

Bei komplementären Datenkombinationen werden unterschiedliche Datenarten oder -werte miteinander kombiniert. Das können zum Beispiel Standortdaten in einer Sammlung und Angaben über alltägliche Vorlieben von Nutzern in einer anderen Sammlung sein. In diesem Fall können die Daten in einen neuen Zusammenhang gebracht werden. Zwar wird dies regelmäßig auch zu einer quantitativen Vergrößerung des Datenpools führen, die jedoch hinter dem prägenden Wettbewerbsfaktor des Zugangs zu Daten zurücktritt.

6. Zusammenfassung und Ausblick

Daten können an unterschiedlichen Anknüpfungspunkten im Kartellrecht eine Rolle spielen. Auf der Stufe der Marktdefinition bereits können sie selbstständiger Gegenstand von Angebot und Nachfrage sein oder im Zusammenhang mit Plattformgeschäftsmodellen die Marktverhältnisse näher beschreiben. Soweit ein Unternehmen über einen ex-

klusiven Datensatz verfügt, insbesondere bei sachbezogene Daten oder bestimmten Herstellerdaten, kann dieser Umstand eine marktmächtige Position begründen. Ob dies bei aggregierten Big-Data-Beständen ebenso der Fall sein kann, hängt maßgeblich von einer Beurteilung der im Einzelfall wirkenden Wettbewerbsphänomene zugunsten oder zulasten des Wettbewerbs ab. Des Weiteren wird das Verhältnis zwischen Kartellrecht und nicht-kartellrechtlichen Vorschriften, insbesondere mit verbraucher-schützenden Intentionen, zu klären sein. Neben der Anwendbarkeit dieser jeweiligen Vorschriften wird es auch um Probleme bei der Bewertung des jeweiligen Gegenwertes gehen. Schließlich werden Kooperationen im Zusammenhang mit Plattformen oder IT-Outsourcing immer mehr in den Fokus der kartellrechtlichen Bewertung rücken. Begleitet wird dies von den gesetzgeberischen Entwicklungen der 9. GWB-Novelle.

Ass. jur. Robert Hieke*

Big Data

Zum gesetzlichen Schutz und der rechtlichen Zuordnung von Daten

I. Einleitung

Der Umgang mit – und diesem folgend die juristische Diskussion über – maschinell generierte Daten (im Folgenden vereinfacht Maschinen-Daten genannt) nimmt zu.¹ In den Vordergrund treten dabei insbesondere Fragen, die sich auf den Schutz und die Verkehrsfähigkeit des Wirtschaftsgutes „Daten“² beziehen. Derartige (oftmals auch unter dem Stichwort „Big Data“ diskutierte)³ Fragestellungen werden nicht nur bei der Nutzung komplexer Fertigungsmaschinen in „Industrie 4.0“⁴ oder „additiver Fertigungsverfahren“⁵ relevant, sondern auch bei der Verarbeitung von Daten beim Cloud Computing,⁶ im Verkehrswesen (smart cars)⁷ oder in der Immobilienwirtschaft (smart housing).⁸ Ebenso ist im privaten Bereich eine Zunahme von datengenerierenden Alltagsgegenständen, wie z. B. Smart TV⁹ oder Smartphone¹⁰ zu verzeichnen.

Der Beitrag setzt sich mit dem rechtlichen Schutz von Maschinen-Daten auseinander und bedingt damit zugleich eine Diskussion zur güterrechtlichen Zuordnung von Daten zugunsten eines Berechtigten.

Zur Beantwortung der Frage, wie Daten rechtlich geschützt sind, wird zunächst kurz aufgezeigt, welche mit der Dateneigenschaft in Verbindung stehenden Rechtsobjekte Bezugspunkt des rechtlichen Schutzes sein können (II.). Sodann wird ein Überblick gegeben, inwieweit diese Rechtsobjekte von der Rechtsordnung einem Schutz unterstellt sind (III.).

II. Relevante Rechtsobjekte

Da Daten nicht eigenständig existieren können, benötigen sie einen Datenträger.¹¹ Der eigentliche (insbesondere auch wirtschaftliche) Wert der Daten kann sich zunächst aus der

Bedeutung der in den Daten selbst enthaltenen Informationen ergeben. Oftmals folgt aber der Wert der Daten nicht aus den Daten selbst, sondern vielmehr erst aus den sich ergebenden Informationen bzw. Inhalten, wenn die Daten ihrer Bestimmung nach ausgeführt werden.¹² Auch kann sich ein besonderer Wert in Bezug auf Daten dadurch ergeben, dass

* Der Aufsatz basiert auf einem im Oktober 2015 in Chemnitz im Rahmen eines Workshops des Forschungsprojektes S-CPS „Ressourcen-Cockpit für Sozio-Cyber-Physische Systeme“ gehaltenen Vortrag des Verfassers. Mehr über den Autor erfahren Sie auf Seite III.

- 1 Insoweit wird schon von Daten als dem neuen „Öl“ oder „Rohstoff“ der Zukunft gesprochen, vgl. *Schefzig*, K&R, Beihefter 3/2015, 3, 3 sowie *Dorner*, CR 2014, 617, 618 m. w. N.
- 2 Zur Einordnung der Daten als Wirtschaftsgut vgl. *Zech*, CR 2015, 137, 138 m. w. N.
- 3 „Unter ‚Big Data‘ wird das Prinzip des Einsatzes großer und vielfältiger Datenmengen verstanden, die typischerweise von miteinander vernetzten Maschinen generiert – und regelmäßig ohne konkret vorformulierte Erwartungshaltung an das Ergebnis – in Echtzeit analysiert werden“, s. *Dorner*, CR 2015, 617, 617 m. w. N.
- 4 Komplette Produktionsprozesse werden mittlerweile durch die Kommunikations- und Interaktionsfähigkeit der zur Produktion eingesetzten Maschinen mitbeeinflusst, s. *Heun/Assion*, CR 2015, 812, 812.
- 5 *Ensthaler*, InTeR 2015, 38 ff.; *Ensthaler/Müller, A.-K.*, in: VDI Handlungsfelder, additive Handlungsfelder April 2016, S. 38 f.; *Gebhardt*, RAW 2016, 41 ff.
- 6 Vgl. hierzu etwa *Heymann*, CR, 2015, 807, 807 ff.
- 7 Vgl. hierzu etwa *Robnagel*, SVR, 2014, 281, 281 ff.
- 8 *Zech*, CR 2015, 137, 137 m. w. N.
- 9 Im Jahr 2015 verfügten ca. 20 % der deutschen TV-Haushalte über mindestens ein direkt internetfähiges TV-Gerät, s. Die Medienanstalten, Digitalisierungsbericht 2015, S. 49, abrufbar unter http://www.die-medienanstalten.de/fileadmin/Download/Publikationen/Digitalisierungsbericht2015/Digitalisierungsbericht_2015_deutsch.pdf, (zuletzt abgerufen am 12.8.2016).
- 10 44 Millionen Deutsche nutzen ein Smartphone, Pressemitteilung von Bitkom vom 25.3.2015, abrufbar unter <https://www.bitkom.org/Presse/Presseinformation/44-Millionen-Deutsche-nutzen-ein-Smartphone.html>, zuletzt abgerufen am 12.8.2016.
- 11 *Schefzig*, K&R, Beihefter 3/2015, 3, 3; *Zech*, CR 2015, 137, 138.
- 12 *Schefzig*, K&R, Beihefter 3/2015, 3, 3.

sie systematisch dargestellt werden und aufgrund dieser systematisierten Darstellung ein einfaches Auffinden der Daten und damit auch Zugreifen auf die Daten ermöglicht wird. Demnach kommen als insoweit relevante Bezugspunkte (mindestens)¹³ die folgenden vier Rechtsobjekte in Betracht: erstens die Daten selbst, zweitens der Datenträger, drittens die systematisierte Darstellung der Daten (also die Datenbank) und viertens der Inhalt der Daten.¹⁴

1. Daten selbst

Die Daten selbst bzw. als solche lassen sich definieren als (an sich interpretationsfreie) Zeichengebilde, die auf einem Datenträger niedergelegt sind und durch Maschinen bzw. Informationstechnik gelesen, verarbeitet und veranschaulicht werden können (syntaktische Ebene).¹⁵ Durch diese Veranschaulichung wird der Rezipient in die Lage versetzt, aus dem Datum bzw. den Daten Informationen abzuleiten.¹⁶

2. Datenträger

Der Datenträger ist das Speichermedium, auf dem die Daten gespeichert sind (z. B. CD, Festplatte, USB-Stick sowie sonstige zur Speicherung von Daten geeignete lokale oder – wie beim sog. Cloud-Computing – aus der Ferne abrufbare Geräte).¹⁷ Daten sind immer an ein körperlich greifbares Speichermedium gebunden, wenngleich die Bestimmung des konkreten Datenträgers aufgrund der technischen Entwicklung zunehmend komplexer und schwieriger wird.¹⁸ Dies gilt namentlich für Daten in Netzwerk- sowie Cloud-Umgebungen.¹⁹ Weiter erschwerend kommt hinzu, dass es sich bei einer „Datenübertragung“ eigentlich um einen Kopiervorgang handelt, so dass ein Datum (als eine mit dem Original identische Kopie) gleichzeitig auf verschiedenen Datenträgern gespeichert sein kann.²⁰

3. Datenbanken

Auch die systematische Darstellung der Daten, also die Datenbank, kann Bezugspunkt des von der Rechtsordnung gewährten Schutzes sein. Der Schutz folgt dann letztlich entweder aus der Art und Weise der konkreten systematischen Darstellung oder aus der Investition in die systematische Darstellung.

4. Dateninhalt

Der Inhalt der Daten betrifft ihre Bedeutung (semantische Ebene).²¹ Wie bereits erwähnt, ergibt sich der eigentliche Wert der Daten in der Regel nicht aus den Daten selbst, sondern oftmals erst aus den sich ergebenden Informationen bzw. Inhalten, wenn die Daten bestimmungsgemäß ausgeführt werden. So ergibt sich etwa bei Big Data-Anwendungen der besondere Wert nicht bereits aus den – oftmals als Nebenprodukt – erfassten Daten, sondern erst aus der nachfolgenden Analyse dieser erfassten Daten.²² Weitere, einen besonderen Wert generierende, Ergebnisse des bestimmungsgemäßen Ausführens von Daten können z. B. Computerprogramme oder Musikstücke sein (vgl. § 2 Abs. 1 Nr. 1 und 2 UrhG).²³

III. Gesetzlicher Schutz und Zuordnung von Daten

Neben einem aus vertraglichen Vereinbarungen resultierenden Schutz von Maschinen-Daten, kann sich ein zivilrechtlicher Schutz von Daten insbesondere aus dem Sachen- und dem Deliktsrecht ergeben. Darüber hinaus existieren im Wettbewerbs-, im Straf-, im Urheber- sowie im Datenschutzrecht im Zusammenhang mit der Dateneigenschaft stehende Schutzvorschriften.

tieren im Wettbewerbs-, im Straf-, im Urheber- sowie im Datenschutzrecht im Zusammenhang mit der Dateneigenschaft stehende Schutzvorschriften.

1. Sachenrechtlicher Schutz und Zuordnung

Das Sachenrecht (§§ 854 - 1296 BGB) regelt die Vermögenszuordnung von Sachen.²⁴ Daher können Eigentum, beschränkt dingliche Rechte sowie der Besitz grundsätzlich²⁵ nur an Sachen bestehen.²⁶ Folglich kann sich auch ein etwaiger an Eigentum, beschränkt dingliche Rechte oder Besitz anknüpfender rechtlicher Schutz nur aus der Sacheigenschaft ergeben.

Nach § 90 BGB sind Sachen körperliche Gegenstände. Körperlich sind die Gegenstände dann, wenn sie greifbar oder zumindest sinnlich wahrnehmbar und beherrschbar sind.²⁷ Das Erfordernis der Beherrschbarkeit des Gegenstandes ist im Sinne einer räumlichen Abgrenzung des Gegenstandes im Raum zu verstehen, wobei sich diese räumliche Abgrenztheit nicht nur aus der eigenen körperlichen Begrenzung des Gegenstandes, sondern auch aus dem körperlichen Zusammenhalt durch seine Fassung in einem Behältnis bzw. seiner Fixierung durch ein technisches Hilfsmittel ergeben kann.²⁸ Daher sind Daten als solche mangels der (den Sachbegriff kennzeichnenden) abgrenzbaren Körperlichkeit keine Sachen.²⁹

a) Mittelbarer sachenrechtlicher Schutz

Die Sacheigenschaft kommt aber dem Datenträger zu, auf dem das Datum oder die Daten gespeichert sind.³⁰ Insoweit kann der Datenträger als das die Daten als solche fassende Behältnis bzw. fixierende technische Hilfsmittel angesehen werden. Zu beachten ist dabei, dass nach überwiegender Auffassung nur der Datenträger eine Sache im Sinne von

13 Nicht eingegangen wird hier etwa auf die Frage, inwieweit sich zusätzliche Pflichten aus der Konnektivität von miteinander oder mit der Außenwelt (über Daten) kommunizierenden Gegenständen – etwa nach dem TKG – ergeben, vgl. hierzu *Heun/Assion*, CR 2015, 812, 815 f.

14 *Schefzig*, K&R, Beihefter 3/2015, 3, 3.

15 *Zech*, CR 2015, 137, 138 m. w. N.

16 *Specht*, CR 2016, 288, 290 m. w. N.

17 *Schefzig*, K&R, Beihefter 3/2015, 3, 3.

18 *Zech*, CR 2015, 137, 138; *Lehmann/Giedke*, CR 2013, 608, 611 ff.

19 Vgl. hierzu *Hoppen*, CR 2015, 802, 803 f.; Jedes in der Cloud bereitgestellte Datum befindet sich letztlich auf einer realen Hardwareressource bzw. einem realen Speicherplatz, wobei allerdings insbesondere die Virtualisierungstechnik ermöglicht, dass die in der Cloud gespeicherten Daten auf mehreren Servern – aber immerhin zumindest für den jeweiligen Cloud-Betreiber nachvollziehbar – verteilt liegen können, vgl. hierzu ausführlich *Lehmann/Giedke*, CR 2013, 608, 611 ff.

20 *Hoppen*, CR 2015, 802, 803.

21 *Schefzig*, K&R, Beihefter 3/2015, 3, 3.

22 *Zech*, CR 2015, 137, 138.

23 *Schefzig*, K&R, Beihefter 3/2015, 3, 3.

24 *Wolf/Wellenhofer*, Sachenrecht, 24. Aufl. 2008, § 1 Rn. 1.

25 Keine Sachen sind Tiere (§ 90a S. 1 BGB). Auf sie sind jedoch, soweit nicht ein anderes bestimmt, die für Sachen geltenden Vorschriften entsprechend anwendbar (§ 90a S. 3 BGB).

26 Bezugspunkt des Eigentums (vgl. § 903 BGB), des Besitzes (vgl. § 854 BGB) sowie von beschränkt dinglichen Rechten (vgl. etwa §§ 1030, 1018, 1090, 1093, 1204, 1113, 1191, 1105, 1094 BGB) ist jeweils die Sache im Sinne des BGB.

27 *Stresemann*, in: Münchener Kommentar zum BGB, 7. Aufl. 2015, § 90 Rn. 1.

28 *Fritzsche*, in: Beck'scher Online-Kommentar BGB, Bamberger/Roth, 37. Edition, Stand: 1.8.2015, § 90 Rn. 7 m. w. N.; *Stresemann*, in: Münchener Kommentar zum BGB (Fn. 27), § 90 Rn. 8.

29 *Stresemann*, in: Münchener Kommentar zum BGB (Fn. 27), § 90 Rn. 25.

30 *Stresemann*, in: Münchener Kommentar zum BGB (Fn. 27), § 90 Rn. 25.

§ 90 BGB ist, während die auf ihm gespeicherten Daten nicht körperliche Gegenstände bleiben.³¹ Nach § 903 S. 1 BGB kann der Eigentümer einer Sache, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen,³² mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen. Der Eigentümer des Datenträgers kann also grundsätzlich (positiv) über den Datenträger und damit mittelbar auch über die auf ihm gespeicherten Daten nach Belieben verfahren sowie den Datenträger und damit auch mittelbar die auf ihm gespeicherten Daten nutzen. Zudem hat der Eigentümer (negativ) grundsätzlich das Recht, andere von der Einwirkung auf den Datenträger und damit auch mittelbar das Recht, andere von der Einwirkung auf die (auf dem Datenträger gespeicherten) Daten auszuschließen.

Mithin stehen dem Eigentümer des Datenträgers alle aus dem Eigentum folgenden Schutzrechte zu, die sich mittelbar (bzw. „reflexartig“)³³ auch auf die auf dem Datenträger gespeicherten Daten beziehen. Gleiches gilt hinsichtlich des Besitzers des Datenträgers in Bezug auf den aus dem Besitz folgenden Schutz. Zu denken ist aus sachenrechtlicher Sicht etwa an Ansprüche auf Herausgabe des Datenträgers, die aus dem Eigentum (§ 985 BGB) oder aus dem Besitz (§ 861 BGB) folgen, sowie an Ansprüche auf Beseitigung und Unterlassung (z. B. § 1004, § 862 BGB).

b) Mittelbare sachenrechtliche Zuordnung

Das Sachenrecht gewährt über das Eigentum am Datenträger aber nicht nur einen mittelbaren Schutz der Daten, sondern trifft damit zugleich eine mittelbare Zuordnung der Daten zugunsten desjenigen Eigentümers eines Datenträgers, auf dem bestimmte Daten erstmalig gespeichert werden. Denn dieser Eigentümer, der gem. § 903 S. 1 BGB – soweit nicht das Gesetz oder Rechte Dritter entgegenstehen – mit dem Datenträger nach Belieben verfahren und andere von der Einwirkung auf den Datenträger ausschließen kann, ist damit allein in der Position auf die (auf seinem Datenträger gespeicherten) Daten zuzugreifen, sie zu nutzen und über sie zu entscheiden.³⁴ Das Eigentum am Datenträger vermittelt somit praktisch die Möglichkeit, die auf dem Datenträger gespeicherten Daten zu nutzen, also etwa die in den Daten enthaltenen bzw. die durch das bestimmungsgemäße Ausführen der Daten entstehenden Informationen zu verwerten. Entsprechendes gilt hinsichtlich des (berechtigten) Besitzes am Datenträger. Mangels Sacheigenschaft der Daten muss jedoch derjenige, der Daten erhebt, dafür Sorge tragen, dass er die Daten auf einem in seinem Eigentum oder in seinem (berechtigten) Besitz befindlichen Datenträger speichert oder, sofern er einem Dritten den Zugriff auf die Daten gewährt, darauf achten, dass er sich etwaige Rechte an den Daten oder an dem Datenträger, an dem die Daten übertragen werden, vertraglich sichert.

aa) Daten als Nutzungen

Zum Teil wird hierzu vertreten, dass aufgenommene Daten als Nutzungen (§§ 99 f. BGB) anderer Sachen einzuordnen seien.³⁵ Darüber hinaus wird zudem vereinzelt vertreten, dass über die §§ 953, 988, 818 BGB dem Eigentümer der anderen Sache die Nutzungen zuzuweisen seien, wobei die andere Sache je nach Fallgestaltung entweder der Aufnahmegegenstand oder das Aufnahmegerät sein könne.³⁶ Hierzu ist zunächst festzuhalten, dass es für die hier in Frage stehende Zuordnung von Daten zu einem Rechtsträger im Ergebnis irrelevant ist, ob Daten als Nutzungen im Sinne

von § 99 f. BGB – sei es als unmittelbare Sachfrüchte (§ 99 Abs. 1 BGB),³⁷ als unmittelbare Rechtsfrüchte (§ 99 Abs. 2 BGB),³⁸ als mittelbare Sach- bzw. Rechtsfrüchte (§ 99 Abs. 3 BGB)³⁹ oder als Gebrauchsvorteile (§ 100 BGB)⁴⁰ – einzuordnen sind, da die §§ 99 f. BGB selbst keine Rechtsfolgen anordnen. Die Rechtsfolgen, die sich aus einer Qualifikation als Nutzungen (§ 99 f. BGB) ergeben, werden erst durch andere Vorschriften angeordnet.⁴¹ Für die eigentumsrechtliche Zuordnung von Nutzungen sind insoweit die §§ 953 bis 957 BGB sowie die §§ 987 bis 993 BGB maßgeblich.

Die §§ 953 bis 957 BGB sind aber bereits deshalb nicht anwendbar, weil diese regeln, wer das Eigentum an Erzeugnissen oder Bestandteilen erwirbt. Damit setzen die §§ 953

31 Vgl. *Stresemann*, in: Münchener Kommentar zum BGB (Fn. 27), § 90 Rn. 25 sowie *Fritzsche*, in: Beck'scher Online-Kommentar BGB (Fn. 28), § 90 Rn. 26 jeweils m. w. N. auch zur Gegenmeinung.

32 Eigentumsbeschränkende Regelungen enthält in Bezug auf Daten vor allem das BDSG, insbesondere wenn personenbezogene Daten (§ 3 Abs. 1 BDSG) erhoben und auf dem Datenträger gespeichert werden. Daneben können sich Eigentumsbeschränkungen durch Rechte Dritter aus dinglichen Rechten Dritter an dem Datenträger selbst (z. B. aus einem Pfandrecht an dem Datenträger) sowie aus Ausschließkeitsrechten Dritter ergeben (z. B. das Sacheigentum am Datenträger kollidiert mit Urheberrechten eines Musikers oder Programmierers). Zudem kann sich eine (die Eigentümerbefugnis beschränkende) Wirkung aus schuldrechtlichen Vereinbarungen ergeben, so etwa, wenn der Eigentümer des Datenträgers mit einem Dritten vereinbart, dass die auf dem Datenträger befindlichen Daten von dem Dritten genutzt werden können (vgl. auch §§ 986, 1004 Abs. 2 BGB).

33 So *Zech*, CR 2015, 137, 142.

34 Zu Kfz-Daten vgl. *Robnagel*, SVR 2014, 281, 282.

35 Vgl. etwa *Zech*, CR 2015, 137, 142, der in der Aufnahme von Daten und deren Weiterverwendung einen Gebrauchsvorteil im Sinn von § 100 BGB sieht.

36 Vgl. etwa *Grosskopf*, IPRB 2011, 259, 260, der Daten als Früchte (§ 99 BGB) ansieht und sie über die §§ 953 ff. BGB dem Eigentümer der anderen Sache zuweist.

37 Aufgenommene Daten werden aber mangels „Natürlichkeit“ kaum als Erzeugnisse im Sinn von § 99 Abs. 1 Alt. 1 BGB weder des Aufnahmegegerätes noch des Aufnahmegegenstandes zu qualifizieren sein (zur Einordnung von Erzeugnissen als „natürliche“ Produkte einer Sache, vgl. etwa *Vieweg*, in: Herberger/Martinek/Rübmann u. a., jurisPK-BGB, 7. Aufl. 2014, § 99 Rn. 5 sowie *Stresemann*, in: Münchener Kommentar zum BGB (Fn. 27), § 99 Rn. 1). Auch stellen Daten (mit der überwiegenden Auffassung) keine bestimmungsgemäße Ausbeute im Sinn von § 99 Abs. 1 Alt. 2 BGB des Aufnahmegegenstandes dar, da die Ausbeute als solche nach überwiegender Auffassung aus der Sachsubstanz der Muttersache zu entnehmen ist und damit Sachqualität (§ 90 BGB) aufweisen muss (vgl. hierzu *Vieweg*, in: Herberger/Martinek/Rübmann u. a., jurisPK-BGB (Fn. 37), § 99 Rn. 7 m. w. N.; zweifelnd *Fritzsche*, in: Beck'scher Online-Kommentar BGB (Fn. 28), § 90 Rn. 7).

38 Die Einordnung von Daten als unmittelbare Rechtsfrüchte (§ 99 Abs. 2 BGB) des Eigentumsrechts bezüglich des Aufnahmegegenstandes wird zu verneinen sein, da die Erträge des Eigentumsrechts selbst nicht unter Abs. 2, sondern unter Abs. 1 des § 99 BGB fallen (vgl. *Vieweg*, in: Herberger/Martinek/Rübmann u. a., jurisPK-BGB (Fn. 37), § 99 Rn. 9 m. w. N.).

39 Ebenso wenig werden Daten in aller Regel mittelbare Sach- oder Rechtsfrüchte im Sinn von § 99 Abs. 3 BGB des Aufnahmegegerätes oder des Aufnahmegegenstandes bzw. eines Rechtes hieran sein, da in aller Regel die aufgenommenen Daten nicht als Gegenleistung für die entgeltliche Überlassung zur Nutzung oder zum Gebrauch durch den Berechtigten an andere gewährt werden (vgl. *Vieweg*, in: Herberger/Martinek/Rübmann u. a., jurisPK-BGB (Fn. 37), § 99 Rn. 12).

40 Da Gebrauchsvorteile selbst keine Sachqualität aufzuweisen müssen (vgl. *Vieweg*, in: Herberger/Martinek/Rübmann u. a., jurisPK-BGB (Fn. 37), § 100 Rn. 6), werden Daten am ehesten als Gebrauchsvorteile im Sinn von § 100 BGB des Aufnahmegegerätes, aber nicht des Aufnahmegegenstandes („[d]er Vorteil muss sich gerade aus dem Gebrauch der Sache oder des Rechts ergeben“, s. *Fritzsche*, in: Beck'scher Online-Kommentar BGB (Fn. 28), § 100 Rn. 5) eingeordnet werden können (so auch *Zech*, CR 2015, 137, 142 sowie *Assion*, CR 2016, 84, 85). Ob der Eigentümer oder Besitzer des Aufnahmegegenstandes die Aufnahme verhindern kann, hängt von seinen Rechtspositionen hinsichtlich des Aufnahmegegenstandes ab.

41 *Vieweg*, in: Herberger/Martinek/Rübmann u. a., jurisPK-BGB (Fn. 37), § 99 Rn. 16 sowie § 100 Rn. 15 jeweils mit Aufzählung von Beispielen.

bis 957 BGB aber gerade die Sacheigenschaft von Erzeugnissen oder Bestandteilen voraus, da nur Sachen Bezugspunkt des Eigentums sein können (vgl. § 903 BGB).⁴² Selbst bei einer Qualifizierung von Daten als Erzeugnisse oder Bestandteile wären also §§ 953 bis 957 BGB mangels der Sacheigenschaft von Daten nicht anwendbar, so dass sich eine Zuweisung der Daten (als Nutzungen des Aufnahmegerätes) allenfalls aus den §§ 987-993 BGB ergeben könnten.

Die §§ 987 ff. BGB regeln die sog. Folgeansprüche der vindikation; setzen also das Verhältnis zwischen dem Eigentümer und dem unrechtmäßigen Besitzer voraus und bezwecken im Ergebnis den Schutz des redlichen und unverklagten unrechtmäßigen Besitzers vor der Inanspruchnahme nach Bereicherungs- und Deliktsrecht.⁴³ Sofern Daten als Nutzungen (§ 100 BGB) – also nach hier vertretener Auffassung am ehesten als Gebrauchsvorteile des Aufnahmegerätes⁴⁴ – angesehen werden, wird damit ebenfalls keine über die gem. § 903 BGB mittelbare bzw. reflexartige Zuordnung der Daten über das Datenträgereigentum hinausgehende Zuweisung der Daten erreicht. Denn die §§ 987 f. BGB ordnen insoweit lediglich an, dass der unrechtmäßige Besitzer des Aufnahmegerätes die Daten an den Eigentümer des Aufnahmegerätes herauszugeben hat. Da das Aufnahmegerät aber nichts anderes ist als der Datenträger, auf dem die Daten erstmals gespeichert wurden, bleibt es bei der allenfalls mittelbaren (bzw. reflexartigen) Zuordnung der Daten zum Eigentümer (bzw. berechtigten Besitzer) des Datenträgers.

bb) Eigentumserwerb durch Speicherung

Ferner wird vereinzelt vertreten, dass das elektromagnetische Aufzeichnen eine Verarbeitung des Datenträgers darstellen würde, so dass der Speichernde bei der Abspeicherung wertvoller Daten gem. § 950 Abs. 1 BGB das Eigentum am Datenträger erwerben könne.⁴⁵

§ 950 Abs. 1 BGB setzt jedoch unter anderem voraus, dass durch Verarbeitung oder Umbildung eines oder mehrerer Stoffe eine neue bewegliche Sache hergestellt wird. Insofern ist schon fraglich, ob Daten überhaupt „Stoffe“ im Sinne des § 950 Abs. 1 BGB sind.⁴⁶ Zudem muss nach dem ausdrücklichen Wortlaut des § 950 Abs. 1 S. 1 BGB das Ergebnis der Verarbeitung bzw. der Umbildung „eine neue bewegliche Sache“ sein. Die Neuheit der Sache bestimmt sich wiederum nach der Verkehrsanschauung unter Berücksichtigung wirtschaftlicher Gesichtspunkte.⁴⁷ Danach können Anhaltspunkte für das Vorliegen einer neuen Sache eine erhebliche Veränderung der Sachsubstanz, die Dauerhaftigkeit der Veränderung oder ein neues äußeres Erscheinungsbild sein.⁴⁸ Daneben kann mit der Verkehrsanschauung auch dann von einer neuen Sache ausgegangen werden, wenn das Ergebnis der Verarbeitung eine eigenständige bzw. eine gegenüber den einzelnen verarbeiteten Sachen weitergehende Funktion hat, etwa dann, wenn „sich durch die Verarbeitung der wesentliche wirtschaftliche Verwendungszweck“ ändert.⁴⁹ Entscheidend ist mithin, „dass zwischen Ausgangsstoff und Verarbeitungsprodukt keine Identität mehr besteht“.⁵⁰

Gemessen hieran werden Datenträger durch die Speicherung von Daten nicht zu einer neuen Sache verarbeitet. Denn ein Datenträger erfährt durch das Speichern von Daten als solches keine substantielle Veränderung. Selbst wenn das Speichern zu einer physikalischen Veränderung „innerhalb“ des Datenträgers führt, ist diese Veränderung jedoch Voraussetzung und Kernstück seiner bestimmungs-

gemäßen Benutzung.⁵¹ Für einen Datenträger ist es typisch, dass er zum einmaligen oder wiederholten Speichern sowie zum Löschen von Daten verwendet werden kann. Zu einer anderen Sache kann er durch Speichern von Daten deshalb ausnahmsweise nur dann werden, wenn er dadurch seine typische Funktion verändert.⁵² Mithin ist festzuhalten, dass in dem Speichern von Daten grundsätzlich keine zu einem Eigentumserwerb nach § 950 Abs. 1 BGB führende Verarbeitung des Datenträgers erblickt werden kann. Denn das Speichern von Daten auf einem Datenträger stellt die bestimmungsgemäße Nutzung eines Datenträgers dar und führt nicht dazu, dass zwischen dem Datenträger ohne Daten (Ausgangsstoff) und dem Datenträger mit Daten (Verarbeitungsprodukt) keine Identität mehr besteht.

2. Deliktsrechtlicher Schutz und Zuordnung

Das Deliktsrecht zielt auf die Wiedergutmachung eines Schadens, indem es eine Schadensersatzpflicht anordnet, wenn unerlaubte Eingriffe in einen fremden Rechtskreis unter den Voraussetzungen bestimmter Tatbestände vorliegen.⁵³ Auch in Bezug auf Maschinen-Daten kann bzw. können neben einigen Sondertatbeständen (z. B. Wettbewerbsverstöße im Sinne des UWG⁵⁴) einer oder mehrere der drei im Gesetz enthaltenen Grundtatbestände des Deliktsrechts, nämlich § 823 Abs. 1, § 823 Abs. 2 oder § 826 BGB erfüllt sein.⁵⁵

42 So auch Zech, CR 2015, 137, 142 sowie Schefzig, K&R, Beihefter 3/2015, 3, 4.

43 Fritzsche, in: Beck'scher Online-Kommentar BGB (Fn. 28), § 987 Rn. 1 f.

44 Vgl. oben Fn. 40.

45 So Zech, CR 2015, 137, 142; vgl. auch LAG Chemnitz, 17.1.2007 – 2 Sa 808/05, MMR 2008, 416, 417 sowie OLG Karlsruhe, 6.10.1986 – 6 U 160/86, BeckRS 2014, 17343: Das Aufspielen eines Computerprogramms auf einen Datenträger stelle einen Verarbeitungsvorgang im Sinn des § 950 BGB dar; a. A. Redeker, CR 2008, 554, 554 ff.

46 Vgl. auch Hoeren, MMR 2013, 468, 490.

47 Füller, in: Münchener Kommentar zum BGB, 6. Aufl. 2013, § 950 Rn. 7 m. w. N.

48 BGH, 10.7.2015 – V ZR 206/14, GRUR 2016, 109, 110 Rn. 17 m. w. N.

49 BGH, 10.7.2015 – V ZR 206/14, GRUR 2016, 109, 110 Rn. 17 m. w. N.

50 BGH, 10.7.2015 – V ZR 206/14, GRUR 2016, 109, 110 Rn. 17.

51 Vgl. BGH, 10.7.2015 – V ZR 206/14, GRUR 2016, 109, 110 Rn. 19: „Ohne seine veränderbare Magnetbeschichtung und die Veränderung dieser Magnetschicht beim Aufnehmen könnte ein Tonband nicht als Speichermedium für Tondokumente verwendet werden. Es wäre ein funktionsloses Kunststoffband.“; a. A. Götting, NJW 2016, 321, 321, der in dem Abstellen auf die „typische Funktion“ ein untaugliches Differenzierungskriterium erblickt, aber in seiner Begründung verkennt, dass die Berechtigung an den aufgenommenen Inhalten (der Daten) von der eigentumsrechtlichen Berechtigung an dem Speichermedium zu trennen ist.

52 Vgl. BGH, 10.7.2015 – V ZR 206/14, GRUR 2016, 109, 110 Rn. 19: „Das wäre etwa dann der Fall, wenn eine unbespielte Musikkassette in einem Musikverlag mit Musiktiteln oder einem Hörbuch bespielt wird, die in dieser Form vertrieben werden sollen. Dann wird [...] aus einem Speichermedium ein Instrument zum Vertrieb der Musiktitel oder des Hörbuchs.“

53 Brox/Walker, Besonderes Schuldrecht, 33. Aufl. 2008, § 40 Rn. 1.

54 Wettbewerbsverstöße zählen ebenfalls zu den unerlaubten Handlungen (Spindler, in: Beck'scher Online-Kommentar BGB, Bamberger/Roth, 37. Edition, Stand: 1.11.2013, § 823 Rn. 0.19). Je nach den gegebenen Besonderheiten des Einzelfalls können auch in Bezug auf Daten Schadensersatz auslösende Wettbewerbsverstöße vorliegen. So kann etwa durch das Löschen bzw. Ausspähen von Daten eine gezielte Behinderung von Wettbewerbern nach § 4 Nr. 10 UWG gegeben sein (vgl. Schefzig, K&R, Beihefter 3/2015, 3, 4) oder eine Verletzung von Geschäfts- und Betriebsgeheimnissen nach § 17 UWG vorliegen (vgl. hierzu III.4. (Geheimnisschutz)).

55 Vgl. Brox/Walker, (Fn. 53), § 40 Rn. 2.

a) Rechtsgutverletzung im Sinne des § 823 Abs. 1 BGB

Von den in § 823 Abs. 1 BGB genannten Schutzgütern sind in Bezug auf Daten das Eigentum und das sonstige Recht von Belang.

aa) Eigentum

Wie bereits dargelegt⁵⁶ existiert mangels Sacheigenschaft kein Eigentum an Daten. Jedoch wurde von einzelnen Gerichten bereits entschieden, dass das Eigentum am Datenträger auch durch Löschen der auf ihm gespeicherten Daten verletzt sein kann.⁵⁷ Begründet wurde dies damit, dass eine Eigentumsverletzung im Sinne des § 823 Abs. 1 BGB nicht nur bei Zerstörung und Beschädigung der Sachsubstanz gegeben sei, sondern bei jeder Einwirkung auf die Sache, die den Eigentümer daran hindert, mit ihr seinem Wunsch entsprechend (§ 903 BGB) zu verfahren.⁵⁸ Die überwiegende Gegenansicht verneint hingegen bei einem „bloßen“ Datenverlust eine Eigentumsverletzung am Datenträger, da nur der Datenträger eine Sache sei, so dass auch nur seine Zerstörung oder Beschädigung zu einer Eigentumsverletzung führen könne, wobei dann natürlich der nach §§ 823 Abs. 1, 249 ff. BGB zu ersetzende Schaden um die auf dem Datenträger gespeicherten Daten wesentlich erhöht sein kann.⁵⁹

Diese Meinung, welcher (nur) im Ergebnis Recht zu geben ist, verkennt, dass auch eine Gebrauchsbeeinträchtigung des Datenträgers eine – von einer von § 823 Abs. 1 BGB nicht geschützten Vermögensbeeinträchtigung abzugrenzende – Eigentumsverletzung im Sinne des § 823 Abs. 1 BGB darstellen kann. Die höchstrichterliche Rechtsprechung⁶⁰ hat sich insoweit längst von einer rein substanzbezogenen Sichtweise gelöst und lässt auch die „nicht unerhebliche Beeinträchtigung der bestimmungsgemäßen Verwendung der Sache“ für eine Verletzung des Eigentums genügen.⁶¹ Mit dieser Formulierung gemeint und somit entscheidend kann nur sein, ob der bestimmungsgemäße Gebrauch der Sache als solche, oder nur der vom Eigentümer spezifisch bezweckte Gebrauch entzogen ist.⁶² Kann beispielsweise der Eigentümer des Datenträgers überhaupt keine Daten mehr auf seinem Datenträger speichern oder von ihm abrufen, weil ihm etwa der Zugriff auf den Datenträger durch den Schädiger gesperrt wird, liegt eine Eigentumsverletzung am Datenträger vor. Löscht hingegen der Schädiger „lediglich“ die auf dem Datenträger befindlichen Daten, ist eine Eigentumsverletzung zu verneinen.⁶³ Diese zunächst – insbesondere aus wirtschaftlicher Sicht – eigenartig anmutende Unterscheidung⁶⁴ ist gerechtfertigt, da es zum Schutz des Eigentums an einem Datenträger gehört, dass man ihn überhaupt nutzen, also insbesondere auf ihm überhaupt Daten speichern oder abrufen kann, nicht aber, dass auf ihm nur ganz bestimmte Daten gespeichert oder abgerufen werden können.⁶⁵

bb) Sonstiges Recht

Aus dem Vergleich zu dem Rechtscharakter der anderen in § 823 Abs. 1 BGB geschützten Rechtsgüter sowie zu dem einzig ausdrücklich aufgeführten Recht „Eigentum“ folgernd, werden als sonstige Rechte im Sinne des § 823 Abs. 1 BGB grundsätzlich nur absolute (eigentumsähnliche)⁶⁶ Rechte anerkannt.⁶⁷ Daneben hat sich das sonstige Recht zudem zum Einfallstor für eine Rechtsfortbildung des Deliktsrechtsschutzes entwickelt, indem sog. Rahmenrechte, wie das Allgemeine Persönlichkeitsrecht oder das Recht am eingerichteten und ausgeübten Gewerbebetrieb hierunter subsumiert werden.⁶⁸ In Bezug auf Maschinen-Daten

sind als sonstiges Recht vor allem der Besitz und das Rahmenrecht des eingerichteten und ausgeübten Gewerbebetriebs von Belang.⁶⁹

(1) Besitz

Neben dem Anwartschaftsrecht als wesensgleiches Minus zum Eigentum⁷⁰ ist der (zumindest berechnete) Besitz als sonstiges Recht im Sinne des § 823 Abs. 1 BGB anerkannt.⁷¹ Daher können – entsprechend der Ausführungen zum Eigentümer eines Datenträgers – der Anwartschaftsberechtigte sowie der (berechnete) Besitzer des Datenträgers Schadensersatzansprüche nach § 823 Abs. 1 BGB geltend ma-

56 Vgl. III.1. (Sachenrechtlicher Schutz).

57 Vgl. OLG Karlsruhe, 7.11.1995 – 3 U 15/95, NJW 1996, 200, 201; OLG Oldenburg, 24.11.2011 – 2 U 98/11, BeckRS 2011, 28832; ebenso Zech, CR 2015, 137, 142; a. A. OLG Dresden, 5.9.2012 – 4 W 961/12, NJW-RR 2013, 27, 28; LG Konstanz, 10.5.1996 – 1 S 292/95, NJW 1996, 2662.

58 OLG Karlsruhe, 7.11.1995 – 3 U 15/95, NJW 1996, 200, 201.

59 Fritzsche, in: Beck'scher Online-Kommentar BGB (Fn. 28), § 90 Rn. 26 m. w. N.

60 Vgl. etwa BGH, 21.12.1970 – II ZR 133/68, NJW 1971, 886, 888.

61 BGH, 31.3.1998 – VI ZR 109/97, NJW 1998, 1942, 1943 m. w. N.

62 Vgl. BGH, 21.12.1970 – II ZR 133/68, NJW 1971, 886, 888: Ein Reeder, der sich zur Abholung von Waren von einer Mühle vertraglich verpflichtete, konnte dieser Pflicht nicht nachkommen, da der Wasserweg zur Mühle durch den Einsturz einer Mauer versperrt wurde, wobei ein Schiff zwischen Mühle und Einsturzstelle eingeschlossen wurde und weitere Schiffe vom Anlaufen der Mühle ausgeschlossen wurden. Der BGH bejahte eine Eigentumsverletzung nur hinsichtlich des eingeschlossenen Schiffes, da es zum Schutzbereich des Eigentumes an einem Schiff gehöre, dass das Schiff überhaupt fahren kann, aber nicht, dass das Schiff für einen ganz bestimmten Transport zur Verfügung steht.

63 Im Fall des (bloßen) Löschens von Daten kann ein Anspruch nach § 823 Abs. 2 BGB i. V. m. § 303a Abs. 1 StGB bestehen, aber nur sofern der Schädiger vorsätzlich handelt, vgl. unten III.2.b)bb) (§ 823 Abs. 2 BGB i. V. m. § 303a Abs. 1 StGB).

64 Aus wirtschaftlicher Sicht macht es zunächst keinen Unterschied, ob Daten nicht genutzt werden können, weil der Zugriff auf den Datenträger gesperrt ist (dann Eigentumsverletzung) oder weil sie gelöscht wurden (dann nicht geschützte Vermögensbeeinträchtigung).

65 „[D]er Schutz des Eigentums als absolutes Recht [kann] nur den Verlust jeglicher Nutzungsmöglichkeit erfassen [...], nicht aber eine bestimmte Nutzung, die der Eigentümer der Sache zugeordnet hat“, s. Spindler, in: Beck'scher Online-Kommentar BGB (Fn. 54), § 823 Rn. 54.

66 Das „sonstige“ Recht kann keine lediglich subjektiv-rechtliche Rechtsposition sein, sondern muss als absolutes eigentumsähnliches Recht ebenso wie das Eigentum durch Zuweisungsgehalt und Ausschussfunktion geprägt sein (vgl. § 903 BGB), s. Lange/Schmidbauer, in: Herberger/Martinek/Rüßmann u. a., jurisPK-BGB (Fn. 37), § 823 Rn. 18.

67 H. M., vgl. nur Spindler, in: Beck'scher Online-Kommentar BGB (Fn. 54), § 823 Rn. 72 m. w. N.; zur Herleitung vgl. Lange/Schmidbauer, in: Herberger/Martinek/Rüßmann u. a., jurisPK-BGB (Fn. 37), § 823 Rn. 18.

68 Spindler, in: Beck'scher Online-Kommentar BGB (Fn. 54), § 823 Rn. 72.

69 Zu den absoluten Rechten zählen zudem etwa alle dinglichen Rechte (z. B. Nutzungsrechte wie Erbaurecht, Nießbrauch, Dienstbarkeit und Verwertungsrechte wie Hypothek, Grundschuld, Reallast, Pfandrecht sowie sonstige dingliche Berechtigungen wie Vorkaufsrechte oder das Anwartschaftsrecht), Immaterialgüterrechte (z. B. Patentrecht, Markenrecht, sonstige gewerbliche Schutzrechte, das Urheberrecht sowie die Firma) und Mitgliedschaftsrechte.

70 Vgl. hierzu Wagner, in: Münchener Kommentar zum BGB (Fn. 47), § 823 Rn. 214 f.

71 Teilweise wird vertreten, dass nur der berechnete Besitz als „sonstiges Recht“ zu werten sei, während nach der Gegenauffassung der Besitz (lediglich) „eigentumsähnliche“ Qualitäten aufweisen müsse, was dann der Fall sei, wenn der Besitzer sowohl abwehrfähige Rechte gegenüber Dritten als auch positive Rechte auf Nutzung der Sache inne habe, so dass nicht nur der berechnete Besitz, sondern auch der entgeltliche, redliche Besitz als „sonstiges Recht“ zu werten sei, vgl. hierzu etwa Wagner, in: Münchener Kommentar zum BGB (Fn. 47), § 823 Rn. 214 sowie Lange/Schmidbauer, in: Herberger/Martinek/Rüßmann u. a., jurisPK-BGB (Fn. 37), § 823 Rn. 20.

chen, wenn der Datenträger zerstört, beschädigt oder dessen bestimmungsgemäßer Gebrauch nicht nur unerheblich beeinträchtigt wird. Von praktischer Bedeutung ist dies etwa dann, wenn der (berechtigte) Besitzer dem Eigentümer für die Beschädigung des Datenträgers (nebst dem darauf gespeicherten Daten) einzustehen hat, da der (berechtigte) Besitzer dann das Haftungsinteresse für den Substanzschaden vom Schädiger nach § 823 Abs. 1 BGB verlangen kann.⁷²

(2) Recht am eingerichteten und ausgeübten Gewerbebetrieb

Das Recht am eingerichteten und ausgeübten Gewerbebetrieb ist von der höchstrichterlichen Rechtsprechung, insbesondere zur Füllung von Schutzlücken⁷³ anerkannt.⁷⁴ Aus dieser bezweckten Lückenfüllung folgt auch der subsidiäre Charakter der Haftung wegen Verletzung des Rechtes am bestehenden und ausgeübten Gewerbebetrieb, so dass diese Haftung ausgeschlossen ist, wenn ein anderes in § 823 Abs. 1 BGB genanntes Rechtsgut oder Recht verletzt, der Tatbestand des § 823 Abs. 2 BGB oder der des § 824 BGB gegeben ist oder eine speziellere Norm den Sachverhalt abschließend regelt.⁷⁵

Das Recht am eingerichteten und ausgeübten Gewerbebetrieb umfasst den Betrieb in seiner Gesamtheit,⁷⁶ so dass ein deliktischer Schutz von Daten selbst oder der Datenbank über dieses sonstige Recht im Sinn von § 823 Abs. 1 BGB gegeben sein kann.⁷⁷ Allerdings bedarf es insoweit einer sorgfältigen Prüfung, ob der Eingriff auch betriebsbezogen, also ob er unmittelbar gegen den Betrieb als solchen gerichtet ist.⁷⁸

b) Schutzgesetzverletzung im Sinne des § 823 Abs. 2 BGB

Ein gewisser deliktischer Schutz von Daten wird auch über § 823 Abs. 2 BGB gewährt.

aa) § 823 Abs. 2 BGB i. V. m. § 303 StGB

Das vorsätzliche⁷⁹ Zerstören oder Beschädigen eines fremden Datenträgers (nebst der darauf gespeicherten Daten) führt etwa zu einer deliktischen Haftung nach § 823 Abs. 2 BGB i. V. m. § 303 StGB. Nach h. M. ist eine Sachbeschädigung nach § 303 Abs. 1 StGB auch durch eine Gebrauchsbeeinträchtigung möglich, sofern durch das Einwirken auf die Sache eine nachhaltige Beeinträchtigung der Brauchbarkeit der Sache herbeigeführt wird, deren Beseitigung nicht nur einen geringfügigen Aufwand erfordert.⁸⁰ Daher kann das vorsätzliche Löschen von Daten einen Anspruch des Eigentümers des Datenträgers nach § 823 Abs. 2 BGB i. V. m. § 303 StGB begründen.⁸¹

bb) § 823 Abs. 2 BGB i. V. m. § 303a StGB

Daneben kann das vorsätzliche unberechtigte Löschen, Unterdrücken, Unbrauchbar machen oder Verändern⁸² von Daten im Sinne von § 202a Abs. 2 StGB,⁸³ also von Daten als solchen, gem. § 823 Abs. 2 BGB i. V. m. § 303a StGB zu einem Schadensersatzanspruch führen.

Nach ganz h. M. ist der Tatbestand des § 303a Abs. 1 StGB dahingehend einzuschränken, dass nur solche Daten erfasst werden, an denen einer anderen Person als dem Schädiger ein unmittelbares rechtlich schutzwürdiges Interesse in Form einer eigentümerähnlichen Verfügungsbefugnis zusteht.⁸⁴ Streitig ist dabei, wie diese „Datenverfügungsbefugnis“ zu bestimmen ist.⁸⁵

(1) Meinungsstand

Nach einer in der Literatur vertretenen Ansicht ist sie nach der sachenrechtlichen Zuordnung des Datenträgers zu bestimmen, so dass der Eigentümer bzw. berechnigte Besitzer des Datenträgers „datenverfügungsbefugt“ wäre.⁸⁶ Die Gegenansicht stellt auf die technische Urheberschaft der Daten (als den „Skripturakt“) als maßgebliches Zuordnungskriterium ab, so dass die Datenverfügungsbefugnis grundsätzlich derjenige innehat, der die Speicherung der Daten unmittelbar selbst bewirkt hat, was auch bei in fremdem Auftrag erstellten Daten gelte, solange der Auftragnehmer die Daten noch nicht dem Auftraggeber übergeben hat.⁸⁷ Die Gegenansicht begründet dies damit, dass zum einen – wovon aber auch die in der Literatur vertretene Ansicht ausgeht und deshalb auf die sachenrechtliche Zuordnung des Datenträgers abstellt – Daten keine Sachen im zivilrechtlichen Sinne seien und zum anderen nicht der Datenträger und dessen Eigentumsverhältnisse der Datenverfügungsbefugnis das Gepräge gebe, sondern die in den Datenspeichern enthaltenen Informationen und deren Urheberschaft.⁸⁸ Warum aber die in den Datenspeichern enthaltenen Informationen sowie deren Urheberschaft (und

72 Vgl. hierzu etwa BGH, 5.11.1991 – VI ZR 145/91, NJW 1992, 553 ff. sowie OLG Köln, 17.12.2001 – 11 W 41/01, BeckRS 2002, 05887 jeweils m. w. N.

73 Erfolgt die das Unternehmen schädigende Handlung nicht zu Wettbewerbszwecken, so ist das Wettbewerbsrecht (vor allem das UWG) nicht anwendbar, so dass (in Ermangelung sonstiger deliktischer Tatbestände) lediglich eine Haftung aus § 826 BGB in Betracht käme, welcher aber eine vorsätzliche sittenwidrige Schädigung verlangt, so dass bei bloßem fahrlässigen Handeln der Unternehmer keinen Schadensersatzanspruch hätte, s. Brox/Walker (Fn. 53), § 41 Rn. 16.

74 Spindler, in: Beck'scher Online-Kommentar BGB (Fn. 54), § 823 Rn. 104.

75 Vgl. hierzu Spindler, in: Beck'scher Online-Kommentar BGB (Fn. 54), § 823 Rn. 114 m. w. N.

76 Vgl. hierzu Spindler, in: Beck'scher Online-Kommentar BGB (Fn. 54), § 823 Rn. 105 m. w. N.

77 Dörner, CR 2015, 617, 619 m. w. N.

78 Vgl. hierzu Spindler, in: Beck'scher Online-Kommentar BGB (Fn. 54), § 823 Rn. 109 m. w. N.

79 Gem. § 823 Abs. 2 S. 2 BGB ist der schuldhafte Verstoß gegen das Schutzgesetz für die Haftung nach § 823 Abs. 2 BGB erforderlich, auch wenn die Zuwiderhandlung gegen das Schutzgesetz selbst ohne Verschulden erfolgen kann; im Übrigen ist aber der Verschuldensmaßstab des Schutzgesetzes maßgeblich, so dass der Sachbeschädiger erkennen und zumindest billigen muss, dass er eine fremde Sache beschädigt oder zerstört, vgl. Spindler, in: Beck'scher Online-Kommentar BGB (Fn. 54), § 823 Rn. 163 m. w. N.

80 Weidemann, in: Beck'scher Online Kommentar StGB, v. Heintschel-Heinegg, 29. Edition, Stand: 1.12.2015, § 303 Rn. 11 m. w. N.

81 Vgl. auch Stree/Hecker, in: Schönke/Schröder, StGB, 29. Aufl. 2014, § 303 Rn. 11 m. w. N.: Strafbarkeit nach § 303 StGB bei Löschen einer Diskette, Tonband- oder Filmaufnahme, soweit damit eine Funktionseinbuße des Datenträgers einhergeht.

82 Die Tathandlungen überschneiden sich zum Teil bewusst, da mit dieser Aufzählung ein möglichst umfassender Schutz gegen unberechtigte Beeinträchtigungen erreicht werden soll, s. und vgl. zu den einzelnen Tathandlungen Weidemann, in: Beck'scher Online Kommentar StGB (Fn. 80), § 303a Rn. 7 ff.

83 Unter Daten im Sinne von § 202a StGB werden Informationen verstanden, die nicht unmittelbar wahrnehmbar und in einer für eine Datenverarbeitungsanlage erkennbaren Form codiert sind, s. Weidemann, in: Beck'scher Online Kommentar StGB (Fn. 80), § 202a Rn. 3 f. m. w. N.

84 Weidemann, in: Beck'scher Online Kommentar StGB (Fn. 80), § 303a Rn. 5 m. w. N.

85 Peschel/Rockstroh, MMR 2014, 571, 573.

86 Vgl. Stree/Hecker, in: Schönke/Schröder StGB (Fn. 81), § 303a Rn. 3; vgl. auch (im Ergebnis ebenfalls auf eine sachenrechtliche Zuordnung abstellend) OLG Naumburg, 27.8.2014 – 6 U 3/14, juris, insbesondere Rn. 30 f.

87 Vgl. OLG Nürnberg, 23.1.2013 – 1 Ws 445/12, BeckRS 2013, 03553; Hoeren, MMR 2013, 486, 487.

88 Vgl. OLG Nürnberg, 23.1.2013 – 1 Ws 445/12, BeckRS 2013, 03553.

gerade nicht der Datenträger als das die Daten umfassende Behältnis) der Datenverfügungsbefugnis das Gepräge geben soll, wird nicht begründet.

(2) Stellungnahme

Gerade das Abstellen auf die in den Datenträgern enthaltenen Informationen erscheint fraglich, da (was auch von Vertretern der Gegenansicht eingeräumt wird) im „Hinblick auf das Rechtsgut des § 303a StGB gerade die Verfügungsbefugnis über die Integrität der Daten von ihrem Inhalt getrennt werden“ soll⁸⁹ und eine Zuordnung nach den „enthaltenen Informationen“ aber gerade Inhalt und Zuordnung gleichstellen würde. Zwar wird sich in der Regel der besondere Wert der Daten aus den in ihnen enthaltenen Informationen ergeben. Weshalb dies aber einer Bestimmung der Datenverfügungsbefugnis anhand der sachenrechtlichen Zuordnung des Datenträgers entgegenstehen soll, ist nicht ersichtlich, zumal die sachenrechtliche Zuordnung zunächst ebenfalls an die Urheberschaft bzw. den „Skripturakt“ anknüpft. Erhebt der Skribent Daten, hat er es in der Hand, ob er die Daten auf einem in seinem Eigentum (bzw. in seinem berechtigten Besitz) befindlichen Datenträger speichert oder nicht. Tut er dies, ist er als Eigentümer (bzw. berechtigter Besitzer) des Datenträgers auch der Datenverfügungsbefugte.⁹⁰ Will er die Daten auf einem fremden Datenträger speichern, so kann er sich zum einen entsprechende Rechte hinsichtlich der Daten (z.B. Nutzungs- oder Rückforderungsrechte bezüglich der Daten) vertraglich vorbehalten, was aber nichts daran ändert, dass die Datenverfügungsbefugnis bei dem Eigentümer (bzw. dem berechtigten Besitzer) des Datenträgers verbleibt. Will der Skribent die erhobenen Daten auf einem fremden Datenträger speichern und gleichwohl der „Datenverfügungsbefugte“ bleiben, muss er mit dem Eigentümer des Datenträgers entsprechende vertragliche Vereinbarungen hinsichtlich des Datenträgers treffen (z.B. die Vereinbarung von dem Skribenten als berechtigten Besitzer des Datenträgers ausweisende Rechte).⁹¹ Die Bestimmung der originären Datenverfügungsbefugnis in Abhängigkeit von der sachenrechtlichen Zuordnung des Datenträgers ermöglicht somit eine klare Zuordnung und entspricht damit zugleich im Rahmen des weit gefassten Tatbestandes des § 303a StGB hinreichend dem verfassungsrechtlichen Bestimmtheitsgebot. Zudem wird damit ein Gleichlauf der strafrechtlichen „Datenverfügungsbefugnis“ mit der zivilrechtlichen „Datenhoheit“ erreicht.⁹² Dies läuft entgegen der Gegenmeinung auch nicht auf eine Kriminalisierung von Vertragsverletzungen hinaus.⁹³ Die Strafbarkeit nach § 303a Abs. 1 StGB hängt allein davon ab, ob der Täter vorsätzlich und unberechtigt Daten löscht, unterdrückt, unbrauchbar macht oder verändert, die in der Verfügungsbefugnis einer anderen Person stehen. Dass sich diese Verfügungsbefugnis in Abhängigkeit von einer sachenrechtlichen Zuordnung ergibt, welche auch auf vertraglichen Abreden beruhen kann, ist insoweit ohne Belang. Auch mit Blick auf das Rechtsgut des § 303a StGB, nämlich die Verwendbarkeit der Daten durch den Berechtigten,⁹⁴ muss die Verfügungsbefugnis über die Daten nicht zwingend mit deren Urheberschaft einhergehen. Ferner ergibt sich eine nähere Beziehung zum Sacheigentum als zur Urheberschaft aus der systematischen Stellung des § 303a StGB in den Eigentumsdelikten, unmittelbar nach der Sachbeschädigung.⁹⁵

cc) § 823 Abs. 2 BGB i. V. m. § 274 Abs. 1 Nr. 2 StGB

Darüber hinaus kann sich eine Haftung nach § 823 Abs. 2 BGB i. V. m. § 274 Abs. 1 Nr. 2 StGB ergeben, wenn beweis-

erhebliche Daten (§ 202a Abs. 2 StGB), über die der Schädiger nicht oder nicht ausschließlich verfügen darf, in der Absicht einem anderen Nachteil zuzufügen, gelöscht, unterdrückt, unbrauchbar gemacht oder verändert werden.

c) Sittenwidrige vorsätzliche Schädigung im Sinne des § 826 BGB

Nach § 826 BGB ist schadensersatzpflichtig, wer in einer gegen die guten Sitten verstoßenden Weise einem anderen vorsätzlich Schaden zufügt. Mithin bedarf es zur Erfüllung des Tatbestandes (erstens) einer Schadenszufügung durch (zweitens) eine sittenwidrige Handlung⁹⁶ und (drittens) den Vorsatz⁹⁷ des Täters.

Zur Bejahung des Schadens im Rahmen des § 826 BGB muss nicht – wie nach § 823 Abs. 1 BGB – ein Rechtsgut oder ein Recht und auch nicht – wie nach § 823 Abs. 2 BGB – ein Schutzgesetz verletzt sein. Vielmehr erfasst § 826 BGB auch den reinen Vermögensschaden.⁹⁸ Daher kann eine schadensersatzauslösende sittenwidrige Handlung auch durch die Beeinträchtigung der Daten als solche⁹⁹ begangen werden.

3. Immaterialgüterrechtlicher Schutz

Das Interesse an der exklusiven Verwendung der im Rahmen von Big Data gewonnenen Datenmengen wird zudem – wenn auch in sehr beschränktem Umfang – im Urheberrecht berücksichtigt. Insoweit werden zwar nicht die Daten als solche, sondern allenfalls deren konkrete Art der Darstellung oder die Investition in die Systematisierung der Darstellung geschützt.

a) Datenbankwerkschutz

Ein (schöpferisches) Datenbankwerk (§ 4 Abs. 2 UrhG) ist vor (vollständiger oder teilweiser) Vervielfältigung sowie gegen Anpassung, Erweiterung, Übersetzung und jede andere Umgestaltung und gegen jede Form der öffentlichen Verbreitung und Wiedergabe geschützt.¹⁰⁰ Bei einer Verletzung des gewährten Schutzes kann der Urheber des Datenbankwerkes vor allem Unterlassungs- und Schadensersatzansprüche sowie Ansprüche auf Vernichtung der Vervielfältigung geltend machen (vgl. §§ 97 ff. UrhG).

Voraussetzung für den Datenbankwerkschutz gem. § 4 Abs. 2 S. 1 UrhG ist neben der systematischen oder methodischen Anordnung der Datenbankelemente sowie deren einzelne Zugänglichkeit,¹⁰¹ dass das Datenbankwerk eine

89 Vgl. Hoeren, MMR 2013, 486, 487.

90 Vgl. auch OLG Naumburg, 27.8.2014 – 6 U 3/14, juris, Rn. 31.

91 Vgl. auch OLG Naumburg, 27.8.2014 – 6 U 3/14, juris, Rn. 31.

92 Vgl. hierzu III. 1. b.) (Mittelbare sachenrechtliche Zuordnung).

93 So aber Hoeren, MMR 2013, 486, 487.

94 Hoeren, MMR 2013, 486, 487.

95 Vgl. Hoeren, MMR 2013, 486, 487.

96 Vgl. hierzu etwa Wagner, in: Münchener Kommentar zum BGB (Fn. 47), § 826 Rn. 8 ff.

97 Vgl. hierzu etwa Wagner, in: Münchener Kommentar zum BGB (Fn. 47), § 826 Rn. 24 ff.

98 Wagner, in: Münchener Kommentar zum BGB (Fn. 47), § 826 Rn. 1; Darüber hinausgehend hat der BGH sogar eine bloße Vermögensgefährdung als Schaden eingestuft, vgl. BGH, 13.9.2004 – II ZR 276/02, NJW 2004, 3706, 3710.

99 Zur Einordnung von Daten bzw. eines Datenbestandes als „selbständiges vermögenswertes Gut“, vgl. BGH, 2.7.1996 – X ZR 64/94, NJW 1996, 2924, 2926.

100 Götz, ZD 2014, 563, 564.

101 Mit der Voraussetzung der einzelnen Zugänglichkeit der Elemente eines Datenbankwerkes soll ausgeschlossen werden, dass bereits als Einheit geschützte Güter nicht noch zusätzlich als Datenbankwerke geschützt werden, s. Dreier, in: Dreier/Schulze, Urheberrechtsgesetz, 5. Aufl. 2015, § 4 UrhG Rn. 18.

persönliche geistige Schöpfung gem. § 4 Abs. 1 UrhG i. V. m. § 2 Abs. 2 UrhG darstellt.¹⁰²

Mithin darf nicht nur ein (aus ungeordneten Rohdaten bestehender) sog. Datenhaufen vorliegen, sondern vielmehr muss zumindest ein System oder eine Methode der Datenanordnung erkennbar sein, welches bzw. welche zudem die für die Urheberschutzfähigkeit des Datenbankwerkes erforderliche schöpferische Eigenart aufweisen muss.¹⁰³ Die systematische oder methodische Anordnung von maschinen generierten Daten wird in aller Regel mittels elektronischer Datenbanken erfolgen. Bei elektronischen Datenbanken ist zu berücksichtigen, dass die Anordnung der Elemente innerhalb der Datenbank von der Datenbanksoftware abhängt, welche aber nach § 4 Abs. 2 S. 2 UrhG als eigenständiger Schutzgegenstand ausdrücklich kein Bestandteil des Datenbankwerkes ist.¹⁰⁴ Daher kann die schöpferische Eigenart der Datenbanksoftware (und damit auch die Anordnung der Daten innerhalb der Datenbank) nichts zur schöpferischen Eigenart des Datenbankwerkes beitragen, so dass bei der Beurteilung der schöpferischen Eigenart des elektronischen Datenbankwerkes im Ergebnis die Schöpfungshöhe der Zugangs- und Abfragemöglichkeiten maßgeblich sein wird.¹⁰⁵ Der Schutz einer reinen Datensammlung als elektronisches Datenbankwerk wird folglich nur dann bejaht werden können, wenn sie, insbesondere aufgrund der schöpferischen Leistung hinsichtlich der Zugangs- und Abfragesysteme, ein Maß an Individualität und Originalität aufweist und deshalb aus der Masse des Alltäglichen herausragt.¹⁰⁶ Übliche oder lediglich auf Zweckmäßigkeitserwägungen beruhende Zugangs- und Abfragesysteme bei elektronischen Datensammlungen werden hingegen mangels Individualität nicht vom Schutzbereich des § 4 Abs. 2 UrhG erfasst. Da in aller Regel (die oftmals rein informativen)¹⁰⁷ Sammlungen von maschinengenerierten Daten keine derartig individuellen und originellen Zugangs- und Abfragesysteme aufweisen, ist die Praxisrelevanz von § 4 Abs. 2 UrhG in Bezug auf Maschinen-Daten als gering einzustufen.¹⁰⁸ Selbst wenn infolge einer hinreichenden Schöpfungshöhe ein geschütztes Datenbankwerk vorliegen sollte, wird oftmals keine Urheberrechtsverletzung am Datenbankwerk angenommen werden können, da eine insoweit urheberrechtsrelevante Handlung (z. B. Vervielfältigung) nur dann gegeben ist, wenn sie sich auf die den Urheberrechtsschutz verleihende schöpferische Eigenart des Datenbankwerkes als solche – also insbesondere auf das kreative Zugangs- bzw. Abfragesystem – und nicht nur auf die urheberrechtlich nicht geschützten Daten des Sammelwerkes bezieht.¹⁰⁹

b) Datenbankherstellerschutz

Von größerer praktischer Relevanz als der Datenbankwerkerschutz nach § 4 Abs. 2 S. 1 UrhG ist in Bezug auf Maschinen-Daten das Leistungsschutzrecht sui generis gem. §§ 87a ff. UrhG.¹¹⁰ Dieses ausschließliche Recht des Datenbankherstellers an der Vervielfältigung, Verbreitung oder öffentlichen Wiedergabe „seiner“ Datenbank (vgl. § 87b Abs. 1 UrhG) knüpft nicht an die individuelle und originelle Herstellung der Datenbank (als Ergebnis seiner persönlichen geistigen Schöpfung) an, sondern an die wirtschaftliche Investition bzw. Leistung in die Beschaffung, Überprüfung oder Darstellung der Daten (vgl. § 87a Abs. 1 UrhG). Geschützt wird mithin die Investition des Datenbankherstellers.

Nach § 87a Abs. 1 S. 1 UrhG ist eine Datenbank im Sinne der §§ 87a ff. UrhG eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind und deren Beschaffung, Überprüfung oder Darstellung eine nach Art oder Umfang wesentliche Investition erfordert. Demnach müssen, ebenso wie bei der Datenbank im Sinne des § 4 Abs. 2 UrhG, auch im Rahmen des Datenbankherstellerschutzes die Daten systematisch oder methodisch angeordnet sein und zudem einzeln zugänglich sein, so dass also auch die Datenbank im Sinne der §§ 87a ff. UrhG – ebenso wie das Datenbankwerk nach § 4 Abs. 2 UrhG – strikt von den Elementen ihres Inhaltes zu trennen ist.¹¹¹ Nicht vom Schutzbereich der §§ 87a ff. UrhG umfasst sind mithin die in der Datenbank enthaltenen einzelnen Daten selbst.¹¹²

Anders als der (eine persönliche geistige Schöpfung voraussetzende) Urheberrechtsschutz von Datenbankwerken, bedarf es im Rahmen des Datenbankherstellerschutzes hingegen einer nach Art oder Umfang wesentlichen Investition bei der Beschaffung, Überprüfung oder Darstellung der Daten. Die Investition kann etwa durch den Einsatz von menschlichen, finanziellen oder technischen Ressourcen oder Mitteln erfolgen.¹¹³ Wesentlich ist die Investition dann, „wenn bei objektiver Betrachtung keine ganz unbedeutenden, von jedermann leicht zu erbringenden Aufwendungen erforderlich waren, um die Datenbank zu erstellen“.¹¹⁴ Hierbei gilt jedoch zu beachten, dass die bloße Datenerzeugung keine Investition im Sinne von § 87a Abs. 1 UrhG darstellt, da zu den Investitionen für die Beschaffung von Daten allein die Mittel zählen, die für die Ermittlung von bereits existierenden Daten und deren Zusammenstellung in der Datenbank aufgewandt werden, also gerade nicht die Mittel, die für die Erzeugung von Daten eingesetzt werden.¹¹⁵ Daher sollten Unternehmen, welche mit einem nicht unerheblichen Aufwand Daten erzeugen, darauf achten und gegebenenfalls entsprechende vertragliche Vorkehrungen dahingehend treffen, dass der Leistungsschutz nicht einem Kooperationspartner zufällt.¹¹⁶ Denn Hersteller einer Datenbank und mithin Inhaber der Rechte an einer Datenbank

102 Vgl. *Ahlberg*, in: Beck'scher Online-Kommentar Urheberrecht, Ahlberg/Götting, 10. Edition, Stand: 1.10.2015, § 4 UrhG Rn. 25.

103 *Dreier*, in: *Dreier/Schulze* (Fn. 101), § 4 UrhG Rn. 17.

104 *Dreier*, in: *Dreier/Schulze* (Fn. 101), § 4 UrhG Rn. 21.

105 *Dreier*, in: *Dreier/Schulze* (Fn. 101), § 4 UrhG Rn. 19 m. w. N.

106 Vgl. etwa OLG Frankfurt a. M., 22.3.2005 – 11 U 64/04, GRUR-RR 2005, 299, 300.

107 Vgl. hierzu OLG Frankfurt a. M., 22.3.2005 – 11 U 64/04, GRUR-RR 2005, 299, 301.

108 Ebenso *Dorner*, CR 2014, 617, 621; *Zieger/Smirra*, MMR 2013, 418, 419; *Peschel/Rockstroh*, MMR 2014, 571, 572; *Götz*, ZD 2014, 563, 563.

109 Zur rechtlichen Trennung von Sammelwerk und Inhalt des Sammelwerks vgl. *Dreier*, in: *Dreier/Schulze* (Fn. 101), § 4 UrhG Rn. 4.

110 Ebenso *Dorner*, CR 2014, 617, 622; *Zieger/Smirra*, MMR 2013, 418, 420; *Peschel/Rockstroh*, MMR 2014, 571, 572.

111 *Dreier*, in: *Dreier/Schulze* (Fn. 101), § 87a UrhG Rn. 3.

112 *Dorner*, CR 2014, 617, 622; Ein Schutz einzelner Daten kann sich allenfalls dann ergeben, wenn sie wiederum einen wesentlichen Teil der Investition in die Datenbank selbst darstellen, vgl. hierzu BGH, 1.12.2010 – I ZR 196/08, GRUR 2011, 724, 726 Rn. 32.

113 BGH, 1.12.2010 – I ZR 196/08, GRUR 2011, 724, 725 Rn. 18.

114 BGH, 1.12.2010 – I ZR 196/08, GRUR 2011, 724, 725 Rn. 23: Investitionen von substanziellem Gewicht sind nicht erforderlich.

115 Vgl. BGH, 1.12.2010 – I ZR 196/08, GRUR 2011, 724, 725 Rn. 19 m. w. N.

116 *Schefzig*, K&R, Beihefter 3/2015, 3, 6.

nach § 87b UrhG ist nach § 87a Abs. 2 UrhG derjenige, der die Investition in die Beschaffung, Überprüfung oder Darstellung des Datenbankinhalts vorgenommen hat.¹¹⁷ Also gerade nicht (zwingend) derjenige, der die Daten erzeugt hat.

4. Geheimnisschutz

Effektiver Geheimnisschutz ist allein juristisch nicht zu gewährleisten, da ein etwaiger vertraglicher Geheimnisschutz nicht gegenüber außenstehenden Dritten wirkt und der gesetzliche – die Offenbarung der Geheimnisse voraussetzende – Geheimnisschutz im Ergebnis zu spät wirkt.¹¹⁸ Hinzu kommt, dass der Geheimnisschutz sowohl in faktischer, insbesondere in technisch-organisatorischer Hinsicht¹¹⁹ als auch in juristischer Hinsicht¹²⁰ ein „Querschnittsthema“ ist.¹²¹ Daher soll auch an dieser Stelle keine umfassende Darstellung des Geheimnisschutzes erfolgen, sondern lediglich ein kurzer Hinweis auf den in Bezug auf Daten durchaus relevanten, den Schutz von Betriebs- und Geschäftsgeheimnissen bezweckenden (und damit zugleich den Wettbewerb vor Verfälschung schützenden)¹²² § 17 UWG gegeben werden.

§ 17 UWG enthält drei Tatbestände, nämlich den Geheimnisverrat durch Beschäftigte (§ 17 Abs. 1 UWG), die Betriebsspionage durch Beschäftigte oder Dritte (§ 17 Abs. 2 Nr. 1 UWG) und die auch als Geheimnishehlerei bezeichnete unbefugte Verwertung rechtswidrig erlangter Geheimnisse (§ 17 Abs. 2 Nr. 2 UWG) und sieht ausdrücklich nur strafrechtliche Rechtsfolgen vor.¹²³ Nach allgemeiner Ansicht ist § 17 UWG ein Schutzgesetz im Sinne des § 823 Abs. 2 BGB, so dass auch zivilrechtliche Schadensersatzansprüche aus dessen Verletzung resultieren können.¹²⁴ Auch können durch die Verletzung von Betriebs- und Geschäftsgeheimnissen neben Schadensersatzansprüchen nach § 9 UWG, § 823 Abs. 1 BGB und § 826 BGB auch Herausgabeansprüche nach § 10 UWG sowie Unterlassungs- und Beseitigungsansprüche nach § 8 UWG und analog § 1004 Abs. 1 BGB begründet sein.¹²⁵ Ferner sind auch Ansprüche wegen angemaßter Eigengeschäftsführung (§§ 687 Abs. 2, 681, 667 BGB) denkbar.¹²⁶

„Ein Geschäfts- oder Betriebsgeheimnis im Sinne von § 17 UWG ist jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem bekundeten, auf wirtschaftlichen Interessen beruhenden Willen des Betriebsinhabers geheimgehalten werden soll.“¹²⁷ Alle lediglich betriebsintern gehaltenen Daten, die im Laufe der Betriebstätigkeit erzeugt oder gesammelt wurden (z. B. Messdaten von Produktionsanlagen sowie auch die daraus gewonnenen Smart Data), dürften daher in aller Regel diese Voraussetzungen erfüllen, sofern sich auch der Geheimhaltungswille auf sie erstreckt.¹²⁸

5. Datenschutz

Sofern sich die Erhebung, Verarbeitung und Nutzung von maschinell generierten Daten auf personenbezogene Daten bezieht, sind die datenschutzrechtlichen Bestimmungen zu beachten.¹²⁹ Gegenstand des Datenschutzes ist nicht der Schutz der Daten an sich, sondern in erster Linie der Schutz des einzelnen Betroffenen vor der mit der Datenverarbeitung einhergehenden Gefahr der Beeinträchtigung von Persönlichkeitsrechten, insbesondere des vom BVerfG im

Volkszählungsurteil konkretisierten Rechtes auf informationelle Selbstbestimmung als Ausfluss des durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrechtes¹³⁰.¹³¹ Die bereits in diesem Urteil angesprochenen Prinzipien der Datensparsamkeit und der Zweckbindung stehen aber gerade im Widerspruch zu dem Konzept von Big Data, bei dem so viel wie möglich Daten für alle denkbaren Zwecke gespeichert und analysiert werden sollen.¹³²

Trotz des subsidiären Charakters des BDSG gegenüber anderen Rechtsvorschriften des Bundes bei personenbezogenen Daten (vgl. § 1 Abs. 3 S. 1 BDSG) – insbesondere gegenüber dem TKG und dem TMG – wird bei Big Data-Anwendungen oftmals das BDSG Anwendung finden.¹³³ Daher soll der folgende kurze Überblick zum Datenschutz ausschließlich anhand des BDSG erfolgen.

Sofern eine Anonymisierung im Sinne von § 3 Abs. 6 BDSG¹³⁴ von Maschinen-Daten mit Personenbezug¹³⁵ nicht möglich oder unzumutbar ist, ist deren Verarbeitung gem. § 4 Abs. 1 BDSG nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder der Betroffene einwilligt.

a) Gesetzliche Erlaubnistatbestände

Eine Rechtfertigung kommt insbesondere nach solchen gesetzlichen Erlaubnistatbeständen in Betracht, die die Erforderlichkeit oder die Wahrung berechtigter Interessen der verantwortlichen Stelle für die Datenerhebung und -speicherung von personenbezogenen Daten genügen lassen.¹³⁶ So ist etwa eine Rechtfertigung nach dem Erlaubnistatbestand des § 28 Abs. 1 Nr. 1 BDSG unter dem Gesichtspunkt der Erforderlichkeit im Rahmen des sog. Fraud Detection denkbar.¹³⁷ Ebenfalls denkbar wäre eine Rechtfertigung nach § 28 Abs. 1 Nr. 2 BDSG wegen Erforderlichkeit und überwiegender berechtigter Interessen der verantwortlichen Stelle bei einer Datenverarbeitung in Customer Relationship Management-Systemen, sofern die entsprechende Datenverarbeitung für das Unternehmen zweckmäßig ist und keine zumutbare Alternative besteht.¹³⁸ Zu beachten ist

117 Vgl. BGH, 22.6.2011 – IZR 159/10, GRUR 2011, 1018, 1020 Rn. 32 m. w. N.

118 Ann, GRUR 2014, 12, 14.

119 Vgl. hierzu Ann, GRUR 2014, 12, 14 f.

120 Vgl. hierzu Dorner, CR 2014, 617, 622.

121 Schefzig, K&R, Beihefter 3/2015, 3, 4.

122 Köhler, in: Köhler/Bornkamm, 35. Aufl. 2017, § 17 UWG Rn. 2.

123 Ohly, in: Ohly/Sosnitza, UWG, 6. Aufl. 2014, § 17 UWG Rn. 2.

124 Ohly, in: Ohly/Sosnitza (Fn. 123), § 17 UWG Rn. 2.

125 Vgl. hierzu Ohly, in: Ohly/Sosnitza (Fn. 123), § 17 UWG Rn. 48 f.

126 Vgl. hierzu Ohly, in: Ohly/Sosnitza (Fn. 123), § 17 UWG Rn. 50.

127 BGH, 26.2.2009 – IZR 28/06, GRUR 2009, 603, 604 Rn. 13 m. w. N.

128 Schefzig, K&R, Beihefter 3/2015, 3, 4; Dorner, CR 2014, 617, 622 f.; Peschel/Rockstroh, MMR 2014, 571, 574.

129 Schefzig, K&R, Beihefter 3/2015, 3, 6; Peschel/Rockstroh, MMR 2014, 571, 574.

130 Vgl. BVerfG, 15.12.1983 – 1 BvR 209/83 u. a., NJW 1984, 419, 421 ff.

131 Gola/Klug/Körffler, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 1 BDSG Rn. 1 f.

132 Roßnagel, ZD 2013, 562, 564.

133 Vgl. auch Peschel/Rockstroh, MMR 2014, 571, 575.

134 Zur Vermeidung der Anwendung des Datenschutzrechtes durch Anonymisieren der Daten vgl. Roßnagel, ZD 2013, 562, 565 f.

135 Personenbezogene Daten sind gem. § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlicher Person. Zur Einordnung von personenbezogenen Daten im Rahmen von Big Data vgl. Roßnagel, ZD 2013, 562, 563.

136 Roßnagel, ZD 2013, 562, 564.

137 Vgl. Ohrtmann/Schwiering, NJW 2014, 2984, 2985 f.

138 Vgl. Ohrtmann/Schwiering, NJW 2014, 2984, 2986.

jedoch, dass die Erlaubnistatbestände in aller Regel eine Abwägung der berechtigten Interessen der verantwortlichen Stelle mit den schutzwürdigen Interessen des Betroffenen an dem Ausschluss des Umgangs mit den personenbezogenen Daten erfordern. Im Rahmen von Big Data-Analysen werden aber oftmals große ungeordnete Datenberge durchsucht und erst bei der Auswertung die Daten herausgefiltert, die zur Beantwortung einer Frage beitragen können, so dass nur schwer alle möglichen schutzwürdigen Interessen der Betroffenen ausgemacht werden können.¹³⁹ Erschwerend kommt hinzu, dass (trotz Vorliegens eines gesetzlichen Erlaubnistatbestandes) der Umgang mit personenbezogenen Daten an dem Ziel der Datenvermeidung und der Datensparsamkeit auszurichten (vgl. § 3a BDSG) und der Grundsatz der Zweckbindung sowie das Verbot der automatisierten Entscheidung (vgl. § 6a BDSG) zu beachten sind.¹⁴⁰

b) Einwilligung der Betroffenen

Soweit sich eine Big Data-Anwendung nicht oder nur mit nicht unerheblichen Unsicherheiten anhand eines gesetzlichen Erlaubnistatbestandes rechtfertigen lässt (und auch keine Anonymisierung der Daten in Betracht kommt), ist die Einwilligung der Betroffenen (§ 4a BDSG) einzuholen. Die Einwilligung muss auf einer freien Entscheidung des Betroffenen beruhen (§ 4a Abs. 1 S. 1 BDSG). Daher muss zum einen der Betroffene seine Entscheidung hinsichtlich der Erteilung seiner Einwilligung in die Datenverarbeitung frei von Zwang treffen können.¹⁴¹ Dies kann etwa dann fraglich sein, wenn dem Betroffenen die Einwilligung unter Ausnutzung einer Machtposition abgenötigt wurde.¹⁴² Zum anderen kann der Betroffene nur dann frei über die Einwilligung entscheiden, wenn er den Umfang der vorgesehenen Verarbeitungen kennt.¹⁴³ Insoweit normiert § 4a Abs. 1 S. 2 BDSG auch die Pflicht, den Betroffenen über den Zweck der Datenverarbeitung zu informieren. Bei Big Data-Analysen müsste also auch der Analysezweck benannt werden. Dies soll aber z. B. bei Big Data, die für alle erdenklichen Zwecke genutzt werden sollen, mangels hinreichender Bestimmtheit nicht möglich sein.¹⁴⁴ Insbesondere sollen AGB darstellende und damit der Inhaltskontrolle (§§ 307 ff. BGB) unterliegende Einwilligungen, die allgemein gehaltene Beschreibungen und Oberbegriffe verwenden, derart globale Einwilligungen in Datenverarbeitungsprozesse darstellen, dass sie mangels hinreichender Transparenz unwirksam sind.¹⁴⁵

c) Schlussfolgerungen aus datenschutzrechtlicher Sicht

Mithin fordert das Datenschutzrecht mit Big Data-Anwendungen beschäftigte Unternehmen nicht nur unwesentlich. So kann bei Big Data-Anwendungen nicht nur die Prüfung des Personenbezugs, sondern gerade auch die Prüfung des Vorliegens eines Erlaubnistatbestandes sehr komplex sein.¹⁴⁶ Sofern Einwilligungen der Betroffenen eingeholt werden, ist auf die rechtliche Wirksamkeit der Einwilligungen zu achten. Insoweit ist auch ein besonderes Augenmerk auf die Hinweispflicht des § 4a Abs. 1 S. 2 BDSG zu legen. Dies gilt umso mehr, als dass bei einem Verstoß gegen die auf den Schutz des Betroffenen abstellenden Normen des BDSG – wozu auch die §§ 4 Abs. 1, 4a BDSG (Verarbeitung ohne Erlaubnis oder korrekte Einwilligung) gehören – ein Schadensersatzanspruch nach § 823 Abs. 2 BGB begründet sein kann.¹⁴⁷ Auch droht etwa eine Schadensersatzpflicht nach § 7 BDSG, wenn eine verantwortliche Stelle dem Be-

troffenen durch eine unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten schädigt, wobei das Verschulden vermutet wird. Bei Vorliegen der entsprechenden Voraussetzungen des § 35 BDSG kann eine Löschung der Daten geboten sein, was gerade bei Big Data-Anwendungen mit einer sofortigen Werteinbuße verbunden sein kann.¹⁴⁸

III. Fazit

Es besteht ein durchaus hinreichender – sich insbesondere aus dem Deliktsrecht ergebender – Schutz von Daten durch die Gewährung gesetzlicher Abwehr- und Schadensersatzansprüche. Werden Daten infolge einer fahrlässigen oder vorsätzlichen Beschädigung des Datenträgers beeinträchtigt, kann sich ein Schadensersatzanspruch aus § 823 Abs. 1 BGB wegen Eigentumsverletzung (bzw. wegen Besitzverletzung als sonstiges Recht) am Datenträger ergeben. Gleiches gilt, wenn (ohne Substanzverletzung des Datenträgers) die Nutzung der Daten vereitelt wird, sofern damit eine nicht unerhebliche Beeinträchtigung der bestimmungsgemäßen Verwendung des Datenträgers verbunden ist. Ist mit dem Löschen oder sonstigen Beeinträchtigung der Daten hingegen keine erhebliche Beeinträchtigung der bestimmungsgemäßen Verwendung des Datenträgers verbunden, kann ein Schadensersatzanspruch nach § 823 Abs. 2 BGB i. V. m. § 303a Abs. 1 StGB (oder gar § 274 Abs. 1 Nr. 2 StGB) begründet sein, allerdings nur sofern der Schädiger (zumindest) vorsätzlich handelt. Fällt dem Schädiger bei einer Beeinträchtigung der Daten ohne erhebliche Beeinträchtigung der bestimmungsgemäßen Verwendung des Datenträgers lediglich Fahrlässigkeit zur Last, kommt zumindest noch eine Haftung aus § 823 Abs. 1 BGB wegen Verletzung des Rechtes am eingerichteten und ausgeübten Gewerbebetrieb in Betracht, allerdings nur wenn der Eingriff unmittelbar betriebsbezogen ist. Handelt der Schädiger vorsätzlich und sittenwidrig, kann eine Beeinträchtigung der Daten als solche einen Schadensersatzanspruch nach § 826 BGB begründen.

Umgekehrt ausgedrückt, versagt ein deliktsrechtlicher Schutz von Daten demnach nur, wenn (mangels Beschädigung oder mangels erheblicher Beeinträchtigung der bestimmungsgemäßen Verwendung des Datenträgers) keine Verletzung des Eigentums oder Besitzes am Datenträger bejaht werden kann und der Schädiger lediglich fahrlässig handelt und (etwa mangels Betriebsbezogenheit des Eingriffs) auch keine Verletzung des Rechtes am eingerichteten

139 *Roßnagel*, ZD 2013, 562, 564.

140 Vgl. hierzu *Ohrtmann/Schwiering*, NJW 2014, 2984, 2987 f.

141 *Spindler/Nink*, in: *Spindler/Schuster*, Recht der elektronischen Medien, 3. Aufl. 2015, § 4a Rn. 6.

142 *Gola/Klug/Körffler*, in: *Gola/Schomerus* (Fn. 131), § 4a BDSG Rn. 19 f. m. w. N.; Ein allgemeines Kopplungsverbot soll hingegen nicht bestehen, s. *Gola/Klug/Körffler*, in: *Gola/Schomerus* (Fn. 131), § 4a BDSG Rn. 21 m. w. N.

143 *Gola/Klug/Körffler*, in: *Gola/Schomerus* (Fn. 131), § 4a BDSG Rn. 26.

144 Vgl. *Roßnagel*, ZD 2013, 562, 564.

145 Vgl. LG Berlin, 30.4.2013 – 15 O 92/12, NJW 2013, 2605, 2606 f.

146 Vgl. auch *Schefzig*, K&R, Beihefter 3/2015, 3, 6.

147 Weitere Schutzgesetze im Sinne von § 823 Abs. 2 BGB sind etwa im ersten Abschnitt des BDSG § 5 (fehlende Schulung und Verpflichtung der Mitarbeiter), § 6a (unzulässige automatisierte Einzelentscheidung), § 9 (Verstoß gegen Erfordernisse der Datensicherung), § 10 (unzulässiges Abrufverfahren) und § 11 (Sorgfaltsmängel bei der Auftragsvergabe bzw. Auftragsdurchführung), vgl. *Gola/Klug/Körffler*, in: *Gola/Schomerus* (Fn. 131), § 1 BDSG Rn. 3.

148 *Schefzig*, K&R, Beihefter 3/2015, 3, 6.

und ausgeübten Gewerbebetrieb vorliegt. Ob dies – wie in der Literatur zum Teil diskutiert¹⁴⁹ – rechtfertigt, ein Dateneigentum (analog § 903 BGB) oder ein Ausschließlichkeitsrecht an Daten als sonstiges Recht im Sinne des § 823 Abs. 1 BGB zu konstruieren, ist jedoch fraglich. Denn abgesehen von den eben genannten Fällen, besteht (insbesondere mittelbar über die Beeinträchtigung des Datenträgers) ein durchaus weitgehender gesetzlicher (aus dem Sachen- und Deliktsrecht folgender) Schutz von Daten, zumal das Gesetz in immaterialgüterrechtlicher, geheimnisschutzrechtlicher sowie datenschutzrechtlicher Hinsicht vereinzelt weitere Anknüpfungspunkte für einen Schutz in Bezug auf Daten gewährt.

Auch trifft das Gesetz mittelbar über das Eigentum bzw. den (berechtigten) Besitz am Datenträger eine sachenrechtliche Zuordnung von Daten und begründet damit nicht nur Herausgabe- und Beseitigungs- bzw. Unterlassungsansprüche, sondern schafft damit zugleich eine zivilrechtliche Güterzuordnung, anhand derer Daten in vermögensrechtlicher Hinsicht ausschließlich einer Person zugeordnet werden.¹⁵⁰ Aufgrund dieser zivilrechtlichen Güterzuordnung der Daten ist der Berechtigte auch hinreichend in der Lage, insbesondere durch vertragliche Gestaltung, über die Nut-

zung und Verwendung „seiner“ Daten selbst zu entscheiden.

Dass das Gesetz diese (mittelbare) zivilrechtliche Zuordnung von Daten vorsieht, ist bei der Diskussion zur Verkehrsfähigkeit der in Daten enthaltenen Informationen zu berücksichtigen.¹⁵¹ Insbesondere bei der Diskussion, ob und in welchem Umfang ein Ausschließlichkeitsrecht an Daten zur Gewährleistung ihrer Verkehrsfähigkeit zu fordern ist, sollte die vom Gesetz getroffene zivilrechtliche Zuordnung von Daten mitbedacht werden.

149 Vgl. etwa *Hoeren*, MMR 2013, 486, 491 (Dateneigentum als „quasidringliches Recht mit Ausschlussfunktion [...] als ‚sonstiges Recht‘ i. S. d. § 823 Abs. 1 BGB“); *Redeker*, CR 2011, 634, 638 f. (das Rechtsgut „Information“ als ein mit dem Besitz vergleichbares Recht im Sinne von § 823 Abs. 1 BGB); *Meier/Wehlau*, NJW 1998, 1585, 1588 f. (Recht des EDV-Nutzers an seinem Datenbestand als sonstiges Recht im Sinn von § 823 Abs. 1 BGB).

150 A. A. *Specht*, CR 2016, 288, 289: „es existiert kein Recht, dass Daten in vermögensrechtlicher Hinsicht einer Person ausschließlich zuordnet“.

151 Zur Diskussion hinsichtlich der Verkehrsfähigkeit digitaler Güter, vgl. *Hauck/Hofmann/Zech*, ZGE/IPJ, 2016, 141 ff.; *Kerber*, ZGE/IPJ, 2016, 149 ff.; *Berger*, ZGE/IPJ, 2016, 170 ff.; *de la Durantaye/Kuschel*, ZGE/IPJ, 2016, 195 ff.; *Pahlow*, ZGE/IPJ, 2016, 218 ff.; *Becker*, ZGE/IPJ, 2016, 239 ff.; *Specht*, ZGE/IPJ, 2016, 289 ff.; *Obergfell*, ZGE/IPJ, 2016, 304 ff.

Christian F. Döpke, LL.M., LL.M., und Tim Jülicher*

Der Defikopter

Rechtliche Anforderungen an den Einsatz von Rettungsdrohnen

Mit telemedizinischen Assistenzsystemen und Defibrillatoren ausgestattete Rettungsdrohnen haben das Potential, die notfallmedizinische Versorgung – vor allem im ländlichen Raum – nachhaltig zu verbessern. Solche „Defikopter“ könnten schon in Kürze flächendeckend eingesetzt werden. Vor diesem Hintergrund untersuchen die Autoren die rechtlichen Anforderungen an einen rettungsdienstlichen Drohneneinsatz mit Blick auf das Luftverkehrs-, Haftungs-, Berufs- und Datenschutzrecht. Sie kommen zu dem Schluss, dass das Luftverkehrsrecht einem rechtskonformen Einsatz de lege lata entgegensteht.

I. Einleitung

Herr Frohsinn ist 82 Jahre alt und lebt in Ringelstein (Sauerland). Eines sommerlichen Nachmittages verspürt er einen stechenden Schmerz in der Brust und wird bewusstlos. Sein Herzmuskel pumpt nicht mehr richtig, sondern zuckt in hoher Frequenz – Symptome eines Kammerflimmerns, das unbehandelt binnen kürzester Zeit zum Tode führen kann.¹

Bei einem solchen Notfall zählt jede Minute, doch das nächste Krankenhaus ist kilometerweit entfernt. Die Rettungsdienstgesetze der Länder verlangen zwar, dass eine Notfallrettung nach Absetzen des Notrufs innerhalb von zehn bis zwölf Minuten gewährleistet sein muss.² Im Alltag kann diese sog. Hilfsfrist aber längst nicht immer eingehalten werden. Dies betrifft nicht nur ländliche Regionen mit

langen Anfahrtszeiten, sondern auch städtische Gebiete mit hohem Verkehrsaufkommen. Essentiell ist deshalb eine Verkürzung der Hilfsfrist durch lebensrettende Sofortmaßnahmen von Ersthelfern.

Bei einem Kammerflimmern hilft vor allem ein automatisierter externer Defibrillator (AED), der auch von Laien bedient werden kann. In Ringelstein gibt es einen solchen AED aber nicht.³ Abhilfe verspricht eine neue Erfindung: Die Defibrillator-Drohne. Im Folgenden soll der Versuch unternommen werden, das Potential dieser Erfindung mit Blick auf seine rechtliche Zulässigkeit zu beleuchten. Dazu wird zunächst die Funktionsweise der Drohne erläutert und anschließend ein Blick auf den maßgeblichen Rechtsrahmen geworfen.

* Der Beitrag beruht auf einer grundlegenden Überarbeitung des Vortrags und Tagungsbandbeitrags der Verfasser zur 17. DSRI-Herbstakademie; siehe *Döpke/Jülicher*, in: Taeger (Hrsg.), DSRTB 2016, S. 935 ff. Mehr über die Autoren erfahren Sie auf Seite III.

1 Die Überlebenswahrscheinlichkeit nimmt bei einem Kammerflimmern mit jeder Minute um 10 % ab, siehe *Klingenheben*, *Herzschrittmachertherapie & Elektrophysiologie* 2005, S. 78, 78.

2 Die Hilfsfrist liegt – je nach Definition des betreffenden Landes – zwischen acht bis zwölf Minuten, in dünn besiedelten Gebieten bei bis zu 15 (Bayern, Brandenburg, Rheinland-Pfalz) oder sogar 17 Minuten (Thüringen).

3 Die nächsten AED befinden sich nach ausgiebiger Recherche in Gesseke (20km) und Meschede (40km).