Studium Rechtswissenschaft

Prof. Dr. Barbara Völzmann-Stickelbrock

Modul 55100
Propädeutikum

Kurseinheit 3:
Data Literacy

Rechts-
wissenschaftliche
Fakultät

FernUniversität in Hagen

Der Inhalt dieses Studienbriefs wird gedruckt auf Recyclingpapier (80 g/m^2, weiß), hergestellt aus 100 % Altpapier.

Inhaltsverzeichnis

Zur Autorin

Der vorliegende Studientext wurde von Prof. Dr. Barbara Völzmann-Stickelbrock verfasst.
Die Autorin ist Inhaberin des Lehrstuhls für Bürgerliches Recht, Wirtschaftsrecht, Gewerblichen Rechtsschutz, Urheberrecht und Zivilprozessrecht an der FernUniversität in Hagen.

Einleitung

Niemand wird heute mehr bezweifeln, dass die Digitalisierung eine der wichtigsten gesellschaftlichen und wirtschaftlichen Entwicklungen unserer Zeit darstellt. Was auch immer man konkret im Auge hat, wenn man von digitalem Wandel oder digitaler Transformation spricht, von Big Data, dem Internet of Things oder Industrie 4.0. In jedem Fall geht damit immer eine massenhafte Datennutzung einher.

Den gewaltigen Chancen der Datennutzung für unterschiedlichste Bereiche Gesundheit, Umwelt und Klima, Energie, Verkehrs- und Städteplanung stehen dabei nicht nur technische und ökonomische, sondern auch rechtliche Herausforderungen und Risiken gegenüber.

Diese manifestieren sich in allen Bereichen des menschlichen Miteinanders, sei es bei der Entwicklung rechtlicher Rahmenbedingungen des autonomen Fahrens, bei Haftungsfragen im Bereich der künstlichen Intelligenz und der Diskussion um die Rechtsfähigkeit autonomer Softwareagenten als neue elektronische Personen (E-Person). Das Wettbewerbs- und Kartellrecht steht vor der Frage, wann regulierend eingegriffen werden muss, um eine Monopolisierung von Daten durch marktmächtige Unternehmen wie Amazon oder Google zu verhindern bzw. die Transparenz für den Verbraucher zu erhalten, wenn Algorithmen als Instrument der Preisbildung eingesetzt werden.

Unter dem Stichwort „Legal Tech" schreitet die Ersetzung juristischer Denkprozesse durch Maschinen voran, die einzelne Arbeitsschritte oder gar gesamte Rechtsberatungsbereiche übernehmen. Etablierte Märkte wie das Bankenwesen unterliegen im Zuge von „FinTech" disruptiven Veränderungen, gleiches gilt auch für die Versicherungswirtschaft („InsurTech"), die zunehmend Systeme zur automatischen Schadensregulierung entwickelt. Mit sog. „Smart Contracts", die Bedingungen eines Vertrages computerbasiert kontrollieren und einzelne Vertragsbestandteile automatisiert ausführen, soll Technologie, etwa nach dem Blockchain-Prinzip, als Garant für die Integrität und Verlässlichkeit der Daten das gegenseitige Vertrauen der Vertragspartner in ihre individuellen Absprachen ersetzen. Im Bereich des öffentlichen Rechts werden zunehmend dezentrale Datenbanken, etwa auf Basis der Blockchain diskutiert, z.B. als Ersatz für Grundbücher oder Handelsregister.

Alle diese Beispiele – und es gibt derer unzählig mehr – verdeutlichen, dass eine digitale Gesellschaft einen verlässlichen Rechtsrahmen für den rechtssicheren und grundrechtskonformen Umgang mit Daten braucht.

Data Literacy als die Fähigkeit, Daten auf kritische Art und Weise zu sammeln, zu managen, zu bewerten und anzuwenden, ist dabei eine zentrale Zukunftskompetenz. Diese zu vermitteln, stellt ganz neue Anforderungen an die Lehre, gerade weil es ein Querschnittsthema ist, das Fragestellungen ganz unterschiedlicher Fachdisziplinen vereint.

Dass diese unterschiedlichen Fachdisziplinen ihrerseits Daten nach ganz verschiedenen Kriterien kategorisieren, macht die Sache nicht leichter.

In den folgenden Kapiteln möchte ich Ihnen einen Einblick in einige der Rechtsfragen im Zusammenhang mit Daten geben und dabei hoffentlich den Blick dafür schärfen, ob und inwieweit

- das geltende Recht Leitlinien für die Datennutzung bereitstellt, anhand derer im digitalen Zeitalter neu auftretende Fragestellungen beantwortet werden können bzw.
- der Gesetzgeber aufgerufen ist, den Herausforderungen durch neue rechtliche Regelungen zu begegnen.

Teil 1 Der juristische Datenbegriff

A. Begriffsbestimmungen in den einzelnen Rechtsgebieten

Eine einheitliche juristische Definition, was unter Daten zu verstehen ist, existiert nicht, obwohl Rechtsfragen im Zusammenhang mit Daten an zahlreichen Stellen eine Rolle spielen. Gesetzliche Definitionen von Daten – sog. Legaldefinitionen – finden sich in ganz unterschiedlichen Normen auf dem Gebiet des Öffentlichen Rechts, des Strafrechts und des Zivil- und Wirtschaftsrechts.

I. Öffentliches Recht - Datenschutzrecht

Der in der öffentlichen Wahrnehmung wohl naheliegendste Bereich ist dabei das Datenschutzrecht. Personenbezogene Daten sind legaldefiniert in:

> Art. 4 Nr. 1 Halbsatz 1 DSGVO
>
> „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen"

Der datenschutzrechtliche Datenbegriff ist damit technikoffen und bezieht sich auf alle Formate sowie alle Speichermöglichkeiten.[1] Sein Zweck ist nicht der Schutz des Datums als Zeichen, sondern nach Art. 1 Abs. 1 DSGVO der Schutz von Informationen über natürliche Personen. Er ist Ausfluss des allgemeinen Persönlichkeitsrechts in Form des Rechts auf informationelle Selbstbestimmung.

Schutzgegenstand des Datenschutzrechts sind nur personenbezogene Daten. Nicht personenbezogene Daten können ohne Einschränkung verwertet werden. Die Abgrenzung voneinander ist aber nicht einfach, denn nach Art. 4 Nr. 1 Halbsatz 2 DSGVO ist maßgebend, ob eine natürliche Person direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Hierunter können etwa auch IP-Adressen oder technische Messdaten fallen, wenn mit diesen die Identifizierung einer Person möglich ist. Der Anteil der echten Rohdaten ist daher auch bei Entwicklungen im Bereich der KI wohl kleiner, als man das bislang angenommen hat.

Für die Bestimmung des Begriffs der „Daten" ist die DSGVO wenig hilfreich, da sie wegen ihres weiten Schutzbereichs Daten und Informationen begrifflich gleichsetzt.

---

1 Erwägungsgrund 15 zur DSGVO.

II. Strafrecht

Im Bereich des Strafrechts geht es vorrangig um den Schutz von Daten vor Datenveränderung. Strafrecht greift ein, wenn es um die Verletzung der Integrität der Daten geht. Gegen Verfälschung wird auf strafrechtlichem Weg über § 303a Schutz gewährt. Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Daten finden weiterhin Erwähnung im Bereich des Computerbetrugs in § 263a und den §§ 268-270 StGB, die sich u.a. mit der Fälschung von technischen Aufzeichnungen und im Bereich der Datenverarbeitung beschäftigen.

Der zweite Aspekt des Schutzes ist der Geheimnisschutz. Er erfolgt strafrechtlich in § 203 StGB, der den Geheimnisverrat sanktioniert, sowie in den neueren Regelungen der §§ 202a-d zum Ausspähen und Abfangen von Daten sowie der Datenhehlerei. In all diesen Fällen geht es um Fälle, in denen sich jemand unzulässig Daten verschafft, sei es durch Softwarediebstahl, aber auch durch unbefugten Zugang zu besonders gesicherten Daten unter Überwindung von Sicherheitsvorkehrungen, d.h. durch das „Hacken" von Computern.

Daten sind in diesem Bereich im zweiten Absatz einer Norm genannt, die das Ausspähen von Daten unter Strafe stellt. Hierauf verweisen die meisten anderen Strafrechtsnormen.

> § 202a Abs. 2 StGB
>
> Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Der Begriff ist relativ eng und erfasst nur maschinenlesbare, codierte Angaben, aus denen erst durch bestimmte kognitive Vorgänge dann Informationen werden. Dabei handelt es sich daher nicht um eine Legaldefinition für jede Art von Daten im Strafrecht, sondern vielmehr nur um eine normbezogene Begriffsanpassung. Ansonsten gilt aber ein allgemeinerer Datenbegriff, der Daten als „durch Zeichen oder kontinuierliche Funktionen kodierte Informationen"[2] beschreibt, also gleichfalls Daten und Informationen einander annähert.

III. Zivilrecht

In den beiden zuvor genannten Bereichen werden Daten über Abwehrrechte gegenüber Eingriffen geschützt. Das Zivilrecht tut sich mit der Einordnung von Daten schwerer. Je nach Regelungs- und Schutzzweck der entsprechenden Normen kann es um Daten im Sinne der DSGVO gehen, aber auch um bloße maschinenlesbare, codierte Angaben. Ersteres gilt etwa für den Umgang mit Arbeitnehmerdaten im Bereich des Arbeitsrechts oder den Zugriff der Erben oder Angehörigen auf die Daten des/r Verstorbenen in sozialen Netzwerken.

Eine klare Zuweisung von Daten zu einer bestimmten Kategorie ist aber oftmals kaum möglich, was auch daran liegt, dann man nach ganz unterschiedlichen Aspekten differenzieren kann.

Neben der Unterscheidung nach personenbezogenen und nicht personenbezogenen Daten, ist die Unterscheidung *nach dem semantischen Inhalt* gängig, wobei man aus juristischer Sicht dann

---

2 DIN-Norm 44300 Nr. 19, 1972.

zumeist unterscheidet zwischen Daten, die sich auf natürliche Personen beziehen, Daten, die sich auf juristische Personen (Unternehmen) beziehen und unter die etwa auch Geschäftsgeheimnisse gefasst werden und reinen Sach- oder Rohdaten. Letztere stehen in keinem unmittelbaren Bezug zu Menschen oder Unternehmen, etwa Maschinen-, Industrie- oder Sensorikdaten.

Andere Differenzierungen beziehen sich auf die *Art der Schöpfung* der Daten und unterscheiden zwischen vom Nutzer[3] freiwillig gelieferten – nutzergenerierten - Daten, z. B. bei seiner Registrierung für einen bestimmten Dienst oder beim Klicken eines Like-Buttons und maschinengenerierten Daten, die von den Dienstleistern selbst erstellt werden, z. B. als Nutzungs- oder Bewegungsprofile mittels Internet-Logs und Cookies.[4]

Weitere denkbare Einteilungen betreffen etwa die Aktualität der Daten (Echtzeitdaten oder historische Daten), die Aufbereitung (strukturierte, halbstrukturierte und unstrukturierte Daten) oder den Einsatzzweck.

Wie schwierig die Abgrenzung und wie groß der „Graubereich" rechtlich nicht eindeutig einer bestimmten Kategorie zuzuordnender Daten ist, zeigt sich beispielhaft im vieldiskutierten Bereich der Datennutzung im Automobilsektor.

Im Fahrzeug anfallende Datenarten – die Übergänge sind fließend:[5]

- Fahrzeugkennung (z.B. Kfz-Kennzeichen)
- technische Fahrzeugeigenschaften (z.B. Reifendruck, Kilometerstand, Füllstände, Fehlerprotokolle)
- Bewegungsdaten (z.B. Strecke, Geschwindigkeit, Pausen, Anzahl der Insassen)
- Merkmale des Fahrers (z.B. biometrische Daten für Authentifikation oder Müdigkeitserkennung, Passwörter)
- Fahrverhalten (z.B. Lenkbewegungen, Beschleunigung, Auffahrverhalten)
- Komfortfunktionen und Servicenutzung (z.B. Sitzeinstellungen, Internetnutzung oder eingestellte Radiosender)
- Umfeldinformationen (z.B. Witterungsbedingungen, Straßenverhältnisse, Verkehrsaufkommen, Fahrzeuge in der Nähe)

Die verschiedenen Datenarten zeigen, dass doch die meisten der von Fahrzeugen erhobenen und gesammelten Daten als solche einzuordnen sind, die sich über einen Account, über Zertifikate oder Standortdaten auf den Fahrzeughalter oder den Fahrer rückbeziehen lassen.

---

3 Der Text verwendet aus Gründen der Verständlichkeit - ebenso wie die genannten Normen - das generische Maskulinum. Er soll aber jeden Menschen (weiblich/männlich/divers) ansprechen. Stereotype Rollenbilder in den Fallgestaltungen wurden nach Kräften vermieden.

4 Hierzu näher *Körber,* NZKart 2016, 303, 304.

5 Übersicht bei *Klinck-Straub/Straub*, ZD 2018, 459, 460.

B. Literatur zur Wiederholung und Vertiefung

Bernhardt, Lea, Algorithmen, Künstliche Intelligenz und Wettbewerb, NZKart 2019, 314 ff.

Börding, Andreas; Jülicher, Tim; Röttgen, Charlotte; v. Schönfeld, Max, Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, CR 2017, 134 ff.

Borges, Georg, Rechtliche Rahmenbedingungen für autonome Systeme, NJW 2018, 977 ff.

Ehlen, Theresa; Brandt, Elena, Die Schutzfähigkeit von Daten – Herausforderungen und Chancen für Big Date Anwender, CR 2016, 570 ff.

Galetzka, Christian; Garling, Sophie; Partheymüller, Johannes, Legal Tech – "smart law" oder Teufelszeug? MMR 2021, 20 ff.

Günther, Jens; Böglmüller, Matthias, Künstliche Intelligenz und Roboter in der Arbeitswelt, BB 2017, 53 ff.

Haupt, Tino, Auf dem Weg zum autonomen Fahren, NZV 2021, 172 ff.

Haupt, Tino, Die Verordnung zum Gesetz zum autonomen Fahren, NZV 2022, 166 ff.

Hilgendorf, Eric, Automatisiertes Fahren und Recht – ein Überblick, JA 2018, 801 ff.

Jakl, Bernhard, Das Recht der Künstlichen Intelligenz – Möglichkeiten und Grenzen zivilrechtlicher Regulierung, MMR 2019, 711 ff.

Klinck-Straub, Judith; Straub, Tobias, Vernetzte Fahrzeuge – portable Daten, ZD 2018, 459 ff.

Körber, Thorsten, „Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, „Datenmacht" und Kartellrecht – Teil 1, NZKart 2016, 303 ff.

Meyer, Stephan, Künstliche Intelligenz und die Rolle des Rechts für die Innovation, ZRP 2018, 233 ff.

Preuß, Nicola, Digitaler Nachlass – Vererbbarkeit eines Kontos bei einem sozialen Netzwerk, NJW 2018, 3146 ff.

Söbbing, Thomas, FinTechs: Rechtliche Herausforderungen bei den Finanztechnologien der Zukunft, BKR 2016, 360 ff.

Spindler, Gerald, Roboter, Automation, künstliche Intelligenz, selbststeuernde Kfz – Braucht das Recht neue Haftungskategorien? CR 2015, 766 ff.

Völzmann-Stickelbrock, Daten in Zwangsvollstreckung und Insolvenz, Festschrift für Jürgen Täger, 2020, 749 ff.

Weichert, Thilo, Der Personenbezug von Kfz-Daten, NZV 2017, 507 ff.

Wendehorst, Christiane, Die Digitalisierung und das BGB, NJW 2016, 2609 ff.

Zech, Herbert, Künstliche Intelligenz und Haftungsfragen, ZfPW 2019, 198 ff.

Teil 2 Rechte an Daten im Zivilrecht

A. Grundlagen

„Meine Daten gehören mir!" – das hört man häufiger, aber stimmt das auch so bzw. was verbirgt sich letztlich dahinter?

Beinhaltet das nur die Befugnis, andere vom Zugriff auf die eigenen Daten abzuhalten oder auch positive Befugnisse, etwa die eigenen Daten „zu Geld" zu machen?

Dass Daten das neue „Öl", der „Treibstoff für die digitale Wirtschaft" sind, wird an vielen Stellen als Beispiel für die große Bedeutung angeführt, die den Daten beigemessen wird.[6] So ganz passt der Vergleich nicht, denn Daten lassen sich im Unterschied zu Öl beliebig oft verwerten, denn anders als physische Rohstoffe, nutzen sich Daten nicht ab. Während ein Barrel Rohöl nur ein einziges Mal verkauft und verarbeitet werden kann, können Daten potentiell mehrfach veräußert und (gleichzeitig) in unterschiedlichen Anwendungen verarbeitet werden.

In jedem Fall ist eine Eigentumszuordnung bei Daten viel schwieriger als bei Öl als einer körperlichen Sache. Denn um als ein Rechtsgut im Sinne des Zivilrechts Gegenstand von Rechtsgeschäften zu sein, müssen Daten abgrenzbar und übertragbar sein.

Das Zivilrecht kennt einerseits „Sachen" und andererseits „Rechte".

Sachen im Sinne des Gesetzes sind nach § 90 BGB nur körperliche Gegenstände. Mangels Körperlichkeit handelt es sich bei Daten mithin nicht um Sachen.

Bei den Rechten gibt es einen festen Katalog, einen sog. „numerus clausus" dinglicher Rechte, wobei hier vor allem die Immaterialgüterrechte (Patent, Gebrauchsmuster, Design, Marke und Urheberrecht) in Betracht kommen. Zwar können Daten, die eine persönliche geistige Schöpfung beinhalten, durch das UrhG geschützt sein. Weiter spielt im Urheberrecht der Schutz von Datenbanken eine erhebliche Rolle.[7] Daten als solche, insbesondere Rohdaten, fallen aber in diese Kategorie nicht ohne weiteres. Bei ihnen fehlt es naturgemäß bereits an einer bestimmten natürlichen Person, die als Urheber der Daten identifiziert werden könnte, jedenfalls aber an der schöpferischen Leistung.

B. Zuordnung von Daten

In der Geschichte stand das Recht schon öfter vor der Situation, über die Zuordnung neuer werthaltiger Güter entscheiden zu müssen, die erst durch neue Technologien entstanden sind, man denke etwa an die Elektrizität oder in jüngerer Zeit an Internet-Domains, die ebenfalls wie Wirtschaftsgüter gehandelt werden.

---

6 Z.B. *Moos/Arning/Schefzig*, K&R 2015, 2.

7 Siehe dazu näher unter Datenarchivierung/Datenmanagement im Teil 3 Schutz von elektronischen Datenbanken durch das Urheberrecht.

Zahlreiche Stimmen aus Wissenschaft, Wirtschaft und Gesellschaft haben sich zu der Frage eines sog. „Data Ownership" geäußert. Bis heute gibt es aber weder in der Wissenschaft, noch in Berlin oder Brüssel eine klare Antwort auf die Frage, wem welche Rechte an Daten zustehen sollen.

Diese Tatsache dürfte nicht mangelnden Anstrengungen oder Ideen, sondern vielmehr der Erkenntnis geschuldet sein, dass es angesichts der Komplexität der Problemstellungen eine einfache und allgemeingültige Lösung schlichtweg nicht gibt.

Die Schwierigkeiten beginnen bereits bei der Frage, wer denn letztlich als der sog. „Data Owner" zu ermitteln ist. Verschiedene Vorschläge haben sich dabei als nicht tragfähig erwiesen.

- Keine Lösung bringt es, wie bei Sachen, auf das Eigentum am Datenträger abzustellen. Dagegen spricht zum einen die weitgehend dezentrale Speicherung von Daten, denn wenn Daten auf einem „fremden" Datenträger gespeichert werden, können sie hierdurch nicht in das Eigentum des Sacheigentümers übergehen. Besonders deutlich wird das bei Cloud-Dienstleistungen, wo der Eigentümer des Servers in keiner Beziehung zu den darauf gespeicherten Daten steht.
- Auch der Dateninhalt ist kein taugliches Kriterium. Die Anknüpfung am Dateninhalt als schutzfähiges Werk versagt bei den ohne geistige Leistung erzeugten Messdaten. Aber auch bei personenbezogenen Daten würde der Urheberschutz überdehnt, wenn jedes Datum unabhängig von der Schöpfungshöhe dem Urheberschutz unterläge.
- Damit bleibt nur die Möglichkeit, beim *Datenerzeuger* anzuknüpfen – aber wer ist das? Teilweise stellt man nur technisch auf die Codierung der Daten ab, den sog. „Skripturakt", der die unmittelbare Erstellung und Speicherung der Daten auslöst.[8] Das berücksichtigt aber nicht, wer wirtschaftlich für die Datenerstellung verantwortlich ist und die Kosten für die Entwicklung, die Produktion und die laufenden Kosten für den datengenerierenden Gegenstand und den benötigten Speicherplatz trägt. Der Datenerzeuger muss folglich im Einzelfall aus einer kombinierten Betrachtung mehrerer tatsächlicher, rechtlicher und ökonomischer Indizien ermittelt werden.

Im Beispiel des vernetzten Kfz zeigt sich sehr schnell die Komplexität derartiger Überlegungen.

Zu den verschiedenen, im vernetzten Kfz anfallenden Datenarten siehe das Beispiel im Teil 1.

1. Mögliche Zuordnungsberechtigte sind etwa:

- Automobilhersteller,
- Vertragshändler,
- Zulieferer,
- Werkstätten- und Pannenhilfsdienste
- Fahrer, Halter und Eigentümer (vor allem im Fall des Leasings abweichend)
- Sachverständige und staatliche Stellen (Bußgeldstellen, Strafverfolgungsbehörden, Gerichte)
- Kfz-Versicherungen
- Serviceprovider und sonstige Diensteanbieter

8 *Hoeren,* MMR 2013, 486 ff.

2. Als datenrelevante Vorgänge kommen beispielsweise in Betracht:

- lokale Generierung und Speicherung von Daten durch Fahrzeugsysteme
- Transfer von Daten aus Fahrzeugsystemen zum Hersteller und von da ggf. zu weiteren Dritten
- Empfang und Speicherung von Daten durch andere Verkehrsteilnehmer, Verkehrsinfrastrukturbetreiber, Mobilitätsdiensteplattformen (z.B. Fahrdienste- oder Carsharing-Anbieter)

Ausgehend von durchschnittlich 80 elektronischen Geräten pro Pkw, mit steigender Tendenz wächst die Menge der in einem Kfz erhobenen Daten und die Zahl der verschiedenen hieran Interessierten stetig an.

Einfache Lösungen gibt es daher kaum. So gehören personenbezogene Fahrerdaten zwar sicherlich dem Fahrer, ebenso wie selbst eingebrachte Nutzungsdaten wie Navigationsziele, Adress- oder Telefondaten. Denkt man an Carsharing-Fälle, Mietwagen etc. stellt sich die Frage des Zugriffs aber schon als schwierig dar. Fahrzeugzustandsdaten können je nach Konstellation dem Halter, dem Eigentümer oder ggf. auch dem Fahrer zugeordnet werden, etwa wenn es um Rückschlüsse auf einen bestimmten Fahrstil geht. Wie greift aber eine dieser Personen auf die Daten zu, wenn sich diese auf einem Datenträger befinden, den der Hersteller durch Zugriffsschutzmechanismen geschützt hat oder diese unmittelbar auf dessen Servern gespeichert werden? Zwar hat der Eigentümer das Kfz einschließlich der Datenverarbeitungsgeräte erworben, der Hersteller hat diese jedoch eingebaut und er stellt ihre Funktionsfähigkeit sicher, zudem haftet er auch im Rahmen der Gewährleistung für Fehler des Fahrzeugs, ist daher an den Daten interessiert, um die Fahrzeuge weiterzuentwickeln und die Beweise für Haftungsfälle zu sichern. Die Fernüberwachung des Fahrzeugzustands dient aber auch dem Fahrer, der so auf dringende Reparaturen und notwendige Wartung hingewiesen werden kann. Im Rahmen der Wartung und Reparatur sind wiederum die Werkstätten auf die Ergebnisse der Diagnosegeräte angewiesen, wobei freie Werkstätten in der Regel keinen Zugriff auf die Daten haben.

Das Bundesministerium für Verkehr und digitale Infrastruktur hat in einer umfangreichen Fallstudie zu einer „Eigentumsordnung für Mobilitätsdaten“[9] verschiedene Zuordnungen vorgeschlagen. So sollen etwa die lokal in Fahrzeugsystemen gespeicherten Daten dem Eigentümer des Kfz zuzuordnen sein, weil der Aufwand des jeweiligen Fahrers bei maschinengenerierten Daten zu vernachlässigen und Investitionen des Herstellers typischerweise mit dem Kaufpreis abgegolten seien. Ganz davon abgesehen, dass damit die rechtliche Zuordnung rein von einer technischen Umsetzung – nämlich der lokalen oder dezentralen Datenspeicherung – abhängig gemacht wird, entspricht eine solche Zuordnung jedenfalls nicht der derzeitigen Rechtswirklichkeit. Der Zugang zu den Fahrzeugdaten und die Datenhoheit, um eine Freigabe an Dritte zu steuern und von der Vermarktung für datenbasierte Geschäftsmodelle zu profitieren, liegt derzeit bei den Herstellern.

9 https://www.uni-kassel.de/fb07/index.php?eID=dumpFile&t=f&f=4043&token=5408d0e9eac3fa0fda9271f06e5d67cc84b646e8

C. Dateneigentum

Ein Dateneigentum, das die Daten mit Wirkung gegenüber jedermann einer bestimmten Person zuweist, könnte nicht nur bei den Fahrzeugdaten die selbstbestimmte Nutzung des Fahrzeugeigentümers ermöglichen, sondern auch in vielen anderen Bereichen für klarere Lösungen sorgen. Ein solches Recht kann mangels Sachqualität der Daten letztlich nur durch den Gesetzgeber geschaffen werden.

Gegen seine Einführung bestehen aber erhebliche Bedenken. Denn der Vermögenswert von Daten wird nicht durch das Recht, sondern vorrangig durch die Marktverhältnisse bestimmt. Schafft man mit dem Dateneigentum ein Ausschließlichkeitsrecht, das die Daten bei einer bestimmten Person monopolisiert, greift man damit in den Markt ein. Ein solcher Eingriff in den Markt ist da notwendig, wo nur auf diese Weise Innovationsschutz gewährt werden kann.[10] Das ist etwa das Prinzip des Patentrechts - Innovation kann nur stattfinden, wenn sicher ist, dass die Kosten, die in die Entwicklung geflossen sind, sich durch die Zuweisung des Rechts für eine bestimmte Zeit amortisieren. Eine solche Anknüpfung an den Amortisationskosten würde daher eher auf die Hersteller von Datenverarbeitungssystemen als „Eigentümer" der Daten abzielen – ein Konzept, das wiederum mit dem Schutz personenbezogener Daten und den damit verbundenen Abwehrrechten natürlicher Personen nur schwer in Einklang zu bringen wäre.

Bei der Schaffung von rechtlichen Rahmenbedingungen für ein Datenrecht ist man daher auf politischer Ebene, von dem Gedanken eines Dateneigentums inzwischen weitgehend wieder abgerückt.[11] Für den gesamten Bereich des Datenwirtschaftsrechts herrscht die Auffassung vor, dass die Schaffung eines absoluten Rechts, das andere Parteien von der Nutzung der Daten ausschließt, eher einen Hemmschuh für Innovationen darstellt. Insbesondere fürchtet man, ohne die Möglichkeit von Big Data Analysen auf dem zukunftsträchtigen Markt der künstlichen Intelligenz ins Hintertreffen zu geraten.

Der ursprüngliche Gedanke, ein Eigentumsrecht an Daten auf europäischer Ebene zu schaffen, wird daher von der Europäischen Kommission nicht mehr weiterverfolgt. Beim Aufbau einer Europäischen Datenwirtschaft setzt man deshalb auch im Bereich der Roh- und Maschinendaten vielmehr auf das Prinzip des „free flow of non personal data"[12]. Das anstelle eines Dateneigentums angedachte „Datenproduzentenrecht" wird in der Literatur weiter intensiv diskutiert,[13] Schritte zu einer Umsetzung, die sich etwa am bestehenden Datenbankherstellerrecht des UrhG orientieren könnte,[14] wurden aber seit 2017 nicht unternommen.

---

10 Als Alternative wird ein Leistungsschutzrecht des Datenerzeugers diskutiert, das dem Datenbankherstellerrecht des UrhG nachgebildet wird und das auf einer niedrigeren Schwelle als das Dateneigentum einen Investitionsschutz gewährt – siehe hierzu auch Teil 4: Datenbankrecht

11 https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf

12 COM/2017/0495 final 2017/0228 (COD) – Vorschlag für eine Verordnung über einen Rahmen für den freien Verkehr nicht personenbezogener Daten, Art. 1.

13 Hierzu vor allem *Wiebe,* CR 2017, 87 ff. und bereits *Zech,* CR 2015, 137 ff.

14 *Wiebe,* GRUR 2017, 338 ff., siehe dazu auch Teil 3 – Der Schutz elektronischer Datenbanken.

D. Datenmacht

Ist mithin – jedenfalls in nächster Zeit – eine absolute Zuordnung von Daten an bestimmte Personen nicht zu erwarten, bleibt es bei der auch heute bereits vielgenutzten Möglichkeit der Beteiligten, über schuldrechtliche Vereinbarungen die Zuordnung der Daten zu regeln, die anders als das Eigentum nicht absolut, sondern nur relativ zwischen den jeweiligen Vertragsparteien gelten.

Allerdings liegen Daten heute vorwiegend in der Cloud und auf sich ständig ausbreitenden marktmächtigen Plattformen. Man kann daher daran zweifeln, ob in solchen multipolaren Rechtsbeziehungen das auf Zweipersonenverhältnisse zugeschnittene Vertragsrecht wirklich noch hinreichenden Schutz gewährleistet. In der Praxis entscheidet vielfach die faktische, technische Zugriffsmöglichkeit auf die Daten[15] darüber, wer die Vertragsbedingungen vorgibt. Dem Vertragspartner bleibt nur noch die Möglichkeit, auf diese Bedingungen einzugehen oder vom Vertragsschluss Abstand zu nehmen.

Angesichts dieser Gefahren wird die Forderung nach sektorspezifischen kartellrechtlichen Regelungen erhoben, die einer Monopolisierung der Daten durch Großunternehmen wie Google oder Facebook Einhalt gebieten, den Datenhandel regulieren und diese zur „Herausgabe" der von Ihnen erhobenen Daten verpflichten sollen.[16]

E. Daten als Gegenleistung

In der digitalen Welt können die im Zusammenhang mit einem bestimmten Vertrag oder Nutzungsvorgang generierten Daten weit über den ursprünglichen Kontext hinaus Bedeutung erlangen.[17] Die systematische Auswertung großer, automatisiert und als Nebenprodukt der Maschinennutzung oder der Interaktion von Menschen und Maschinen erzeugter Datenmengen lässt vielfältige, ökonomisch wertvolle Verwendungsmöglichkeiten zu. Nutzungs- und Nutzerprofile können u.a. gezielt zu Werbezwecken eingesetzt werden.

Im Fallbeispiel des vernetzten Kfz verdeutlicht das etwa eine Untersuchung des ADAC zur Datenauswertung und -übertragung.[18] Anhand von Daten zu Strecken, Fahrstil und Fahrer können konkrete Nutzungsprofile erstellt werden, die beispielsweise auflisten:

- die gefahrenen Kilometer auf Autobahn, Landstraße und in der Stadt
- die Anzahl der einzelnen Fahrtstrecken, aufgeschlüsselt nach Kilometern
- die Lade- und Entladezyklen mit Uhrzeit, Datum, Kilometerstand
- die Einsatzdaten des Elektro- bzw. Verbrennermotors bei Plug-in-Hybriden
- die Betriebsstunden der Fahrzeugbeleuchtung, getrennt nach einzelnen Lichtquellen
- die Zahl der elektromotorischen Gurtstraffungen, um festzustellen, wie oft heftig

15 Diese wird teilweise als „Datenhoheit" bezeichnet, passender ist der Begriff der „Funktionsherrschaft".

16 Zur Entwicklung auf europäischer Ebene *Steinrötter*, RDi 2021, 480, 484 f.

17 Umfassend hierzu *Schweitzer,* GRUR 2019, 569, 570.

18 https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsysteme/daten-modernes-auto/

gebremst wird
- die Einträge für zu hohe Motordrehzahl oder -temperatur
- die Dauer, wie lange der Fahrer die verschiedenen Modi des Automatikgetriebes (Manuell/Sport) nutzt
- die Zahl der Verstellvorgänge des elektrischen Fahrersitzes
- die Anzahl der eingelegten Medien in das CD-/DVD-Laufwerk
- die Dauer und den Zeitpunkt der Telefongespräche

Dass ganz unterschiedliche Adressaten an solchen Informationen Interesse haben, wird dabei ebenso deutlich wie der Umstand, dass Fahrer, Halter und/oder Eigentümer ein berechtigtes Interesse daran haben können, dass diese – überwiegend personenbezogenen Daten nicht weitergegeben werden.

Allerdings lässt sich in diesem Bereich ein gewisses Paradoxon erkennen. Während einerseits im Bereich der Nutzung personenbezogener Daten als Wirtschaftsgut zu Recht auf das Datenschutzrecht verwiesen wird, gehen viele Verbraucher andererseits mit ihren persönlichen Daten sehr freizügig um. Daten werden dabei verbreitet als Tauschmittel für digitale Inhalte oder vermögenswerte Vorteile im E-Commerce eingesetzt.

Um die Rechte von Verbraucherinnen und Verbrauchern zu schützen, hat der nationale Gesetzgeber zum 1.1.2022 neue Regelungen für Verträge über digitale Produkte in das BGB aufgenommen.[19] Das Gesetz markiert nicht nur den „Beginn des digitalen Zeitalters im BGB"[20], sondern verzahnt auch erstmalig Vertragsrecht und Datenschutzrecht. Der Anwendungsbereich beschränkt sich allein auf personenbezogene Daten, die erstmals in § 327 Abs. 3 BGB als Gegenleistung eines Vertrags ausdrücklich anerkannt werden. Sofern Verbraucher digitale Angebote wie Video-, Audio- oder Musikdateien, digitale Spiele, elektronische Bücher oder ähnliches in Anspruch nehmen, die in einer Cloud-Computing-Umgebung oder in sozialen Medien zur Verfügung gestellt werden, gelten vertragliche Rechte wie z.B. die Möglichkeit des Rücktritts, der Nacherfüllung oder der Minderung wie beim Kauf körperlicher Sachen. Dies gilt nicht nur für den Fall, dass hierfür ein Preis gezahlt wird, sondern auch dann, wenn die Gegenleistung ganz oder teilweise in der Zurverfügungstellung von personenbezogenen Daten besteht.

Der erste Schritt hin zu einer rechtlichen Anerkennung des ökonomischen Werts von Daten ist damit getan. Wie dieser Wert letztlich im konkreten Fall zu bemessen ist, wird der Markt bestimmen. Für den Gesetzgeber bleibt weiterhin zu erwägen, ob eine Anerkennung von Daten als Gegenleistung künftig auch
(1) für nicht-digitale Produkte,
(2) für nicht-personenbezogene Daten und
(3) für andere Personen als Verbraucher gelten soll.[21]

19 Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen vom 25.06.2021, BGBl. 2021 I 2123 ff.

20 So *Schmitz/Buschuew*, MMR 2022, 171.

21 Hierzu *Mischau*, ZEuP 2020, 335, 353 ff.

F. Literatur zur Wiederholung und Vertiefung

Bittner, Lydia, Verträge über digitale Produkte – der Beginn des digitalen Zeitalters im BGB, VuR 2022, 9 ff.

Brisch, Klaus; Müller-ter-Jung, Marco, Plädoyer für eine zentrale Verwertbarkeit der Daten aus dem digitalisierten Auto im Zivilprozess, CR 2016, 411 ff.

Fezer, Karl-Heinz, Dateneigentum, MMR 2017, 3 ff.

Hoeren, Thomas, Dateneigentum – Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 ff.

Hornung, Gerrit; Goeble, Thilo, „Data Ownership im vernetzten Automobil, CR 2015, 265 ff.

Kornmeier, Udo; Baranowski, Anne, Das Eigentum an Daten – Zugang statt Zuordnung, BB 2019, 1219 ff.

Markendorf, Merih, Recht an Daten in der deutschen Rechtsordnung, ZD 2018, 409 ff.

Metzger, Axel, Digitale Mobilität – Verträge über Nutzerdaten, GRUR 2019, 129 ff.

Mischau, Lena, Daten als „Gegenleistung" im neuen Verbrauchervertragsrecht, ZEuP 2020, 335 ff.

Moos, Flemming; Arning, Marian Alexander; Schefzig, Jens, Daten als Geschäftsmodell – rechtliche Herausforderungen und Gestaltungsanforderungen im Übergang zum Datenzeitalter, K&R 2015, 2 ff.

Paal, Boris, Daten und Kartellrecht, NZKart 2018, 157 ff.

Roßnagel, Alexander, Fahrzeugdaten – wer darf über sie entscheiden? SVR 2014, 281 ff.

Schmitz, Barbara; Buschuew, Ellen, (Be-)Zahlen mit Daten, MMR 2022, 171 ff.

Schweitzer, Heike, Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, 569 ff.

Steinrötter, Björn, Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts, RDi 2021, 480 ff.

Stender-Vorwachs, Jutta; Steege, Hans, Zivilrechtliche Analyse zur Notwendigkeit eines dinglichen Eigentums an Daten, der Datenzuordnung und des Datenzugangs, NJOZ 2018, 1361 ff.

Wiebe, Andreas, Von Datenrechten zu Datenzugang – Ein rechtlicher Rahmen für die europäische Datenwirtschaft, CR 2017, 87 ff.

Zech, Herbert, Daten als Wirtschaftsgut – Überlegungen zu einem Recht des Datenerzeugers, CR 2015, 137 ff.

Teil 3 Der Schutz elektronischer Datenbanken durch das UrhG

A. Bedeutung

Datenbanken, insbesondere elektronische Datenbanken, haben in den vergangenen Jahrzehnten einen enormen Bedeutungszuwachs erfahren. Sie liegen Suchmaschinen aller Art zugrunde und durchziehen alle Lebensbereiche, sei es in Form von Flug- oder Automobilbörsen, Immobilienmärkten, Preisvergleichsportalen, Fahrplänen etc.

Ebenso benötigten alle Banken, Versicherungen, und jedes Internet-Unternehmen mit Bestellungen, von der Lagerverwaltung bis zum Rechnungswesen Datenbanken als unverzichtbare Grundlage seiner Geschäftstätigkeit. Auch soziale Netzwerke aller Art würden ohne die Nutzung von Datenbankfunktionen gar nicht funktionieren. Für Studierende hat sich die Möglichkeit der Literaturrecherche durch die elektronischen Angebote von Verlagen deutlich verbessert.

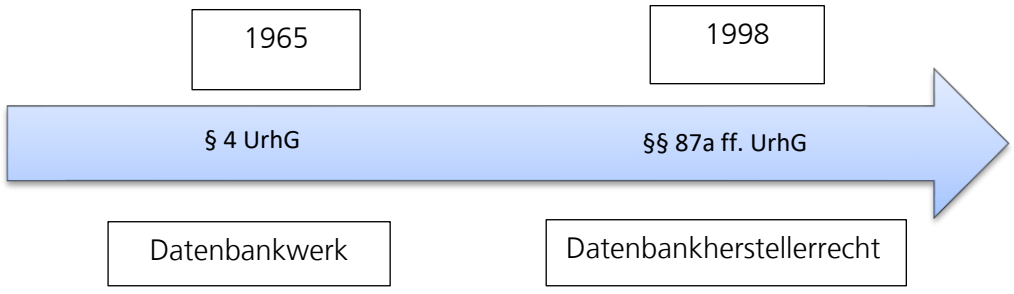
Es ist offensichtlich, dass mit der Erstellung und Pflege elektronischer Datenbanken ein erheblicher Kostenaufwand verbunden ist. Über deren Schutz besteht trotzdem vielfach Unsicherheit. Neben dem Wettbewerbsschutz, der hier naturgemäß ebenfalls eine große Rolle spielt, hält das UrhG zwei verschiedene Schutzsysteme für Datenbanken bereit.

B. Begriff der Datenbank

Es gilt ein weiter Datenbankbegriff, der als gemeinsame Voraussetzung von § 4 UrhG und §§ 87a UrhG nach Art. 1 Abs. 2 DatenbankRL vollharmonisiert ist.
Als Datenbank schutzfähig sind danach:

- Sammlungen von Werken, Daten oder anderen unabhängigen Elementen,
- die systematisch und methodisch angeordnet und
- einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind.

C. Die verschiedenen Schutzmechanismen



I. Werkschutz nach § 4 UrhG

Um einen Schutz als Datenbankwerk nach § 4 UrhG zu genießen, muss der Urheber mit der Auswahl oder Anordnung eine eigene geistige Schöpfung vollbracht haben. In die Sammlung können nicht nur Werke im urheberrechtlichen Sinne, sondern auch jegliche Art wahrnehmbaren Materials, etwa Texte, Töne, Bilder, Zahlen und Daten eingestellt werden. Der EuGH bejaht die erforderliche Originalität dann, wenn der Urheber bei der Auswahl und Anordnung freie und kreative Entscheidungen trifft und der Datenbank damit eine persönliche Note verleiht. Fußballspielpläne sind danach beispielsweise nicht als Datenbankwerk schutzfähig, weil technische Erwägungen, Regeln oder Zwänge keine künstlerische Freiheit bei der Erstellung lassen, auch wenn dabei ein erheblicher Arbeitsaufwand und bedeutende Sachkenntnis erforderlich waren.

Sofern ein Schutz zu bejahen ist, ist der Urheber vor einem Eingriff in alle Verwertungsrechte geschützt, insbesondere kann er sich gegen eine Vervielfältigung und öffentliche Zugänglichmachung der Datenbank durch Dritte zur Wehr setzen. Allerdings erfüllt auf der Basis dieser strengen Kriterien kaum eine Datenbank den Werkcharakter.

II. Schutz „sui generis“ – Das Datenbankherstellerrecht der §§ 87a ff. UrhG

Dass der Werkschutz für Datenbanken unzureichend ist, hat man auf europäischer Ebene schon recht früh erkannt und im Rahmen der EG-Datenbankrichtlinie - für das Jahr 1998 sehr fortschrittlich - ein eigenes übertragbares Immaterialgüterrecht für den Hersteller einer Datenbank geschaffen, welches der Gesetzgeber in §§ 87a ff. UrhG umgesetzt hat.

1. Schutzgegenstand

Geschützt wird durch dies Vorschriften das Amortisationsinteresse des Datenbankherstellers sowie die in der Datenbank verkörperte wesentliche Investition von Kapital oder Arbeit bei der Beschaffung, Überprüfung oder Darstellung der Daten.

Es war und ist für das deutsche UrhG eigentlich systemfremd, nicht die schöpferische Leistung, sondern die Investition zu schützen. Aber die Entwicklung der letzten Jahre zeigt anhand von ähnlichen Regelungen, z. B. zum Leistungsschutzrecht für Presseverleger, um diese vor den großen Suchmaschinen zu schützten, dass sich das UrhG von seinem Blickwinkel des Kreativschutzes mehr und mehr löst und auch handfeste wirtschaftliche Interessen bedient.

2. Schutzvoraussetzungen

a) Datenbank

Ebenso wie bei § 4 UrhG muss es sich zunächst um eine Datenbank in Sinne der genannten Definition handeln.

b) Investition

Für die Zwecke der Beschaffung, Überprüfung oder Darstellung der Daten muss nach § 87a Abs. 1 UrhG eine Investition erforderlich gewesen sein. Darunter fallen auch Daten, wie z.B. Wetterdaten, die grundsätzlich bereits in der Natur vorhanden sind, aber durch Messung gesammelt werden.

Eine wichtige Einschränkung nimmt der EuGH insofern vor, als kein Schutz gewährt wird, soweit es um die Erzeugung neuer Daten geht.[22] D.h. Kosten der Datengenerierung sind nicht berücksichtigungsfähig; wohl aber die Investitionskosten etwa für die Software, mit der die Daten für Zwecke der Datenbank erfasst und dargestellt werden einschließlich deren Programmierung. Die Abgrenzung ist im Einzelnen schwierig, wenn der Hersteller der Datenbank auch bei der Datengenerierung aktiv tätig wird.

c) Nach Art oder Umfang wesentlich

Um nicht jede noch so kleine Datenbank zu schützen, verlangt § 87a Abs. 1 UrhG, dass es sich um eine nach Art oder Umfang wesentliche Investition handelt. Die Rechtsprechung unterscheidet hierbei zwischen **quantitativ** wesentlichen Mitteln, die sich ihrem Umfang nach bemessen lassen, insbesondere solchen finanzieller Art und **qualitativ** wesentlichen Mitteln etwa in Form geistiger Anstrengungen, erheblichen Energieverbrauchs oder sonstiger besonderer Auswendungen.

So kann etwa in einer Datenbank den besonders schwer zu beschaffenden oder besonders aktuellen Daten ein qualitativ höherer Wert zukommen, auch wenn sie quantitativ keinen wesentlichen Bestandteil der Datenbank bilden.

Die Auslegung des unbestimmten Rechtsbegriffs der Wesentlichkeit der geforderten Investition muss durch die Rechtsprechung im Einzelfall erfolgen. Die hierzu ergangenen Entscheidungen zeigen hinsichtlich des quantitativen Aufwands eine große Spannbreite: keine Bedenken bestanden etwa in Bezug auf eine Automobilbörse bei 3,8 Mio. EUR jährlich für die Bereitstellung der technischen Infrastruktur der Datenbank und deren Erhaltung, Pflege und Wartung[23]. Ausreichend wurden aber auch bereits Kosten i.H.v. insgesamt 34.900 EUR für eine Gedichtsammlung erachtet.[24] Was die qualitativen Faktoren angeht, ist von Investitionen von „substantiellem Gewicht die Rede. Diese wurden etwa bejaht hinsichtlich des Personalaufwands für die Überprüfung von 3500 Bewertungen von Patienten für 800 registrierte Zahnärzte.[25]

3. Schutzsubjekt

Datenbankhersteller im Sinne dieses Gesetzes ist nach der Legaldefinition im § 87a Abs. 2 UrhG derjenige, der die Investition im Sinne des Abs. 1 vorgenommen hat.

---

22 EuGH, GRUR 2005, 254, 256 Rn. 42 – Fixtures-Fußballspielpläne II; EuGH, GRUR 2005, 244, 247 Rn. 31 f., 38 – BHB Pferdewetten.

23 BGH, GRUR 2011, 1018 – Automobil-Onlinebörse; hierzu *Völzmann-Stickelbrock*, LMK 2011, 325120.

24 BGH, GRUR 2007, 688 – Gedichttitelliste II; hierzu *Ehmann,* GRUR 2008, 47.

25 BGH, GRUR 2011, 724, 725 – Zweite Zahnarztmeinung.

Inhaber des sog. „sui-generis-Rechts ist mithin nicht wie im Urheberrecht zwingend derjenige, der die Datenbank konzipiert hat, sondern derjenige, der die Initiative ergreift, das Risiko trägt, die Organisationsgewalt über den Datenbankaufbau hat und die hierfür notwendigen Verträge schließt.[26]

4. Schutzdauer

Im Unterschied zu dem 70jährigen Schutz des Urheberrechts beträgt der Leistungsschutz der Datenbank nur 15 Jahre, § 87d UrhG, wobei allerdings spätere wesentliche Investitionen ein neues Schutzrecht begründen können.

5. Schutzumfang

Die Regelung des § 87b Abs. 1 UrhG weist dem Inhaber der Datenbank die Verwertungsrechte der Vervielfältigung, Verbreitung und öffentlichen Wiedergabe einschließlich der öffentlichen Zugänglichmachung zu. Die Vervielfältigung entspricht inhaltlich dem in der Richtlinie verwendeten und eigentlich griffigerem Begriff der „Entnahme" von Daten.

a) Verwertung eines nach Art oder Umfang wesentlichen Teils, S. 1

Der Hersteller kann gegen die Entnahme eines nach Art oder Umfang wesentlichen Teils der Datenbank vorgehen. Auch hier ist nicht allein auf den quantitativen Umfang abzustellen, da sonst große Datenbanken einen geringeren Schutz erfahren als kleine. Daher sind sowohl die quantitative Wesentlichkeit zu prüfen, wobei 10% wohl noch nicht als ausreichend erachtet werden, als auch die qualitative Wesentlichkeit des entnommenen Teils, d.h. die Frage, ob aus der Entnahme speziell dieser Teile ein erheblicher Schaden des Amortisationsinteresses zu resultieren droht. Entscheidend ist, ob gerade in den übernommenen Datensätzen ein wesentlicher Teil der Investition in die Datenbank verkörpert ist, z.B. weil immer die aktuellen Daten entnommen werden zur Erstellung einer Änderungsliste.[27]

b) Systematische oder wiederholte Verwertung unwesentlicher Teile S. 2

Um zu verhindern, dass durch eine mehrfache Entnahme kleinerer Datenmengen auf Dauer die gesamte Datenbank ausgeplündert wird, enthält S. 2 einen Auffangtatbestand, der auch dieses Vorgehen verbietet, sofern es planmäßig erfolgt. Diskutiert wird dies vor allem beim Einsatz sog. Screen Scraping-Software, mit der etwa Flugbörsen oder Automobilbörsen systematisch durchsucht werden.[28] Erfolgt dies durch den einzelnen Endnutzer, können die für sich genommen je-

---

26 *Wiebe,* GRUR 2017, 338, 342 m.w.N.

27 EuGH, GRUR 2005, 244 – Elektronischer Zolltarif.

28 Hierzu näher *Schapiro/Żdanowiecki*, MMR 2015, 497 ff.; *Helbig/Kahler,* WRP 2012, 48 ff.

weils zulässigen Nutzungen nur dann zu einer insgesamt unzulässigen Nutzung zusammengerechnet werden, wenn die Nutzer – was regelmäßig nicht der Fall ist – die Datenbank gemeinschaftlich, also in bewusstem und gewolltem Zusammenwirken vervielfältigen würden.[29]

Problematischer ist der Fall, dass eine derartige Software von Unternehmen eingesetzt wird, beispielsweise indem die frei zugänglichen Datenbanken kopiert und indexiert werden, um sie sodann den Nutzern in der eigenen spezialisierten Internet-Suchmaschine zum Durchsuchen anzubieten. Der EuGH betont in diesem Fall, dass ein ausgewogenes Gleichgewicht der beteiligten legitimen Interessen hergestellt und dabei insbes. auf die potenzielle Beeinträchtigung der Investitionen der Datenbankhersteller abgestellt werden muss. Es ist daher nunmehr stets ein Interessenausgleich und die Darlegung der Hersteller, dass die angegriffenen Handlungen die Amortisation der eigenen Investition gefährden können, erforderlich.[30]

Im Fallbeispiel des vernetzten Kfz zeigt sich sehr schnell, dass das Datenbankherstellerrecht zwar in gewissem Umfang Schutz gewähren kann, aber auch sehr schnell an seine Grenzen gerät.

- Abgrenzung von Datensammlung und Datenerzeugung
  Schwierigkeiten bereitet zunächst die vom EuGH betonte Begrenzung auf „bereits vorhandene Daten", die von jedem Dritten mit gleichem Aufwand gesammelt werden können. Dagegen sind erzeugte Daten ihrer Natur nach nur dem Datenerzeuger selbst bekannt. Für solche Daten greift der Schutz der §§ 87a ff. UrhG nicht.
  Ob die sensorgestützte Datenerhebung im vernetzten Kfz der Datensammlung zugeordnet werden kann, weil sie sich auf bereits existierende Informationen bezieht, die lediglich gemessen werden oder die maschinenerzeugten Daten zunächst nur dem Betreiber bekannt und daher der Datenerzeugung zuzuordnen sind, ist nicht leicht zu beantworten. Jedenfalls für einen großen Teil der Rohdaten, die unsortiert gespeichert werden, lässt sich kein Investitionsschutz über die bestehenden Regelungen des UrhG begründen.
- Herstellereigenschaft:
  In vernetzten Wertschöpfungsketten kommen unterschiedliche Zuordnungsberechtigte in Bezug auf die Daten in Betracht (s.o.). Am ehesten wird als Datenbankhersteller der Hersteller des Kfz anzusehen sein, der die Software einbauen lässt und die Herstellungs- und Entwicklungskosten trägt. Schwieriger wird die Beurteilung, wenn die erhobenen Maschinendaten nicht beim Hersteller gespeichert, sondern unmittelbar an dritte Dienste oder Unternehmen weitergeleitet werden, die ihrerseits nur geringen Aufwand durch das Sammeln der Daten haben. Hier Rechte zuzuweisen, lässt zudem auch die vertraglichen Beziehungen unberücksichtigt, die etwa bestehen, wenn Dienstleister Daten im Auftrag des Produzenten erheben, Daten in verschiedenen Datenbanken und Datenbankclustern gespeichert und verarbeitet werden, die dann unterschiedliche Hersteller haben.

29 BGH GRUR 2011, 1018 Rn. 48 – Automobil-Onlinebörse; hierzu *Völzmann-Stickelbrock*, LMK 2011, 325120.

30 EuGH, GRUR 2021, 1075 - CV-Online Latvia/Melons.

- Big Data Analysen
  Geht man davon aus, dass die Daten aus dem vernetzten Kfz in systematischer Weise gesammelt wurden und damit eine Datenbank des Herstellers im Sinne des UrhG entstanden ist, stellt sich sodann die Frage, wie eine Bearbeitung dieser Daten zu bewerten wäre. Richtigerweise werden durch eine Aggregierung und Veredelung von Daten neue Daten produziert, die ihrerseits dann einer neuen Datenbank des bearbeitenden Unternehmens zuzurechnen wären. Für die Weiterverwendung der Daten wäre dann die Zustimmung des Herstellers der Datenbank erforderlich, der die Daten entnommen wurden,[31] es sei denn, diese dienen zu Forschungszwecken.[32]
  Je nach Art der Datenanalysen könnten hierbei mehrere, aufeinander aufbauende Datenbanken mit unterschiedlichen Herstellern entstehen.

Resümee: Ob und in welchem Umfang ein Datenbankherstellerrecht bei Datensammlung in vernetzten Kfz besteht, ist im Einzelfall zu klären und mit einigen Unsicherheiten behaftet. Daher kann den beteiligten Akteuren derzeit nur eine vertragliche Absicherung ihrer Interessen angeraten werden. Angesichts der Monopolstellung, die ein Datenbankherstellerrecht vermittelt, erscheint für Maschinendaten jedenfalls die bestehende Schutzdauer von 15 Jahren als zu lang.

31 Zum Ganzen *Wiebe,* GRUR 2017, 338, 342 ff.

32 In diesem Fall greift die Freistellung durch die Data-Mining-Schranken, siehe dazu Teil 4 – Datengestützte Forschung.

D. Literatur zur Wiederholung und Vertiefung

Apel, Simon, Kaulartz, Markus, Rechtlicher Schutz von Machine Learning-Modellen, RDi 2020, 24 ff.

Ehmann, Timo, Datenbankurheberrecht, Datenbankherstellerrecht und die Gemeinschaft der Rechtsinhaber - Zugleich Besprechung von BGH „Gedichttitelliste I und II", GRUR 2008, 47 ff.

Götz, Christopher, Big Data und der Schutz von Datenbanken - Überblick und Grenzen, ZD 2014, 563 ff.

Haberstumpf, Helmut, Der Schutz elektronischer Datenbanken nach dem Urheberrechtsgesetz, GRUR 2003, 14 ff.

Hacker, Philipp, Immaterialgüterrechtlicher Schutz von KI-Trainingsdaten, GRUR 2020, 1025 ff.

Helbig, Kathrin, Kahler, Jörg, Umfang und Grenzen des Datenbankschutzes bei dem Screen Scraping von Online-Datenbanken durch Online-Reiseportale, WRP 2012, 48 ff.

Hessel, Stefan, Leffer, Lena, Rechtlicher Schutz maschinengenerierter Daten, MMR 2020, 647 ff.

Krekel, Jan F., Die digitale Datenbank - aktuelle Probleme im Recht des Datenbankherstellers, WRP 2011, 436 ff.

Leistner, Matthias, Datenbankschutz - Abgrenzung zwischen Datensammlung und Datengenerierung, CR 2018, 17 ff.

Leistner, Matthias, Was lange währt …: EuGH entscheidet zur Schutzfähigkeit geografischer Karten als Datenbanken, GRUR 2016, 42 ff.

Schapiro, Leo, Żdanowiecki, Konrad, Screen Scraping - Rechtlicher Status quo in Zeiten von Big Data, MMR 2015, 497 ff.

Wiebe, Andreas, Der Schutz von Datenbanken - ungeliebtes Stiefkind des Immaterialgüterrechts, CR 2014, 1 ff.

Wiebe, Andreas, Schutz von Maschinendaten durch das sui-generis-Schutzrecht für Datenbanken, GRUR 2017, 338 ff.

Teil 4 Datengestützte Forschung

A. Bedeutung

In allen Bereichen des täglichen Lebens bilden Datensammlungen heute den „Rohstoff", aus dem durch Datenanalysen neue Erkenntnisse gewonnen werden. Diese haben nicht nur im Zusammenhang mit der wissenschaftlichen Forschung hohe Bedeutung, sondern sie werden auch in großem Umfang sowohl von privaten als auch öffentlichen Einrichtungen eingesetzt, um große Datenmengen in verschiedenen Lebensbereichen und zu unterschiedlichen Zwecken zu analysieren.[33]

Insbesondere die Entwicklung von Algorithmen im Bereich künstlicher Intelligenz bedarf einer großen Menge von Trainingsdaten. Der europäische Gesetzgeber trägt diesem Umstand Rechnung, indem er durch neue Schrankenregelungen zum sog. Text und Data Mining Rechtssicherheit für die automatisierte Auswertung von Daten mit Hilfe von Algorithmen geschaffen hat.

Für eine Datenanalyse, die nicht auf urheberrechtlich geschützte Daten zugreift, sondern auf reine, ungeordnete Rohdaten, bedarf es naturgemäß keiner Erlaubnis eines Urhebers oder Datenbankherstellers.[34] Die in Teil 3 aufgezeigten Schwierigkeiten bei der Frage, ob Daten im Einzelfall einem Datenbankschutz unterliegen, relativieren sich aber durch die Freistellung des Data-Mining jedenfalls in gewissem Umfang.

B. Begriff des Text- und Data-Mining (TDM)

Der Begriff ist in Art. 2 Nr. 2 der DSM-Richtlinie[35] legal definiert.

> Text und Data Mining bezeichnet eine Technik für die automatisierte Analyse von Texten und Daten in digitaler Form, mit deren Hilfe Informationen unter anderem — aber nicht ausschließlich — über Muster, Trends und Korrelationen gewonnen werden können.

Der deutsche Gesetzgeber formuliert etwas abweichend, aber in der Sache identisch in

> § 44b Abs. 1 UrhG
> Text und Data Mining ist die automatisierte Analyse von einzelnen oder mehreren digitalen oder digitalisierten Werken, um daraus Informationen insbesondere über Muster, Trends und Korrelationen zu gewinnen.

33 Erwägungsgrund 18 der DSM-RL.

34 Hierzu *Raue,* ZUM 2019, 684, 685.

35 Richtlinie 2019/790 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt vom 19. April 2019.

Data Mining verläuft dabei in mehreren Phasen, von der Identifizierung und Extrahierung von relevanten Datensätze, über die Filterung bis hin zur eigentlichen Analyse mit Hilfe eines für die Fragestellung entwickelten Algorithmus.[36]

C. Urheberrechtliche Zulässigkeit

Erforderlich war eine gesetzliche Regelung, weil die Daten mithin für jede automatisierte Analyse zumindest kurzfristig in den Arbeitsspeicher eines Computers geladen und dadurch vervielfältigt werden. Dieser Vorgang greift in das Vervielfältigungsrecht des Urhebers nach § 16 UrhG ein und ist grundsätzlich nur mit dessen Zustimmung zulässig.[37]

Art. 3 und Art. 4 der DSM-Richtlinie stellen daher klar, dass Text und Data Mining keine urheberrechtlich relevante Handlung ist. Der deutsche Gesetzgeber hat dies in den neuen §§ 44b UrhG und § 60d UrhG umgesetzt.

I. § 60d UrhG

So erklärt § 60d UrhG Vervielfältigungen für Text und Data Mining für Zwecke der wissenschaftlichen Forschung für zulässig, sofern diese durch Forschungsorganisationen, d.h. Hochschulen, Forschungsinstitute oder sonstige Einrichtungen, die wissenschaftliche Forschung betreiben, erfolgen. Diese müssen zudem (1.) nicht kommerzielle Zwecke verfolgen, (2.) sämtliche Gewinne in die wissenschaftliche Forschung reinvestieren oder (3.) im Rahmen eines staatlich anerkannten Auftrags im öffentlichen Interesse tätig sein.

Auch öffentliche Bibliotheken, Museen, Archive und schließlich auch der einzelne Forscher, der nicht kommerzielle Zwecke verfolgt, darf die Datensammlungen analysieren und die Vervielfältigungen anderen Personen für deren gemeinsame wissenschaftliche Forschung sowie Dritten zur Überprüfung der Qualität wissenschaftlicher Forschung zur Verfügung stellen. Sie dürfen folglich solange aufbewahrt werden, wie es für die jeweiligen Zwecke notwendig ist.

Dies ist wichtig, da Forschungsergebnisse zur Wahrung guter wissenschaftlicher Praxis reproduzierbar und nachprüfbar gestaltet werden müssen, um Anschlussforschung zu ermöglichen.[38] Um im Gegenzug die Daten gegen Missbrauch zu sichern, ist eine Aufbewahrung in Forschungsdatenrepositorien zu empfehlen.[39]

---

36 *Spindler,* GRUR 2016, 1112 f.

37 *Raue,* ZUM 2021, 793.

38 Hierzu umfassend *Wirth*, ZUM 2020, 585, 590 ff., der auch vertragliche Pflichten zur Löschung von für die Forschung zur Verfügung gestellten Daten nach Beendigung der Forschungsarbeiten für rechtlich nicht durchsetzbar hält.

39 *Raue,* ZUM 2021, 793, 799; *Kleinkopf/Jacke/Gärtner,* MMR 2021, 196, 197 für 10jährige Aufbewahrung.

II. § 44b UrhG

Neben dieser privilegierten Nutzung für Forschungszwecke erweitert die neue allgemeine Text und Data Mining Ausnahme des § 44b UrhG[40] den Kreis der Berechtigten auf „Jedermann", um damit vor allem die Innovationsbereitschaft privater Unternehmen zu steigern.[41] Diese dürfen auch kommerzielle Zwecke verfolgen. Anders als im Bereich der Forschung sind die Vervielfältigungen aber zu löschen, wenn sie für das Text und Data Mining nicht mehr erforderlich sind.

Schwierigkeiten kann dies gerade für das Training von KI-Algorithmen bereiten, bei denen eine stetige Interaktion mit Nutzern notwendig ist und im Evaluationsprozess auch auf ältere Daten zurückgegriffen werden muss. Da nicht ganz eindeutig ist, wie die Erforderlichkeit in § 44b Abs. 2 UrhG zu bewerten ist, wenn der eigentliche Mining-Prozess bereits abgeschlossen ist, kann es sich empfehlen, bei umfangreichen Vorhaben zur Sicherheit dennoch Lizenzvereinbarungen mit den Rechteinhabern zu schließen (sofern dies bei vielfältigen Datenquellen praktikabel ist).[42]

Schließlich darf der Rechteinhaber nach § 44b Abs. 3 UrhG einen Nutzungsvorbehalt erklären, um weiterhin Lizenzen für das Text und Data Mining vergeben zu können. Um der Datenanalysen im Internet Rechnung zu tragen, muss ein solcher Vorbehalt dann aber – etwa in den Metadaten oder den Geschäftsbedingungen in maschinenlesbarer Form erklärt werden.

D. Geltung für Datenbanken

Dass die Befugnis zu automatisierten Datenanalysen auch für Datenbanken gilt, hat der Gesetzgeber in § 87c Abs. 1 Ziff. 4 und 5 UrhG klargestellt. Danach ist die Vervielfältigung eines nach Art oder Umfang wesentlichen Teils einer Datenbank u.a. zulässig, wenn sie zu Zwecken des Text und Data Mining gemäß § 44b UrhG oder zu Zwecken des Text und Data Mining für Zwecke der wissenschaftlichen Forschung gemäß § 60d UrhG erfolgt.

Stets zu beachten ist, dass sich die Zulässigkeit des Text und Data Mining nur auf Werke oder Datenbanken bezieht, die dem Nutzer „rechtmäßig zugänglich" sind. Das trifft z.B. auf frei im Internet zugängliche Werke wie öffentliche Websites zu, Werke, für die der Nutzer über eine entsprechende Lizenz verfügt oder die unter Open Access Bedingungen veröffentlicht wurden.[43]

Die Text und Data Mining Ausnahme schafft folglich kein Recht auf Zugang zu Daten, sondern setzt diesen voraus. Die schwierige Frage, wem welche Rechte an Daten zustehen und wem die Daten zuzuordnen sind, wird dadurch nicht beantwortet, sondern muss vor der Durchführung von Datenanalysen im Wege des Data Mining beantwortet werden.

---

40 Die bisherige Schrankenregelung des § 44a UrhG, der flüchtige Zwischenspeicherungen erlaubt, reicht für Datenanalysen in aller Regel nicht aus, da diese eine dauerhafte Abspeicherung erfordern, hierzu *Raue*, ZUM 2021, 793, 795.

41 BT-Drucks. 19/27426, 87.

42 Hierzu zu Recht kritisch *Raue,* ZUM 2021, 793, 796

43 Dazu *Schack*, GRUR 2021, 904, 907.

E. Literatur zur Wiederholung und Vertiefung

Kleinkopf, Felicitas, Jacke, Janina, Gärtner, Markus, Text und Data Mining - Urheberrechtliche Grenzen der Nachnutzung wissenschaftlicher Korpora bei computergestützten Verfahren und digitalen Ressourcen, MMR 2021, 196 ff.

Raue, Benjamin, Die Freistellung von Datenanalysen durch die neuen Text und Data Mining-Schranken (§§ 44b, 60d UrhG), ZUM 2021, 793 ff.

Raue, Benjamin, Rechtsicherheit für datengestützte Forschung, ZUM 2019, 684 ff.

Schack, Haimo, Schutzgegenstand, „Ausnahmen oder Beschränkungen" des Urheberrechts, GRUR 2021, 904 ff.

Spindler, Gerold, Text- und Data Mining – urheber- und datenschutzrechtliche Fragen, GRUR 2016, 1112 ff.

Wirth, Thomas, Die Pflicht zur Löschung von Forschungsdaten – Urheber- und Datenschutzrecht im Widerspruch zu den Erfordernissen guter wissenschaftlicher Praxis? ZUM 2020, 585 ff.

F. Juristische Fachzeitschriften zum Zivilrecht (Auswahl)

BB	**Betriebsberater**
BKR	**Bank- und Kapitalmarktrecht**
CR	**Computer und Recht**
GRUR	**Gewerblicher Rechtsschutz und Urheberrecht**
GRUR Int.	**Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil**
ICC	**International Review of Intellectual Property and Competition Law**
JA	**Juristische Arbeitsblätter**
JR	**Juristische Rundschau**
JuS	**Juristische Schulung**
Jura	**Juristische Ausbildung**
JZ	**Juristenzeitung**
K&R	**Kommunikation und Recht**
LMK	**Lindenmaier-Möhring Kommentierte BGH-Rechtsprechung**
MDR	**Monatsschrift für Deutsches Recht**
MMR	**Multimedia und Recht**
NJW	**Neue Juristische Wochenschrift**
NJW-RR	**Neue Juristische Wochenschrift - Rechtsprechungsreport**
NZKart	**Neue Zeitschrift für Kartellrecht**
NZV	**Neue Zeitschrift für Verkehrsrecht**
RDi	**Recht Digital**
SVR	**Straßenverkehrsrecht**
VuR	**Verbraucher und Recht**
WRP	**Wettbewerb in Recht und Praxis**
ZD	**Zeitschrift für Datenschutz**
ZGE/IPJ	**Zeitschrift für Geistiges Eigentum/Intellectual Property Report**
ZEuP	**Zeitschrift für Europäisches Privatrecht**
ZfPW	**Zeitschrift für die Privatrechtswissenschaft**

G. Englischsprachige Literatur zum Datenrecht

Becker, Maximilian, Rights in Data – Industry 4.0. and the IP Rights of the Future, ZGE/IPJ 9 (2017), 253 ff.

Berger, Christian, Property Rights to Personal Data? – An Exploration of Commercial Data Law, ZGE/IPJ 9 (2017), 340 ff.

Fink, Leonard, Big Data and Artificial Intelligence, ZGE/IJP 9 (2017), 288 ff.

Geiger, Christophe, Frosio, Giancarlo, Bulayenko, Oleksandr, Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data? Legal Analysis and Policy Recommendations, ICC 2018, 814 ff.

Leistner, Matthias, The Commission's Digital Markets and Services Package – New Rules for Big Tech and Big Data, GRUR Int. 2021, 515 ff.

Kerber, Wolfgang, New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int. 2016, 989 ff.

Podszun, Rupprecht, Competition and Data, ZGE/IPJ 9 (2017), 406 ff.

Spindler, Gerald, Data and Property Rights, ZGE/IPJ 9 (2017), 399 ff.

000000000
(10/24)

55100-03-S#1