zwar durchaus Schwächen, insbesondere in der Drittabwehr,[45] seien aber aufgrund ihrer höheren Flexibilität geeigneter, um der „dynamischen Entwicklung“ der digitalen Märkte und Geschäftsmodelle sowie den Anforderungen des Einzelfalls gerecht zu werden.[46] Sofern einige grundlegende Aspekte für jeden Datennutzungsvertrag eingehalten würden, sei eine allgemeine gesetzliche Regelung dadurch verzichtbar.[47] Hier stelle sich vor allem die Frage, zu wessen Gunsten überhaupt entschieden werden sollte, im Sinne einer „One size fits all“-Lösung.[48] Eine gesetzliche Lösung würde zwangsläufig einen Beteiligten bevorzugen, was der Vielzahl unterschiedlicher Fall- und Interessenkonstellationen kaum gerecht würde.[49]

Den Nutzen einer solchen Lösung stellt Ensthaler in Frage: Bei einer vertraglichen Regelung sei noch nicht die Frage beantwortet, wem die Daten ursprünglich zugeordnet sind, wem sie also gehören.[50] Es werde nur derjenige überhaupt eine Gegenleistung erbringen, der etwas erhält, was ihm vorher nicht gehörte. Die Frage der Zuordnung sei daher losgelöst von vertraglichen Gestaltungsmöglichkeiten zu beantworten.

3.4 Übertragbares Ausschließlichkeitsrecht des wirtschaftlich verantwortlichen Datenerzeugers

Specht/Rohmer befürworten ein am Investitionsschutz der § 87a ff. UrhG orientiertes Ausschließlichkeitsrecht.[51] Obwohl einzelne Daten gerade nicht von den §§ 87a ff. UrhG geschützt würden, gelte für das Zuweisungsrecht an Daten weiterhin das Prinzip, nach dem derjenige ein Ausschließlichkeitsrecht über etwas erlangt, der wesentlich in die Beschaffung etc. des Betroffenen investiert.[52] Specht/Rohmer wollen dabei zwischen personenbezogenen und nicht personenbezogenen Daten unterscheiden, sie räumen aber ein, dass die Trennung im Einzelfall nur schwer möglich ist.[53]

3.5 Erweiterung des Eigentumsbegriffs

In eine ähnliche Richtung äußern sich Schwartmann/Hentsch, die das UrhG ebenfalls als Vorbild für ein neues Datenverwertungsrecht bewerten.[54] Dafür wollen sie Daten zunächst kategorisieren, damit abgestufte Schutzkonzepte angewandt werden können. Zudem schlagen sie vor, dass der Gesetzgeber den Eigentumsbegriff des Art. 14 Abs. 1 GG auch auf „Unkörperliches“ erstreckt.[55]

3.6 Datenschutzrechtlicher Löschungsanspruch vs. Eigentumsrecht

Wie einleitend erläutert,[56] tritt ein datenschutzrechtliches Problem hinzu, das gegen die Annahme eines Eigentumsrechts an Einzeldaten sprechen dürfte bzw. kaum mit besagten Konstruktionen in Übereinstimmung zu bringen ist: Soweit Einzeldaten zugleich inhaltlich die Qualität personenbezogener Daten haben oder ihnen diese z. B. in Kombination mit anderen Datensätzen und der daraus erzeugten Personenbeziehbarkeit anwächst, besteht der jederzeitige, grundrechtlich im allgemeinen Persönlichkeitsrecht und im Recht auf informationelle Selbstbestimmung verankerte Löschungsanspruch des Betroffenen. Was wäre das aber für ein – an sich durch Art. 14 GG im Grundrechtschutz verankertes – Eigentumsrecht an Einzeldaten, wenn es mit einem dauerhaften Konflikt mit der jederzeitigen, privat-autonom bzw. in Art. 2 Abs. 1 GG (Recht auf informationelle Selbstbestimmung) gründenden Auflösung durch Ausübung des datenschutzrechtlichen Löschungsanspruchs behaftet wäre. Ein Wesensmerkmal des Eigentums – seine zeitlich unbefristete Geltung –

wäre damit im Grunde schon von Beginn an mit einer „schwebenden Entziehbarkeit“ durch beliebige Dritte behaftet und im Kern entwertet.[57]

III. Rechte an Datensammlungen – Recht des Datenbankherstellers

Da sich nach hiesiger Auffassung mit den Mitteln des Zivilrechts kein Eigentumsschutz für einzelne Datensätze herleiten lassen kann und soll, liegt der Schlüssel für die Gestaltung von Datentransaktionen in den Rechten des Datenbankherstellers. Daher werden in der nachfolgenden Betrachtung die einzelnen Tatbestandskomponenten dieses Rechts näher beleuchtet und auf etwaigen Ergänzungsbedarf hingewiesen.

1. Voraussetzungen der §§ 87a ff. UrhG

1.1 Begriffsbestimmungen

§ 87a Abs. 1 UrhG beschreibt die Datenbank als eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet sowie einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Dabei gelten (wirtschaftliche) Aufwendungen zur Beschaffung der Daten (beispielsweise Installation, Entwicklung oder Betrieb von Sensortechnik) nach ständiger Rechtsprechung jedoch nicht als Investitionen im Sinne des § 87a Abs. 1 UrhG.[58] Lediglich direkte Investitionen in die Datenbank werden erfasst.[59] Hersteller einer Datenbank ist derjenige, der die Investition im genannten Sinne vorgenommen hat. Er muss daher nicht unmittelbar selbst an der Herstellung der Datenbank beteiligt sein, entscheidend ist vielmehr, wer das wirtschaftliche Risiko trägt, das mit dem Aufbau und Erhalt einer Datenbank zusammenhängt.[60] Sofern sich die Tätigkeiten des Datenbankherstellers nicht unter den Investitionsbegriff einordnen lassen, obgleich der Datenbankhersteller viel in die Datenbeschaffung, aber vergleichsweise wenig in die Systematik der Datenbank als solche investiert,[61] kann aufgrund des subsidiären Verhältnisses des Wettbewerbsrechts zum RDB in diesem Fall der wettbewerbsrechtliche Leistungsschutz greifen.[62]

1.2 Reichweite des Schutzes

Die gesetzliche Definition unterstreicht, dass dem Datenbankbegriff ein äußerst weites Verständnis zugrunde liegt. Der Rechtsschutz hängt – anders als vor Einführung der DatenbankRL 96/9/EG, die die §§ 87a ff. UrhG umsetzten – weder von einer festgelegten (z. B. elektronischen) Form ab,[63] noch bedarf er einer bestimmten Anzahl von Daten oder Elementen.[64] Damit ist nicht allein die „schöpferische“ Datenbank geschützt, bei der die Auswahl oder Anordnung des Stoffs innerhalb der Datenbank eine eigene geistige Schöpfung ihres Urhebers darstellen,[65] sondern vielmehr besteht ein Datenbankschutzrecht sui generis, das wesentliche Investitionen in die Beschaffung, Überprüfung oder Darstellung des Datenbankinhalts schützt. Das RDB beschreibt also im Kern die Schutzfähigkeit der Investition in eine Ordnungsstruktur zur elektronischen Auslese von Datensätzen, nicht aber die Schutzfähigkeit der einzelnen Daten als solche.[66] Die Schutzfähigkeit dieser Ordnungsstruktur zielt entsprechend auf die Kontextualität von Datensätzen, dagegen nicht notwendigerweise auf den Inhalt des Einzeldatums ab. Dass es hier Berührungen, Verdichtungen und eine Nähebeziehung zum Inhalt von Einzeldaten bzw. einer parametrisierbaren Gesamtheit von Einzeldaten gibt oder geben kann, liegt in der Natur der Sache. Als Konsequenz beschränkt sich der Schutzbereich der §§ 87a ff. UrhG auf Investitionen in vorhandene Daten und deren Sammlung bzw. Einordnung.[67] Der Schutz klammert daher solche Investitionen aus, die eingesetzt werden, um die Daten zu erzeugen, aus denen der Inhalt einer Datenbank besteht. Erst noch zu generierende Daten sind von den Vorschriften nicht umfasst.

An dieser Stelle wird erneut deutlich, dass es beim Datenbankrecht nicht um den Schutz der zu erhebenden und entsprechend einzuordnenden Daten geht.[68] §§ 87a ff. UrhG sind nicht auf die Inhalte – also die eingebrachten Daten – bezogen und begründen kein (neues) Informationsschutzrecht.[69] Die eigentliche Frage nach der Datenhoheit lässt sich auf Grundlage der im Datenbankrecht benannten Kriterien nach derzeitiger Rechtslage nicht abschließend beantworten. Allerdings bietet der von der EU-Kommission für Ende 2017 angekündigte Konsultationsprozess zur Überprüfung der Datenbank-Richtlinie Gelegenheit, über eine gegebenenfalls zweckmäßige Erweiterung des Schutzumfangs zu diskutieren.

1.2.1 Übertragung auf Metadaten

Bei der Bestimmung des Datenbankbegriffs erlangen zwei Themenbereiche besondere Bedeutung: Zum einen ist zu überlegen, ob der sui-generis-Schutz durch entsprechende Auslegung oder Ergänzung der Tatbestandsmerkmale auch auf Metadaten als solche zu erstrecken ist. Mit Blick auf das unter Kap. II.1.3 Gesagte könnte ein solches Verständnis eine sinnvolle Erweiterung darstellen (insbesondere soweit Metadaten zugleich Betriebs- und Geschäftsgeheimnisse darstellen).

1.2.2 Übertragung auf semi- und vorstrukturierte Daten

Zum anderen ist zu erörtern, ob das RDB auch auf semi-strukturierte oder vorstrukturierte Daten Anwendung finden soll. Konkret geht es um die Frage, wann die Datensammlung bereits als systematisch oder methodisch angeordnet anzusehen ist und wann ein bloßer „Datenhaufen“ vorliegt. Für die Abgrenzung stellt der Europäische Gerichtshof darauf ab, ob die Sammlung ein technisches oder anderes Mittel umfasst (z. B. einen Index oder eine Gliederung), das es ermöglicht, jedes in der Sammlung enthaltene unabhängige Element zu lokalisieren.[70] Eine Datenbank liegt danach vor, wenn sich jeder ihrer Bestandteile durch dieses Mittel auffinden lässt, während es bei einem „Datenhaufen“ an einem solchen Mittel fehlt.

1.3 Vertragspartner im Nicht-EU-Ausland

Bei einer getroffenen Vereinbarung mit einem Nicht-EU-Vertragspartner über die Zuweisung von Datennutzungsbefugnissen muss berücksichtigt werden, ob der ausländische Vertragspartner überhaupt Inhaber von Rechten an der Datenbank gem. § 87a UrhG sein kann[71] bzw. welche Schwierigkeiten es gegebenenfalls bei der Rechtsdurchsetzung gibt.

1.4 Europäische Rechtslage als weltweiter Modellcharakter?

So lückenhaft der ohne die privatautonome Lösung korrigierte Datenbankschutz ist, so groß ist auch die Chance, mit entscheidenden Veränderungen auf europäischer Ebene einen weltweiten „Modellcharakter“ zu erzeugen.[72] Entscheidend dafür sei, das neue Leistungsschutzrecht in eine strikte subsidiäre Anordnung mit den „Instrumenten des ergänzenden wettbewerbsrechtlichen Leistungsschutzes“ zu stellen, und des Weiteren, dass die Schrankenbestimmungen an das europäische Urheberrecht angepasst werden.[73] Ein Grund für die betreffende Möglichkeit sei, dass bislang weltweit Probleme im Umgang mit dem Datenbankschutz bestehen.[74]

2. Betriebs- und Geschäftsgeheimnisse

Zech[75] weist darauf hin, dass sich ein ausschließliches Recht an Daten nicht nur im Wege des Eigentums, sondern auch durch faktische Exklusivität erreichen lasse, indem die Daten geheim gehalten werden (Schutz der faktischen Exklusivität). Werde das Geheimnis jedoch offenbart, ende diese Exklusivität und es bestehe, anders als beim echten Ausschließlichkeitsrecht, keine (rechtlich gewährte) Exklusivität mehr.

Neben diese maßgebliche Säule, um die Transaktionsfähigkeit von Datensammlungen mit geeigneten In-

strumentarien (Datenbanklizenzverträgen, Übertragungen von Rechten an Datenbanken etc.) rechtlich abzubilden und umzusetzen, treten – sowohl was den Kontext von Datensammlungen als auch was gegebenenfalls den Schutz von Einzeldaten betrifft – der Schutz von Betriebs- und Geschäftsgeheimnissen (§ 17 UWG) und der – weniger klar konturierte – allgemeine Know-how-Schutz als zweite Säule. Durch sie werden quasi-proprietäre Rechte sowohl an Datensammlungen als auch gegebenenfalls an Einzeldaten begründet, die allerdings im Kern und entsprechend dem gesetzlichen Schutzrahmen als zivil- und strafrechtliche Abwehrrechte gegenüber unbefugten Zugriffen, Eingriffen und Verwertungen konzipiert sind.

Die im Juli 2016 in Kraft getretene europäische Richtlinie zum Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) wird das unterschiedliche Schutzniveau in den Mitgliedstaaten weitgehend harmonisieren und einen unionsweiten Mindeststandard schaffen. Für den deutschen Rechtsrahmen bedeutet dies neben systematischen Änderungen – bislang besteht kein rechtsgebietsübergreifendes Gesetz für den Geheimnisschutz in Deutschland (vgl. z. B. § 611 BGB, §§ 17, 18 UWG, § 823 BGB) – insbesondere inhaltliche Neuerungen: So besteht ein Geschäftsgeheimnis zukünftig (u. a.) nur, wenn die betreffende Information von kommerziellem Wert und Gegenstand angemessener Geheimhaltungsmaßnahmen seitens des Geheimnisinhabers ist (Art. 2 Nr. 1 der Richtlinie). Insbesondere ersteres Merkmal ist vor dem Hintergrund problematisch, dass sich ein „Datenwert“, wie gezeigt, gerade erst als eine Datenmenge ergeben kann. Hier offenbart sich, dass der Vorschrift Art. 39 Abs. 2 des TRIPS-Abkommens zugrunde lag und nicht an die heutigen Gegebenheiten angepasst wurde. Auf der Rechtsfolgenseite nähert sich die Richtlinie den gewerblichen Schutzrechten an, indem der Geheimnisinhaber nunmehr auch Rückruf- und Vernichtungsansprüche geltend machen kann (Art. 12 der Richtlinie). Ebenso werden der Geheimnisschutz in Gerichtsverfahren (Art. 9) und der Schutz von Whistleblowern gestärkt.

IV. Initiative „Aufbau der Europäischen Datenwirtschaft“

In ihrem Positionspapier vom Januar 2017[76] und zuletzt in einem Verordnungsvorschlag für den freien Verkehr nicht personenbezogener Daten vom September 2017[77] hat die Europäische Kommission erneut die hohe wirtschaftliche Bedeutung von Daten und Datendiensten hervorgehoben sowie weitere Eckpunkte für den Aufbau einer europäischen Datenwirtschaft skizziert. Der Wert der EU-Datenwirtschaft erreichte 2015 mit 272 Mrd. Euro bereits 1,87 % des EU-Bruttoinlandsprodukts.[78] Schätzungen zufolge wird dieser Wert bis 2020 auf 3,17 % anwachsen. Auf der anderen Seite werden nur etwa 4 % aller Daten überhaupt in Ländern der EU gespeichert.[79] Diese Entwicklung nimmt die Kommission zum Anlass, den Rechtsrahmen für einen digitalen Binnenmarkt weiter auszubauen, um das Datenpotenzial innerhalb der EU künftig voll auszuschöpfen.[80]

Durch technische Entwicklungen, insbesondere die Möglichkeit der Konnektivität von Daten, sind neue Wege entstanden, über die auf Daten zugegriffen werden kann. Der traditionelle physische Datenzugriff wird zunehmend durch Fernzugang abgelöst.[81] Um diese Möglichkeiten nutzen zu können, will die Kommission ungerechtfertigte Beschränkungen des freien Datenverkehrs beseitigen und die in weiten Bereichen herrschende Rechtsunsicherheit beheben. Derartige „digitale Grenzkontrollen“[82] bestehen insbesondere in behördlichen Auflagen in Bezug auf den Ort der Speicherung und die Verarbeitung von Daten, sei es in Form von Rechtsvorschriften, Verwaltungsvorschriften oder Verwaltungspraktiken.

Der Verordnungsvorschlag hinsichtlich nicht personenbezogener Daten ergänzt die europäischen Vorschrif-

ten über den Schutz personenbezogener Daten, insbesondere der Datenschutz-Grundverordnung. Darin bekräftigt die Kommission ihr Ziel, einen stärker vom Wettbewerb geprägten und integrierten Binnenmarkt für Datenverarbeitungsdienste und -tätigkeiten aufzubauen.[83] Dies soll insbesondere durch den Abbau von Binnenmarktgrenzen (d. h. Geoblocking) und eine erleichterte Übertragung von Daten erfolgen.

Über die Schaffung eines freien Datenverkehrs gelangt die Kommission in dem Positionspapier von Januar 2017 zur Frage des Dateneigentums, ohne sie jedoch abschließend zu beantworten. Vielmehr gibt sie Hinweise, wie ein Recht des Datenerzeugers an nicht personenbezogenen Daten ausgestaltet sein könnte.[84] Dem Eigentümer oder langfristigen Nutzer (d. h. dem Besitzer) des Geräts könne das Recht zustehen, jene Daten zu nutzen oder anderen deren Nutzung zu gestatten. Dadurch habe der Datenerzeuger zum einen mehr Entscheidungsfreiheit in Bezug auf die Frage, was mit den von seiner Maschine erzeugten Daten geschehe, zum anderen helfe dies, den ausschließlichen Zugang zu den Daten zu vermeiden.[85] Gleichzeitig seien aber Ausnahmen zu schaffen, etwa aus Verkehrsmanagement- oder aus Umweltgründen.

Ein Recht des Datenerzeugers ist jedoch aus verschiedenen Gründen abzulehnen.[86] Zum einen gilt, dass bestehende Regelungen des Zivil- und Strafrechts bereits ausreichende Instrumentarien zum Schutz der Daten bieten.[87] Zum anderen stellt sich insbesondere bei maschinengenerierten Daten die schwierige Frage, wer als Datenerzeuger anzusehen ist. Nach der Kommission werden solche Daten „ohne den unmittelbaren Eingriff eines Menschen im Rahmen von Computerprozessen, Anwendungen oder Diensten oder auch durch Sensoren erzeugt, die Informationen von virtuellen oder realen Geräten der Maschinen oder von einer Software erhalten.“.[88] Als Datenerzeuger kommen daher verschiedene Rechtssubjekte in Betracht, etwa der Hersteller des Geräts oder der Software, deren Eigentümer, Nutzer, derjenige, der in die Entwicklung des Geräts investiert hat, oder derjenige, der das Gerät betreibt und dafür gezahlt hat.[89]

V. Schlussbetrachtung

Die Diskussion um die Zweckmäßigkeit der Schaffung eines Dateneigentums und die damit verbundene Frage nach Datenhoheit befindet sich im Fluss. Die Betrachtung der verschiedenen Ansätze zeigt jedoch, dass das Einzeldatum für sich allein in der Regel nicht eigentumsrechtlich schützenswert ist. Hierfür sprechen neben Schwierigkeiten bei der technischen Umsetzung von Sicherungssystemen insbesondere gesamtökonomische Gründe. Eine generalisierte Zuweisung von Ausschließlichkeitsrechten an Daten, ohne zugleich diese Rechtsposition wieder relativierende Zugangs- und Teilhaberechte zu regeln, birgt ein hohes Risiko, vor allem innovationshemmend zu wirken und den gewünschten „Free Flow of Data“ erst gar nicht entstehen zu lassen. Dagegen bietet der Schutz von Einzeldaten und Datensammlungen im Wege vertraglicher Vereinbarungen bzw. über das sui-generis-Recht Mittel und Wege, um dynamischen Entwicklungen und verschiedensten Einzelfallgestaltungen angemessen Rechnung tragen zu können.

Sinnvollerweise sollte sich der Schutz aber nicht auf einzelne Datensätze, sondern auf Datensammlungen konzentrieren. Dies zeigt sich etwa am Beispiel der Metadaten, deren Wert sich erst aus der Zusammenfügung und Korrelation unterschiedlicher Daten und Datenarten ergeben kann. Den gesetzlichen Rahmen hierfür bilden die §§ 87a ff. UrhG mit dem Datenbankschutzrecht sui generis, das nicht an eine schöpferische Höhe geknüpft ist. Die Vorschriften werden flankiert vom Know-how-Schutz (insbesondere gemäß §§ 17, 18 UWG), für den nach Inkrafttreten der europäischen Know-how-Schutz-Richtlinie nunmehr ein einheitlicher Mindeststandard in den Mitgliedstaaten gelten wird.

Datengewinnung und Schaffung einer europäischen Datenökonomie

Daten sind oft in Texten, Bildern oder Datenbanken enthalten und müssen für die Generierung von Datenwertschöpfungsketten zunächst mittels Text und Data Mining Technologien extrahiert werden. Wie auch schon in der Debatte um die Schaffung eines „Dateneigentums“ gezeigt, können aber auch Urheber- und Leistungsschutzrechte hier unerwünschte praktische Zugangshürden generieren.

Der folgende Beitrag widmet sich der Problematik aus Sicht eines Start-ups und bespricht aktuelle Entwicklungen zum Text und Data Mining (TDM) sowie der Erweiterung des Presseverlegerleistungsschutzrechtes auf EU-Ebene. Als sachgerechte Lösungsoption wird eine einfache TDM-Schranke vorgeschlagen, die sich an der mit internationalen Urheberrechtsverträgen kompatiblen Fair-Use-Doktrin orientiert.

Text und Data Mining im Kontext von Smart Data – eine wirtschaftliche Perspektive

Patrick Bunk, Ubermetrics Technologies GmbH

Im Rahmen der Smart-Data-Forschungsprojekte sollen Datenwertschöpfungsketten etabliert werden, um sowohl großen als auch kleinen und mittleren Unternehmen den Zugang zu Schlüsseltechnologien des Digitalisierungsprozesses und mithin eine Teilhabe an der beginnenden europäischen Datenökonomie zu verschaffen. Diese Perspektive wird durch die derzeitige Position der Bundesregierung zur europäischen Urheberrechtsreform sowie die deutsche Regulierung zum Text und Data Mining (TDM) aus Sicht des Urheberrechts nicht befördert.

Derzeit wird auf europäischer Ebene diskutiert, ob eine Erlaubnis für TDM, beschränkt auf Forschungseinrichtungen und nur zum Zweck der Forschung, geschaffen werden sollte.[90] Als Auswirkung ist zu befürchten, dass im Umkehrschluss TDM durch private Anbieter oder kommerzielle Zwecke stets die Zustimmung des Urhebers erfordern wird.[91] Gleichzeitig soll im Rahmen der Reform der Schutz auf Erzeugnisse von Presseverlegern ausgeweitet werden, ohne dass es auf die für den Werkscharakter normalerweise entscheidende Schöpfungshöhe ankommt oder eine Schranke für kleinste Textausschnitte vorgesehen ist.[92] Damit würden auch gewöhnliche Texte bis hin zu einzelnen Wörtern geschützt, sobald sie in einer Presseveröffentlichung enthalten sind, und damit für 20 Jahre der öffentlichen Nutzung entzogen.

In Deutschland soll mit dem Urheberrechts-Wissensgesellschafts-Gesetz[93] eine TDM-Erlaubnis in § 60d UrhWissG-E ebenfalls nur nichtkommerzielle Forschungszwecke erfassen. Der in der Praxis an Bedeutung zunehmende Einsatz von TDM-Technologien durch Unternehmen und Start-ups könnte somit durch das eher impraktikable Erfordernis, Lizenzen einzuholen, erschwert und die Wettbewerbsfähigkeit auf internationalen Märkten dadurch geschmälert werden.

Um die Effekte dieser Reformvorhaben auf Datenwertschöpfungsketten nachzuvollziehen, ist es hilfreich, zunächst den im juristischen Bereich neuen Begriff „Text und Data Mining“ zu beleuchten.

1. Text und Data Mining

Text und Data Mining (TDM) ist zunächst einmal definitionsgemäß jeder Prozess, bei dem höherwertige Informationen oder Zusammenhänge aus Texten oder Daten extrahiert werden. Diese Prozesse sind seit Jahrzehnten fester Bestandteil der Informatik und finden sich in unzähligen Anwendungsgebieten.

Ein klassisches Beispiel für TDM ist die Suchfunktion auf einem Windows-, Mac- oder Linux-Betriebssystem. Diese Funktion analysiert alle Dokumente auf dem PC, fertigt automatisch Kopien aller Sätze in allen Dokumenten an und speichert diese strukturiert in einer Datenbank ab. Sobald der Nutzer nun durch Eingabe eines beliebigen Teils des Dokumentes in die Suchmaske nach einem Dokument sucht, werden die Informationen in Bruchteilen einer Sekunde aus der Datenbank abgerufen, und nicht aus dem Originaldokument.

Es gibt noch zahlreiche weitere Beispiele für TDM:

- Rechtschreibkorrektur und Grammatikprüfung sowie viele andere maschinelle Analysen menschlicher Sprache
- Mustererkennungsverfahren, die es z. B. ermöglichen, auf dem Smartphone in E-Mails enthaltene Telefonnummern anzuklicken
- Trend-Erkennung und -Analyse
- Spam-Erkennung
- Internet-Suchmaschinen wie Bing, Google, Qwant oder Cliqz

Auch die meisten Verfahren, die auf künstlicher Intelligenz (KI) basieren, sind definitionsgemäß TDM-Technologien, da sie höherwertige Informationen als Regeln aus den Daten- oder Test-Beständen „erlernen“. Jüngste Durchbrüche in den letzten 5 Jahren haben gezeigt, dass KI-Technologie in der Lage ist, monotone

Informations-Extraktion und Klassifikationsaufgaben zu übernehmen. Beispielsweise können die betreffenden Anwendungen Texte nach der Sprache sortieren, in der diese geschrieben sind, eine Kontonummer auf einer Rechnung als solche erkennen oder Tiere auf Bildern identifizieren.

2. Wie funktionieren die heute üblichen Künstliche-Intelligenz-Algorithmen, basierend auf Deep Learning?

Die KI-Technologie schafft eine vereinfachte Version eines Neurons, einer menschlichen Gehirnzelle, und simuliert diese. In der Praxis werden Hunderte solcher künstlicher Neuronen geschaffen, die miteinander verbunden sind. Dieses Neuronennetzwerk erhält bestimmte Eingabedaten, wie z. B. Tierbilder oder Sätze, zusammen mit einer Klassifikation, aus der per Algorithmus dann Regeln abgeleitet werden sollen. Dafür muss man den betreffenden Algorithmen so lange unterschiedliche klassifizierte Objekte präsentieren, bis einige der simulierten Neuronen einige Aspekte des Problems erlernen. Sobald das erreicht ist, kann ein Algorithmus Aufgaben übernehmen, die vorher nur von Menschen ausgeführt werden konnten.

Hierfür benötigt man allerdings eine sehr große Menge an Daten als Ausgangsbasis, um das Erlernen von Mustern zu ermöglichen. Dies sind normalerweise Hunderte Millionen bis Milliarden von Texten und Bildern. Gerade KMUs haben jedoch keine derartig großen, eigens geschaffenen Datenbestände. Diese fallen vielmehr nur bei sehr wenigen großen IT-Unternehmen wie beispielsweise Google und Facebook an. Alle anderen Anwender in der Wissenschaft und der Wirtschaft nutzen daher die öffentlich frei zugänglichen Datenbestände des Internets, z. B. Wikipedia, als Basis, auf der die KI-Technologien Strukturen in den jeweiligen Daten erlernen können.

3. Die aktuelle Rechtslage

Derzeit ist noch umstritten, ob für TDM eine urheberrechtliche Erlaubnis eingeholt werden muss, denn wie auch der Regierungsentwurf des UrhWissG-E bestätigt: Die „automatisierte Auswertung selbst, der Kern des sogenannten Text und Data Mining, ist keine urheberrechtlich relevante Handlung“.

Diese Aussage reflektiert allerdings nicht die Praxis des TDM. Für die Entwicklung, Evaluierung oder Verbesserung von TDM-Verfahren ist stets ein gleichbleibender, möglichst großer Korpus von Daten notwendig, um die Güte des Algorithmus messen zu können. Dieser vorstrukturierte Korpus besteht stets aus einer Vielzahl von bereinigten, für das jeweilige Problem repräsentativen Dokumenten oder Datenreihen. Diese sind zumindest vorübergehende Kopien, die naturgemäß unter das Urheberrecht fallen. Theoretisch ist eine zustimmungsfreie Nutzung flüchtiger, beiläufiger Kopien möglich, wenn diese als integraler und wesentlicher Teil eines technischen Verfahrens benötigt werden, der alleinige Zweck eine rechtmäßige Nutzung ist und diese Kopien keine eigenständige wirtschaftliche Bedeutung haben (vgl. § 44a UrhG). Diese Ausnahme kann bisher nur für solche TDM-Verfahren greifen, bei denen der Korpus unmittelbar nach der Informationsextraktion gelöscht wird.[94] Dies würde jedoch jede Neu-Entwicklung, Evaluation oder Verbesserung von TDM-Algorithmen in Europa in der Praxis verhindern. Darüber hinaus ist es im Einsatzfeld von TDM-Algorithmen häufig aus Anwenderperspektive oder aufgrund datenschutzrechtlicher Grundsätze erforderlich, die erzielten Analyseresultate durch Offenlegung der Originalquellen nachvollziehbar gestalten zu können.[95]

Diese Problematik stellt TDM-Technologien nutzende Unternehmen vor zwei wesentliche Herausforderungen:

1. Sie müssen bei Millionen von Texten feststellen, ob diese urheberrechtlich geschützt sind. Hierfür ist eine individuelle Wertung notwendig, um zu beur-

teilen, ob dem jeweiligen Text eine geistig-individuelle, kreative Schöpfungsleistung zugrunde liegt, wobei der Schutz nicht nur für Schöpfungen eigentümlicher Prägung, sondern auch für Werke von geringem schöpferischen Wert („kleine Münze“) einschlägig sein kann.[96]
2. Um Nutzungslizenzen einzuholen, müssen sie feststellen, wer die Urheber oder Inhaber der Verwertungsrechte des jeweiligen Werkes sind.

Berücksichtigt man die Tatsache, dass das Ziel des TDM-Einsatzes in der Regel lediglich die Informationsentnahme ist – ein Prozess, der durchgeführt durch einen Menschen als bloßer Werkgenuss frei ist – stellt sich die Frage, ob der Urheberrechtsschutz hier angebracht ist. Denn dessen Sinn und Zweck ist der Schutz der geistigen Schöpfung, und nicht der Schutz der Information.[97] Informationen als solche sollten nach dem Telos der bestehenden Schutzsystematik gemeinfrei bleiben, um nicht den gesellschaftlichen Austausch und Fortschritt zu behindern.[98] Solange die originäre Werkverwertung vom TDM nicht betroffen ist, müsste eine TDM-Schranke insofern lediglich sicherstellen, dass das TDM nicht zum Einfallstor für andere urheberrechtsrelevante Nutzungsarten wird.[99]

Im Entwurf der EU-Kommission heißt es: „Text und Data Mining können auch in Bezug auf bloße Tatsachen oder Daten durchgeführt werden, die nicht durch das Urheberrecht geschützt sind und in solchen Fällen wäre keine Genehmigung erforderlich.“[100] Das bedeutet im Umkehrschluss, auch nach Auslegung des deutschen Bundesrats, dass bei allen TDM-Prozessen, bei denen das Risiko nicht ausgeschlossen werden kann, dass die Daten urheberrechtlich geschützt sein könnten, in Europa in Zukunft zunächst eine explizite Zustimmung des jeweiligen Urhebers eingeholt oder der jeweilige TDM-Prozess unterlassen werden müsste.

4. Haftungsminimierung durch Filterung von geschützten Werken als alternativer Ansatz?

Unternehmen werden sich in Folge dieses Regulierungsvorschlags die Frage stellen, ob es möglich, ist die Haftungsrisiken durch eine Vorab-Filterung aller potenziell urheberrechtlich geschützten Werke zu vermeiden. Dies ist ökonomisch aus Risikogesichtspunkten geboten: Selbst bei einer optimistischen Abschätzung müsste man davon ausgehen, dass 1 % eines Prozentes aller Dokumente in einem Korpus urheberrechtlich relevante Teile enthalten könnten, und man würde mit dem TDM-Prozess auf diesem Korpus in Bezug auf die betreffenden Dokumente eine urheberrechtliche Verletzungshandlung begehen. Bei Korpus-Größen von 10 Milliarden Texten bedeutet dies, dass man bei einem TDM-Prozess von dem Risiko einer Urheberrechtsverletzung in 1 Million Fällen ausgehen müsste. Dies würde bei üblichen Schadenssummen im gewerblichen Bereich ein Haftungsrisiko von mehreren Millionen Euro pro TDM-Prozess bedeuten. Bei solchen wirtschaftlichen Risiken sind TDM-Prozesse in Europa nicht einmal innerhalb von Forschungsabteilungen von Unternehmen tragbar.

Daher würde die vorgeschlagene EU-Regulierung den Aufbau einer umfassenden Copyright-Filter-Infrastruktur erfordern. Jedoch ist dieser aktuell nicht möglich.

Denn um festzustellen, ob ein Text eine ausreichend große Kopie eines anderen urheberrechtlich geschützten Textes eines Dritten enthält, müsste man alle Texte aller Urheberrechtsinhaber speichern, um diese dann mit dem fraglichen Text zu vergleichen – dieser Vorgang selbst ist jedoch bereits eine Urheberrechtsverletzung nach der aktuellen Auslegung des europäischen Rechts.

Optimisten mögen einwenden, dass die Informatik dafür doch sicher eine Lösung finden würde. Die Absurdität des Regulierungsvorschlages besteht jedoch

darin, dass selbst in dem Fall, dass dies algorithmisch möglich wäre, die Prüfung, ob ein Artikel urheberrechtlich geschützt ist, definitionsgemäß selbst ein TDM-Prozess ist. Dies würde bedeuten, dass bereits der Prüfprozess an sich immer dann, wenn er einen urheberrechtlich schützenwerten Teil in einem Dokument identifiziert, eine schadensersatzfähige Urheberrechtsverletzung durch die Analyse des urheberrechtlich geschützten Textteiles verursachen würde.

Insofern muss gefolgert werden, dass die Filterung von urheberrechtlichem Material keine Option für eine Risikominimierung ist. Das bedeutet in der praktischen Folge unabsehbare Nachteile für die wettbewerbsfähige Entwicklung von TDM- und KI-Technologien in Europa und würde der postulierten Entwicklung einer europäischen Datenökonomie diametral entgegenstehen.

5. Wettbewerbsfolgen

Eine weitere Folge dieses Vorschlags ist eine permanente Veränderung der Wettbewerbsstruktur im Bereich der KI-Technologien.

Wie festgestellt wurde, ist es unmöglich zu beweisen, dass die Training-Sets für KI-Technologien frei von urheberrechtlich geschütztem Material sind. Man benötigt demzufolge Lizenzen für sehr große Datenbestände, um KI-Technologien entwickeln zu können. Für Unternehmen ohne marktbeherrschende Stellung, z. B. KMUs und Start-ups, ist es praktisch unmöglich, Verträge mit jedem Urheberrechtsinhaber in Europa auszuhandeln. Eine Ausnahmeregelung für Start-ups löst dieses Problem noch nicht, da selbst unter den sehr erfolgreichen Start-ups so gut wie keines selbst eine marktbeherrschende Stellung erreicht. Das bedeutet für alle KMUs und Start-ups, dass die Transaktionskosten für die Verhandlung mit jedem Urheberrechtsinhaber in Europa prohibitiv hoch sind und zudem die Machtasymmetrie im Verhandlungsfall eine Marktlösung gesellschaftlich ineffizient gestaltet.

Was passiert mit den großen US-Akteuren wie Google?

Google crawlt das Internet und trainiert seine Algorithmen unter der Fair-Use-Doktrin[101] in den USA. Die Fair-Use-Doktrin erlaubt die Nutzung urheberrechtlich geschützten Materials für Zwecke wie die kritische Auseinandersetzung, Kommentierung, Nachrichtenberichterstattung, Lehre, Wissenschaft oder Forschung (vgl. 17 U.S.C. § 107), aber auch Tätigkeiten kommerzieller Suchmaschinen können darunterfallen.[102] Bei der Feststellung, ob die Verwendung eines Werkes im Einzelfall als Fair Use zu qualifizieren ist, kommt es entscheidend auf folgende Kriterien an (4-Faktoren-Test):

- Zweck und Charakter der Nutzung, einschließlich der Frage, ob die Nutzung kommerzieller Art ist oder gemeinnützigen Bildungszwecken dient,
- die Natur des geschützten Werkes,
- Umfang und Wesentlichkeit des genutzten Teils in Relation zum Gesamtwerk und
- den Effekt, den die Nutzung auf dem potenziellen Markt auf den Wert des geschützten Werkes haben kann.

Die Rechtsprechung des Surpreme Courts misst der Frage besondere Bedeutung zu, ob die Nutzung eines Werkes transformativ ist, also etwas Neues hinzufügt, einen neuen Zweck verfolgt oder das Werk durch sie in einem neuen Kontext erscheint.[103]

Darauf hat der EU-Kommissionsvorschlag an sich keine Auswirkung. Auch eine juristische „Nachbesserung“, wenn überhaupt möglich, würde aufgrund der ökonomischen Sachzwänge der Urheber daran nichts ändern.

Google ist eine sehr große Suchmaschine mit vielen Benutzern in Europa. Im Internet gefunden zu werden, ist immer noch für alle Unternehmen und Urheber sehr wichtig, vor allem für Verlage. Insofern

sind Standardverträge für bereits marktmächtige bzw. marktbeherrschende Unternehmen eine umsetzbare Option.[104] Wegen der Kopplung an die Suchfunktion ist es naheliegend, dass hier eine hohe Bereitschaft zur vertraglichen Bindung besteht. Weniger marktmächtige Unternehmen, zu denen insbesondere Start-ups gehören, werden einen solchen Vorteil kaum nutzen können. Im Bereich von Zukunftstechnologien wie KI könnten somit Monopolstellungen verstärkt und Markteintrittsbarrieren für europäische Unternehmen geschaffen werden, ohne dass ein wettbewerbswidriges Verhalten der marktmächtigen bzw. marktbeherrschenden Unternehmen selbst vorliegt.

Eine vergleichbare Situation hat sich bereits in Folge des deutschen Presseverlegerleistungsschutzrechtes gezeigt: In diesem Fall erhielt Google von allen deutschen Verlagen kostenlose Lizenzen zur Anzeige von Snippets (kleinen Textausschnitten). Die Wettbewerbsbehörden sahen hierin keinen Verstoß gegen das Wettbewerbsrecht.[105] Gleichzeitig verlangten viele Verlage von allen kleineren Anbietern kostenpflichtige Lizenzen.[106] In der Folge besteht die Gefahr, dass kleine Anbieter benachteiligt sind und langfristig deren Verdrängung vom Markt droht.

Darüber hinaus könnten Verlage Konkurrenzverhältnisse aus dem Primär- auf den Sekundärmarkt der Datenveredler und Informationsintermediäre verlagern. Wenn beispielsweise ein Suchmaschinenanbieter, der vom Verlag A finanziert wird, keine Lizenzen vom Verlagskonkurrenten B erhält und dessen Suchmaschine wiederum nicht auf Texte des Verlags A zurückgreifen kann, können die Analyseergebnisse nur einen Ausschnitt der Lebenswirklichkeit abbilden und dürften somit an Qualität einbüßen. Können sich diese Anbieter nicht auf dem Markt behaupten, drohen langfristig die Marktkonzentration auf wenige marktbeherrschende Anbieter und damit eine Angebotsreduktion. Die Sicherung von Medien- und Meinungsvielfalt im Suchmaschinensektor ist jedoch ein wichtiges Anliegen.[107]

Die Etablierung von Lizenzmodellen, bei denen erfolgreiche TDM- oder KI-Technologien nutzende oder entwickelnde Unternehmen einen Teil ihrer Gewinne an Urheberrechtsinhaber zahlen, ist nur realisierbar, soweit für diese Unternehmen auch im internationalen Kontext ein profitables Geschäftsmodell verbleibt. Um konkurrenzfähig zu bleiben, könnten TDM- oder KI-Technologien verwendende Unternehmen jedoch ihren Geschäftssitz in Länder mit einer der Fair-Use-Doktrin vergleichbaren Rechtslage verlagern. Diese Gewinne und wertschöpfungsstarke Arbeitsplätze für KI-Entwickler würden somit nicht in Europa geschaffen.

In der Folge wird die europäische Wirtschaft auf KI-Systeme außereuropäischer Anbieter angewiesen sein. Der Vorschlag der EU-Kommission beinhaltet deshalb in Verkennung der technischen Entwicklungsbedingungen für KI eine Verfestigung der natürlichen Monopolposition bestehender marktmächtiger außereuropäischer Marktteilnehmer.

6. Wie könnte dieses Problem gelöst werden?

Einige Entwürfe von Stellungnahmen der Parlaments-Ausschüsse sehen eine weiter gefasste TDM-Schranke vor,[108] müssten aber noch vom jeweiligen Ausschuss angenommen werden und sich im dann folgenden Trilog-Verfahren zwischen Kommission, Rat und Parlament durchsetzen.

Eine einfache TDM-Schranke könnte sich an der mit internationalen Urheberrechtsverträgen kompatiblen Fair-Use-Doktrin orientieren und gleichzeitig die Interessen der Urheber wahren:

> „Nutzungshandlungen, die zum TDM erforderlich sind, sind ohne Zustimmung des Urhebers sowohl für Forschungseinrichtungen als auch für private Anbieter und sowohl zu gemeinnützigen und kommerziellen Zwecken zu erlauben, unter der Bedingung, dass

- der Zugriff auf die Originalquellen rechtmäßig ist oder diese öffentlich zugänglich sind,
- die Verwertung der Originalquelle durch die Analyse sowie Verbreitung der Analyseergebnisse nicht erschwert wird, insbesondere keine Substituierungswirkung eintritt,
- das Werk lediglich für die Extraktion von Information oder einer anderweitigen vom Urheber gestatteten Nutzung verwendet wird."

Durch diese Einschränkungen könnte sichergestellt werden, dass die jeweiligen Urheber bei einer Verwertung ihres Werkes weder durch den Einsatz von TDM noch durch die Verbreitung der betreffenden Analyseergebnisse beeinträchtigt werden.

7. Fazit

Auf dem Weg in eine europäische Datenökonomie sollten öffentliche Informationen weiterhin jedem zugänglich und für jeden auffindbar sein. Das Urheberrecht sollte bis auf sehr begrenzte Ausnahmen weiterhin nur den künstlerischen Ausdruck und nicht die in einer künstlerischen Arbeit verarbeiteten Fakten und Sachzusammenhänge schützen.

Die vorgeschlagene TDM-Regulierung durchbricht ohne Not durch unvermeidliche urheberrechtliche Haftungsrisiken die Entwicklung einer passfähigen Systematik für eine europäische Datenökonomie. Bei legalem Zugang zu einem öffentlichen Dokument sollte kein Unterschied in Bezug darauf gemacht werden, ob die darin enthaltenen Informationen durch einen Menschen oder eine Maschine verarbeitet werden. Computer und Algorithmen haben keine Freude am künstlerischen Ausdruck eines Werkes, der durch das Urheberrecht geschützt ist. Zumindest noch nicht. Mit dem Versuch, im Ergebnis lediglich die Geschäftsmodelle europäischer Verlage mit neuen urheberrechtlichen Abgaben auf Suchmaschinen-Technologien zu subventionieren, wird die EU stattdessen die Dominanz einiger weniger US-Technologieunternehmen massiv stärken und damit deren Verhandlungsmacht gegenüber Verlagen erhöhen. Dies wird, wie gezeigt, absehbar auf Kosten der Wettbewerbsfähigkeit und der Innovationskraft europäischer Unternehmen geschehen.

In Europa bestehende Kompetenzen in Schlüsseltechnologien wie Datenanalyse und Künstliche-Intelligenz-Systemen würden absehbar durch dieses Vorhaben wirtschaftlich nur zum Vorteil von wenigen US-amerikanischen Technologieunternehmen genutzt werden können.

Die Notwendigkeit, den Journalismus zu finanzieren, ist nachvollziehbar. Das Problem ist ökonomisch bedingt. Die vorgeschlagene Regulierung wird aber im Hinblick auf die Entwicklungsbedingungen der europäischen Datenökonomie das Gegenteil ihres eigentlichen Zieles erreichen: Klassische Verlags-Geschäftsmodelle werden mittelfristig geschädigt und lediglich eine Handvoll marktmächtiger Internet-Akteure wird profitieren.

Daten als Wirtschaftsgut: Kurzüberblick über den Rechtsrahmen

Die Vielzahl der betroffenen Rechtsmaterien und Begrifflichkeiten bei der Betrachtung von Daten als Wirtschaftsgut ist für Laien, wie auch Juristen, oftmals verwirrend und verhindert sachgerechte Detaillösungen. Der folgende Abschnitt soll deshalb einen groben Überblick über die unterschiedlichen Begrifflichkeiten und Rechtsinstrumente geben. Mit der komprimierten Präsentation soll das Begriffsverständnis komplexer Rechtsmaterien erleichtert werden.

Wesentliche Relevanz im Zusammenhang mit Daten als Wirtschaftsgut haben die folgenden Fragen: Wann greift Urheberrechtsschutz ein? Was ist unter dem Datenbankherstellerrecht sui generis zu verstehen? Wie können Unternehmer ihre Betriebs- und Geschäftsgeheimnisse schützen? Eine Neuheit stellt das Presseverlegerleistungsschutzrecht dar. Wenn sich Dritte unberechtigt Zugang zu Daten verschaffen, können auch Strafnormen einschlägig sein.

Urheberrechtlich geschützte Werke

Anforderungen an den Werkscharakter
Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören beispielsweise Sprach- und Schriftwerke, Computerprogramme, Musik, pantomimische Werke, Tanzkunst, Kunstwerke, Lichtbilder, Filme, Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen (vgl. § 2 UrhG). Amtliche Werke wie beispielsweise Gesetze oder amtliche Bekanntmachungen genießen keinen urheberrechtlichen Schutz (§ 5 UrhG).

Werke im Sinne des Urhebergesetzes sind nur persönliche geistige Schöpfungen. Auch bei kleinsten Textausschnitten kann der Werkscharakter vorliegen.[109] 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.[110]

Verwertungsrechte
Der Urheber hat grundsätzlich das ausschließliche Recht, sein Werk zu verwerten, d. h. zu nutzen, anderen dessen Nutzung zu gestatten oder von dessen Nutzung auszuschließen. Diese Nutzungen umfassen insbesondere das Recht zur Bearbeitung, Vervielfältigung, Verbreitung, Ausstellung und öffentlichen Wiedergabe, das wiederum u. a. das Recht zur öffentlichen Zugänglichmachung beinhaltet (vgl. §§ 15 ff. UrhG). Sonderbestimmungen für Computerprogramme finden sich in §§ 69a ff. UrhG.

Der Urheber kann Dritten Nutzungsrechte für einzelne oder alle Nutzungsarten einräumen. Unterschieden wird hierbei zwischen einfachen und ausschließlichen Nutzungsrechten, die räumlich, zeitlich oder inhaltlich beschränkt eingeräumt werden können (vgl. §§ 31 ff. UrhG).

Digitale Kopien fallen in der Regel unter das Vervielfältigungsrecht, das grundsätzlich auch bei jeder Form der Übertragung eines urheberrechtlich geschützten Werkes auf ein anderes Speichermedium einschlägig ist, unabhängig davon, ob Kopien privat oder öffentlich hergestellt werden und ob sie flüchtig oder dauerhaft oder in einem anderen Format erfolgen.[111] Im Onlinekontext ebenfalls von Relevanz ist das Recht zur öffentlichen Zugänglichmachung. Diese kann auch bei bereits online veröffentlichten Werken einschlägig sein, wenn ein Werk mittels eines anderen technischen Verfahrens, das sich von dem bisher verwendeten unterscheidet, oder für ein neues Publikum wiedergegeben wird. Das Publikum ist neu, wenn der Urheber die ursprüngliche öffentliche Wiedergabe nicht an dieses Publikum richtete, beispielsweise bei beschränkter Abrufbarkeit oder Zugriffskontrollen.[112]

Urheberrechtsschranken
Das Urheberrecht ist beschränkt durch sogenannte Schranken, unter deren Bedingungen Werke zustimmungsfrei genutzt werden können. Im Kontext von Smart Data ist u. a. die flüchtige Kopie nach § 44a UrhG von Relevanz, wonach vorübergehende Vervielfältigungen, die technisch unumgänglich sind, zulässig bleiben. Daneben sind weitere Schranken für Wissenschaft und Lehre im Urheberrechts-Wissensgesellschafts-Gesetz[113] sowie im Entwurf einer Text-und-Data-Mining-Schranke im Entwurf einer Richtlinie über das Urheberrecht im digitalen Binnenmarkt[114] geplant.

Open Source
Werke unter Open-Source-Lizenz sind in der Regel kostenfrei nutzbar, unterliegen jedoch zum Teil ebenfalls einschränkenden Lizenzbestimmungen. Zu nennen sind hier Copyleft-Klauseln, nach denen sämtliche Weiterentwicklungen eines Werkes unter denselben Lizenzbedingungen freizugeben sind.

Folgen von Urheberrechtsverletzungen
Urheber haben bei Verletzungen des Urheberrechts Anspruch auf Unterlassung und Schadensersatz sowie darauf, Vervielfältigungsstücke vernichten zu lassen (§§ 97, 98 UrhG). Daneben ist die vorsätzliche unerlaubte Verwertung urheberrechtlich geschützter Werke strafbar (§ 106 UrhG).

Datenbankwerke (§ 4 UrhG)

Besteht eine entsprechende Schöpfungshöhe in der Anordnung und Gestaltung einer Datenbank, so kann die Datenbank ein urheberrechtlich geschütztes Werk im Sinne des § 4 UrhG darstellen. Die Schöpfungshöhe eines Werks wird in der Regel zu verneinen sein, wenn sich die Anordnung oder Darstellung bereits aus der Natur der Sache ergibt oder durch Gesetze der Zweckmäßigkeit, der Logik oder durch Notwendigkeiten vorgegeben ist und kein ausreichender Spielraum für individuell-geistige Formgestaltung verbleibt.[115] Elektronische Datenbanken müssten über ein Ausgabeformat verfügen, das die Daten systematisch und methodisch geordnet zugänglich macht.[116] Für die Werkeigenschaft entscheidend ist die Originalität der Verknüpfungs- und Abfragemöglichkeiten.[117]

Datenbankherstellerrecht sui generis (§ 87a UrhG)

Datenbankhersteller können Schutz nach § 87a UrhG geltend machen, wenn die Daten systematisch oder methodisch angeordnet sowie einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und ihre Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert.[119] Kein Schutz besteht mangels systematischer oder methodischer Anordnung der einzelnen Elemente für bloße „Datenhaufen", d. h. für Rohdaten, die noch nicht besonders angeordnet wurden, selbst wenn die Beschaffung der Rohdaten eine wesentliche Investition erforderte.[120] Unerheblich ist hingegen eine ungeordnete interne Datenablage, wenn das Abfragesystem eine systematische oder methodische Ordnung herbeiführt.[121] Entscheidend ist die Verbindung eines Datenbestands mit einem Abfragesystem, das zielgerichtete Recherchen nach Einzelelementen in diesem Datenbestand ermöglicht.[122] Das OLG Köln[123] entschied, dass eine Bearbeitung der in die Datenbank aufgenommenen Einzelinformationen nicht erforderlich ist.[124]

Eine weitere Voraussetzung ist die wesentliche Investition: diese kann finanzieller Natur sein oder im Einsatz von Zeit, Arbeit und Energie bestehen.[125] Berücksichtigungsfähig sind beispielsweise Investitionen in die Aufbereitung des Datenbestandes, die Konzeption von Verknüpfungen und die Erarbeitung von Abfrageoptionen, nicht jedoch die zur Erzeugung der Daten selbst eingesetzten Mittel.[126] Dies bedeutet, dass Mittel erfasst werden, die zur Ermittlung und Zusammenstellung bereits vorhandener Daten verwendet werden, nicht jedoch die Mittel, die zur Erzeugung der Elemente verwendet werden.[127] Da auch die Richtigkeits- und die Zuverlässigkeitsprüfung von der Rechtsprechung als berücksichtigungsfähige Kosten anerkannt werden,[128] kann davon ausgegangen werden, dass bei Data-Mining-Verfahren, die in vorhandenen Datenbeständen verborgene Zusammenhänge analysieren und identifizieren, die datenbankbezogenen Investitionskosten zu berücksichtigen sind.[129] Insoweit ist zu prüfen, ob Investitionen bzw. Arbeitsaufwand in die Strukturierung und Aufbereitung der (bereits vorhandenen) Daten oder eher in die Erzeugung der Rohdaten bzw. „neuer" Daten fließen.

Die §§ 87a ff. UrhG schützen nicht die in der Datenbank enthaltenen Informationen.[130] Der sui-generis-Schutz des Datenbankherstellers soll nicht zur Entstehung eines neuen Rechts an den einzelnen in der Datenbank gesammelten Elementen als solchen führen.[131] „Schutzgegenstand sind nicht die einzelnen in die Datenbank aufgenommenen Informationen, sondern die Datenbank als Gesamtheit des unter wesentlichem Investitionsaufwand gesammelten, geordneten und einzeln zugänglich gemachten Inhalts als immaterielles Gut."[132] Der Urheber kann nur die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Datenbank insgesamt oder nach Art/Umfang wesentlicher Teile untersagen. Nach § 87b Abs. 1 S. 2 UrhG steht dem 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".

Presseverlegerleistungsschutzrecht

Die Einführung dieses Leistungsschutzrechts gewährt Herstellern eines Presseerzeugnisses ab Veröffentlichung für ein Jahr das ausschließliche Recht, das Presseerzeugnis oder Teile davon zu gewerblichen Zwecken öffentlich zugänglich zu machen (§§ 87f, 87g Abs. 2 UrhG). Zu Presseerzeugnissen zählen

> „redaktionell-technische Festlegungen journalistischer Beiträge im Rahmen einer unter einem Titel auf beliebigen Trägern periodisch veröffentlichten Sammlung, die bei Würdigung der Gesamtumstände als überwiegend verlagstypisch anzusehen ist und die nicht überwiegend der Eigenwerbung dient. Journalistische Beiträge sind insbesondere Artikel und Abbildungen, die der Informationsvermittlung, Meinungsbildung oder Unterhaltung dienen".

Auch Blogs können Presseerzeugnisse darstellen, wenn sie als eine redaktionell ausgewählte Sammlung journalistischer Beiträge gewertet werden können.[133]

Das Schutzrecht besteht nicht gegenüber jedermann, sondern nur gegenüber gewerblichen Anbietern von Suchmaschinen sowie gewerblichen Anbietern von Diensten, die Inhalte entsprechend aufbereiten (§ 87g Abs. 4 UrhG). Dem Presseverleger steht nur das Recht der öffentlichen Zugänglichmachung des Originals zu gewerblichen Zwecken zu, wodurch die Vervielfältigung ausdrücklich nicht eingeschränkt wird.[134] Sobald Presseerzeugnisse die Schöpfungshöhe erreichen, können sie aber Urheberrechtsschutz genießen.

Eine Verlinkung bleibt jedoch weiterhin möglich,[135] hierfür erstreckt sich das neue Schutzrecht nicht auf einzelne Wörter und kleinste Textausschnitte.[136] Umstritten ist die zulässige Länge dieser „kleinsten Textausschnitte", insbesondere im Zusammenhang mit der Anzeige sogenannter Snippets. Textausschnitte mit einem Umfang von mindestens 25 Wörtern können nach aktueller Rechtsprechung des OLG München nicht als kleinste Textausschnitte im Sinne des § 87f Abs. 1 S. 1 UrhG angesehen werden.[137]

Das im Vorschlag der EU-Kommission vorgesehene Leistungsschutzrecht im Entwurf der Richtlinie über das Urheberrecht im digitalen Binnenmarkt[138] würde weiter gehen, da im Entwurf keine Beschränkungen auf bestimmte Verpflichtete oder Textlängen enthalten sind sowie auch das Recht der Vervielfältigung „bei digitaler Nutzung" den Presseverlagen vorbehalten sein soll. Zusätzlich würde sich die Schutzdauer von 1 Jahr auf 20 Jahre verlängern, wenn dieser Entwurf in Kraft treten würde.

Geschäfts- und Betriebsgeheimnisse

Über die Auswertung von Sensordaten, beispielsweise aus Maschinen, können Rückschlüsse auf die Herstellung von Maschinen und Produkten oder den Einsatz dieser Maschinen im Betrieb hergeleitet werden. Somit könnten Betriebs- und Geschäftsgeheimnisse sowohl der Maschinenhersteller als auch der Maschinenbetreiber hergeleitet werden und unternehmensbezogenes Wissen abfließen.

Bisher ist der Schutz von Betriebs- und Geschäftsgeheimnissen in den §§ 17, 18 UWG dergestalt geregelt, dass Ansprüche auf Unterlassung und Schadensersatz bestehen, wenn auf ein Unternehmen bezogene Tatsachen, Umstände oder Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat, unbefugt offengelegt werden.[139]

Die Neuregelung wird entsprechend Artikel 2 Nr. 1 (a)–(c) der Richtlinie (EU) 2016/943 Betriebs- und Geschäftsgeheimnisse definieren als

- geheim (nicht allgemein bekannt oder nicht ohne weiteres zugänglich),
- von kommerziellem Wert, weil sie geheim sind, und
- Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen.

Möchten nach der künftigen Rechtslage Beteiligte Daten als Betriebs- oder Geschäftsgeheimnisse schützen, wird ein Geheimhaltungsinteresse nicht bereits vermutet, sondern es müssen aktiv „angemessene“ Geheimhaltungsmaßnahmen ergriffen werden. Dies könnte zu einer vergleichbaren Situation wie im Datenschutzrecht führen: Wird der Zugriff auf die Daten nicht durch technische Mittel oder organisatorische Maßnahmen derart erschwert, dass ein Datenzugriff unverhältnismäßigen Aufwand erfordert, dürfte auch kein rechtlicher Schutz bestehen. Um zu verhindern, dass Wettbewerber Kenntnis unternehmensbezogener Daten erhalten, könnten sich gegebenenfalls bekannte Mechanismen aus dem Datenschutzrecht anbieten, wie beispielsweise Datentrennung, Zugriffskontrolle und Anonymisierung (Entfernung des Unternehmensbezugs).

Strafbarkeit des Abfangens und Ausspähens von Daten

Strafrechtliche Konsequenzen drohen für Personen, die sich oder anderen unbefugt

- Zugang zu Daten, die nicht für sie bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschaffen oder
- unter Anwendung von technischen Mitteln nicht für sie bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschaffen (§§ 202a, 202b StGB).

Die Strafvorschriften beziehen sich jedoch nur auf solche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Datenberechtigter
Berechtigt ist in der Regel die speichernde Stelle, wobei es nicht darauf ankommt, ob diese Person auch Eigentümer des Datenträgers ist. Die Berechtigung kann übertragen werden, beispielsweise durch Überlassung der Nutzung, wenn dadurch auch die Berechtigung zur Nutzung der Programmdaten übertragen wurde.[140]

Überwindung der Zugangssicherung
Die besondere Sicherung muss den Zweck haben, den Zugang zu verhindern.[141] Zudem wird verlangt, dass die Überwindung der Zugangssicherung nicht ohne weiteres möglich ist, sondern einen nicht unerheblichen zeitlichen oder technischen Aufwand erfordert.[142]

Unbefugt
Nicht strafbar sind sogenannte Penetrationstests, die dem Aufspüren von Sicherheitslücken im EDV-System dienen, soweit das Einverständnis des Datenberechtigten vorliegt.

Vorsatz
Täter müssen mindestens billigend in Kauf nehmen, gegen Zugang gesicherte Daten Dritter unbefugt auszulesen.

Über die Autoren

Autoren

DR. ALEXANDER DUISBERG

... ist Partner bei Bird & Bird in München. Er ist Leiter der AG „Daten als Wirtschaftsgut“ in der Smart-Data-Begleitforschung, Rechtsexperte in sämtlichen Bereichen der Digitalisierung wie „Big Data“, „Cloud Computing“, „IoT“ und „Industrie 4.0“ sowie Schiedsrichter am WIPO Arbitration and Mediation Centre.

PATRICK BUNK

... ist Gründer und CEO der ubermetrics Technologies GmbH. Er studierte Ökonomie in Berlin und an der Northwestern University in den USA. Er ist Experte für quantitative Methoden zur Analyse der Informationsverbreitung sowie von deren Markteinflüssen.

Herausgeber

PD DR. OLIVER RAABE

... ist Leiter der Forschungsgruppe „Informationsrecht für technische Systeme und Rechtsinformatik“ am Karlsruher Institut für Technologie sowie Direktor am FZI Forschungszentrum Informatik und leitet die Fachgruppe Rechtsrahmen der Smart-Data-Begleitforschung. Er ist Jurist und habilitierte in der Informatik.

MANUELA WAGNER

... Ass. iur. Sie ist Promovendin am Zentrum für Angewandte Rechtswissenschaft des Karlsruher Instituts für Technologie. Sie betreut Forschungsprojekte zu den rechtlichen Themenschwerpunkten Datenschutz und Energierecht. Mit PD Dr. Raabe leitet sie die Fachgruppe Rechtsrahmen der Smart-Data-Begleitforschung.

Mitglieder der Fachgruppe Rechtsrahmen

Amon, Peter
Siemens AG, Projekt Virtuose-DE

Bremert, Benjamin
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Projekt iTesa

Bretfeld, Jürgen
Advaneo GmbH

Bretthauer, Dr. Sebastian
Johann Wolfgang Goethe-Universität Frankfurt am Main, Projekt Smart Regio

Bunk, Patrick
Ubermetrics GmbH, Projekt Smart Data Web

Drepper, Dr. Johannes
Leiter Arbeitsgruppe Datenschutz der Fachgruppe Rechtsrahmen, TMF e. V., Projekt SAHRA

Duisberg, Dr. Alexander
Leiter der Arbeitsgruppe Daten als Wirtschaftsgut, Bird & Bird

Eckhardt, Dr. Jens
Derra, Meyer und Partner Rechtsanwälte PartGmbB

Elteste, Thomas
DB-Systel, Projekt SD4M

Fasching, Peter
UK Erlangen, Projekt KDI

Freitag, Gerald
DB-Systel, Projekt SD4M

Friederici, Florian
Fraunhofer FOKUS, Projekt Virtuose-DE

Fröhlich, Sven
Technische Universität Dresden, Projekt ExCELL

Gläß, Valérie LL.M.
Leiterin Arbeitsgruppe Datenschutz der Fachgruppe Rechtsrahmen, TMF e. V., Projekt SAHRA

Gül, Serhan
Fraunhofer HHI, Projekt Virtuose-DE

Guzman, Liliana
Fraunhofer IESE, Projekt PRO-OPT

Hilber, Dr. Marc LL.M.
Oppenhoff & Partner

Janneck, Kai
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Projekt iTesa

Jeske, Henning
Technische Universität Dresden, Projekt ExCELL

Klein, Achim
Universität Hohenheim, Projekt InnOplan

Lenk, Dr. Alexander
BMW Group

Maier, Florian
Fraunhofer IAO, Projekt Smart Energy Hub

Meiers, Thomas
Fraunhofer HHI, Projekt sd-kama

Oppermann, Henrik
USU Software AG, Projekt SAKE

Premm, Marc
Universität Hohenheim, Projekt InnOplan

Runde, Dr. Detlef
Fraunhofer HHI, Projekt sd-kama

Schallaböck, Jan
iRights.Law Rechtsanwälte, Projekt Smart Data Web

Schmidt, Martin
Cautus Service GmbH

Spiecker genannt Döhmann, Prof. Dr. Indra LL.M.
Johann Wolfgang Goethe-Universität Frankfurt am Main, Projekt Smart Regio

Stecher, Björn
Initiative D 21

Steinmann, Jonas
TMF e. V., Projekt SAHRA

Steffen, Dr. Matthias
Bayer AG, Projekt Sidap

Troemel, Marc
Vico Research & Consulting GmbH, Projekt Smart Data Web

Ursinus, Sven
BITMi Bundesverband IT-Mittelstand e. V.

von Grafenstein, Maximilian LL.M.
Alexander von Humboldt Institut für Internet und Gesellschaft

Wachovius, Juliane
Hochschule für Angewandte Wissenschaften Hof, Institut für Informationssysteme der Hochschule Hof (iisys)

Wacker, Richard
YellowMap AG

Weber, Prof. Dr. Beatrix MLE
Leiterin der Arbeitsgruppe Daten als Wirtschaftsgut, Hochschule für Angewandte Wissenschaften Hof, Projekt sd-kama

Weichert, Dr. Thilo
Netzwerk Datenschutzexpertise

Willkomm, Dr. Marlene
Stellvertretende Leiterin der Hochwasserschutz-zentrale Köln, Stadtentwässerungsbetriebe Köln, AöR Projekt sd-kama

Wimmer, Max
Hochschule für Angewandte Wissenschaften Hof, Projekt sd-kama

Xu, PD Dr. habil. Feiyu
DFKI Deutsches Forschungszentrum für Künstliche Intelligenz, Projekt SD4M

Zwingelberg, Harald
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Projekt iTesa

Fußnoten

* Besonderer Dank geht an Dr. Benedikt Vogel, LLM, Bird & Bird LLP, für die wertvolle Unterstützung bei der Erstellung.

1 Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 17.01.2017, „Aufbau einer europäischen Datenwirtschaft“, COM(2017) 9 final.

2 „Open Data in Deutschland“ Sieben Forderungen der Fachgruppe „Wirtschaftliche Potenziale und gesellschaftliche Akzeptanz“ der Smart-Data-Begleitforschung, abrufbar unter: http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smart-data-brosch%C3%BCre_open_data_deutschland.pdf?__blob=publicationFile&v=9.

3 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über das Urheberrecht im digitalen Binnenmarkt vom 14.09.2016, COM(2016) 593 final.

4 Wiebe, CR 2017, 87 (91) spricht in diesem Zusammenhang auch vom „Grundsatz des Gemeingebrauchs von Informationen“.

5 Vgl. Erwägungsgrund 3 der PSI Richtlinie.

6 Zur Interoperabilität insbesondere Kerber/Schweitzer, Interoperability in the Digital Economy, in: Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 8(1), 2017, 39.

7 Als Metadaten werden Daten bezeichnet, die Informationen über weitere Daten enthalten (vgl. Harrach, Risiko-Assessments für Datenqualität, S. 21) und es den Anwendern ermöglichen, Datensammlungen zu verstehen und weiterzugeben (vgl. ISO/IEC-Spezifikation 11179 [ISO99]).

8 Zech, Information als Schutzgegenstand (2012), S. 37 ff. trifft eine Einteilung der Informationen in semantische (durch eine bestimmte Bedeutung) und syntaktische (durch Zeichen repräsentierte) Information.

9 Wobei natürlich auch hier Kontextualität sich durch die bei der Messung miterhobenen bzw. hinzugefügten Metadaten (z.B. Ort und Zeit der Messung, Messparameter, etc.) ergibt und hinzutritt.

10 Heymann, CR 2016, 650 (657).

11 Vgl. statt vieler Europäische Kommission, Legal study on Ownership and Access to Data – Final report 2016, S. 61 f., abrufbar unter https://bookshop.europa.eu/en/legal-study-on-ownership-and-access-to-data-pbKK0416811/ m.w.Nachw.

12 Zech, CR 2015, 137 (144); vgl. auch Dorner, CR 2014, 617 (618) m.w.Nachw.

13 Vgl. hierzu Heun/Assion, CR 2015, 812 (818). Kritisch zu Vertragsgestaltungsmöglichkeiten Ensthaler, NJW 2016, 3473 (3474); siehe auch unten Kapitel 3.3.

14 Vgl.: Peschel/Rockstroh, MMR 2014, 571 (572).

15 St. Rspr. seit BVerfG, Urt. v. 15.12.1983, BVer-fGE 65, 1 (43f.).

16 Ensthaler, NJW 2016, 3473 (3475).

17 Ensthaler, NJW 2016, 3473 (3475).

18 Hoeren, MMR 2013, 486.

[19] Boesche/Rataj Zivil- und datenschutzrechtliche Zuordnung von Daten vernetzter Elektrokraftfahrzeuge, S. 42, abrufbar unter http://schaufenster-elektromobilitaet.org/media/media/documents/dokumente_der_begleit__und_wirkungsforschung/EP21_Zivil-_und_datenschutzrechtliche_Zuordnung.pdf .

[20] Heun/Assion, CR 2015, 812 (818).

[21] Heun/Assion, CR 2015, 812 (814).

[22] Grosskopf, IPRB 2011, 259.

[23] Grosskopf, IPRB 2011, 259.

[24] Specht, CR 2016, 288 (292).

[25] Weichert, NJW 2001, 1463 (1476) mit Verweis auf Ladeur, DuD 2000, 12 (18); Kilian, Gedächtnisschrift für Wilhelm Steinmüller, 195 (207 ff.).

[26] Bundesministerium für Verkehr und digitale Infrastruktur, Wir brauchen ein Datengesetz in Deutschland, 20.03.2017, abrufbar unter http://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html.

[27] Vgl. auch die Nachweise in den Kapiteln 2.1.2 und 2.3.

[28] Bundesministerium für Verkehr und digitale Infrastruktur, a. a. O.

[29] Bundesministerium für Verkehr und digitale Infrastruktur, a. a. O.

[30] Vgl. Bundesministerium für Verkehr und digitale Infrastruktur, a. a. O.

[31] Etwa Specht, CR 2016, 288 (296); Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblyté/Wiedemann, GRUR Int. 2016, 914 f.; Grützmacher, CR 2016, 485 (495); Schefzig, K&R 2015, Heft 9, Beihefter 3, 3 (6). Siehe auch Dorner, CR 2014, 617 (626), der insbesondere auf kontinuierlich ansteigende Investitionen in Big Data-Anwendungen verweist, die nicht auf ein Schutzdefizit hindeuteten.

[32] In Bezug auf nicht personenbezogene Daten ausführlich Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, in: Gewerblicher Rechtsschutz und Urheberrecht. Internationaler Teil (GRUR Int), 2016, 989, Kap. VIII.

[33] Dorner, CR 2014, 617 /626).

[34] BVerfG, Urt. v. 15.12.1983, BVerfGE 65, 1 (44). In jüngerer Zeit wird das Urteil jedoch vereinzelt dahingehend ausgelegt, 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 entgegensteht“; so Specht, CR 2016, 288 (293); vgl. auch Specht/Rohmer, PinG 2016, 127.

[35] Siehe oben, Fn. 11.

[36] Kerber, a. a. O. (Fn. 32), Kap. IV.

[37] Zusammenfassend Kerber, a. a. O. (Fn. 32), Kap. VIII.

[38] Hoppen, CR 2015, 802.

[39] In diesem Sinne auch Heymann, CR 2015, 807 (808).

40 Hoppen, CR 2015, 802 (806); ebenso Heymann, CR 2015, 807 (811).

41 Heymann, CR 2015, 807 (809).

42 Heymann, CR 2015, 807 (810f.).

43 Heymann, CR 2015, 807 (810).

44 Sahl, PinG 04.16, 146 (150).

45 Sahl, PinG 04.16, 146 (149); ebenso Becker, GRUR Newsletter 01/2016, 7.

46 Sahl, PinG 04.16, 146 (150).

47 Assion/Mackert, PinG 04.16, 161 (161); Sahl, PinG 04.16, 146 (150).

48 Sahl, PinG 04.16, 146 (149).

49 Siehe auch Becker, GRUR Newsletter 01/2016, 7.

50 Ensthaler, NJW 2016, 3473 (3474).

51 Specht/Rohmer, PinG 04.16, 127 (131).

52 Specht/Rohmer, PinG 04.16, 127 (131).

53 Specht/Rohmer, PinG 04.16, 127 (129).

54 Schwartmann/Hentsch, PinG 04.16, 117 (120).

55 Schwartmann/Hentsch, PinG 04.16, 117 (120f.).

56 Siehe oben, II. 1.6.

57 Zum Spannungsfeld zwischen „Dateneigentum“ und Datenschutz siehe Härting, CR 2016, 646 (648 f.).

58 EuGH, MMR 2005, 29; BGH, MMR 2005, 754.

59 Allgemein siehe Zdanowiecki, in Bräutigam/Kindt (Hrsg.), Digitalisierte Wirtschaft/Industrie 4.0 (2015), S. 19 ff., abrufbar unter: http://www.bdi.eu/Gutachten_Digitalisierte-Wirtschaft_Industrie-40.pdf.

60 Erwägungsgrund 41 der RL 96/9/EG.

61 Vgl. Sahl, PinG 04.16, 146 (148).

62 Siehe dazu Leistner, Der Rechtsschutz von Datenbanken im deutschen und europäischen Recht (2010), S. 343ff.

63 Vgl. Art. 1 Abs. 1 der DatenbankRL 96/9/EG, die die §§ 87a ff. UrhG umsetzen, die Datenbanken „in jeglicher Form“ erfasst.

64 So noch der Vorschlag des Europäischen Parlaments in seiner Stellungnahme vom 23.06.1993 zum Vorschlag für die DatenbankRL, ABlEG Nr. C 194, S. 144.

65 Siehe hierzu Götz, ZD 2014, 563 (564) m.w.Nachw.; Leistner, Der Rechtsschutz von Datenbanken im deutschen und europäischen Recht (2010), S. 343ff.

66 Dorner, CR 2014, 617 (622); Zech, CR 2015, 137 (143).

67 EuGH, Urt. v. 9.11.2004, Az. C-203/02, EuZW 2004, 757 (759 u. 760).

68 Siehe auch Specht, CR 2016, 288 (293 f.); Drexl/Hilty/Desaunettes/Greiner/Kim/Richter/Surblyté/Wiedemann, GRUR Int. 2016, 914 (915).

69 Ensthaler, NJW 2016, 3473 (3474).

70 EuGH, GRUR 2005, 254 (255), Rn. 30f.

71 Assion/Mackert, PinG 04.16, 161 (161f.).

72 Leistner, in Handwörterbuch des Europäischen Privatrechts Band 1, 2009, 298 (301).

73 Leistner, in Handwörterbuch des Europäischen Privatrechts Band 1, 2009, 298 (301).

74 Leistner, in Handwörterbuch des Europäischen Privatrechts Band 1, 2009, 298 (301).

75 Zech, CR 2015, 137 (140).

76 Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen v. 10.01.2017, „Aufbau einer europäischen Datenwirtschaft", COM(2017) 9 final.

77 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über einen Rahmen für den freien Verkehr von nicht personenbezogenen Daten in der Europäischen Union v. 13.09.2017, COM(2017) 495 final.

78 Europäische Kommission, a. a. O. (Fn. 77), S. 2.

79 Vgl. Wiebe, CR 2017, 87.

80 Europäische Kommission, a. a. O. (Fn. 77), S. 8.

81 Europäische Kommission, a. a. O. (Fn. 77), S. 4.

82 Europäische Kommission, a. a. O. (Fn. 77), S. 5.

83 Europäische Kommission, a. a. O. (Fn. 78), S. 2.

84 Ausführlich dazu auch Wiebe, CR 2017, 87 ff..

85 Europäische Kommission, a. a. O. (Fn. 77), S. 14.

86 Siehe bereits oben Kap. 2.1.1.

87 Van Asbroeck/Debussche/César, Data Ownership: A new EU right in data, abrufbar unter https://sites-twobirds.vuture.net/52/1373/uploads/supplementary-paper-on-data-ownership.pdf.

88 Europäische Kommission, a. a. O. (Fn. 71), S. 10.

89 Wiebe, CR 2017, 87 (90). Zur Problematik siehe auch Specht, CR 2016, 288 (295).

90 Art. 3 des Vorschlags der EU-Kommission: Proposal for a Directive of the Parliament and the Council on copyright in the Digital Single Market, COM(2016) 593 final, vom 14.9.2016.

91 Bundesrat Drucksache 535/16, S. 7.

92 Art. 11 COM(2016) 593 final.

93 Entwurf eines Gesetzes zur Angleichung des Urheberrechts an die aktuellen Erfordernisse der Wissensgesellschaft (Urheberrechts-Wissensgesellschafts-Gesetz – UrhWissG-E)

94 Siehe zu den einzelnen Anforderungen: Triaille/de Meeûs d'Argenteuil/de Francquen, Study on the legal framework of text and data mining (TDM), funded by the European Commission, March 2014.

95 Bundesrat Drucksache 535/16, S. 7.

96 Bundestag Drucksache. 1V/270, 38.

97 Raue GRUR 2017, 11 (13).

98 Raue GRUR 2017, 11 (13).

99 Schack ZUM 2016, 266 (269).

100 Gesetzesentwurf der Bundesregierung zur Angleichung des Urheberrechts an die aktuellen Erfordernisse der Wissensgesellschaft, S. 44.

101 Siehe beispielsweise den Fall Authors Guild v. Google, Inc. Court of Appeals for the Second Circuit New York, Entscheidung vom 16. Oktober 2015 – 13-4829-cv.

102 KELLY v. ARRIBA SOFT CORPORATION, United States Court of Appeals, Ninth Circuit, Entscheidung vom 6. Februar 2002 – No. 00-55521.

103 Campbell v. Acuff-Rose Music, Inc., Supreme Court of the United States, 510 U.S. 569, 579, 114 S.Ct. 1164, 127 L.Ed.2d 500, Entscheidung vom 7. März 1994.

104 Das Verlangen der Einwilligung in die unentgeltliche Darstellung von Textausschnitten seitens des eine Internetseite betreibenden Presseverlegers wurde vom Bundeskartellamt nicht als Missbrauch der marktbeherrschenden Stellung eines Suchmaschinenbetreibers gewertet, BKartA Bonn, Beschluss vom 8. September 2015 – B 6 - 126/14.

105 BKartA Bonn, Beschluss vom 8. September 2015 – B 6 - 126/14.

106 OLG München, Urteil vom 14. Juli 2016 – 29 U 953/16.

107 Paal ZRP 2015, 34.

108 Committee on Industry, Research and Energy, Draft Opinion, vom 02.03.2017, abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-592.363%2b01%2bDOC%2bPDF%2bV0%2f%2fEN; Committee on the Internal Market and Consumer Protection, Draft Opinion vom 20.02.2017, abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-599.682%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

109 Vgl. EuGH, Urteil vom 16. Juli 2009 – C-5/08; OLG München, Urteil vom 14. Juli 2016 – 29 U 953/16 –, Rn. 63 f.

110 Wandtke/Bullinger/Bullinger UrhG § 2 Rn. 156, 159.

111 Vgl. Dreier/Schulze/Schulze UrhG § 16 Rn. 4; Wandtke/Bullinger/Heerma UrhG § 16 Rn. 5, 16-17.

112 OLG München, Urteil vom 14. Juli 2016 – 29 U 953/16 –, Rn. 72, mit Verweis auf EuGH, Beschluss vom 21. Oktober 2014 – C-348/13 –, BGH, Urteil vom 9. Juli 2015 – I ZR 46/12.

113 Entwurf eines Gesetzes zur Angleichung des Urheberrechts an die aktuellen Erfordernisse der Wissensgesellschaft (Urheberrechts-Wissensgesellschafts-Gesetz – UrhWissG-E)

114 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über das Urheberrecht im digitalen Binnenmarkt vom 14.09.2016, COM(2016) 593 final.

115 Zur Abgrenzung von Werken mit geringer Schöpfungshöhe siehe beispielsweise Bisges GRUR 2015, 540.

116 Dreier/Schulze/Dreier UrhG § 4 Rn. 17

117 Dreier/Schulze/Dreier UrhG § 4 Rn. 19

118 Der Begriff „sui generis“ steht für ein Recht eigener Art, da es sich bei dem Datenbankherstellerrecht nicht um ein Urheberrecht handelt. Der Schutz ist unabhängig vom urheberrechtlichen Schutz für Datenbankwerke i. S. d. § 4 UrhG.

119 Auch bei Annahme eines Datenbankwerkes nach § 4 UrhG kann der Schutz des Datenbankherstellers grundsätzlich daneben bestehen (Dreier/Schulze, Teil 2. Verwandte Schutzrechte, Abschnitt 6. Schutz des Datenbankherstellers, Vorbemerkung, Rn. 8).

120 Dreier/Schulze/Dreier UrhG § 87a Rn. 7.

121 OLG Köln MMR 2007, 443.

122 Wandtke/Bullinger/Thum/Hermes UrhG § 87a Rn. 19.

123 OLG Köln MMR 2007, 443.

124 A. A. Dreier/Schulze/Dreier UrhG § 87a Rn. 7: Allein der informationelle Mehrwertdienst der Datenbearbeitung solle geschützt werden.

125 Erwägungsgrund 40 der Datenbankrichtlinie RL 96/9/EG.

126 EuGH, Urteil vom 9. 11. 2004 - C-203/02.

127 Dreier/Schulze/Dreier UrhG § 87a Rn. 13

128 EuGH, Urteil vom 9. 11. 2004 - C-203/02.

128 BeckOK UrhR/Koch UrhG § 87a Rn. 21.

130 Wandtke/Bullinger/Thum/Hermes UrhG § 87a Rn. 5.

131 Erwägungsgrund 46 RL 96/9/EG.

132 OLG Köln MMR 2007, 443.

133 BT-Drucks. 17/11470, 8.

134 Vgl. BT-Drucks. 17/11470, 7.

135 Wandtke/Bullinger/Jani UrhG § 87f Rn. 12; Bundestag-Drucksache 17/11470, 6.

136 Dreier/Schulze/Dreier UrhG § 87f Rn. 3.

137 OLG München, Urteil vom 14. Juli 2016 – 29 U 953/16.

138 Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über das Urheberrecht im digitalen Binnenmarkt vom 14.09.2016, COM(2016) 593 final.

139 vgl. BVerfG, Beschluss vom 14. März 2006 – 1 BvR 2087/03, 1 BvR 2111/03 –, BVerfGE 115, 205-259.

140 Fischer, StGB, 63. Aufl. 2016, § 202a RN. 7a; Schönke/Schröder/Eisele/Lenckner StGB § 202a Rn. 9; MüKoStGB/Graf StGB § 202a Rn. 19.

141 Bundestag Drucksache 16/3656, S. 9, 10.

142 MüKoStGB/Graf StGB § 202a Rn. 26.