Arbeitsgruppe „Digitaler Neustart“

der Konferenz der Justizministerinnen und Justizminister der Länder

Bericht vom 15. Mai 2017

unter Mitwirkung der Länder
Baden-Württemberg, Bayern, Berlin, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen (Federführung), Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein

Inhaltsverzeichnis

Zusammenfassung und Ergebnisse

A. Allgemeines

In Folge der voranschreitenden Digitalisierung und Vernetzung nimmt die technische, ökonomische, aber auch gesellschaftliche Relevanz von (digitalen) Daten und Datendiensten in allen Lebensbereichen stetig zu. Hinter Schlagwörtern wie „Industrie 4.0“, „Internet der Dinge“ oder „Big Data“ verbergen sich gewaltige Möglichkeiten für unterschiedlichste Bereiche – von Gesundheit, Umwelt und Ernährungssicherheit über Klimapolitik und Ressourceneffizienz bis hin zu Energie, intelligenten Verkehrssystemen und intelligenten Städten.[1] Den damit verbundenen Chancen für Unternehmen und Gesellschaft stehen dabei nicht nur technische und ökonomische Herausforderungen gegenüber. Eine digitale Gesellschaft braucht auch einen verlässlichen Rechtsrahmen, damit Freiheit, Gleichheit, Demokratie und Gerechtigkeit gewahrt bleiben. Allen Bürgerinnen und Bürgern, aber auch den Unternehmen, muss ein rechtssicherer und grundrechtskonformer Umgang mit digitalen Daten ermöglicht werden.

Vor diesem Hintergrund haben sich die Justizministerinnen und Justizminister der Länder bereits auf ihrer Frühjahrskonferenz im Juni 2015 mit den Folgen der Digitalisierung auf das Zivilrecht befasst und beschlossen, eine Arbeitsgruppe einzurichten, die der Frage nachgeht, ob gesetzgeberischer Handlungsbedarf besteht. Unter der Federführung des Justizministeriums Nordrhein-Westfalen und unter Beteiligung der Länder Baden-Württemberg, Bayern, Berlin, Hamburg, Hessen, Niedersachsen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein sowie des Bundesministeriums der Justiz und für Verbraucherschutz widmete sich die Arbeitsgruppe vier Themenbereichen:

(1.) Die erste grundsätzliche Frage betrifft die Rechtsqualität von digitalen Daten. Daten können große emotionale, für Unternehmen auch existentielle, Bedeutung und einen hohen ökonomischen Wert haben. Der Handel mit Daten ist alltäglich. Juristische Laien gehen ganz selbstverständlich davon aus, dass Daten ihnen „gehören“. Derzeit ist aber nur das Eigentum am Speichermedium geschützt, unter bestimmten Voraussetzungen auch der Informationsgehalt der Daten, z. B. durch das Urheberrecht. Die Arbeitsgruppe ist der Frage nachgegangen, ob die Rechtsqualität von digitalen Daten gesetzlich zu bestimmen ist, etwa durch die Schaffung eines Ausschließlichkeitsrechts.

(2.) Einen weiteren Themenbereich bildet das Vertragsrecht. Die Digitalisierung hat neue Perspektiven für Handel und Dienstleistungen eröffnet, neue Geschäftsformen haben sich etabliert. Darauf ausgerichtete Vereinbarungen, wie etwa Verträge über Streaming- und Cloud Computing-Dienste oder die

[1] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau einer Europäischen Datenwirtschaft“, COM(2017) 9 final, S. 2.

„Mitgliedschaft“ in einem sozialen Netzwerk, lassen sich den im Bürgerlichen Gesetzbuch normierten Vertragstypen aber nicht ohne Weiteres zuordnen. Die zentrale Fragestellung lautet insoweit, ob neue Vertragstypen in das Bürgerliche Gesetzbuch (BGB) aufgenommen oder die vorhandenen Vertragstypen um eine digitale Variante ergänzt werden sollten. Überdies hat die Arbeitsgruppe aber auch geprüft, ob tragfähige Regelungen zum Vertragsschluss mittels Maschinenkommunikation und zur Haftung bei Verwendung (teil-)autonomer Systeme existieren.

(3.) Ob der bestehende Schutz des Persönlichkeitsrechts den Herausforderungen des digitalen Wandels genügt, ist Gegenstand des dritten Themenbereichs. Hierzu hat die Arbeitsgruppe den Umgang mit Phänomenen der „digitalen Welt“ an den Grundsätzen gemessen, die zum Schutz des allgemeinen Persönlichkeitsrechts entwickelt worden sind. Sie ist dabei zielgerichtet der Frage nachgegangen, ob die Rechtsordnung eine digitale Persönlichkeit anerkennen und schützen muss.

(4.) Schließlich hat sich die Arbeitsgruppe mit der Thematik des „Digitalen Nachlasses“ befasst. Gegenstand der unter diesem Oberbegriff vorgenommenen Prüfungen ist vor allem das postmortale Schicksal von Rechtspositionen, die der Erblasser aufgrund elektronischer/digitaler Kommunikation innehatte.

Die Überlegungen der Arbeitsgruppe sind von dem Grundsatz getragen, dass kein gesetzgeberischer Handlungsbedarf besteht, soweit und solange das geltende („analoge“) Recht tragfähige Normen für die Folgen der Digitalisierung bereithält und es den Gerichten überantwortet werden kann, die neuen Sachverhalte durch Subsumtion unter vorhandene Normen sachgerechten Lösungen zuzuführen. Zudem ist eine Etablierung unterschiedlicher Regelungsregime für analoge und digitale Sachverhalte und damit eine (weitere) Fragmentierung des Zivilrechts zu vermeiden. Etwaigem gesetzgeberischen Handlungsbedarf ist daher primär dadurch Rechnung zu tragen, dass die bereits vorhandenen Regelungsregime ggf. durch gezielte Sondervorschriften ergänzt werden.

Eine besondere Herausforderung ergibt sich aus der Dynamik, mit welcher sich digitale Phänomene entwickeln. Ununterbrochen etablieren sich neue Geschäftsmodelle digitaler Art, aus denen sich neue rechtliche Fragen und Problemfelder ergeben. Damit geht einher, dass sich zu vielen Aspekten bisher weder richtungsweisende Rechtsprechung noch eine gefestigte Literaturmeinung bilden konnte, an der man gesetzgeberischen Handlungsbedarf festmachen könnte. Deshalb hat die Arbeitsgruppe eine übergreifende Gesamtbetrachtung einer Vielzahl von Fallgestaltungen vorgenommen. Nach eingehender Prüfung hat sie die aus ihrer Sicht relevanten Probleme identifiziert, auf konkrete Fragestellungen zugespitzt und einer näheren Betrachtung unterzogen. Es ist auf diese Weise ein umfangreiches Papier entstanden, welches über die Landesjustizverwaltungen hinaus als Grundlage für die zivilrechtliche Auseinandersetzung mit den Folgen der Digitalisierung dienen kann.

Wegen ihrer Dynamik bedarf es der fortlaufenden Betrachtung der digitalen Entwicklung und der durch sie hervorgerufenen Rechtsfragen. Dies gilt auch bzw. gerade in den Bereichen, in denen von der Arbeitsgruppe derzeit kein (akuter) gesetzgeberischer Handlungsbedarf gesehen wird, weil das geltende Recht Antworten ermöglicht und dem Umgang der Rechtsprechung mit einem bestimmten Phänomen nicht vorgegriffen werden soll. Insoweit ist auch von Bedeutung, dass die Arbeitsgruppe sich entsprechend ihres Arbeitsauftrags im Wesentlichen auf das bürgerliche Recht und die Frage konzentriert hat, ob das BGB in seiner derzeitigen Fassung den Herausforderungen des digitalen Wandels genügt. Andere Rechtsgebiete, wie etwa das Urheberrecht, das Datenschutzrecht sowie das Telekommunikations- und Telemedienrecht haben insoweit Beachtung gefunden, wie sie für zivilrechtliche Fragestellungen von Bedeutung sind.

Schließlich gilt es weiterhin, die Entwicklung auf europäischer Ebene konstruktiv zu begleiten. Anlass hierfür geben insbesondere die Maßnahmen der EU-Kommission im Rahmen ihrer Strategie für einen digitalen Binnenmarkt.[2] Die Arbeitsgruppe hatte in diesem Zusammenhang bereits zu den beiden Richtlinienvorschlägen der EU-Kommission über bestimmte vertragsrechtliche Aspekte des Online-Warenhandels und anderer Formen des Fernabsatzes von Waren[3] bzw. über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte[4] eine Stellungnahme erarbeitet, die zur Grundlage der Beschlussfassung des Bundesrates (Drs. 614/15 und 615/16) wurde. Daran anknüpfend soll der vorliegende Bericht auch bei den noch laufenden Verhandlungen zu diesen Richtlinienvorschlägen Berücksichtigung finden. Vor allem kann er aber auch einen wichtigen Beitrag zum Dialog leisten, den die EU-Kommission mit Blick auf den „Aufbau einer europäischen Datenwirtschaft“[5] anstrebt.

B. Dateneigentum

Daten können als Rechtsobjekt bzw. als Wirtschaftsgut auf zweifache Weise voneinander abgegrenzt werden. Möglich ist zum einen eine Abgrenzung auf der inhaltlichen Bedeutungsebene (semantische Information), etwa in der Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten. Hieran knüpft das Recht schon heute unter mehreren Gesichtspunkten Rechtswirkungen an. Abhängig vom Dateninhalt kann etwa das Datenschutzrecht anwendbar sein;

---

[2] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen **„**Strategie für einen digitalen Binnenmarkt für Europa“, COM(2015) 192 final.

[3] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte des Online-Warenhandels und anderer Formen des Fernabsatzes von Waren, COM(2015) 635 final.

[4] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final.

[5] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Aufbau einer Europäischen Datenwirtschaft“, COM(2017) 9 final.

ferner können Immaterialgüterrechte bestehen. Aber auch unabhängig von ihrer Bedeutung lassen sich Daten abgrenzen, nämlich auf der Zeichenebene (syntaktische Information). Als Rechtsobjekt wäre dann eine Menge von Zahlenreihungen aus „Nullen und Einsen“ (binäre Codes) geschützt, sei es als Daten oder als Datenstrom. Dem Arbeitsauftrag der Arbeitsgruppe folgend lag der Schwerpunkt der vorliegenden Prüfung auf dieser abstrakteren Ebene.

Die Befürworter der Schaffung eines absoluten Rechts an Daten verweisen auf die – nicht zu bestreitende – ökonomische Bedeutung von Daten und machen Schutzlücken im geltenden Recht aus, die aus ihrer Sicht die wirtschaftliche Nutz- und Handelbarkeit von Daten einschränken. Indes kann Beurteilungsmaßstab für die Einführung eines solchen Rechts kein allumfassender, jeden denkbaren Einzelfall erfassender Schutz von digitalen Daten sein. Eigentumsrechtliche Schutzrechtszuweisungen greifen in die Wettbewerbs- und Informationsfreiheit ein und bedürfen deshalb einer Rechtfertigung. Hierfür ist Voraussetzung, dass sie nachweislich wirtschaftliche, gesellschaftliche oder andere Vorteile für die Wohlfahrt gegenüber der geltenden Rechtslage versprächen. Das Fehlen eines besonderen Datenrechts müsste etwa zur Folge haben, dass gesellschaftlich wünschenswerte Investitionen in die Hervorbringung neuer Daten oder die Nutzung vorhandener Daten ausbleiben. Derartige Lücken, die einen Handlungsbedarf auslösten, erscheinen derzeit nicht gegeben:

- Digitale Daten sind unter verschiedenen rechtlichen Ansatzpunkten gegen den unbefugten Zugriff durch Dritte geschützt. Grob lassen sich unterscheiden der vertragliche und der gesetzliche, auch im Verhältnis zu Dritten wirkende Schutz. Gesetzlich geschützt werden Daten direkt oder mittelbar durch den Eigentumsschutz am Speichermedium. Damit lässt sich in der Praxis eine Vielzahl von Fällen zufriedenstellend lösen, da dieser Schutz nur dann nicht greift, wenn Daten auf fremden Speichern abgelegt sind, wie etwa beim Cloud Computing. Darüber hinaus werden Daten als solche (bspw. im Deliktsrecht) sowie der Dateninhalt (bspw. im Urheber- oder Datenschutzrecht) gesetzlich geschützt. Insgesamt kann der Schutz von Daten im Zivilrecht als eine Art „Flickenteppich“ bezeichnet werden, der sich aus vielen unterschiedlichen Teilen zusammensetzt, die in ihrer Gesamtheit aber ein hinreichend geschlossenes Schutzsystem bilden.
- Der Handel mit Daten vollzieht sich in Ermangelung eines absoluten Rechts an Daten nach geltendem Recht dadurch, dass der Veräußerer dem Erwerber – auf vertraglicher Grundlage – eine faktische Position verschafft (bspw. Zugriff auf die Daten im Wege eines Downloads). Das Fehlen einer rechtlich absoluten Zuordnung von digitalen Daten wirkt sich nicht negativ aus. Auch ohne sachenrechtliches Verfügungsgeschäft kann etwa der Erwerber grundsätzlich mit den erworbenen Daten als Wirtschaftsgut (faktisch) so verfahren, wie ihm beliebt. Zwar ist nicht ausgeschlossen, dass diese Nutzungsmöglichkeit durch die Rechte Dritter eingeschränkt ist. Solche Einschränkungen haben jedoch ihren Ursprung vornehmlich im Vertrags- und Urheberrecht.

- Im Übrigen liegen keine Äußerungen von Verbänden (sei es von Seiten der Wirtschaft oder der Verbraucher) oder sonstige Stimmen vor, die mit Blick auf den Datenhandel ein Bedürfnis für eine stärkere rechtliche Zuordnung von Daten sähen. Insoweit ist vielmehr zu beachten, dass die mit einem Verzicht auf ein formalisiertes Verfahren verbundene Flexibilität der Vertragserfüllung sogar handelsfördernd wirken kann, da sie ggf. zu einer Reduzierung von Transaktionskosten führt.

- Im Zuge der technischen Entwicklung gibt es zunehmend Sachverhalte, in denen Maschinen Daten selbst (jedenfalls ohne unmittelbare Mitwirkung eines Menschen) erzeugen. Hervorzuheben ist das sog. „Internet der Dinge“, also die Ausbreitung des Internets auf physische Gegenstände, auf die aus der Ferne online zugegriffen werden kann und die ihre Umgebung vermessen und beeinflussen können. Zwangsläufig stellt sich hier die Frage, wem diese automatisch generierten Daten zuzuordnen sind.

  Mangels einer die Zuweisung ausdrücklich regelnden Norm werden die Daten derzeit im Grundsatz demjenigen zugeordnet, der faktisch auf sie zugreifen kann. Maßgeblich ist danach in erster Linie, wer die Daten speichern, verarbeiten, verkaufen oder löschen kann. Das geltende Recht kennt allerdings zahlreiche Ausnahmen, wenn sich z. B. aus etwaigen Rechten am Dateninhalt (z. B. Urheberrecht) oder aus Verträgen eine abweichende Zuordnung ergibt. Unerwünschte Ergebnisse können zudem unter Rückgriff auf das Wettbewerbsrecht korrigiert werden. Damit kann insbesondere der Entwicklung begegnet werden, dass wenige Großunternehmen große Datenmengen sammeln, die anderen (kleineren) Unternehmen nicht zur Verfügung stehen. Demzufolge ist bereits das geltende Recht geeignet, eine sachgerechte Zuordnung automatisch generierter digitaler Daten zu gewährleisten.

  Demgegenüber ist nicht erkennbar, dass mit einer gesetzlichen Zuordnung eines absoluten Rechts an automatisch generierten Daten besondere Anreize geschaffen würden, Daten zu erfassen oder öffentlich zugänglich zu machen. In einem funktionierenden Markt führt das freie Zusammenwirken der Beteiligten grundsätzlich zu besseren (vertraglich flexibel geregelten) Ergebnissen als eine pauschale und statische gesetzliche Festschreibung eines absoluten Rechts an Daten. Das gilt jedenfalls dann, wenn etwaigen Defiziten bzw. Fehlentwicklungen mit den geeigneten sachnächsten Instrumenten entgegen getreten wird (z. B. AGB-Recht, Datenschutzrecht, Wettbewerbsrecht, Kartellrecht).

- Zur Vollstreckung von Ansprüchen, die auf ein Tun oder Unterlassen in Bezug auf Daten gerichtet sind, kann auf die allgemeinen Zwangsvollstreckungsregeln nach §§ 887, 888 ZPO zurückgegriffen werden. Besonderer Vorschriften bedarf es hierfür nicht.

  Die Zwangsvollstreckung wegen einer Geldforderung in Datenbestände als Vermögensgegenstand ist demgegenüber zwar komplizierter. Aber auch die

insoweit bestehenden Schwierigkeiten lassen sich mit dem geltenden Zwangsvollstreckungsrecht sachgerecht lösen, zumal sie ohnehin nur auftreten, wenn die betreffenden Daten weder auf einem (körperlichen) Speichermedium abgelegt sind, das nach § 808 ZPO gepfändet werden kann, noch als Immaterialgüterrecht (§§ 87a ff. UrhG) gemäß § 857 ZPO pfändbar sind.

Die Lösung besteht entsprechend der höchstrichterlichen Rechtsprechung zur Zwangsvollstreckung in Internet-Domains darin, dass die Gesamtheit der Ansprüche, die dem (berechtigten) Inhaber der Daten als „sonstiges Vermögensrecht“ zustehen, Gegenstand der Pfändung nach § 857 Abs. 1 ZPO ist. Die Verwertung der gepfändeten Ansprüche kann – ebenfalls wie bei Internet-Domains – durch Überweisung zum Schätzwert, durch Versteigerung im Internet oder durch freihändige Veräußerung erfolgen.

- Der Schutz von Daten in der Insolvenz des Cloudbetreibers und bei der Zwangsvollstreckung in das Speichermedium ist hinreichend gewährleistet. Das geltende Recht bietet einem Cloudnutzer mit dem Aussonderungsrecht gemäß § 47 InsO bzw. mit der Möglichkeit, sich auf ein die Veräußerung hinderndes Recht i. S. v. § 771 ZPO zu berufen, grundsätzlich taugliche Grundlagen, in diesen Fällen wieder an seine Daten zu gelangen.

Die vorstehenden Ergebnisse lassen sich auch auf Überlegungen übertragen, anknüpfend an die Bedeutungsebene von Daten einen neuen Typus absoluter Rechte zu schaffen. Auch insoweit wird derzeit kein Handlungsbedarf gesehen. Das auf dem Recht auf informationelle Selbstbestimmung fußende Datenschutzrecht, die bestehenden Immaterialgüterrechte (Urheberrecht, Patentrecht etc.) sowie die Regelungen zum Schutz von Betriebs- und Geschäftsgeheimnissen gewährleisten in Ergänzung der allgemeinen zivilrechtlichen Regelungen einen tragfähigen Rechtsrahmen für den Umgang mit digitalen Daten.

Im Übrigen wäre die Schaffung eines absoluten Rechts an Daten mit erheblichen Schwierigkeiten verbunden. Dies gilt zunächst hinsichtlich der Abgrenzung, an welchen Daten ein absolutes Recht bestehen soll. Insbesondere unter den Aspekten Rechtsklarheit und Rechtssicherheit dürfte problematisch sein, unabhängig vom Dateninhalt bzw. des Überschreitens einer „Erheblichkeitsschwelle“ jedes digitale Datum erfassen zu wollen. Fraglich wäre zudem, nach welchen Kriterien Daten zugeordnet werden sollten. Denkbar ist etwa eine Zuordnung nach der persönlichen Betroffenheit, nach dem Schaffensprozess (Skripturakt) oder nach der Verkehrsanschauung. Schließlich wäre eine Klärung herbeizuführen, wie sich das Recht an Daten zu anderen Rechten verhalten sollte. Dies gilt vor allem mit Blick auf mögliche Kollisionen mit dem Recht am Speichermedium sowie den (sonstigen) Rechten am Dateninhalt.

Festzuhalten ist demzufolge, dass für die gesetzliche Bestimmung einer besonderen Rechtsqualität von Daten bzw. die Schaffung eines absoluten Rechts an Daten derzeit kein Bedarf besteht.

C. Digitales Vertragsrecht

Im Zusammenhang mit modernen digitalen Phänomenen, die entweder durch die Autonomie von Maschinen oder Produkten oder durch einen „digitalen“ Vertragsgegenstand gekennzeichnet sind, stellt sich ein breites Spektrum vertragsrechtlicher Fragen.

Angesichts der großen Bandbreite an Phänomenen und der mit ihnen zusammenhängenden bürgerlich-rechtlichen Fragestellungen hat sich die Arbeitsgruppe mit Erscheinungsformen befasst, die für einen weiten Kreis potentieller Regelungsadressaten von aktueller praktischer Bedeutung sind. Sie hat dies vor allem unter dem Blickwinkel getan, ob es – entsprechend einem aktuell auf EU-Ebene verhandelten Richtlinienvorschlag mit Bezug auf Verträge über digitale Inhalte – eines eigenständigen Rechtsregimes für „digitale Verträge“ bedarf, oder ob es ausreicht, das geltende, in der „analogen“ Welt bewährte Schuldrecht in einzelnen Aspekten zu ergänzen. Die Prüfung hat – um es vorwegzunehmen – ergeben, dass im Bereich des Schuldrechts nur ein punktueller gesetzgeberischer Handlungsbedarf besteht.

Vertragsschluss durch Roboter

Vertragsschlüsse unter Beteiligung kommunizierender „intelligenter“ Gegenstände im „Internet der Dinge“ werfen bürgerlich-rechtliche Fragen auf. Mit Blick auf die voranschreitende Vernetzung von Maschinen und ganzen Produktionsanlagen in der „Industrie 4.0“ sowie die zunehmende Verbreitung von „Smart Products“ in allen Lebensbereichen müssen sich diese Fragen verlässlich beantworten lassen. Wenn etwa eine Produktionsanlage eigenständig Teile ordert oder ein Kühlschrank automatisiert Milch nachbestellt und auch die Entgegennahme sowie Beantwortung der Erklärung automatisiert erfolgt, muss der Rechtsrahmen die Feststellung ermöglichen, ob ein Vertrag zustande gekommen ist und welchen Inhalt er hat. Ist im Zusammenhang mit einem Bestellprozess zwischen Maschinen („M2M“) ein Fehler unterlaufen, muss beurteilt werden können, ob und unter welchen Voraussetzungen eine Anfechtung Erfolg verspricht. Die Rechtsgeschäftslehre führt insoweit zu sach- und interessengerechten Lösungen. Die Regelungen des BGB sind hinreichend abstrakt gehalten, um mit ihnen auch Phänomene der modernen Kommunikationstechnologien interessengerecht bewältigen zu können. Auch die von einem Computer autonom erzeugte Erklärung lässt sich letztlich auf den Willen desjenigen zurückführen, der sich des Computers bedient und dem die Erklärung deshalb zuzurechnen ist. In der Konsequenz ist dann auch bei der Auslegung von „M2M“-Kommunikation auf die hinter den Maschinen stehenden menschlichen Akteure abzustellen. Dies gilt gleichermaßen bei der Beurteilung, ob eine Erklärung der Anfechtbarkeit wegen Irrtums unterliegt. Dass sich dabei nicht einfache Abgrenzungsfragen stellen können, ist „digitalen“ und „analogen“ Sachverhalten gemeinsam und erfordert keine Sonderregelungen.

Haftungsrechtliche Fragen im Internet der Dinge

Das „Internet der Dinge“ wirft neben rechtsgeschäftlichen aber auch haftungsrechtliche Fragen auf. Eine in Prozessabläufe eingebundene autonom agierende Maschine oder ein Smart Product – z. B. ein selbstfahrender Rasenmäher – können durch Fehlleistungen Schäden verursachen. Rechtsfragen stellen sich insoweit nicht nur hinsichtlich der vertraglichen Haftung, sondern auch – und gerade – mit Bezug auf die außervertragliche Haftung. Kommunizieren Maschinen miteinander, wie es charakteristisch für die „Industrie 4.0“ ist, können Kommunikationsfehler zu Produktionsmängeln oder -ausfällen führen. Die möglichen Fehler und Kausalverläufe sowie die mit ihnen und ihrer Aufklärbarkeit verbundenen Risiken werden die Beteiligten dabei vorab häufig – insbesondere bei komplexen Wertschöpfungsketten – nur schwer abschätzen können. Das geltende Schuldrecht gibt ihnen die Möglichkeit, für vertragliche Haftungsansprüche interessengerechte Vereinbarungen zu treffen. Insoweit ist derzeit nicht erkennbar, dass Anlass für ein Tätigwerden des Gesetzgebers besteht. Schwieriger liegen die Dinge jedoch im Bereich der außervertraglichen Haftung. Herausforderungen ergeben sich dabei weniger bei der verschuldensabhängigen Produzentenhaftung. Die Pflichten des Herstellers von Robotern unterscheiden sich nicht grundlegend von den Pflichten, die mit der Herstellung anderer Produkte einhergehen. Eine Haftungslücke beim Betrieb autonomer Systeme zeichnet sich aber im Bereich der verschuldensunabhängigen Haftung ab. Der Betrieb autonomer Systeme geht mit dem Risiko einher, dass sie schadensverursachende Aktionen vornehmen, die für den Hersteller trotz aller Sorgfalt nicht absehbar waren und ihm deshalb nicht anzulasten sind. Auch den Betreiber des autonomen Systems wird nur dann ein Verschulden treffen, wenn er bei dessen Einsatz Sorgfaltspflichten verletzt hat. Es ist gewissermaßen die Kehrseite der erwünschten „Eigenständigkeit“ autonomer Systeme, dass sich ihr Verhalten nicht mit Gewissheit vorhersagen und später nachvollziehen lässt. Liegt ein unvermeidbarer Entwicklungsfehler vor, trifft den Hersteller auch keine Produkthaftung. Besteht in solchen Fällen keine Gefährdungshaftung, wie sie z. B. das Straßenverkehrsrecht für Halter von Kraftfahrzeugen bestimmt, droht eine Haftungslücke. In diesem Punkt zeichnet sich ab, dass der Gesetzgeber tätig werden muss. Im Zentrum steht dabei die Frage, wie die Haftungsrisiken im Zusammenhang mit der Herstellung und Nutzung autonomer Systeme interessengerecht verteilt werden sollen. Knüpft man – unter den Aspekten der Beherrschbarkeit der Risiken und des Einstehenmüssens für geschaffene Gefahren – an Risikosphären an, kommen (weil Roboter keine Träger von Rechten und Pflichten sein können) für eine Schadenszurechnung der Hersteller und der Betreiber in Betracht. Die Antwort auf die Frage, wem das Risiko letztlich zuzuweisen ist, wird durch das geltende Recht nicht vorgezeichnet. Sie berührt neben juristischen auch ökonomische Aspekte. Die Arbeitsgruppe hat sich deshalb darauf beschränkt, vier – in keinem Alternativverhältnis zueinander stehende – Lösungsansätze aufzuzeigen, mit denen die sich abzeichnende Haftungslücke geschlossen werden kann. Denkbar ist die – ggf. mit einer Versicherungspflicht

zu verbindende – Einführung einer gesetzlichen Gefährdungshaftung des Betreibers autonomer Systeme nach dem Vorbild der straßenverkehrsrechtlichen Halterhaftung und der Tierhalterhaftung. Möglich wäre aber auch eine Verschärfung der Produkthaftung oder die Einführung eines neuen, eigenständigen gesetzlichen Haftungsregimes. Da sich Haftungsfragen beim Internet der Dinge nicht nur im nationalen Kontext stellen, muss auch eine Regelung auf EU-Ebene in Betracht gezogen werden, wie sie das Europäische Parlament seit kurzem fordert.

Cloud Computing

Ein Phänomen, dessen praktische Bedeutung durch die Vernetzung von Rechenressourcen stetig zunimmt, ist die als Cloud Computing bezeichnete Auslagerung informationstechnischer Strukturen und Abläufe. Es handelt sich um einen Wachstumsmarkt, der – auch auf EU-Ebene thematisierte – Rechtsfragen aufwirft. Cloud Computing bedeutet die Virtualisierung von Ressourcen wie Speicherplatz oder Rechenleistung. Nutzer speichern Daten oder führen Programme aus, indem sie webbasiert auf nicht lokale Speicher- und Rechenkapazitäten zugreifen. Die Erscheinungsformen, in denen dies geschieht, sind vielfältig. Sie unterscheiden sich zum einen nach dem potentiellen Nutzerkreis der Cloud Services. Zum anderen lässt sich danach differenzieren, welche Leistung der Anbieter von Cloud Services bereitstellt. Es kann sich dabei z. B. um reine Rechen- und Speicherressourcen („Infrastructure as a Service“) oder auch die Bereitstellung von Anwendungssoftware („Software as a Service“) handeln. Der Vielgestaltigkeit des Phänomens entspricht die Vielzahl der Fragen, die sich bereits bei der schuldrechtlichen Einordnung einfach strukturierter Rechtsverhältnisse zeigen und für die es keine pauschalen Antworten geben kann. Die Arbeitsgruppe hat sich den praktisch besonders wichtigen Fragen gewidmet, die sich im Verhältnis zwischen Anbieter und Nutzer bei Diensten ergeben, die einem offenen Nutzerkreis angeboten werden (Public Cloud). Sie hat unter Auseinandersetzung mit Rechtsprechung und Schrifttum herausgearbeitet, welche Vertragstypen in Betracht kommen und wie sich die verschiedenen Cloud Services vertragstypologisch einordnen lassen. In diversen Fallgestaltungen gibt es eine klare Tendenz, einen Mietvertrag anzunehmen. Das geltende Mietrecht hält dabei überwiegend sach- und interessengerechte Lösungen bereit, die von den Vertragsparteien ggf. durch privatautonome Regelungen ergänzt werden können. Punktuell hat die Arbeitsgruppe jedoch einen Bedarf für ergänzende Regelungen und Klarstellungen durch den Gesetzgeber ausgemacht. So können sich Mietverträge nach geltendem Recht nur auf körperliche Gegenstände beziehen. Es sollte deshalb wie im Kaufrecht klargestellt werden, dass das Mietrecht auch auf sonstige Gegenstände Anwendung finden kann. Als problematisch erweist sich auch die Frage, mit welcher Frist der Anbieter einen Vertrag über Cloud Services beenden kann. Bei einer Kündigung durch den Anbieter wird der Nutzer ein erhebliches Interesse daran haben, über einen gewissen Zeitrahmen zu verfügen, in dem er sich einen neuen Vertragspartner suchen kann. Im geltenden Mietrecht finden sich verschiedene Kündigungsfristen, die teilweise nicht den Interessen der Parteien eines Vertrags über Cloud Services entsprechen. Es bedarf insoweit entweder einer gesetzlichen

Klarstellung oder einer Erweiterung des Fristenkatalogs. Der Gesetzgeber sollte zudem ausdrücklich im Mietrecht verankern, dass der Nutzer gegen den Anbieter nach Vertragsbeendigung einen Anspruch auf die Rückgabe von Daten hat.

Streaming

Die Bereitstellung von Video- und Audioinhalten in Formen, bei denen Nutzer entscheiden können, welche Titel sie zu welchen Zeitpunkten konsumieren, findet zunehmend über das Internet statt. Ein Verbraucher muss keinen Datenträger mehr kaufen oder mieten, um zu einem von ihm bestimmten Zeitpunkt einen Spielfilm zu sehen oder ein Musikstück zu hören. Verfügt er über eine hinreichend leistungsfähige Internetverbindung und steht ihm ein ausreichendes Datenvolumen zur Verfügung, bedarf es für den Werkgenuss nicht einmal der Herstellung einer dauerhaften digitalen Kopie auf eigenen Rechenressourcen. Technisch möglich ist dies durch Streaming, bei dem Daten konstant zum Nutzer „strömen". Streaming eignet sich zum einen für die Bereitstellung von Werken zum individuellen webbasierten Abruf (On-Demand-Streaming). Zum anderen ermöglicht Streaming die Übertragung von Inhalten zu einem vom Anbieter bestimmten Zeitpunkt bzw. in Echtzeit (Live-Streaming). Insgesamt handelt es sich um einen durch unterschiedliche Geschäftsmodelle geprägten Wachstumsmarkt. Beachtung in Rechtsprechung und Literatur haben bislang vor allem unter urheberrechtlichen Aspekten illegale Streaming-Angebote gefunden. Dabei wirft das Phänomen durchaus auch unter vertragsrechtlichen Aspekten Fragen auf. So bedarf es bei Verträgen über Streaming-Leistungen einer vertragstypologischen Einordnung, die je nach vereinbartem Leistungsinhalt sehr unterschiedlich ausfallen kann und nicht höchstrichterlich geklärt ist. Entgeltliche Verträge über Live-Streaming weisen Ähnlichkeiten zum Bezahlfernsehen auf und lassen sich als Dienstvertrag einordnen. Auf entgeltliches On-Demand-Streaming kann Miet- oder Dienstvertragsrecht anwendbar sein. Die erforderliche Abgrenzung mag dabei Schwierigkeiten bereiten. Angesichts des breiten Spektrums von Streaming-Angeboten und in Ermangelung einer spezifischen Gemeinsamkeit von Streaming-Verträgen fehlt es jedoch an hinreichenden Anknüpfungspunkten für die Schaffung eines einheitlichen Vertragstypus. Hat der Vertrag ein konkretes Werk zum Gegenstand, erscheint eine Einordnung als Mietvertrag sachgerecht. Wird einem Nutzer im Rahmen eines Abonnements der Zugriff auf eine Werksammlung ermöglicht, deren Zusammenstellung und ständige Veränderung dem Anbieter vorbehalten bleibt, spricht vieles für die Anwendbarkeit von Dienstvertragsrecht. Bei unentgeltlichen Verträgen über Live-Streaming führt das Auftragsrecht zu angemessenen Ergebnissen. Die Arbeitsgruppe ist zu dem Ergebnis gelangt, dass das Bürgerliche Gesetzbuch derzeit aus Sicht aller Beteiligten für die praktisch bedeutsamen Rechtsfragen des Streaming zufriedenstellende Antworten bereithält. Für ein Tätigwerden des Gesetzgebers besteht demgemäß aktuell kein Anlass.

Soziale Netzwerke

Neben einem stetig zunehmenden Angebot an Streaming-Leistungen wird das Internet in wachsendem Maße durch soziale Netzwerke geprägt. Sie ermöglichen Nutzern über eine Netzwerkplattform das Konstituieren sozialer Beziehungen, den Austausch von Inhalten und das aktive Mitgestalten von Kommunikationsprozessen. In Deutschland machen – nicht anders als in anderen Teilen der Welt – breite Bevölkerungskreise von dieser Möglichkeit Gebrauch. Die Arbeitsgruppe hatte deshalb Anlass zu prüfen, ob die Etablierung sozialer Netzwerke neben vieldiskutierten Aspekten aus anderen Rechtsbereichen vertragsrechtliche Fragen aufwirft, die gesetzliche Regelungen erfordern. Ein Regelungsbedürfnis ließe sich – obgleich die Praxis mit insoweit bestehenden Unsicherheiten bislang gut umgehen konnte – hinsichtlich der vertragstypologischen Einordnung vertreten. Eine gesetzliche Einordnung würde allerdings voraussetzen, dass es sich um ein Phänomen mit einem weitgehend gleichen und gleichbleibenden Erscheinungsbild handelt. Entsprechend dem informationstechnischen Fortschritt sowie unterschiedlichen und sich fortlaufend ändernden Nutzerbedürfnissen und Funktionalitäten sind soziale Netzwerke in ihrer konkreten Ausgestaltung jedoch flüchtig. Eine Regelung erscheint damit – abgesehen davon, dass sie weder von der Praxis noch im Schrifttum gefordert wird – in zukunftsfester Weise kaum möglich. Angesichts des hohen Anteils und der hohen absoluten Zahl minderjähriger Nutzer mag es unbefriedigend erscheinen, dass die vor der Nutzung eines sozialen Netzwerks regelmäßig erforderliche datenschutzrechtliche Einwilligung in die Verarbeitung personenbezogener Daten schon ab dem 16. Lebensjahr wirksam erteilt werden kann, die bürgerlich-rechtlich unbeschränkte Geschäftsfähigkeit jedoch erst ab dem 18. Lebensjahr gegeben ist. Eine Harmonisierung wäre auf nationaler Ebene jedoch nur durch eine Angleichung nach unten – d. h. eine Herabsetzung des zivilrechtlichen Minderjährigenschutzes – möglich. Für eine solche Verschiebung zu Lasten Minderjähriger besteht offenkundig keine Veranlassung.

„Bezahlen mit Daten“

Die Nutzung eines sozialen Netzwerks ist in der Praxis in weitem Umfang möglich, ohne eine finanzielle Gegenleistung erbringen zu müssen. Anbieter sozialer Netzwerke stellen Nutzern für ihre Leistung überwiegend keine Geldbeträge in Rechnung. Das dominierende – sehr erfolgreiche – Geschäftsmodell fußt vielmehr darauf, persönliche Daten von Nutzern sowie von bzw. mit ihnen kommunizierte Inhalte zu monetarisieren, also wirtschaftlich zu verwerten. Soziale Netzwerke eignen sich in besonderem Maße für das Generieren von Erträgen über personalisierte Werbung. Demgemäß sind sie – was der Mehrzahl der Nutzer durchaus bewusst ist – darauf ausgelegt, dass „mit Daten bezahlt“ wird. Gemeinsam hat die Leistung des Nutzers mit einer Geldzahlung, dass dem Betreiber für die Bereitstellung seines Dienstes ein wirtschaftlicher Wert – ein Entgelt – zugewendet wird. Mit Blick auf die Zweckbindung der wechselseitigen Leistungen liegt beim Vertrag über die „kostenlose“ Nutzung eines sozialen Netzwerks mithin ein Synallagma vor. Daten als Gegenstand des Leistungsaustauschs im Rahmen eines Schuldverhältnisses sind bislang aber nicht geregelt. Es gibt – auch in anderen

Mitgliedstaaten der Europäischen Union – kein „Datenschuldrecht". Das dem persönlichkeitsrechtlichen Schutz dienende Datenschutzrecht hat nicht die Funktion, den Leistungsaustausch durch Verträge zu regeln, und stellt keinen Regelungsrahmen für die Äquivalenz in Leistungsaustauschbeziehungen dar. Andererseits kann es, weil die verwerteten Nutzerdaten durchweg personenbezogen sind, bei der Beurteilung zivilrechtlicher Fragen nicht ausgeklammert werden. Es ist vielmehr zentraler Anknüpfungspunkt, weil die Leistung des Nutzers bei näherer Betrachtung nicht in der Hingabe von Daten, sondern in der datenschutzrechtlichen Einwilligung in die kommerzielle Verwertung personenbezogener Daten liegt. Die datenschutzrechtliche Einwilligung ist dabei die den Typus des Vertragsverhältnisses nicht prägende Gegenleistung. Dass der Nutzer datenschutzrechtlich das unentziehbare Recht hat, über die Erteilung der Einwilligung freiwillig zu entscheiden und eine erteilte Einwilligung im Nachhinein zu widerrufen, lässt sich zivilrechtlich problemlos über die Annahme einer auflösenden Bedingung, eine Unklagbarkeit sowie den Ausschluss von Ansprüchen wegen Nichterfüllung bewältigen. Mit Bezug auf das zivilrechtliche Widerrufsrecht von Verbrauchern besteht nur ganz punktuell ein (nicht drängender) Regelungsbedarf. Bedenklich erscheint jedoch, dass die vom Nutzer zu erbringende Hauptleistung im Synallagma formularmäßig über „Nutzungsbedingungen" bzw. „Datenrichtlinien", also in Formen vereinbart wird, die dem Nutzer die von ihm zu erbringende Leistung nicht in gleicher Weise wie die Verpflichtung zur Zahlung eines Geldbetrags vor Augen führen. Für den elektronischen Geschäftsverkehr enthält das geltende Recht die „Button"-Lösung: Ein Verbraucher muss bei einer Bestellung ausdrücklich bestätigen, dass er sich zu einer Zahlung verpflichtet. Die Arbeitsgruppe sieht es als sach- und interessengerecht an, eine solche „Button"-Lösung auch für das „Bezahlen mit Daten" gesetzlich zu verankern. Erwägenswert erscheint auch eine gesetzliche Klarstellung, dass es nicht zu Lasten einer Vertragspartei zu werten ist, wenn die von ihr zu erbringende Gegenleistung nicht in einer Geldzahlung, sondern in einer Einwilligung in die Nutzung personenbezogener Daten besteht.

Erwerb digitaler Inhalte im Wege des Downloads

Digitale Inhalte werden in unterschiedlichen Formen über das Internet bereitgestellt. Mag es bei Video- und Audioinhalten eine Tendenz geben, den Werkgenuss zunehmend in der Form des Streamings zu ermöglichen, erfolgt der internetbasierte Erwerb dauerhafter Nutzungsrechte an Inhalten in weitem Umfang im Wege des Downloads. Die gesellschaftliche und ökonomische Relevanz solcher Erwerbsvorgänge ist erheblich. Technisch läuft der Erwerb in der Weise ab, dass der Erwerber die Inhalte in Dateiform über das Internet empfängt und sie auf ihm zur Verfügung stehenden Rechenressourcen abspeichert. Anders als beim Streaming benötigt er für den Werkgenuss dann keine Internetverbindung mehr. Die geltenden bürgerlich-rechtlichen Regelungen sind für den so erfolgenden Erwerb digitaler Inhalte zum rezeptiven Werkgenuss – also von Videos, Musik, Hörbüchern, E-Books u. a. – sach- und interessengerecht. Das gilt zum einen für die im BGB bereits enthaltenen spezifischen Regelungen zum Widerrufsrecht und zu Informationspflichten bei Verbraucherverträgen über digitale Inhalte. Es gilt aber

auch für die allgemeinen Regelungen. Bedeutung kommt dabei dem Umstand zu, dass in der Praxis für viele theoretisch streitanfällige Sachverhalte geeignete Lösungen gefunden werden. Vertragstypologisch ist der Vertrag über den Erwerb digitaler Inhalte im Wege des Downloads nach herrschender Meinung als Kaufvertrag über einen sonstigen Gegenstand einzuordnen, auf den die Regelungen über den Sachkauf entsprechende Anwendung finden. Die kaufrechtlichen Gewährleistungsregelungen tragen den Interessen der Beteiligten sachgerecht und ausgewogen Rechnung. Es bedarf keiner Rechtsänderungen, damit die dem geltenden Schuldrecht zugrundeliegenden gesetzgeberischen Wertungsentscheidungen beim Erwerb digitaler Inhalte im Wege des Downloads zum Tragen kommen. Soweit teilweise unter verbraucherpolitischen Aspekten die Einführung neuer Käuferrechte gefordert wird – etwa ein Recht des Verbrauchers, digitale Inhalte vor Beginn der Widerrufsfrist online zu erproben oder diese später erneut herunterzuladen – ergibt sich bei näherer Betrachtung, dass solche Rechte im Widerspruch zur Rechtslage bei „analogen“ Gütern stehen würden. Ein schuldrechtlicher Anspruch auf Nutzung erworbener digitaler Inhalte ohne Bindung an ein bestimmtes Gerät und ein bestimmtes technisches System mag verbraucherpolitisch wünschenswert sein. Er muss aber das Urheberrecht berücksichtigen und setzt eine Interoperabilität durch technische Normung voraus, für die das bürgerliche Recht nicht der richtige Regelungsort ist.

WAP-Billing und Zahlungswege im Internet

Mit der immer größeren Bandbreite digitaler Leistungen geht auch eine Zunahme von Missbrauchsmöglichkeiten einher. Exemplarisch ist insoweit das sog. WAP-Billing. Es handelt sich um ein Verfahren, das Nutzern von Geräten mit mobiler Datenverbindung erlaubt, online bei einem Drittanbieter bezogene Leistungen – z. B. eine heruntergeladene Datei – über die Rechnung des Mobilfunkanbieters zu bezahlen. Das geltende Telekommunikationsrecht sieht die Möglichkeit, dass Rechnungspositionen von Drittanbietern in die Telefonrechnung einfließen, ausdrücklich vor. Während Zahlungswege im Internet in ihren verschiedenen Ausprägungen über die Umsetzung der Zweiten Zahlungsdiensterichtlinie in deutsches Recht hinaus aktuell keinen Anlass für gesetzgeberische Maßnahmen geben, liegt es beim WAP-Billing anders. Nach den geltenden telekommunikationsrechtlichen Vorschriften und ihrer Handhabung in der Praxis ist es für Inhaber von Mobilfunkanschlüssen beschwerlich, sich gegen unberechtigte Forderungen, die Dritte im Wege des WAP-Billing geltend machen, zur Wehr zu setzen. Unseriöse Drittanbieter nutzen dies, um rechtlich nicht wirksam vereinbarte Leistungen abzurechnen. Da die Beträge verhältnismäßig gering sind, werden sie in der Praxis, vor allem wenn eine Sperrung des Telefonanschlusses droht, beglichen. Es bedarf daher weitergehender Regelungen zum Schutz der Verbraucher vor solchen Praktiken. Erwägenswert ist zum einen, den Einzug von Forderungen Dritter über die Telefonrechnung grundsätzlich zu verbieten, wenn der Verbraucher dem Einzug nicht einzelfallbezogen zustimmt. Gleichermaßen sollte in Betracht gezo-

gen werden, Verbrauchern ein Recht zu gewähren, gegenüber dem Telekommunikationsanbieter der Einziehung der Forderung eines Dritten fristgebunden zu widersprechen.

Virtuelle Währungen

Mit der fortschreitenden Digitalisierung hat nicht nur das Spektrum der über das Internet vertraglich vereinbarten Leistungen zugenommen. In Gestalt virtueller Währungen haben sich auch geldähnliche neue Tauschmittel entwickelt. Zu den bekanntesten virtuellen Währungen gehören Bitcoins. Es handelt sich um Datenmengen, die durch den Einsatz von Rechenleistung generiert werden. Unter Verwendung kryptographischer Schlüssel werden Bitcoins ohne Steuerung durch und ohne Umwege über eine zentrale Instanz transferiert. Transaktionen werden in die Blockchain, eine Art offenes, dezentral gespeichertes Kontobuch eingestellt. Das Design gewährleistet, dass derjenige, der Bitcoins verwendet, vorher ihr Inhaber geworden ist und sie noch nicht ausgegeben hat. Aufgrund dieser Eigenschaften lassen sich Bitcoins zivilrechtlich schwer einordnen. Wegen ihres virtuellen Charakters stellen sie keine körperliche Sache dar. Mangels Existenz eines Schuldners sind sie auch keine Forderungen. Ihre Inhaberschaft erschöpft sich in der faktischen, von einer Akzeptanz der virtuellen Währung als Gegenleistung abhängigen Möglichkeit zu Transaktionen. Mit Blick auf die Vertragsfreiheit steht dies jedoch nicht der Möglichkeit entgegen, Bitcoins zum Gegenstand eines Leistungsaustauschs zu machen. Es kann sich dann aber z. B. die Frage stellen, wie der Austausch von Bitcoins gegen Geld vertragstypologisch zu qualifizieren ist. Sind die rechtlichen Rahmenbedingungen bei Verwendung von Bitcoins im internetbasierten Handel auch schwer einzuordnen, gibt es bislang – wohl auch wegen des begrenzten Kreises von Nutzern – keine Erkenntnisse zu praktischen Schwierigkeiten. Das mag damit zusammenhängen, dass das durch die Blockchain-Technologie geprägte System der virtuellen Währung gerade auf eine Freiheit von regelnden Eingriffen ausgerichtet ist. Jedenfalls derzeit ist ein gesetzgeberischer Handlungsbedarf nicht ersichtlich. Im Ergebnis gilt dies auch für vollstreckungsrechtliche Fragen. Eine Zwangsvollstreckung in Bitcoins ist nach den geltenden Bestimmungen möglich, wenn der Schuldner mitwirkt. In Fällen einer fehlenden Mitwirkung mögen ihr unter technischen Gesichtspunkten Grenzen gesetzt sein. Praktische Probleme sind insoweit aber bislang nicht bekannt geworden. Für den Gesetzgeber besteht deshalb aktuell kein Anlass, regelnd einzugreifen.

D. Digitales Persönlichkeitsrecht

Persönlichkeitsrechtsverletzungen erfahren in der „digitalen Welt“ besondere Ausprägungen. Zum einen hat die Digitalisierung gänzlich neue Verletzungshandlungen hervorgebracht (z. B. herabsetzende Wortkombinationen durch Autocomplete-Funktion von Suchmaschinen). Vor allem weisen digitale Sachverhalte aber Besonderheiten in der Art und Weise der Beeinträchtigung des Persönlichkeitsrechts auf. Hervorzuheben sind insoweit persönlichkeitsrechtsverletzende Beiträge in sozialen Netzwerken. Sie sind – häufig zudem im Schutz der

Anonymität – nicht nur schnell verfasst und leicht geteilt. Im Vergleich zu „analogen Kommunikationsformen“ besonders prägend ist die Perpetuierung der Persönlichkeitsrechtsverletzung, da die Beiträge grundsätzlich dauerhaft, überall und jederzeit abrufbar sind.

Indes kann mit dem geltenden Recht, insbesondere unter Heranziehung der in der analogen Welt entwickelten Kriterien zum allgemeinen Persönlichkeitsrecht, diesen Besonderheiten grundsätzlich angemessen Rechnung getragen werden. Dies belegt die bisherige Rechtsprechung sowohl zur Verbreitung herabsetzender Tatsachenbehauptungen oder Werturteile als auch zu nicht herabsetzenden Veröffentlichungen oder Verbreitungen, die unter dem Gesichtspunkt des Rechts auf informationelle Selbstbestimmung ebenfalls persönlichkeitsrelevant sein können („Recht auf Vergessenwerden“). Die digitalen Phänomene lassen sich sämtlich als Attribute der Persönlichkeit in der „analogen“ Welt begreifen. Vor diesem Hintergrund verneint die Arbeitsgruppe derzeit die Frage, ob die Rechtsordnung eine darüber hinausgehende „digitale Persönlichkeit“ anerkennen und schützen müsse. Ungeachtet dessen bleibt zudem abzuwarten, inwiefern die EU-Datenschutzgrundverordnung (EU-DGSVO) dem nationalen Gesetzgeber überhaupt noch Raum für eine eigene Gestaltung dieses Bereichs lässt.

Darüber hinaus besteht aus Sicht der Arbeitsgruppe gegenwärtig in folgenden Bereichen kein gesetzgeberischer Handlungsbedarf:

- § 13 Abs. 6 TMG, wonach der Diensteanbieter i. S. d. Rechts auf informationelle Selbstbestimmung die Nutzung der Telemedien anonym oder pseudonym ermöglichen muss, steht zwar im Spannungsverhältnis zum Bedürfnis, Rechtsverletzungen im Internet effektiv verfolgen zu können. Über die Einführung einer Klarnamenpflicht bzw. eine entsprechende Lockerung der Vorschrift bedarf es angesichts der grundrechtlichen Dimension aber zunächst einer gesellschaftlichen Diskussion, bevor der Gesetzgeber tätig werden sollte.
- Beim Profildiebstahl im Internet handelt es sich um eine besondere Ausprägung des – bereits aus der analogen Welt bekannten – Profildiebstahls. Neben strafrechtlichen Sanktionen kann solchen Eingriffen schon heute auch zivilrechtlich durch die Geltendmachung von Unterlassungs-, Beseitigungs-, Schadensersatz- und ggf. sogar Schmerzensgeldansprüchen begegnet werden.
- Das allgemeine Persönlichkeitsrecht kann auch durch „ungewollte Einflüsse Dritter“, wie etwa unerwünschte Werbe-E-Mails oder Online-Werbeblocker betroffen sein. Die Rechtslage hier ist weitestgehend geklärt. Ggf. noch offene Fragen sollten zunächst der Rechtsprechung überlassen bleiben.

Punktuellen Handlungsbedarf für den Gesetzgeber sieht die Arbeitsgruppe demgegenüber mit Blick auf die (faktische) Durchsetzung zivilrechtlicher Ansprüche, die aus dem allgemeinen Persönlichkeitsrecht erwachsen.

- Um einen ihm unbekannten Täter einer Persönlichkeitsrechtsverletzung im Internet zu ermitteln, hat der Betroffene nach derzeit geltendem Recht allenfalls

die Möglichkeit, Strafantrag zu stellen, um nach Einleitung des Ermittlungsverfahrens über sein strafprozessuales Akteneinsichtsrecht die von der Staatsanwaltschaft ermittelte Identität des Beschuldigten zu erfahren. Einem (direkten) Auskunftsanspruch gegen den Intermediär (Betreiber von Suchmaschinen, Internetforen, Online-Archiven, Host-Providern, Access Providern etc.) steht nach geltender Rechtslage entgegen, dass dieser wegen § 12 Abs. 2 TMG Dritten gegenüber grundsätzlich keine Auskunft über Bestandsdaten erteilen darf und die Durchsetzung des allgemeinen Persönlichkeitsrechts – anders als etwa die Durchsetzung des Rechts am geistigen Eigentum – nicht zu den in § 14 Abs. 2 TMG aufgelisteten Ausnahmen zählt. Spätestens im Zusammenhang mit der Implementierung der EU-DSGVO in das nationale Recht ist daher eine entsprechende Erweiterung des Ausnahmekatalogs in § 14 Abs. 2 TMG – wie vom Bundesrat bereits im November 2015 gefordert – vorzunehmen oder jedenfalls eine vergleichbare Regelung zu treffen, die dem Betroffenen eine effektive Wahrnehmung seiner Rechte ermöglicht. Das von der Arbeitsgruppe festgestellte Bedürfnis eines individuellen Auskunftsanspruchs bei Persönlichkeitsrechtsverletzungen im Internet hat die Bundesregierung zwischenzeitlich im Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG-E) aufgegriffen. Das Gesetzgebungsverfahren ist allerdings noch nicht abgeschlossen. Die Arbeitsgruppe schlägt überdies vor, den Auskunftsanspruch, der von der Rechtsprechung bislang auf § 242 BGB gestützt wird, selbständig – ebenso wie im gewerblichen Rechtsschutz geschehen – gesetzlich zu kodifizieren. Dies könnte etwa im Telemediengesetz oder aber – indes nicht nur bezogen auf strafbare Inhalte – im NetzDG geschehen. Es erscheint zudem sinnvoll, die Auskunft über Bestands- oder Nutzungsdaten von einer vorherigen richterlichen Anordnung abhängig zu machen, vergleichbar dem – allerdings auf Verkehrsdaten zugeschnittenen – § 101 Abs. 9 UrhG.

- Sind Täter oder Teilnehmer einer Persönlichkeitsrechtsverletzung bekannt, können sie auf Unterlassung, Beseitigung und Widerruf in Anspruch genommen werden. Bleiben diese hingegen unbekannt, kann der Einzelne sich zwar noch an den Intermediär wenden. Die gegenwärtige Praxis der Intermediäre im Umgang mit entsprechenden Anliegen ist jedoch unbefriedigend.

  In der Regel kann der Betroffene Direktansprüche gegenüber einem Intermediär nur erfolgreich geltend machen, wenn dieser eine ihm zumutbare Prüfpflicht verletzt hat. Dies erfordert wiederum, dass ihn der Betroffene zuvor qualifiziert auf die Persönlichkeitsverletzung hingewiesen hat. In der Praxis setzen die Intermediäre diese rechtlichen Vorgaben unterschiedlich um. Dies gilt zum einen für die Möglichkeit zur Abgabe des qualifizierten Hinweises und die technische Abwicklung des sich anschließenden Löschungsverfahrens (Prüfverfahren). Aber auch die „Löschungspolitik“ einer Vielzahl von Intermediären steht zu Recht in der Kritik. Insbesondere die bisherigen Bemühungen von Plattformanbietern, effektiv gegen Persönlichkeitsrechtsverletzungen vorzugehen, reichen vielerorts nicht aus. Vor diesem Hintergrund besteht aus

Sicht der Arbeitsgruppe das Bedürfnis nach einem einheitlichen und verbraucherfreundlichen Löschungsverfahren der Diensteanbieter bei Persönlichkeitsrechtsverletzungen im Internet.

Zentral ist dabei zunächst die Forderung nach einem unkompliziert auffindbaren Löschantragsformular über eine Buttonlösung in der Nähe des zu löschenden Beitrags. Das Löschantragsformular sollte in der Sprache der Veröffentlichung und ergänzend in englischer Sprache abgefasst sein. Mit der Möglichkeit zur Übermittlung des Löschgesuchs soll gewährleistet werden, dass der Betroffene dem Intermediär unkompliziert den erforderlichen qualifizierten Hinweis auf die Persönlichkeitsrechtsverletzung erteilen und damit das Löschungsverfahren „in Gang setzen" kann.

In Anlehnung an die bestehende Rechtsprechung ist für das Löschungsverfahren grundsätzlich eine vorherige Anhörung des Verfassers des Beitrags zu fordern, in Eil- und Evidenzfällen eine nachträgliche. Das zu fordernde unkomplizierte Löschungsverfahren darf andererseits nicht zu einer voraussetzungslosen Löschung führen. Im Hinblick auf das einzuhaltende Löschverfahren ist vielmehr auf die Voraussetzungen des zugrundeliegenden materiell-rechtlichen Löschungsanspruches unter Abwägung der Beeinträchtigung des Betroffenen mit dem Grundrecht auf Meinungsfreiheit des Äußernden und unter Wahrung der Grundsätze des Meinungspluralismus abzustellen. Diese Abwägung und die Prüfung der Voraussetzungen ist daher durch den Intermediär im Verfahren durch den ausreichenden Einsatz geeigneten und geschulten Personals sicherzustellen. Erforderlich hierfür dürfte zudem sein, dass die Intermediäre ihre Kriterien zur Löschung und das dazugehörige Verfahren offenlegen. Eine Markierung des sich im Löschungsverfahren befindlichen Beitrags könnte darüber hinaus zu mehr Sensibilität der Nutzer führen. Ferner sind die Beteiligten über den Ausgang des Löschungsverfahrens zu informieren. Zur Vereinfachung der Rechtsdurchsetzung bietet es sich zudem an, einen sog. „Ombudsmann" für Streitigkeiten im Zusammenhang mit Persönlichkeitsrechtsverletzungen im Internet einzuführen und auf europäischer Ebene auf eine Pflicht zur Benennung eines inländischen Zustellungsbevollmächtigten hinzuwirken.

Schließlich erscheint es aufgrund des ungleichen Kräfteverhältnisses zwischen den Netzdiensteanbietern und den Nutzern sinnvoll, ein gesetzlich normiertes Löschungsverfahren mit einem Verbandsklagerecht dergestalt zu flankieren, dass qualifizierten und gelisteten Verbänden und Einrichtungen bei Zuwiderhandlungen gegen die Verfahrensvorschriften (bspw. kein Vorhalten eines Löschantragsformulars) Ansprüche eingeräumt werden.

Forderungen nach gesetzlichen Vorgaben für das Löschungsverfahren von Diensteanbietern sind ebenfalls im NetzDG-Entwurf der Bundesregierung aufgegriffen. Vorgesehen sind eine gesetzliche Berichtspflicht für soziale Netzwerke über den Umgang mit Hasskriminalität und anderen strafbaren Inhalten, ein wirk-

sames Beschwerdemanagement sowie die Benennung eines inländischen Zustellungsbevollmächtigten. Schon wegen des – auf bestimmte strafbewehrte Handlungen – beschränkten Anwendungsbereichs erfüllt der Gesetzentwurf die Forderung der Arbeitsgruppe nach einem einheitlichen und verbraucherfreundlichen Löschungsverfahren jedoch nur unzureichend. Im Übrigen bleibt auch hier das weitere Gesetzgebungsverfahren abzuwarten.

E. Digitaler Nachlass

Hinter der Thematik des digitalen Nachlasses verbirgt sich eine zweistufige Prüfung des postmortalen Schicksals von Rechtspositionen, die der Erblasser aufgrund elektronischer Kommunikation innehatte (bspw. Nutzer-Accounts oder Foren-Einträge). Auf der ersten Stufe sind die einzelnen Rechtspositionen nach ihrer Übergangsfähigkeit (Vererbbarkeit) abzugrenzen. Hinsichtlich der übergangsfähigen Rechtspositionen ist sodann auf der zweiten Stufe – wie auch beim übrigen Nachlass – über den Übergangsmodus zu entscheiden. Hierzu gehört neben der Bestimmung der Berechtigten am Nachlass sowie der (praktischen) Nachlassabwicklung insbesondere auch die Frage, wie der Erbe Kenntnis vom konkreten Umfang des Nachlasses erlangen kann.

Die Diskussion um den digitalen Nachlass zeichnet sich durch eine Vielzahl unterschiedlicher Frage- und Problemstellungen aus. Gleichwohl gilt auch hier der Grundsatz der Universalsukzession. Danach geht mit dem Tode einer Person (Erbfall) deren Vermögen (Erbschaft) als Ganzes auf eine oder mehrere andere Personen (Erben) über. Nicht hiervon erfasst werden lediglich unvererbliche Rechtspositionen, wie etwa höchstpersönliche Rechte ohne Vermögenswert und schuldrechtliche Ansprüche, wenn der Inhalt der den Ansprüchen zugrundeliegenden Vertragsbeziehung so stark auf die Person des Berechtigten oder des Verpflichteten zugeschnitten ist, dass sie bei einem Gläubiger- oder Schuldnerwechsel in ihrem Wesen verändert würde (bspw. Partnerschaftsvermittlungsverträge).

Die Universalsukzession führt dazu, dass auch Accounts des Erblassers auf den Erben übergehen. Dieser Übergang erfolgt im Wege des Eintritts des Erben in die bestehende Vertragsbeziehung, die zum Nachlass gehört und aus der sich zugleich entsprechende Auskunftsansprüche bzw. Einsichtnahmerechte für den Erben ergeben. Dies gilt insbesondere auch für Accounts in sozialen Netzwerken. Auch bei diesen Verträgen ist die vom Anbieter zu erbringende Leistung in aller Regel nicht in einem solchen Maß auf die Person des Berechtigten zugeschnitten, dass ein Subjektwechsel die Leistung in ihrem Wesen verändern würde. Nur die Inhalte, die mittels dieser Accounts vom Nutzer geschaffen oder kommuniziert werden, sind in vielen Fällen höchstpersönlich, nicht aber die Leistungen des Providers im Rahmen der Vertragsbeziehung. Die Vertragsbeziehung mit ihren Rechten und Pflichten besteht vom Grundsatz her unabhängig von den Inhalten, die der Nutzer auf der ihm zur Verfügung gestellten Seite einstellt.

Soweit der Erblasser seine elektronische Kommunikation auf einem eigenen Speichermedium abgelegt hat (bspw. abgerufene E-Mails), erfolgt die erbrechtliche

Übertragung zusammen mit dem Übergang des Eigentums am Speichermedium. Berechtigt sind auch hier ausschließlich die Erben.

Daran anknüpfend besteht aus Sicht der Arbeitsgruppe derzeit im Bereich des digitalen Nachlasses kein grundlegender Handlungsbedarf. Die erbrechtlichen Vorschriften ermöglichen eine angemessene Handhabung des digitalen Nachlasses. Dies gilt auch mit Blick auf die nachfolgenden Aspekte:

- Der Grundsatz der Univeralsukzession führt dazu, dass nächste Angehörige, die keine Erben sind, grundsätzlich keinen Zugriff auf den digitalen Nachlass haben. Trotz der teils privaten Inhalte, die sich in der elektronischen Kommunikation des Erblassers befinden können, ist dies aber angemessen. Wie auch bei Nachlassgegenständen der „analogen Welt“, die privaten Inhalt haben (Briefe, Tagebuchaufzeichnungen, Fotos etc.), ist es sachgerecht, dass die Angehörigen auf die Geltendmachung des postmortalen Persönlichkeitsrechts in Form eines Abwehrrechts beschränkt sind.
- Da es beim Übergang des digitalen Nachlasses maßgeblich auf die Erbenstellung ankommt, hat der Erblasser unter Rückgriff auf das geltende Erbrecht vielseitige Möglichkeiten, im Rahmen letztwilliger Verfügungen die Berechtigung an seinem digitalen Nachlass zu regeln.
- Im Hinblick auf Regelungen in allgemeinen Geschäftsbedingungen, die den digitalen Nachlass (etwa den Übergang von Accounts) betreffen (in der Praxis insbesondere Kündigungsklauseln, Legitimationsklauseln und Abwicklungsklauseln) reichen jedenfalls derzeit die geltenden Vorschriften in §§ 305 ff. BGB aus, um eine wirksame und angemessene Kontrolle auch in Bezug auf digitale Sachverhalte zu ermöglichen. Danach sind insbesondere verbreitete Klauseln, die die Unvererbbarkeit eines Accounts vorsehen, unwirksam.
- Beim erbrechtlichen Übergang von E-Books sowie Musik- und Videodownloads greift der urheberrechtliche Erschöpfungsgrundsatz nicht ein. Dies hat zwar zur Folge, dass die Anbieter durch allgemeine Geschäftsbedingungen die Nutzung der digitalen Inhalte auf den Tod befristen können, und aus Sicht der Erben zudem im Einzelfall unklar sein kann, ob sie die digitalen Inhalte des Erblassers weiter nutzen dürfen. Angesichts der aktuell geringen Verbreitung derartiger Klauseln und des Umstandes, dass Änderungen in diesem Bereich entweder Brüche in der Rechtsordnung oder sehr weitreichende Folgen auch für die Übertragung unter Lebenden nach sich ziehen würden, bleibt aber vorerst abzuwarten, wie sich der Markt für beschränkte Nutzungsrechte entwickelt.

Mit dem Eintritt in die Vertragsbeziehungen des Erblassers wird der Erbe zugleich Inhaber sämtlicher Ansprüche des Erblassers gegen dessen Vertragspartner. Hierzu gehören auch Auskunftsansprüche gegen Telekommunikationsanbieter, etwa mit Blick auf ein verwendetes Passwort oder den Zugang zu noch nicht abgerufenen E-Mails. § 88 TKG, wonach Telekommunikationsanbieter den Inhalt

der Telekommunikation und ihre näheren Umstände grundsätzlich nicht an „andere“ weitergeben dürfen, steht dem zwar nicht entgegen. Zwingend erscheint eine gesetzliche Regelung auch insofern nicht. Gleichwohl erschwert der Umstand, dass für den Rechtsanwender nicht ohne Weiteres ersichtlich ist, ob und inwieweit Erbrecht und Telekommunikationsrecht aufeinander abgestimmt sind, die Rechtsanwendung. Vor diesem Hintergrund könnte eine gesetzliche Klarstellung erwogen werden.

Schließlich könnten die für Miterben im Vergleich zum Alleinerben erschwerten Möglichkeiten, eine Haftungsbeschränkung herbeizuführen, im Hinblick auf digitale Sachverhalte und das dort bestehende gesteigerte Bedürfnis nach frühzeitigen Informationen über die Werthaltigkeit des Nachlasses künftig gesetzlichen Regelungsbedarf begründen. Diesem könnte zu gegebener Zeit dadurch Rechnung getragen werden, Auskunftsrechte vorläufiger Erben zu stärken, die Ausschlagungsfrist zu verlängern oder die Möglichkeiten für Miterben, Haftungsbeschränkungen herbeizuführen, zu erleichtern.

F. Gesetzgeberischer Handlungsbedarf

Zusammenfassend ergibt sich aus den dargestellten Erwägungen gesetzgeberischer Handlungsbedarf hinsichtlich folgender Punkte:

(1.) Beim Einsatz autonomer Systeme (wie Robotern) droht im außervertraglichen Bereich eine Haftungslücke. Falls die insoweit notwendigen Lösungen nicht in angemessener Zeit auf europäischer Ebene gefunden werden können, sollte der nationale Gesetzgeber tätig werden. Insoweit kommt insbesondere eine stärkere Betreiberhaftung oder eine verschärfte Herstellerhaftung in Betracht. Auch eine kumulative Haftungserweiterung ist denkbar.

(2.) Im Hinblick auf Cloud Computing-Verträge und ähnliche Vertragsverhältnisse sollte durch eine dem § 453 Absatz 1 BGB vergleichbare Regelung im Mietrecht klargestellt werden, dass das Mietrecht auch auf andere („sonstige“) Gegenstände als auf Sachen Anwendung finden kann. Im Zuge dessen sollte zudem eine Klarstellung erfolgen, welche Kündigungsfristen des § 580a BGB Anwendung finden. Alternativ wäre der entsprechende Fristenkatalog zu erweitern. Ferner sollte ein Anspruch des Nutzers gegen den Anbieter auf Herausgabe von Daten gesetzlich verankert werden.

(3.) Im Allgemeinen Schuldrecht sollte allgemein klargestellt werden, dass ein Entgelt auch in der Erteilung einer Einwilligung in die Verarbeitung personenbezogener Daten für kommerzielle Zwecke des Vertragspartners bestehen kann („Bezahlen mit Daten“).

(4.) Mit Blick auf das Erfordernis der Freiwilligkeit einer datenschutzrechtlichen Einwilligung sollte bestimmt werden, dass ein zivilrechtlicher Anspruch auf Erteilung einer solchen Einwilligung nicht klagbar ist und aus der Nichterfüllung eines auf Erteilung einer datenschutzrechtlichen Einwilligung gerichteten Anspruchs keine anderweitigen Ansprüche hergeleitet werden können.

(5.) Zum Schutz von Verbrauchern empfiehlt sich für das „Bezahlen mit Daten“ eine „Button-Lösung“, die in § 312j Absatz 3 BGB verankert werden sollte. Für den Fall, dass der Verbraucher eine datenschutzrechtliche Einwilligung als Zusatzentgelt leisten soll, sollte § 312a Absatz 3 BGB ergänzt werden. Des Weiteren sollte eine Ergänzung von § 312j Absatz 4 BGB in dem Sinne erwogen werden, dass ein Verstoß gegen den neu gefassten § 312j Absatz 3 BGB, soweit er einen Fall des „Bezahlens mit Daten“ betrifft, nicht das Zustandekommen des Vertrags hindert, sondern lediglich zur Folge hat, dass der Verbraucher an den Vertrag nicht gebunden ist.

(6.) Es sollte gesetzlich bestimmt werden, dass es nicht zu Lasten einer Vertragspartei zu werten ist, wenn die von ihr zu erbringende Gegenleistung nicht in einer Geldzahlung, sondern in ihrer Einwilligung in die Nutzung personenbezogener Daten besteht.

(7.) Mit Blick auf § 357 Absatz 9 BGB, mit welchem Artikel 14 Absatz 4 lit. b. der Verbraucherrechterichtlinie umgesetzt worden ist, sollte erwogen werden, für Widerrufsfälle ausdrücklich zu regeln, dass (auch) den Anbieter keine Wertersatzpflicht trifft.

(8.) Dem derzeitigen Missbrauch der Abrechnung über Leistungen von Drittanbietern im Rahmen der Telefon- oder Mobilfunkrechnung ist durch Änderungen im Telekommunikationsgesetz (TKG) zu begegnen. Dabei sollte insbesondere ein grundsätzliches Verbot, Forderungen von Drittanbietern über die Telefonrechnung einzuziehen in Betracht gezogen werden, soweit nicht der Verbraucher in jedem Einzelfall ausdrücklich zugestimmt hat. Ebenso sollte ein fristgebundenes Widerspruchsrecht gegenüber dem Telekommunikationsanbieter gegen die Einziehung der konkreten Forderung erwogen werden.

(9.) Der Ausnahmekatalog in § 14 Absatz 2 Telemediengesetz (TMG) sollte erweitert oder eine vergleichbare Regelung eingeführt werden, um einen individuellen Auskunftsanspruch bei Persönlichkeitsrechtsverletzungen im Internet gegen den Intermediär zu schaffen.

(10.) Es sollte ein einheitliches und verbraucherfreundliches Löschungsverfahren bei Persönlichkeitsrechtsverletzungen im Internet geschaffen werden.

(11.) Das in § 88 TKG geregelte Fernmeldegeheimnis steht zwar derzeit dem (bereits aus dem Vertragsverhältnis mit dem Provider bestehenden) Auskunftsanspruch des Erben nicht entgegen. Insoweit wäre indes zur Schaffung von Rechtssicherheit eine (klarstellende) gesetzliche Regelung innerhalb des TKG (unter Berücksichtigung der Datenschutzgrundverordnung) sinnvoll.

Vorgehensweise der Arbeitsgruppe

Die 86. Konferenz der Justizministerinnen und Justizminister hat mit Beschluss vom 18. Juni 2015 die Arbeitsgruppe unter Federführung des Justizministeriums Nordrhein-Westfalen zur Aufarbeitung der Folgen der Digitalisierung auf das Zivilrecht eingesetzt. In dem Beschluss heißt es u.a.:

> *„…4. Die Konferenz der Justizministerinnen und Justizminister hält es für sinnvoll zu prüfen, ob neue Vertragstypen über digitale Inhalte in das Bürgerliche Gesetzbuch aufgenommen werden oder vorhandene Vertragstypen um eine digitale Variante ergänzt werden sollten. Daneben sollte geprüft werden, ob die Rechtsqualität von digitalen Daten gesetzlich zu bestimmen ist, etwa durch die Schaffung eines absoluten Rechts (z. B. Dateneigentum).*
>
> *5. Die Prüfung sollte sich auch darauf erstrecken, ob als Teil der Persönlichkeit der dahinterstehenden Person eine „digitale" Persönlichkeit existiert, die vom Schutzbereich des allgemeinen Persönlichkeitsrechts erfasst und durch weitere gesetzgeberische Maßnahmen zu schützen ist (z. B. durch ein Recht auf einen umfassenden „Digitalen Neustart")….."*

Die Arbeitsgruppe sollte bei ihren Prüfungen mögliche Auswirkungen auf das Urheberrecht, das Datenschutzrecht und das Telekommunikations- und -medienrecht berücksichtigen. Zudem sollten die Entwicklungen auch auf europäischer Ebene in diesen Rechtsgebieten im Blick behalten werden.

Angeschlossen haben sich der Arbeitsgruppe die Länder Baden-Württemberg, Bayern, Berlin, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt und Schleswig-Holstein. Ferner hat das Bundesministerium der Justiz und für Verbraucherschutz in der Arbeitsgruppe mitgewirkt.

Im Oktober 2015 hat die Arbeitsgruppe ihre Arbeit aufgenommen und anknüpfend an die vorgegebenen Themenbereiche Unterarbeitsgruppen mit Federführung durch jeweils eine Landesjustizverwaltung gebildet:

- „Dateneigentum" (Federführung: Nordrhein-Westfalen),
- „Digitales Vertragsrecht" (Federführung: Sachsen-Anhalt),
- „Digitales Persönlichkeitsrecht" (Federführung: Hessen),
- „Digitaler Nachlass" (Federführung: Hamburg).

In einem ersten Arbeitsschritt haben sich die Unterarbeitsgruppen einer Bestandsaufnahme der bereits in der Rechtswissenschaft diskutierten und/oder der in der Praxis auftretenden Probleme gewidmet und die Fragestellungen herausgearbeitet, die in besonderem Maße einer weiteren Prüfung bedurften. Daran anknüpfend haben sie einen Problemaufriss vorbereitet, Thesen und Prämissen formuliert so-

wie eine Agenda für die weitere Bearbeitung ihres jeweiligen Themas vorgeschlagen. Die erzielten Arbeitsergebnisse wurden sodann von der Arbeitsgruppe in einem Zwischenbericht zusammengefasst, welcher der Konferenz der Justizministerinnen und Justizminister im Juni 2016 vorgelegt wurde.

In Vorbereitung auf den vorliegenden Bericht haben die Unterarbeitsgruppen in einem zweiten Arbeitsschritt die zuvor beschlossene Agenda weiterverfolgt. Die insbesondere mit Blick auf einen etwaigen Regelungsbedarf vorgenommene nähere Befassung mit den zuvor als prüfungswürdig erkannten Aspekten diente jeweils der Klärung,

- ob eine gesetzliche Regelung angezeigt ist,
- ob eine bestimmte Rechtsfrage der Rechtsprechung zur Klärung überlassen bleiben sollte oder
- ob eine Regelung aus generellen Erwägungen unterbleiben sollte.

Die hierzu gefertigten Arbeitspapiere haben die Unterarbeitsgruppen sodann entsprechend der oben genannten Themenbereiche und in fortlaufender Abstimmung mit der Arbeitsgruppe zu Kapiteln in diesem Bericht zusammengeführt. Soweit dies aus Sicht der Arbeitsgruppe geboten erschien, wurden dabei auch konkrete Empfehlungen für gesetzgeberische Maßnahmen aufgenommen. Die in Teilbereichen unterschiedliche Aufbereitung und Darstellung der Prüfungen und Ergebnisse sind der Bearbeitung durch unterschiedliche Verfasser aus der jeweiligen Unterarbeitsgruppe geschuldet.

Die Unterarbeitsgruppen haben neben Literatur und Rechtsprechung zahlreiche weitere Erkenntnisquellen genutzt. So wurden unter anderem die sich aus den Gutachten, Diskussionen und Beschlüssen des 71. Deutschen Juristentages in Essen vom 13. - 16. September 2016 ergebenden Gesichtspunkte berücksichtigt. Zudem fand bei mehreren Veranstaltungen der beteiligten Landesjustizverwaltungen ein gezielter fachlicher Austausch zwischen den Arbeitsgruppenmitgliedern und Vertretern von Wissenschaft, Wirtschaft sowie Politik statt. Hervorzuheben sind insbesondere:

- Am 23. Mai 2016 stellten sich Wissenschaftler und Praktiker vor einem ausgewählten Fachpublikum den Fragen des Justizministeriums Nordrhein-Westfalen zu den drei Themenschwerpunkten „Dateneigentum“, „Digitales Vertragsrecht“ und „Digitales Persönlichkeitsrecht“.
- Am 22. Juni 2016 richtete die Justizbehörde Hamburg gemeinsam mit dem Deutschen Juristentag e.V. und der Bucerius Law School eine Diskussionsveranstaltung zu Thema „Die Kosten des Kostenlosen – Daten als Entgelt im Internet“ aus.
- Am 9. Februar 2017 veranstaltete das Justizministerium Nordrhein-Westfalen gemeinsam mit der Universität Siegen eine Tagung zum Thema

„Rechte an Daten“. Neben der Frage, ob es eines Vermögensrechts an Personendaten bedarf, war Gegenstand dieser forschungsorientierten Tagung vor allem, ob der deutsche Rechtsrahmen einer Ergänzung zum Umgang mit nicht-personenbezogenen Daten bedarf. Im Fokus standen dabei insbesondere Industriedaten wie z. B. Datenbestände von Rechenzentren oder Sensordaten aus Maschinenparks.

- Am 26. und 27. April 2017 fand in der Vertretung des Landes Sachsen-Anhalt bei der Europäischen Union in Brüssel eine Sondersitzung der Unterarbeitsgruppe „Digitales Vertragsrecht“ statt. Anlass war u.a. ein Expertengespräch mit hochrangigen Vertretern der Europäischen Kommission sowie des Europäischen Parlaments zum Kommissionsvorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte.

Die Prüfungen der Arbeitsgruppe orientierten sich unter Berücksichtigung des zur Verfügung stehenden Zeitrahmens zur Erstellung des Berichts an den Fragestellungen und Problemfeldern, die als besonders wichtig sowie für einen großen Kreis von Adressaten relevant und daher überprüfungswert herausgearbeitet worden waren. Der vorliegende Bericht verfolgt daher nicht den Anspruch einer vollständigen Überprüfung aller im Zusammenhang mit den Auswirkungen der Digitalisierung auf das Recht stehenden Fragen, sondern versteht sich als ein Beitrag der Länder zur aktuellen Diskussion über die zivilrechtlichen Folgen der Digitalisierung.

Kapitel 1: Dateneigentum

A. Vorbemerkung

Ausgangspunkt ist die von der Konferenz der Justizministerinnen und Justizminister aufgeworfene Frage,

> „[…] ob die Rechtsqualität von digitalen Daten gesetzlich zu bestimmen ist, etwa durch die Schaffung eines absoluten Rechts (z. B. Dateneigentum).“[6]

Hierauf soll das vorliegende Kapitel zum Thema „Dateneigentum“ eine Antwort geben. Nach einer Erörterung des Datenbegriffs (B.) erfolgt ein erster Überblick, wie Daten als solche (also unabhängig von einem Speichermedium und vom Inhalt) nach geltendem Recht behandelt werden (C.). Daran schließen sich Überlegungen zur möglichen Gestaltung eines absoluten Rechts an (D.), bevor die für ein solches Recht in Betracht kommenden Fallgruppen umfassend daraufhin analysiert werden, ob das geltende Recht bereits einen ausreichenden Rechtsrahmen bietet. Die Ergebnisse dieser Analyse werden zunächst im Einzelnen dargestellt (E.) und sodann zusammenfassend – auch anhand des Meinungsbildes in der Fachliteratur und der Praxis – gewürdigt (F.). Abgeschlossen wird das Kapitel durch das Gesamtergebnis der Arbeitsgruppe (G.).

B. Datenbegriff

I. Definition

DIN 4430, Teil 2 Nr. 2.1.13[7] definiert Daten im technischen Sinne als ein „Gebilde aus Zeichen oder kontinuierlichen Funktionen, die aufgrund bekannter oder unterstellter Abmachungen Informationen darstellen, vorrangig zum Zwecke der Verarbeitung oder als deren Ergebnis“.

Vorliegend stehen allein *digitale Daten* in Rede.[8] Darunter werden diejenigen Daten verstanden, die nach einem bestimmten Code dargestellt sind und die deshalb von Computern oder anderen Geräten zur digitalen Datenverarbeitung gelesen und/oder verarbeitet werden können.[9]

---

[6] Ziffer 4 Satz 2 des Beschlusses der 86. Konferenz der Justizministerinnen und Justizminister am 17. und 18. Juni 2015 zu TOP I.8 „Digitaler Neustart“, abrufbar unter https://www.justiz.nrw/JM/leitung/jumiko/beschluesse/2015/fruehjahrskonferenz_15/TOP-I_8---Digitaler-Neustart-_oA_.pdf (letzter Abruf: 1.3.2017).

[7] Zitiert nach Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 11.

[8] Soweit im Folgenden von Daten gesprochen wird, sind digitale Daten gemeint.

[9] Vgl. *Zech*, Daten als Wirtschaftsgut - Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (138); *ders.*, "Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1153); siehe auch die Definition in § 202a Abs. 2 StGB: „Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht wahrnehmbar gespeichert sind oder übermittelt werden.“

Die juristische Betrachtung richtet sich vornehmlich auf Daten in Form syntaktischer Informationen, also auf die bloße Zeichenmenge.[10] Von den syntaktischen Informationen werden in der Literatur verschiedene andere Formen von Daten/Informationen unterschieden, etwa die durch ihren Aussagegehalt gekennzeichneten semantischen Informationen und die als verkörperter Gegenstand verstandenen strukturellen Informationen.[11]

Das BGB enthält in seiner geltenden Fassung in § 312f Abs. 3 BGB[12] eine Legaldefinition von digitalen Inhalten. Digitale Inhalte sind danach nicht auf einem körperlichen Datenträger befindliche Daten, die in digitaler Form hergestellt und bereitgestellt werden. Ausweislich der Gesetzesbegründung der Bundesregierung[13] fallen hierunter etwa Computerprogramme, Anwendungen (Apps), Spiele, Musik, Videos oder Texte. Ob die Daten heruntergeladen, gespeichert und hiernach sichtbar gemacht würden oder während des Herunterladens in Echtzeit sichtbar gemacht würden (Streaming), sei dabei unerheblich.

Daten weisen drei für die juristische Betrachtung wesentliche (Negativ-)Merkmale auf: Nicht-Rivalität, Nicht-Exklusivität und Nicht-Abnutzbarkeit.[14] Die Nicht-Rivalität folgt daraus, dass Daten von einer unbegrenzten Vielzahl von Nutzern verwendet werden können, ohne dass die Nutzung durch die jeweils anderen dadurch beeinträchtigt wird. Sie sind beliebig kopierbar und – sofern sie einmal öffentlich zugänglich waren – faktisch jedermann zugänglich (also nicht-exklusiv). Eine gewisse Exklusivität kann auf technischem Wege (Geheimhaltung, IT-Sicherheit, z. B. Verschlüsselung) und auf rechtlichem Wege, insbesondere durch Zuweisung von Ausschließlichkeitsrechten (z. B. Immaterialgüterrechten) erzielt werden. Daten als solche sind ferner nicht abnutzbar. Im Gegensatz zu Speichermedien unterliegen sie keiner Abnutzung oder Alterung, weshalb Verschleiß (anders als im Falle körperlicher Sachen) nicht als Rechtfertigung für die Zuweisung von Eigentum an Daten dienen kann.

II. Abgrenzung zum Speichermedium

Abzugrenzen von digitalen Daten sind Speichermedien. Unzweifelhaft sind übliche Speichermedien wie Festplatten, CD-ROMs und USB-Sticks Sachen i. S. v. § 90 BGB, die nach allgemeinen Regeln Gegenstand von relativen und absoluten Rechten sein können. Klärungsbedürftige grundsätzliche Rechtsfragen stellen sich insoweit nicht.

---

[10] Vgl. *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, S. 815 (816).

[11] Näher *Zech*, Information als Schutzgegenstand, 2012, S. 13 ff.

[12] Die Vorschrift und die Legaldefinition gehen zurück auf die Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates über die Rechte der Verbraucher (Verbraucherrechterichtlinie), 2011, ABl. L 304/64, vgl. insbes. Erwägungsgrund 19.

[13] BT-Drs. 17/12637, S. 55.

[14] Hierzu und zum Folgenden vgl. nur *Zech*, Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (139).

Die Bestimmung des Speichermediums, auf dem ein konkretes Datum gespeichert ist, kann insbesondere bei der Nutzung des Internets an technische Grenzen stoßen.[15] Ob Daten auf einem eigenen oder fremden Server oder lokal auf dem Rechner eines Nutzers gespeichert werden, kann neben den vom Nutzer vorgenommenen Einstellungen auch von der Entscheidung z. B. eines E-Mail-Dienstes, eines Plattform-Betreibers etc. abhängen; bei mehrfacher Speicherung (auch in Arbeitsspeichern), bei Sicherungskopien und beim Einsatz dezentraler Systeme (wie bei der Auslagerung von Daten im Wege des Cloud Computing) kann sich die Frage nach dem konkreten Speicherort eines konkreten Datums als technisch kaum noch lösbar oder sogar als unlösbar erweisen.[16]

Zwar sind Daten stets auf einem Speichermedium abgelegt.[17] Daten sind aber im Rechtssinn (vgl. § 93 BGB) nicht Bestandteil des Speichermediums. Insbesondere folgt die Berechtigung an den gespeicherten Inhalten anderen Regeln als das Eigentum an den Speichermedien.[18]

III. Abgrenzung zum Dateninhalt

Abzugrenzen von (bloßen) Daten sind ferner die Dateninhalte, also die gespeicherten Informationen (wie Texte, Bilder, Messwerte, Programme). Das Recht knüpft unter mehreren Gesichtspunkten Rechtswirkungen an den Dateninhalt. Abhängig vom Dateninhalt kann etwa das Datenschutzrecht anwendbar sein; ferner können Immaterialgüterrechte bestehen. Dem Arbeitsauftrag der Arbeitsgruppe folgend stehen – unabhängig von ihrem Inhalt und von der Verkörperung in einem Speichermedium – Daten als solche im Fokus dieses Kapitels. Das „Recht am Dateninhalt“ gewinnt insoweit aber zweifache Bedeutung. Zum einen lässt sich die Frage des Regelungsbedarfs im Zusammenhang mit digitalen Daten nur angemessen beantworten, wenn man das geltende Recht insgesamt daraufhin untersucht, ob es bereits einen ausreichenden Rechtsrahmen für diese „Gebilde“ bietet. So kann etwa von den Immaterialgüterrechten (am Dateninhalt) eine

---

[15] Näher aus technischer Sicht *Hoppen*, Sicherung von Eigentumsrechten an Daten, CR 2015, 802 (803 f.).

[16] Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, 165 (185 f.); *Heymann*, Der Schutz von Daten bei der Cloud Verarbeitung, CR 2015, 807; *Zech*, Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (138).

[17] So *Zech*, Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (138), der trotz des stets vorhandenen Speichermediums die Betrachtung der Daten als solche für geboten hält, weil „die Identifizierung des körperlichen Datenträgers zunehmend schwieriger geworden [sei], da durch die erleichterte Speicherung und Übertragung von Daten diese häufig an einer Vielzahl von auch weit entfernten Orten gespeichert werden können und die exakte Bestimmung des körperlichen Trägers zunehmend an Bedeutung verliert“; Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (182), spricht von der „Sacheigenschaft von Daten vermittels des stets denknotwendig existierenden Datenträgers“.

[18] BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.

Schutzwirkung ausstrahlen, die letztlich auch einen hinreichenden Schutz der Daten als solche gewährleistet. Zum anderen gibt es gerade mit Blick auf den wirtschaftlichen Zuweisungsgehalt personenbezogener Daten verschiedene Vorschläge, das Datenschutzrecht in Bezug auf bestimmte Dateninhalte weiterzuentwickeln, bspw. durch Einführung einer datenschutzrechtlichen Lizenz nach dem Muster des Urheberrechts. Auf diese Überlegungen wird zu einem späteren Zeitpunkt eingegangen.[19]

C. Daten im geltenden Recht

Die Beantwortung der Frage, ob die Rechtsqualität von digitalen Daten gesetzlich zu bestimmen ist, etwa durch die Schaffung eines absoluten Rechts (z. B. Dateneigentum), hängt maßgeblich davon ab, wie das geltende Recht Daten behandelt. Nachfolgend werden Daten daher zunächst sachenrechtlich in eine Kategorie eingeordnet und – daran anknüpfend – ein Überblick darüber gegeben, welche Regelungen das geltende Recht bereits für sie bereithält.

I. Fehlende Sachqualität der Daten

Sachen i. S. d. BGB sind nach § 90 BGB nur körperliche Gegenstände. Nicht notwendig ist, dass die Materie, aus der die Sache besteht, eine feste Form besitzt; sie kann auch flüssig oder gasförmig sein, soweit sie nur technisch beherrschbar und einer sinnlichen Wahrnehmung zugänglich ist, mag diese auch erst durch eine technische Einrichtung (z. B. eine Gasuhr) ermöglicht werden; auch Wärmeträger in Rohrleitungen, wie Dampf, Kondensat oder Heizwasser, sind deshalb Sachen. Der Begriff der Sache bezeichnet danach einen nach natürlicher Anschauung für sich allein bestehenden, im Verkehrsleben besonders bezeichneten und bewerteten körperlichen Gegenstand. Sachen müssen untereinander unterscheidbar sein; die dafür notwendige Abgrenzung kann gegeben sein z. B. durch den eigenen körperlichen Zusammenhalt der Sache, durch ihre Fassung in einem Behältnis oder durch technische Hilfsmittel, wie Grenzsteine oder die rechtlich maßgebliche Einzeichnung in einer Karte.[20]

Das trifft zwar auf typische Speichermedien wie Festplatten, CD-ROMs und USB-Sticks zu. Betrachtet man jedoch Daten insoliert, treten diese physisch nur in Gestalt elektrischer/magnetischer Ladungen (bzw. – abhängig von Speichermedium – in anderer Form wie Löcher auf Lochkarten oder Vertiefungen auf CD-ROMs) in Erscheinung, sei es auf Speichermedien, bei ihrer Übermittlung in Kabelverbindungen oder kabellos mittels elektromagnetischer Wellen oder aber bei

---

[19] Siehe unten (F.II.).
[20] MüKo/*Stresemann*, BGB, § 90 Rn. 8.

ihrer Darstellung, insbesondere visuell auf Bildschirmen. Diese Erscheinungsformen sind flüchtig und damit grundsätzlich nicht hinreichend verfestigt, um als körperlich i. S. v. § 90 BGB zu gelten.[21]

Es wäre spitzfindig, die physikalische Betrachtung bis ins Detail fortzusetzen und der Frage nachzugehen, ob nicht auch Elektronen auf einem Speichermedium oder elektromagnetische Wellen körperlich sind. Speicherformen unterliegen technischem Wandel. Die Voraussetzungen eines Rechtsinstituts wie des Eigentums sollten jedoch abstrakt und generalisierend festgestellt werden können, um handhabbar und glaubwürdig zu bleiben. Insoweit können auch Parallelen zur rechtlichen Qualifikation von elektrischem Strom[22] und von Software[23] nach geltendem Recht fruchtbar gemacht werden. Im Ergebnis sind daher die Einzelheiten der physikalischen Erscheinung von digitalen Daten letztlich offen zu lassen und Daten generell nicht als Sachen i. S. v. § 90 BGB zu begreifen.[24]

II. Daten als Gegenstände

Das BGB unterscheidet hinsichtlich möglicher Rechtsobjekte zwischen körperlichen und unkörperlichen Gegenständen; die körperlichen, also diejenigen, die man entweder anfassen oder aber jedenfalls sinnlich wahrnehmen und technisch beherrschen kann, nennt es Sachen (§ 90 BGB). Der im Gesetz nicht definierte Oberbegriff „Gegenstände“ umfasst alle individualisierbaren, vermögenswerten Objekte und Güter, über die Rechtsmacht i. S. v. Herrschafts- oder Nutzungsrechten ausgeübt werden kann.[25]

Wie elektrische Energie, die in Stromleitungen geliefert wird,[26] können Daten, sobald sie in einer zur Datenverarbeitung geeigneten Form erfasst wurden, im Raum abgegrenzt und technisch beherrscht werden. Sie unterfallen damit grundsätzlich dem Gegenstandsbegriff. Eine Ausnahme kommt allenfalls dann in Betracht, wenn Daten nicht statisch auf einem Speichermedium gespeichert sind,

---

[21] So überzeugend die wohl einhellige Ansicht; statt vieler: LG Konstanz, Urt. v. 10.5.1996 – 1 S 292/95, NJW 1996, 2662; OLG Dresden, Beschl. v. 5.9.2012 – 4 W 961/12, NJW-RR 2013, 27 (28); MüKo/*Stresemann*, BGB, § 90 Rn. 25; Palandt/*Ellenberger*, BGB, § 90 Rn. 2, jeweils m. w. N.

[22] Vgl. zur Verneinung der Sacheigenschaft von elektrischem Strom und zur Behandlung von Strom als sonstiger Gegenstand im Kaufrecht gem. § 453 Abs. 1 BGB *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (insbes. 488 f.).

[23] Z.B. BGH, Urt. v. 15.11.2006 – XII ZR 120/04, NJW 2007, 2394, Rn. 15 (auf einem Datenträger verkörperte Standardsoftware als bewegliche Sache).

[24] Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 17.

[25] Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (175); *ders.*, Absolute Rechte an der Nutzung einer Domain − eine zentrale Weichenstellung für die Rechtsentwicklung, WRP 2011, 543; MüKo/*Stresemann*, BGB, § 90 Rn. 1.

[26] Vgl. MüKo/*Stresemann*, BGB, § 90 Rn. 5: Die Luft/Der Wind sind als solche nicht technisch beherrschbar und scheiden deshalb als rechtlich relevante Objekte aus. Sobald der Wind aber durch eine Windkraftanlage in elektrische Energie umgewandelt und in eine Leitung eingespeist wird, handelt es sich um einen Gegenstand.

sondern nur in einer zur Datenübertragung geeigneten Leitung in Gestalt elektrischer/magnetischer Ladung oder ausschließlich in Form elektromagnetischer Wellen bei kabelloser Übertragung in Erscheinung treten. Ob solche Wellen und Ladungen hinreichend im Raum abgegrenzt sind und technisch beherrscht werden können, um als Gegenstand im Rechtssinne behandelt zu werden, dürfte von den Umständen des Einzelfalls abhängen. Mit Blick darauf, dass es sich bei dem Ausnahmetatbestand um einen eher theoretischen Fall handeln dürfte, hat die Arbeitsgruppe ihren weiteren Untersuchungen zugrunde gelegt, dass Daten ein außerhalb der am Wirtschaftsleben teilnehmenden Rechtssubjekte existierender Gegenstand und ein immaterielles Wirtschaftsgut sind.[27]

III. Behandlung von Daten im geltenden Recht

Auch wenn Daten nach heutigem Recht keine Sachen i. S. v. § 90 BGB sind und kein allgemeines Immaterialgüterrecht an digitalen Daten besteht, spielen Daten im geltenden Zivilrecht durchaus eine erhebliche Rolle. Wenn auch nicht als Gegenstand von Eigentum, Besitz oder Pfandrechten (1.), umso mehr aber als Vertragsgegenstand sind Daten zivilrechtliches Allgemeingut (2.). Bei näherer Betrachtung ergibt sich, dass das geltende Recht auch bereits absolute (also nicht nur gegenüber einem Vertragspartner, sondern [auch] gegen fremde Dritte wirkende) Rechte an Daten kennt (3.).

1. Kein Eigentum, Besitz oder Pfandrecht an Daten

Oben ist ausgeführt worden, dass Daten nach geltendem Recht zwar Gegenstände aber keine Sachen i. S. d. BGB sind. Danach scheiden Daten – wie in allen anderen EU-Mitgliedstaaten[28] – als Gegenstände von Eigentum (§ 903 BGB), Besitz (§ 854 BGB) und Pfandrechten (§ 1204 BGB) aus.[29]

2. Daten als Vertragsgegenstand

Daten können gehandelt werden. Sie sind als immaterielle Wirtschaftsgüter[30] taugliche Gegenstände von Verträgen.[31] Ansprüche (gemäß der Legaldefinition in § 194 Abs. 1 BGB verstanden als das Recht, von einem anderen ein Tun oder Unterlassen zu verlangen) können sich auf Daten beziehen. Aus der fehlenden

---

[27] Vgl. auch *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (621); *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (138).

[28] So *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (380).

[29] Vgl. BGH, Urt. v. 13.10.2015 – VI ZR 271/14, MDR 2016, 84, Rn. 20.

[30] Vgl. OLG Düsseldorf, Urt. v. 17.10.2011 – 14e O 219/10, CR 2012, 801 (802) (Kundendaten als immaterielles Gut, das gemäß § 667 vom Beauftragten herauszugeben ist [Hinweis auf BGH, Urt. v. 17.4.1996 – VIII ZR 5/95, MDR 1996, 1122 – Rz. 27]); *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (138), unter Hinweis auf BGHZ 133, 155; MüKo/*Stresemann*, BGB, § 90 Rn. 25.

[31] Leible/Lehmann/Zech/*Peukert*, Unkörperliche Güter im Zivilrecht, S. 2011, 95 (109 ff.); *Weber/Chrobak*, Der digitale Nachlass, Jusletter IT 24 (Sept. 2015), Rn. 21.

Anerkennung einer Sach- oder Rechtsqualität von Daten im geltenden Zivilrecht ergeben sich grundsätzlich keine Schranken für die Vertragsgestaltung. In der Rechtspraxis können Rechte und Pflichten in Bezug auf Daten deshalb in verschiedensten Formen Gegenstand von Verträgen sein, ohne dass deren Wirksamkeit grundsätzlich in Zweifel stünde. Mangels Sach- und Rechtsqualität werden dabei faktische Positionen ausgetauscht, ein dingliches Verfügungsgeschäft fehlt regelmäßig.[32]

Verträge über Daten begründen (relative) Rechtspositionen im Verhältnis der Vertragsparteien zueinander. Das sind neben den im Vertrag ausdrücklich geregelten Rechten und Pflichten auch Nebenrechte und Nebenpflichten (vgl. etwa § 241 Abs. 2 BGB). Ferner gelten die gesetzlichen Ansprüche, die das BGB den Vertragsparteien einräumt und die grundsätzlich auch auf digitale Daten Anwendung finden, soweit diese Vertragsgegenstand sind. So hat ein Auftragnehmer etwa Daten, die er zur Ausführung des Auftrags vom dem Auftraggeber erhält, bei Beendigung des Auftrags herauszugeben (§§ 667, 675 BGB).[33] Daten können – namentlich bei der Rückabwicklung von Verträgen – Gegenstand von Bereicherungsansprüchen sein.

3. Absolute Rechte an Daten

Vorstehendes gilt grundsätzlich nur im Verhältnis der Vertragsparteien zueinander. Absolute Rechte an Daten, die einen zivilrechtlichen Schutz gegenüber jedermann gewähren, sieht das geltende Recht nicht ausdrücklich vor. Gleichwohl sind Daten auch nach geltendem Recht nicht schutzlos dem Zugriff Dritter ausgesetzt, die nicht Vertragspartner sind.

In den §§ 202a, 202b, 202c und § 303a StGB finden sich Straftatbestände, die Daten unabhängig von einem Speichermedium und von ihrem Inhalt schützen. Nach § 202a StGB (Ausspähen von Daten) wird etwa bestraft, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. Strafbar ist ferner das Abfangen von Daten (wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft) und die Datenveränderung (wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert). Diese Straftatbestände setzen keinen bestimmten Dateninhalt voraus. Nach § 202a Abs. 2 StGB sind Daten i. S. d. Straftatbestände vielmehr alle Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden. Zu betonen ist ferner,

---

[32] Leible/Lehmann/Zech/*Peukert*, Unkörperliche Güter im Zivilrecht, S. 2011, 95 (99, 110); *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (146).

[33] Vgl. OLG Düsseldorf, Urt. v. 27.9.2012 – I-6 U 241/11, CR 2012, 801 (802).

dass mit dem Straftatbestand des Ausspähens von Daten auch die unbefugte Kopie (Vervielfältigung) strafbewehrt sein kann, der Umstand, dass der Berechtigte „seine“ Daten weiterhin unverändert nutzen kann, der Bestrafung also nicht entgegensteht.

Bei den genannten Straftatbeständen handelt es sich nach wohl einhelliger Ansicht um Schutzgesetze i. S. v. § 823 Abs. 2 BGB. Das Ausspähen und Abfangen sowie die unbefugte Veränderung von Daten kann deshalb zivilrechtliche Ansprüche des Verletzten gegen den Täter auf Schadensersatz und Unterlassung begründen.[34]

Unter welchen Aspekten Daten nach geltendem Recht darüber hinaus absolut geschützt sind, wird nachfolgend unter E. im Rahmen der Prüfung der Regelungsbedürftigkeit dargestellt.

D. Überlegungen zur möglichen Ausgestaltung eines absoluten Rechts an Daten

Um sich die gesetzgeberischen Alternativen zu vergegenwärtigen, sei zunächst aufgezeigt, welche Optionen bestünden, ein absolutes Recht an Daten auszugestalten, und zwar hinsichtlich des Schutzumfangs (I.), der dogmatischen Verortung (II.) sowie der personellen Zuordnung (III.).

I. Schutzumfang

Gelangte man zu dem Ergebnis, dass ein absolutes Recht an Daten kodifiziert werden sollte, stellte sich als erstes die Frage, welcher Schutzumfang diesem Recht sinnvollerweise zukäme. Hierzu sind vorab das Eigentum (1.) und die Immaterialgüterrechte (2.) als mögliche Bezugspunkte und Vorbilder für ein neu zu schaffendes absolutes Recht an Daten in den Blick zu nehmen.

1. (Sach-)Eigentum als Bezugspunkt

Als Bezugspunkt böte sich zunächst das Eigentum an als umfassendstes Recht zu tatsächlichen (Benutzung, Verbrauch) und rechtlichen (Belastung, Veräußerung) Herrschaftshandlungen, das die Rechtsordnung an einer Sache zulässt.[35] Nach § 903 Satz 1 BGB kann der Eigentümer einer Sache, soweit nicht das Gesetz oder

---

[34] Vgl. OLG Naumburg, Urt. v. 27.8.2014 – 6 U 3/14, DAR 2015, 27 (zu einem Anspruch nach § 1004 Abs. 2 BGB i.V. m. § 823 Abs. 2 BGB i.V. m. §§ 202a, 202c StGB hinsichtlich der Daten, die bei der Geschwindigkeitsmessung mit einer Geschwindigkeitsmessanlage entstehen); OLG Celle, Urt. v. 22.12.2010 – 7 U 49/09, NJW-RR 2011, 1047 (zu einem Anspruch aus § 823 Abs. 2 BGB i. V. m. § 202a StGB wegen Kundendaten); Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (195 f.), der auf die Unbestimmtheit dieser Straftatbestände hinweist, soweit sie eine zivilrechtliche Zuordnung von Daten unterstellen.

[35] Vgl. Palandt/*Bassenge*, BGB, vor § 903 Rn. 1; für ein Dateneigentum in Analogie zu § 903 BGB spricht sich aus *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (489).

Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen. Das (Sach-)Eigentum ist mithin als umfassendes Herrschaftsrecht konzipiert, wesensmäßig begrenzt nur durch Rechte Dritter oder gesetzliche Schranken.

Die Befugnisse des (Sach-)Eigentümers wirken in positiver und negativer Richtung: Die positive Wirkung besteht in rechtlicher Hinsicht (der Eigentümer kann die Sache übereignen, das Eigentum aufgeben, es belasten und die Benutzung regeln) wie in tatsächlicher Hinsicht (er kann die Sache verändern, verbrauchen und vernichten, er kann sie in Besitz nehmen, den Besitz beenden und übertragen). Die negative Wirkung des Eigentums besteht insbesondere in dem Ausschließungsrecht des (Sach-)Eigentümers, der Einwirkungen auf die Sache (etwa durch Wegnahme, Zerstörung, Beschädigung, aber auch durch Benutzung) verhindern kann.[36]

2. Immaterialgüterrechte als Bezugspunkt

Als weiterer möglicher Bezugspunkt für die Schaffung eines neuen absoluten Rechts an Daten kommen Immaterialgüterrechte in Betracht. So ist das Urheberrecht ein absolutes Recht, das dem Urheber die Befugnis einräumt, seine (materiellen und ideellen) Interessen an einem Werk gegenüber Dritten durchzusetzen.[37] Dazu zählt insbesondere das ausschließliche Recht des Urhebers, das Werk in körperlicher Form zu verwerten und in unkörperlicher Form öffentlich wiederzugeben (§ 15 UrhG, u.a. Vervielfältigungsrecht, Verbreitungsrecht, Ausstellungsrecht, Senderecht, Recht der Wiedergabe durch Bild- oder Tonträger).

Nicht ohne Grund wird das Urheberrecht auch als „geistiges Eigentum“ („intellectual property“) bezeichnet. Auch der Urheber hat nämlich in Bezug auf sein Werk positive Handlungsbefugnisse (z. B. das Vervielfältigungs-, Verbreitungs-, Aufführungs-, Vorführungs-, Senderecht) und negative Rechte. Zu diesen gehört die Ausschlusswirkung, aufgrund derer der Urheber Abwehransprüche gegen jeden Dritten geltend machen kann, der seine Interessen stört.[38] Weitere Parallelen kommen hinzu, wie die Zuordnung des vollen Wertes des Werkes und die Einschränkung durch Gesetze und Rechte Dritter.[39]

---

[36] Vgl. Palandt/*Bassenge*, BGB, § 903 Rn. 4 ff.
[37] Vgl. Rehbinder/*Peukert*, Urheberrecht, Rn. 126.
[38] Vgl. Rehbinder/*Peukert*, Urheberrecht, Rn. 142.
[39] Vgl. Rehbinder/*Peukert*, Urheberrecht, Rn. 143 ff., 148 ff.

3. Möglicher Schutzumfang

Wie das (Sach-)Eigentum und das Urheberrecht (als Beispiel für Immaterialgüterrechte) könnte ein neu zu schaffendes absolutes Recht an Daten dem Berechtigten positive (a) und negative (b) Befugnisse einräumen. Es könnte als Vollrecht[40] oder aber nur hinsichtlich einzelner Befugnisse begründet werden. Dazu könnten zählen:[41]

a. Positive Rechte

(1) Zugangsrecht

Der Berechtigte kann die Daten geheim halten oder Dritten den Zugang ermöglichen, sei es exklusiv (Zugang nur für einen oder bestimmte Dritte) oder allgemein (öffentliche Zugänglichmachung).

(2) Herausgaberecht

Neben dem Recht, über den Zugang zu Daten zu entscheiden, könnte dem Berechtigten ein Herausgaberecht an Daten zustehen, die sich in der Sachherrschaft[42] Dritter befinden. Das ist zum einen denkbar für Daten, die sich bei Dritten befinden, ohne dass diese ein „Recht zum Besitz“ haben; hier wäre an ein Recht auf Herausgabe im Wege der Übertragung (Kopie) an den Berechtigten und Löschung beim Datenbesitzer zu denken. Ferner könnte ein Recht auf Herausgabe von Daten bestehen, auf die der Berechtigte nicht (mehr) zugreifen kann, die Dritten aber zugänglich sind; dieses Recht könnte (vergleichbar § 985 BGB) auf eine exklusive Herausgabe gerichtet sein, bei der beim Dritten keine Kopie der Daten mehr verbleibt, oder aber (wie das Zugangsrecht nach § 25 UrhG) nur auf Herausgabe einer Kopie, so dass der Verpflichtete weiterhin auf die Daten zugreifen kann.

(3) Nutzungsrecht

Der Berechtigte kann nach Belieben entscheiden, inwieweit er Dritten die Nutzung der Daten ermöglicht. In Betracht kommt eine exklusive Nutzung allein durch den Begünstigten oder eine nicht exklusive Nutzung (Teilhabe), die die Nutzung durch den Berechtigten und weitere Dritte nicht ausschließt. In beiden

---

[40] So *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (489 f.): Vollrecht an Daten in Analogie zu § 903, soweit das sachenrechtliche System wesensgemäß auf Daten anwendbar ist.

[41] Vgl. *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (490 f.); *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (139).

[42] BGH, Urt. v. 17.4.1996 – VIII ZR 5/95, NJW 1996, 2159 (2161), geht bei folgenden Ausführungen von einem „Besitz an Daten“ aus, ohne dessen Möglichkeit zu problematisieren: „Gem. § 667 BGB hat die M deshalb dem Kl. nach Beendigung des Teilnahmevertrags alles herauszugeben, was sie zur Ausführung des Auftrags erhalten hat. Dazu gehört der tatsächliche Besitz der Kundendaten und das Recht, diese Daten zum Zwecke von Aussendungen im Rahmen des Toyota-Kundenkontaktprogramms zu speichern und zu nutzen. Beides kann nur dadurch herausgegeben werden, daß der Kl. eine Kopie seiner Daten zurückerhält und die M gleichzeitig die Daten im eigenen Bestand löscht.“

Fällen kann die Nutzung zeitlich und/oder sachlich beschränkt eingeräumt werden (etwa: Gestattung der Nutzung einer Musikdatei durch Abspielen für einen Monat). Insbesondere im Bereich von Big Data ist als mögliche Nutzungsart die Datenanalyse zu erwähnen.[43]

(4) Verfügungsrecht

Der Berechtigte kann die Daten verändern, sie durch Löschung vernichten oder auf Dritte übertragen (etwa indem er sie vor der Löschung einem Dritten zugänglich macht und diesem die Position des Berechtigten überträgt). Jedenfalls theoretisch denkbar ist die Befugnis, ein absolutes Recht an Daten dinglich zu belasten.

b. Negative Rechte

Als negative Befugnis ginge mit dem positiven Recht eine Ausschlusswirkung einher, also das Recht, jede Störung durch Dritte, die der ungehinderten Ausübung der positiven Rechte entgegensteht, abzuwehren. Ein solches Ausschlussrecht könnte zum einen in Gestalt eines Unterlassungsanspruchs bestehen (gerichtet etwa auf Unterlassung unberechtigten Zugriffs auf Daten). Zum anderen kommt ein Beseitigungsanspruch in Betracht, etwa gerichtet auf Löschung unbefugt erlangter Daten.

II. Dogmatische Verortung

Will man ein absolutes Recht an Daten einführen, kommt dogmatisch (und gesetzgeberisch) neben der Schaffung einer neuen, eigenständigen Kategorie die Anknüpfung an ein bestehendes absolutes Recht in Betracht. Wie bereits erwähnt, bieten sich hierfür das (Sach-)Eigentum als umfassendes Recht an Sachen und die bestehenden Immaterialgüterrechte wie das Patentrecht und das Urheberrecht an, ggf. ergänzt um Leistungsschutzrechte.[44]

1. Erste Einschätzung

Ein konkreter Vorschlag zur Verortung eines absoluten Rechts an Daten wäre verfrüht. Zu erwähnen sind jedoch gewisse Zweifel daran, ob eine – enge – Anlehnung an das (Sach-)Eigentum geeignet wäre, die Besonderheiten von Daten als Gegenstand eines absoluten Rechts zufriedenstellend zu erfassen.[45] Der Schutz des (Sach-)Eigentums basiert ökonomisch auf dem Gedanken der Einräumung einer exklusiven Nutzungsmöglichkeit. (Körperliche) Sachen sind regelmäßig nur exklusiv (von einer Person oder einer endlichen Zahl von Personen) nutzbar, weil

---

[43] Zur Wertschöpfungskette bei Big Data-Sachverhalten vgl. *Zech*, "Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1152).

[44] *Zech*, "Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1153 f.).

[45] Vgl. *Härting*, Internetrecht, S. 619: Jegliche Anleihen an eigentumsähnliche Befugnisse („meine Daten“) seien verfehlt.

jeder Gebrauch der Sache ihre Nutzbarkeit durch andere potentielle Nutzer einschränkt und den Kreis der Nutzungsmöglichkeiten verkleinert.[46] Deshalb ist es möglich und sinnvoll, die Nutzung körperlicher Sachen durch Schaffung des dinglichen Rechts „Eigentum" zu monopolisieren und einem (oder mehreren) Eigentümer(n) exklusiv zuzuweisen.

Vergleicht man diesen Befund mit der Situation bei Daten, ergibt sich ein ganz anderes Bild: Daten sind technisch frei verfügbar und können ohne Substanzverlust beliebig oft kopiert werden, wobei das „Original" und die Kopie grundsätzlich keine qualitativen Unterschiede aufweisen. Sie sind nichtrivalisierend (nichtrival), die aktuelle Nutzung durch eine Person beeinträchtigt also nicht die Nutzung durch beliebig viele andere Personen.[47] Anders als bei (körperlichen) Sachen besteht bei Daten deshalb keine Notwendigkeit, die Nutzungsmöglichkeit durch Schaffung eines absoluten Rechts (Daten-„Eigentum") zu monopolisieren. Das zeigt sich auch daran, dass Daten ohne rechtliche Regelung nicht exklusiv sind: Daten sind nur solange geheim, wie ihre Nutzung durch andere faktisch verhindert wird. Sind sie einmal (namentlich im Internet) öffentlich zugänglich gemacht worden, kann ihre Nutzung durch Dritte nicht mehr faktisch, sondern (allenfalls) rechtlich verhindert werden.[48] Zu erwähnen ist schließlich, dass Daten, anders als die meisten Sachen, grundsätzlich nicht abnutzbar sind, woran die technische Abnutzung von Speichermedien nichts ändert.[49]

Dagegen weisen die spezifischen Eigenschaften von Daten gewisse Parallelen zur Abgrenzung von eigenschöpferischem Werk einerseits und Werkstücken andererseits im Urheberrecht auf: Das „Original" der Daten gleicht dem urheberrechtlich geschützten Werk, von dem Kopien – wie im Urheberrecht Werkstücke – gefertigt werden können. Auch der gesetzgeberische Zweck der Immaterialgüterrechte legt eine Parallele zu Daten nahe: Erst die rechtliche Verknappung (durch Schaffung eines Urheber-, Patent-, Marken- oder Designrechts) ermöglicht es dem Kreativen, die Früchte seiner Arbeit zu ziehen, wodurch zugleich im Allgemeininteresse ein Anreiz für geistige, künstlerische oder erfinderische Tätigkeit geschaffen wird.[50] Diese Erwägung passt eher zu Daten als der oben erörterte Zweck des Sacheigentumsrechts, obgleich der Kreativität als Schutzgut nicht in jedem Fall

---

[46] Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (178).

[47] Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, 165 (179); *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (139).

[48] Vgl. *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (139).

[49] *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (139 f.).

[50] Vgl. Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (179).

eine maßgebende Bedeutung zukäme, wenn man – unabhängig vom Dateninhalt und damit von der Schöpfungshöhe – jedes digitale Datum erfassen wollte.[51]

Ob die Schaffung eines gänzlich neuen Rechts an Daten erforderlich und trotz des Grundsatzes des Numerus clausus der Sachenrechte[52] dogmatisch umsetzbar wäre, bedarf eingehender Prüfung.[53]

2. Besondere Ansätze

a. Recht an Daten als Registerrecht

Teilweise wird vorgeschlagen, nur solche Daten zu schützen, die in einem (Online-)Register eingetragen sind.[54] Dafür sprechen die Rechtsklarheit[55] und Rechtssicherheit, aufgrund derer auch andere Immaterialgüterrechte als Registerrechte ausgestaltet sind. Auf der anderen Seite wird angesichts der enormen Masse der als Schutzgut in Betracht kommenden Daten zu prüfen sein, ob ein Registerverfahren praktikabel ist. Denkbar wäre indes eine technische Lösung, etwa dergestalt dass nur solche Dateien geschützt werden, die aufgrund einer dauerhaften Codierung (eines digitalen Wasserzeichens) einem Berechtigten zugewiesen werden.

b. Datenschutz als Dateneigentums- oder Datenverwertungsrecht

Vor dem Hintergrund des ökonomischen Werts personenbezogener Daten wird bereits heute die Weiterentwicklung des Datenschutzrechts diskutiert. Gegenstand dieser Diskussion sind insbesondere die Schaffung eines an das bestehende Urheberrecht angelehnte „Datennutzungsrechts“[56] sowie die Rechtskonstruktion eines „immaterialgüterrechtlichen Eigentumsrechts an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten“[57]. Hierbei handelt es sich allerdings

---

[51] Vgl. aber kritisch Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (201).

[52] Dazu Staudinger/*Seiler*, BGB, Eckpfeiler des Zivilrechts, 2014, Sachenrecht − Allgemeine Lehren, Rn. 37.

[53] Zweifelnd *Weber/Chrobak*, Der digitale Nachlass, Jusletter IT 24 (Sept. 2015), Rn. 73; keine Bedenken mit Blick auf den Numerus-clausus-Grundsatz hat dagegen Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (201).

[54] *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (146).

[55] Vgl. Staudinger/*Seiler*, BGB, Eckpfeiler des Zivilrechts, 2014, Sachenrecht − Allgemeine Lehren, Rn. 62, zum sachenrechtlichen Publizitätsgrundsatz.

[56] *Zech*, "Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1154); *Wandtke*, Ökonomischer Wert von persönlichen Daten – Diskussion des „Warencharakters“ von Daten aus persönlichkeits- und urheberrechtlicher Sicht, MMR 2017, 6.

[57] *Fezer*, Theorie des immaterialgüterrechtlichen Eigentums an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten, MMR 2017, 3.

jeweils „nur“ um eine vom Dateninhalt (Personenbezogenheit) abhängige Rechtsposition, sodass diese Ansätze keinen unmittelbaren Beitrag zu einem Konzept für ein absolutes Recht an Daten als solche leisten.[58]

3. Offene Fragen

Fraglich ist, ob Daten (in jedem Fall) hinreichend abgrenzbar sind, um Gegenstand eines absoluten Rechts zu sein.[59] Will man das absolute Recht an Daten nicht als bloßes Registerrecht formalisieren, wäre ggf. zu erwägen, es auf Dateien zu beschränken.[60]

Zu klären wäre, ob und in welcher Form ein etwaiges absolutes Recht an Daten dem Berechtigten zwangsweise entzogen werden könnte, namentlich im Wege der Zwangsvollstreckung. Dabei kann wohl nicht außer Betracht bleiben, ob sich aus dem Dateninhalt Einschränkungen der Vollstreckbarkeit ergeben.[61]

Ein Recht an Daten kann mit anderen Rechten kollidieren. Klärungsbedürftig ist insbesondere das Verhältnis eines absoluten Rechts an Daten zu dem Recht am Speichermedium und zum Recht am Dateninhalt.[62] Dabei stellt sich auch die Frage, ob der Inhaber des Dateneigentums bzw. des absoluten Rechts an Daten die Herausgabe des Speichermediums verlangen kann oder ob das Recht an den Daten subsidiär gegenüber dem Sacheigentum am Speichermedium ist.[63]

III. Personelle Zuordnung

Schwierigkeiten bereitet auch die Beantwortung der Frage, wem ein absolutes Recht an Daten zuzuordnen wäre.

1. Problematik

Neben recht klaren Fällen (wie der Eingabe und Speicherung eines Textes auf einem PC durch eine Privatperson) gibt es viele Konstellationen, in denen nicht unmittelbar einleuchtet, welchem Beteiligten ein absolutes Recht an Daten zustehen sollte. Beispielhaft zu nennen sind die Formulierung und Speicherung eines Textes durch einen Arbeitnehmer oder Auftragnehmer (Frage, ob die Daten

---

[58] Siehe zu diesen Ansätzen aber auch die Ausführungen unter F. II. 4.
[59] Zum sachenrechtlichen Grundsatz der Bestimmtheit vgl. Staudinger/*Seiler*, BGB, Eckpfeiler des Zivilrechts, 2014, Sachenrecht − Allgemeine Lehren, Rn. 59.
[60] Definition von Datei laut Wikipedia: Bestand meist inhaltlich zusammengehöriger Daten, der auf einem Datenträger oder Speichermedium gespeichert ist.
[61] Vgl. *Zech*, "Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1155).
[62] Vgl. BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109; *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (491).
[63] Vgl. Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 37.

dem Arbeitnehmer/Auftragnehmer oder dem Auftraggeber/Arbeitgeber zuzuordnen sind)[64] oder die automatische Erzeugung von Daten durch ein Fahrzeug oder eine Maschine (je nach Lage des Einzelfalls könnten die Daten bspw. zustehen dem Eigentümer des Fahrzeugs, dem Besitzer/Fahrer, einem Auftraggeber [etwa einem Landwirt, der einen Lohnunternehmer beauftragt hat], dem Hersteller der Maschine/des Fahrzeugs, einem IT-Dienst, der die Daten erfasst, einer Werkstatt, die das Fahrzeug/die Maschine wartet).[65] Unklar ist auch, ob der Empfänger Rechte an ungefragt per E-Mail übersandten Daten oder ungefragt auf seinem Computer installierter Schadsoftware erwirbt.

2. Lösungsansätze

Denkbar sind unterschiedliche Zuordnungskriterien. Diskutiert wird etwa die Zuordnung des Rechts an Daten nach der persönlichen Betroffenheit oder anhand des Sacheigentums an dem Speichermedium, auf dem die Daten gespeichert sind.[66] Diese Ansätze erscheinen jedoch für ein Recht an Daten, das gerade unabhängig von dem Dateninhalt und dem Speichermedium bestehen soll, weniger geeignet. Näher zu betrachten sind daher die Zuordnungen nach dem Schaffensprozess (Skripturakt, a) und nach der Verkehrsanschauung (b).

a. Skripturakt

Vertreten wird zum einen ein eher technischer Ansatz, der – in Anlehnung an die Praxis im Strafrecht[67] – einen Skripturakt für maßgeblich für die personelle Zuordnung des absoluten Rechts an Daten hält.[68] Skribent ist danach der technische „Ersteller“ der Daten, sodass in einem Arbeitsverhältnis zunächst der Arbeitnehmer berechtigt sein soll, bis er die Daten aushändigt.[69] Danach hätte allerdings ein Hacker, der auf fremden Computern Schadsoftware installiert, ein absolutes Recht an dieser Software mit der Folge, dass der Besitzer des Computers die Schadsoftware ohne Zustimmung des Hackers nicht löschen dürfte. Um solche Ergebnisse zu vermeiden, sollen von dem Grundsatz der Maßgeblichkeit des

---

[64] Vgl. http://www.spiegel.de/karriere/berufsleben/soziale-netzwerke-wann-gehoeren-facebook-freunde-dem-chef-a-1012782.html zur Frage, wem die Daten aus teils beruflich, teils privat genutzten Netzwerken gehören.

[65] Vgl. *Sahl*, Daten als Basis der digitalen Wirtschaft und Gesellschaft, RDV 2015, 236 (242): Unklar sei, wem ein neues Schutzrecht an nicht-personenbezogenen Maschinendaten zuzuordnen sei. Theoretisch kämen fast alle Beteiligten in Betracht; ein nachvollziehbares Interesse habe fast jeder Beteiligte. Aus rechtlicher Perspektive gebe es jedenfalls keine zwingende Antwort.

[66] Vgl. Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 24 f.; dagegen wohl BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.

[67] Vgl. OLG Naumburg, Urt. v. 27.8.2014 – 6 U 3/14, DAR 2015, 27; OLG Nürnberg, Beschl. v. 23.1.2013 – 1 Ws 445/12, CR 2013, 212; BayObLG, Urt. v. 24.6.1993 – 5 St RR 5/93, CR 1993, 779 (780).

[68] *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486.

[69] OLG Nürnberg, Beschl. v. 23.1.2013 – 1 Ws 445/12, CR 2013, 212 (2013); *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (487).

Skripturaktes wertungsgerechte Ausnahmen gelten, wenn der Eigentümer des Speichermediums die Skriptur nicht in irgendeiner Form mitveranlasst hat.[70] Erfolgt die Skriptur automatisch oder arbeitsteilig, soll nach der Wesentlichkeit des Beeinflussungsmoments abgegrenzt werden.[71]

b. Verkehrsanschauung

Andere sehen in der Verkehrsanschauung das maßgebliche Zuordnungskriterium für das absolute Recht an Daten, dem im Zweifel Vorrang gegenüber einer technisch-naturwissenschaftlichen Betrachtung zukomme.[72]

Abzustellen ist danach auf denjenigen, der wirtschaftlich die Erzeugung der Daten, also das Codieren, veranlasst hat. Bei komplexen Maschinen ist dies nach Ansicht von Zech[73] regelmäßig der wirtschaftliche Betreiber, etwa der Halter eines Fahrzeugs oder der Unternehmensinhaber, der Produktionsmaschinen einsetzt. Dieser sorge dafür, dass die Aufnahme- bzw. Messvorrichtung unterhalten und effizient eingesetzt wird, und trage die dafür erforderlichen Aufwendungen.

IV. Zwischenergebnis

Als – im Bedarfsfall näher zu überprüfende[74] – Hypothese ist festzuhalten, dass ein etwaiges absolutes Recht an Daten sich eher an Kategorien des Immaterialgüterrechts als an denjenigen des (Sach-)Eigentums orientieren sollte. Dabei könnte der Schutzumfang flexibel bestimmt werden (von einem umfassenden Herrschaftsrecht bis hin zur Einräumung nur einzelner positiver oder negativer Befugnisse), ohne neben dem (Sach-)Eigentum und den Immaterialgüterrechten einen neuen Typus absoluter Rechte schaffen zu müssen. Problematisch erscheint es dagegen, abstrakt (durch eine auf die Vielzahl denkbarer Fallkonstellationen anwendbaren Formel) zu bestimmen, welchem Beteiligten ein absolutes Recht an Daten zustehen soll.

E. Regelungsbedarf im Einzelnen

Das Eigentum und das Erbrecht werden gewährleistet; Inhalt und Schranken werden durch die Gesetze bestimmt (Art. 14 Abs. 1 GG). Das Grundgesetz hat dem Gesetzgeber den Auftrag zugewiesen, eine Eigentumsordnung zu schaffen, die sowohl den privaten Interessen des Einzelnen als auch denen der Allgemeinheit gerecht wird. Ihm obliegt hierbei eine doppelte Aufgabe: Einerseits muss er im

---

[70] *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (488).
[71] *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (488).
[72] Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (200).
[73] *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (144).
[74] Vgl. die abweichende Ansicht von Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 37, die eine Analogie zu § 903 nach geltendem Recht für den besten Ansatz halten.

Privatrecht die für den Rechtsverkehr und die Rechtsbeziehungen der Bürger untereinander maßgeblichen Vorschriften schaffen (z. B. für die Übertragung oder Belastung von Eigentum, das Nachbarrecht sowie das Ersatzrecht bei Beeinträchtigung des Eigentums durch Dritte); andererseits hat er den Belangen der Allgemeinheit in den (meist) öffentlich-rechtlichen Regelungen Rechnung zu tragen.[75]

Ob danach die Schaffung eines Eigentums oder eines anderen absoluten Rechts an Daten verfassungsrechtlich geboten ist oder zumindest rechtspolitisch wünschenswert wäre, um sowohl die Interessen der „Inhaber" von Daten zu schützen, als auch die sich im Zuge der Digitalisierung bietenden ökonomischen Chancen zu wahren, hängt maßgeblich davon ab, wie Daten derzeit im Zivilrecht behandelt werden. Ist das geltende Recht in seiner Ausformung durch die Rechtsprechung in der Lage, sach- und interessengerecht mit Daten umzugehen, muss der Gesetzgeber nicht tätig werden. Zeigen sich umgekehrt Defizite bei dem zivilrechtlichen Schutz von Daten oder dem Rechtsrahmen für die Internetwirtschaft, wäre zu prüfen, ob und in welcher Weise diese auch aus verfassungsrechtlichen Gründen behoben werden müssten, indem ein absolutes Recht an Daten geschaffen wird.

Bei der Prüfung des Regelungsbedarfs ist ein weit gespannter Blickwinkel angezeigt. Es ist nicht nur die Behandlung von Daten als solche zu betrachten. Relevant sind vielmehr auch diejenigen Rechte, die sich aus dem Dateninhalt und mit Blick auf das Speichermedium ergeben. Folgt nämlich bspw. aus dem Eigentum an einem Server oder aus dem Urheberrecht am Dateninhalt ein ausreichender Rechtsrahmen, spricht dies gegen die Annahme eines Bedarfs für die Schaffung eines absoluten Rechts an Daten.

Die Arbeitsgruppe hat daher die für ein absolutes Recht in Betracht kommenden Fallgruppen umfassend daraufhin analysiert, ob das geltende Recht einen ausreichenden Rechtsrahmen bietet, und zwar mit allen bestehenden Vorschriften, auch soweit sie auf den Dateninhalt oder auf die Rechtsverhältnisse am Speichermedium abstellen. In die Überlegungen einbezogen wurde dabei zugleich der umfassende Schutz, den geistige Schöpfungen und Betriebsgeheimnisse im Immaterialgüter-, Wettbewerbs- und Deliktsrecht genießen.

I. Daten als sonstiges Recht i. S. v. § 823 Abs. 1 BGB?

1. Problemstellung

Nach § 823 Abs. 1 BGB geschützt sind das Leben, der Körper, die Gesundheit, die Freiheit und das Eigentum sowie ein „sonstiges Recht". Daten profitieren in vielen Fällen dadurch mittelbar vom deliktsrechtlichen Schutz des Eigentums, dass ihre Veränderung oder Löschung das Speichermedium physikalisch verändert. Im Gegensatz zu Daten ist der Datenträger ein körperlicher Gegenstand und

---

[75] BVerfG, Beschl. v. 15.7.1981 – 1 BvL 77/78, BVerfGE 58, 300 = NJW 1982, 745, Rn. 137; vgl. auch *Hoffmann/Luch/Schulz/Borchers*, Die digitale Dimension der Grundrechte, S. 203 ff.

damit als Eigentum von § 823 Abs. 1 BGB erfasst. Ist der Berechtigte also Eigentümer des Datenträgers, sind auch die darauf abgelegten Daten deliktsrechtlich geschützt.[76]

Entsprechendes gilt, wenn zwar kein Eigentum, aber berechtigter Besitz am Datenträger besteht, der nach höchstrichterlicher Rechtsprechung und herrschender Literaturmeinung als sonstiges Recht nach § 823 Abs. 1 BGB geschützt wird.[77] Soll er dazu dienen, eine bestimmte Nutzung der Sache (Speichermedium) zu ermöglichen, stellt es eine Rechtsgutverletzung i. S. v. § 823 Abs. 1 BGB dar, wenn der Besitzer an dieser Nutzung durch einen rechtswidrigen Eingriff (Veränderung oder Löschung von Daten) gehindert wird.[78]

Wer Daten auf einem Datenträger ablegt, der weder in seinem Eigentum noch in seinem (berechtigten) Besitz steht, genießt danach grundsätzlich keinen deliktsrechtlicher Schutz gemäß § 823 Abs. 1 BGB, soweit sich etwas anderes nicht mit Blick auf den Dateninhalt ergibt, etwa weil das als sonstiges Recht i. S. v. § 823 Abs. 1 BGB anerkannte allgemeine Persönlichkeitsrecht berührt ist. In solchen Fällen werden häufig vertragliche Ansprüche bestehen, etwa wenn Daten in der Cloud abgelegt werden und der Cloud-Betreiber vertraglich für die Löschung der Daten haftet. Eine (vertragliche) Haftung kommt dann auch bei einer nur fahrlässigen Beeinträchtigung der Daten in Betracht. Besteht keine vertragliche Verbindung zum Täter, sind die Grundsätze der Drittschadensliquidation zu prüfen.[79]

Fehlt es dagegen an Eigentum und (berechtigtem) Besitz am Datenträger und bestehen auch keine vertraglichen Ansprüche, kann der Rechtsschutz der Daten auf vorsätzliche Eingriffe beschränkt sein, die jedenfalls unter § 823 Abs. 2 BGB i. V. m. § 303a StGB (bzw. andere einschlägige Strafnormen) fallen, ggf. auch unter § 826 BGB. Dieser Befund führt zu der Frage, ob der Zugriff auf die Daten als solche (unabhängig von den Verhältnissen an dem Datenträger und vom Dateninhalt) ein sonstiges Recht i. S. v. § 823 Abs. 1 BGB verletzt. Wäre das der Fall, würden auch fahrlässige Handlungen erfasst.

2. Grundsätze

Dem Wortlaut von § 823 Abs. 1 BGB lassen sich keine Voraussetzungen für die Annahme eines sonstigen Rechts entnehmen. Der Umstand, dass ein sonstiges Recht (und nicht ein Rechtsgut) erwähnt wird, kann allerdings als Hinweis darauf

---

[76] OLG Karlsruhe, Urt. v. 7.11.1995 – 3 U 15/95, NJW 1996, 200; MüKo/*Wagner*, BGB, § 823 Rn. 165; *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 47 f.; BeckOGK/*Spindler*, BGB, § 823 Rn. 135 f.

[77] Statt vieler: Palandt/*Sprau*, BGB, § 823 Rn. 13 m. w. N.

[78] Vgl. BGH, Urt. v. 9.12.2014 – VI ZR 155/14, NJW 2015, 1174; *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 48.

[79] Skeptisch *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 48: Es fehle an einer Schadensverlagerung, weil der Eigentümer oder berechtigte Besitzer des Datenträgers durch den Eingriff selbst einen Schaden erleide. Das erscheint indes nicht zwingend, da ein relevanter Schaden häufig allein oder jedenfalls weit überwiegend bei dem Vertragspartner, der Daten abgelegt hat, eintreten wird.

verstanden werden, dass das sonstige Recht dem Eigentum vergleichbar sein muss. Als Recht erwähnt § 823 Abs. 1 BGB nämlich nur das Eigentum ausdrücklich. Das Leben, der Körper, die Gesundheit und die Freiheit sind hingegen Rechtsgüter (und keine Rechte). Das spricht dafür, dass nicht jede beliebige subjektive Rechtsposition sonstiges Recht i. S. v. § 823 Abs. 1 BGB sein kann.[80] Anerkannt ist vielmehr, dass nur absolute, ausschließliche Rechte in Betracht kommen.[81]

Kennzeichnend für ein absolutes Recht sind zwei Kriterien, nämlich eine Zuordnungs- (oder Nutzungs-)Funktion und eine Ausschlussfunktion. Die in Rede stehende Position muss sich also zum einen dem Gut einer Person zuordnen lassen, was allerdings wenig Unterscheidungskraft hat, da dies auch für schuldrechtliche Ansprüche gilt. Entscheidender ist daher die Ausschlussfunktion. Die Position muss ihren Inhaber ermächtigen, Eingriffe von jedermann (also nicht nur von einzelnen Dritten, z. B. Vertragspartnern) auszuschließen.[82]

Zu berücksichtigen ist ferner, dass den „sonstigen Rechten“ des § 823 Abs. 1 BGB eine Auffangfunktion zukommt. Der offene Tatbestand dient als Einfallstor für Rechtsfortbildung, namentlich für die Einwirkung des Verfassungsrechts.[83] Dies zeigt sich beispielhaft an der Anerkennung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb und des allgemeinen Persönlichkeitsrechts als sonstige Rechte. Andererseits ist nicht jede grundrechtlich geschützte Position auch ein sonstiges Recht.[84] Bspw. ist das Nutzungsrecht an einer Internet-Domain zwar nach Art. 14 GG geschützt.[85] Durch die Registrierung des Domainnamens erwirbt der Inhaber der Internetadresse aber nach höchstrichterlicher Rechtsprechung weder Eigentum am Domainnamen noch ein sonstiges Recht i. S. v. § 823 Abs. 1 BGB. Die ausschließliche Stellung, die darauf beruht, dass ein Domainname nur einmal vergeben wird, ist allein technisch bedingt. Eine derartige rein faktische Ausschließlichkeit begründet, so der Bundesgerichtshof (BGH) im Einklang mit der vorstehend skizzierten Systematik, kein absolutes Recht.[86]

Bei der Entscheidung, welche Positionen in welchem Umfang als sonstige Rechte deliktsrechtlichen Schutz genießen sollen, ist schließlich die Funktion von § 823 Abs. 1 BGB im System des Deliktsrechts im Blick zu behalten. Diese besteht ganz

---

[80] Herberger/Martinek/Rüßmann u.a./*Lange/Schmidbauer*, jurisPK-BGB, § 823 Rn. 18.
[81] Statt vieler: Palandt/*Sprau*, BGB, § 823 Rn. 11.
[82] Vgl. MüKo/*Wagner*, BGB, § 823 Rn. 205; BeckOGK/*Spindler*, BGB, § 823 Rn. 158.
[83] Vgl. Herberger/Martinek/Rüßmann u.a./*Lange/Schmidbauer*, jurisPK-BGB, § 823 Rn. 18; BeckOGK/*Spindler*, BGB, § 823 Rn. 158.
[84] Vgl. BGH, Urt. v. 18.1.2012 – I ZR 187/10, BGHZ 192, 204 = NJW 2012, 2034 − Rn. 27.
[85] BVerfG, Nichtannahmebeschl. v. 24.11.2004 – 1 BvR 1306/02, BVerfGK 4, 210 = NJW 2005, 589.
[86] BGH Urt. v. 18.1.2012 – I ZR 187/10, BGHZ 192, 204 = NJW 2012, 2034 Rn. 21 ff. m. w. N.

maßgeblich in der Ausklammerung reiner Vermögensschäden aus der allgemeinen Fahrlässigkeitshaftung.[87] Diese Struktur spricht für eine eher restriktive Anerkennung von sonstigen Rechten.[88]

3. Daten als sonstiges Recht?

Einzelne Stimmen in der (meist neueren) Literatur bejahen die Einordnung von Daten oder eines „Rechts am eigenen Datenbestand" bzw. eines „Rechts auf das eigene Datum" als sonstiges Recht i. S. v. § 823 Abs. 1 BGB.[89] Dabei wird der Schutz teilweise auf qualifizierte Fälle beschränkt, etwa auf eine „Datensammlung von erheblicher Bedeutung".[90] In der Rechtsprechung[91] und von der wohl überwiegenden Anzahl der Literaturstimmen[92] wird die Anerkennung eines solchen sonstigen Rechts indes abgelehnt. Für beide Ansichten sprechen erhebliche Gründe:

a. Gründe für die Einordnung als sonstiges Recht

Lange Zeit wurden Daten typischerweise auf eigenen Computern und Servern gespeichert. Der über das Eigentum am Speichermedium vermittelte Schutz von Daten bereitete hier keine besonderen Schwierigkeiten. Seit einiger Zeit entwickelt sich in der Praxis indes eine zunehmende Virtualisierung des Datenwesens. Daten werden in großem Umfang auf fremden Servern gespeichert. Diese sind häufig identifizierbar (i. S. d. Überlassung von Speicherplatz auf einem konkreten fremden Server). Gerade im Cloud Computing können Daten aber auch fragmentiert

---

[87] Vgl. MüKo/*Wagner*, BGB§ 823 Rn. 207.

[88] BeckOGK/*Spindler*, BGB, § 823 Rn. 183 a.E.

[89] BeckOGK/*Spindler*, BGB, § 823 Rn. 183 ff.; BeckOK/*Spindler*, BGB, § 823 Rn. 93 (Stand: Aug. 2015); *ders.*, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, JZ 2016, 805 (813 f.); *Bartsch*, Die Vertraulichkeit und Integrität informationstechnischer Systeme als sonstiges Recht nach § 823 Abs. 1 BGB, CR 2008, 613; Conrad/Grützmacher/*Bartsch*, Recht der Daten und Datenbanken im Unternehmen, S. 297; *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (491) [zweifelnd dagegen Conrad/Grützmacher/*Hoeren*, Recht der Daten und Datenbanken im Unternehmen, S. 303 (306)]; *Meier/Wehlau*, Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585 (1588 f.); *Redeker*, Information als eigenständiges Rechtsgut − Zur Rechtsnatur der Information und dem daraus resultierenden Schutz, CR 2011, 634 (638); *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (143); *Zech*, "Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1158), jeweils m. w. N.; wohl auch Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (202 ff.); *ders.*, Absolute Rechte an der Nutzung einer Domain − eine zentrale Weichenstellung für die Rechtsentwicklung, WRP 2011, 543.

[90] So Conrad/Grützmacher/*Bartsch*, Recht der Daten und Datenbanken im Unternehmen, S. 301; gegen eine derartige Einschränkung BeckOGK/*Spindler*, BGB, § 823 Rn. 186.

[91] Vgl. OLG Dresden, Beschl. v. 5.9.2012 – 4 W 961/12, NJW-RR 2013, 27 (28); offen gelassen von OLG Karlsruhe, Urt. v. 7.11.1995 – 3 U 15/95, NJW 1996, 200 − Rn. 8 (bei juris).

[92] *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 52 ff.; MüKo/*Wagner*, BGB, § 823 Rn. 165 m. w. N.; Staudinger/*Hager*, BGB, § 823 Rn. B 192; Soergel/*Beater*, BGB, § 823 Rn. 106; Palandt/*Sprau*, BGB, § 823 Rn. 9, 19.

auf unterschiedlichen und im Laufe der Zeit wechselnden, über den Globus verteilten Servern gespeichert sein mit der Folge, dass kaum oder gar nicht feststellbar ist, wann welche Daten wo gespeichert waren. In solchen Fällen greift der Schutz der Daten über den Eigentumsschutz am Speichermedium nicht mehr.[93]

Richtig ist auch der Hinweis, dass es in vielen Fällen unter Wertungsgesichtspunkt problematisch sei, danach zu differenzieren, ob Daten auf einem eigenen Datenträger gespeichert oder bspw. in einer Cloud abgelegt seien. Den Daten kann nämlich in beiden Fällen dieselbe wirtschaftliche und emotionale Bedeutung zukommen.[94] Ferner wird darauf verwiesen, die Anerkennung eines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch das Bundesverfassungsgericht (BVerfG)[95] gebiete den Schutz von Daten nach § 823 Abs. 1 BGB.[96]

b. Gründe gegen die Einordnung als sonstiges Recht

Überwiegende Gründe sprechen hingegen derzeit sowohl de lege lata als auch de lege ferenda gegen die Anerkennung von Daten bzw. eines Rechts am eigenen Datenbestand als sonstiges Recht i. S. v. § 823 Abs. 1 BGB.[97]

Eine Einordnung als deliktsrechtlich geschütztes Recht erfordert – wie oben im Einzelnen ausgeführt – eine absolute, gegenüber jedermann wirkende, von der Rechtsordnung eingeräumte Rechtsposition. Will man nicht mit der überkommenen, in gefestigter höchstrichterlicher Rechtsprechung ausgeformten Dogmatik brechen, reichen dagegen grundsätzlich Ausschlussrechte auf vertraglicher Grundlage, die nur gegenüber einzelnen Vertragspartnern bestehen, nicht aus. Auch eine technische oder faktische Ausschließlichkeit begründet kein hinreichendes absolutes Recht.[98] Damit liegen die Voraussetzungen für eine entsprechende Einordnung bei digitalen Daten nicht vor. Der Zugang zu Daten und

---

[93] So etwa Conrad/Grützmacher/*Bartsch*, Recht der Daten und Datenbanken im Unternehmen, S. 297; BeckOGK/*Spindler*, BGB, § 823 Rn. 136 f., 183 ff.; *ders.*, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, JZ 2016, 805 (813 f.).

[94] Vgl. Conrad/Grützmacher/*Bartsch*, Recht der Daten und Datenbanken im Unternehmen, S. 300; BeckOGK/*Spindler*, BGB, § 823 Rn. 137.

[95] BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, BVerfGE 120, 274 = NJW 2008, 822.

[96] Conrad/Grützmacher/*Bartsch*, Recht der Daten und Datenbanken im Unternehmen, S. 300; BeckOGK/*Spindler*, BGB, § 823 Rn. 184, 187; *ders.*, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, JZ 2016, 805 (813 f.).

[97] Ebenso *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 52 ff.; *ders.*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, NJW-Beil. 2016, 29 (32); Conrad/Grützmacher/*Hoeren*, Recht der Daten und Datenbanken im Unternehmen, S. 305 f.; MüKo/*Wagner*, BGB, § 823 Rn. 165; Leible/Lehmann/Zech/*Spickhoff*, Unkörperliche Güter im Zivilrecht, 2011, S. 233 (243 f.); Staudinger/*Hager*, BGB, § 823 Rn. B 192; *Wendehorst*, Die Digitalisierung und das BGB, NJW 2016, 2609 (2613); skeptisch auch *Zech*, Information als Schutzgegenstand, 2012, S. 386 (für einen Schutz des Speichernden aber S. 434 ff.); differenzierend *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (489 f.).

[98] Vgl. BGH, Urt. v. 18.1.2012 – I ZR 187/10, BGHZ 192, 204 = NJW 2012, 2034 − Rn. 23 f.

damit zugleich der Ausschluss Dritter vom Zugriff beruht auf tatsächlichen und technischen Vorkehrungen (etwa der Aufbewahrung eines PC in einem verschlossenen Raum oder einem Passwortschutz). Bei der Auslagerung von Daten auf fremde Rechner wird häufig zwar ein schuldrechtlicher Anspruch hinzukommen. So wird ein Cloudnutzer von dem Cloudbetreiber regelmäßig einerseits den Zugang zu den abgelegten Daten und andererseits den Ausschluss des Zugriffs Dritter auf diese Daten verlangen können. Auch damit beruht die ausschließliche Zugriffsmöglichkeit aber allenfalls auf faktischen, technischen Gründen und relativen (schuldrechtlichen) Ansprüchen.[99]

Hinzu kommen rechtstechnische Bedenken: Ein „Recht am eigenen Datenbestand“ ließe sich inhaltlich kaum fixieren und in seinem Schutzbereich definieren.[100] Teilweise wird sogar vorgeschlagen, Daten nicht stets, sondern nur oberhalb einer gewissen, im Einzelfall zu bestimmenden Erheblichkeitsschwelle als sonstiges Recht anzuerkennen.[101] Ferner wäre bspw. unklar, ob neben der Löschung und Veränderung von Daten auch deren Kopie (Vervielfältigung) und Nutzung (z. B. zu Analysezwecken) von § 823 Abs. 1 BGB erfasst werden sollte, obwohl die „Datensubstanz“ bei dem Berechtigten dabei nicht beeinträchtigt wird.[102] Ohnehin wäre klärungsbedürftig, wem ein absolutes Recht an Daten eigentlich zustehen sollte. Das ist in vielen Fallgruppen unklar,[103] müsste aber, um unzuträgliche Rechtsunsicherheit zu vermeiden, jedenfalls dann geregelt werden, wenn man ein absolutes Recht an Daten ausdrücklich in den Katalog von § 823 Abs. 1 BGB aufnehmen wollte.[104] Probleme könnten sich zudem aus kollidierenden Rechtspositionen am Dateninhalt ergeben, etwa aus dem Datenschutzrecht.[105] Entsprechende Schwierigkeiten entstünden auch dann, wenn die Rechtsprechung ohne ein Eingreifen des Gesetzgebers Rechte an Daten als sonstiges Recht i. S. v. § 823 Abs. 1 BGB anerkennen wollte.[106]

---

[99] *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 52; a.A. BeckOGK/*Spindler*, BGB, § 823 Rn. 185, allerdings ohne Begründung, warum ein bloßer technisch verfestigter Zugang zu Daten genügen soll.

[100] MüKo/*Wagner*, BGB, § 823 Rn. 165; *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (489 f.).

[101] So etwa Conrad/Grützmacher/*Bartsch*, Recht der Daten und Datenbanken im Unternehmen, S. 300 ff.

[102] Vgl. *Zech*, "Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1158).

[103] Insbesondere bei automatisch generierten Daten, etwa von einem PKW, vgl. *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 56; näher unter 5.

[104] *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 56 f.; *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (490); *Zech*, Information als Schutzgegenstand, 2012, S. 386.

[105] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (384 f.).

[106] Vgl. *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 52.

Auch der Verweis auf die Anerkennung eines Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch das BVerfG führt zu keiner anderen Bewertung. Das BVerfG sieht das genannte Grundrecht als besondere Ausprägung des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.[107] Der Schutz des allgemeinen Persönlichkeitsrechts ist indes bereits über dessen Anerkennung als sonstiges Recht zivilrechtlich umgesetzt. Maßgeblich ist insoweit der Inhalt der betreffenden Daten, nicht aber das Datum als solches. Ergibt sich mit Blick auf den Dateninhalt eine Beeinträchtigung des allgemeinen Persönlichkeitsrechts, besteht bereits nach geltender Rechtslage ein hinreichender deliktsrechtlicher Schutz aufgrund der gefestigten Rechtsprechung betreffend das allgemeine Persönlichkeitsrecht als sonstiges Recht. Eine vom Dateninhalt losgelöste Beeinträchtigung des allgemeinen Persönlichkeitsrechts ist ohnehin kaum vorstellbar. Ein Argument für eine Erweiterung des deliktsrechtlichen Schutzes von Daten als solchen kann nach alledem in diesem Zusammenhang nicht abgeleitet werden.

c. Subsidiarität gesetzgeberischer Eingriffe

Das Deliktsrecht ermöglicht in besonderem Maße ein Aufgreifen neuer Entwicklungen durch die Rechtsprechung. Das folgt in erster Linie daraus, dass die Aufzählung der geschützten Rechtsgüter und Rechte in § 823 Abs. 1 BGB nicht abschließend gefasst ist, sondern ausdrücklich auch „ein sonstiges Recht“ erwähnt. Der Schutz zusätzlicher Rechte und Rechtsgüter ist im Gesetz also bereits angelegt.

Die Rechtsprechung hat von dieser Möglichkeit in der Vergangenheit Gebrauch gemacht. Prominentestes Beispiel hierfür ist wohl das allgemeine Persönlichkeitsrecht, das in § 823 Abs. 1 BGB nicht erwähnt wird, dessen deliktsrechtlicher Schutz aber allgemein anerkannt ist. Der deliktische Schutz des allgemeinen Persönlichkeitsrechts (ebenso wie bspw. derjenige des eingerichteten und ausgeübten Gewerbebetriebes) ist von der höchstrichterlichen Rechtsprechung ausgeformt worden, ohne dass (bislang) ein durchgreifender Bedarf gesehen wurde, diesen Schutz auch im Wortlaut des Gesetzes in Erscheinung treten zu lassen. Eine entsprechende Handhabung ist auch hinsichtlich des deliktsrechtlichen Schutzes von digitalen Daten (bzw. eines Rechts am eigenen Datenbestand) angezeigt. Falls zukünftig bspw. in der Wirtschaft oder von Seiten der Verbraucher ein unzureichender deliktsrechtlicher Schutz von Daten moniert werden sollte oder sich auf andere Weise in der Praxis Hinweise auf Defizite in diesem Bereich zeigen, wäre zunächst abzuwarten, wie die Rechtsprechung mit entsprechenden Streitfällen umgeht. Ein gesetzgeberischer Eingriff sollte erst dann erwogen werden, falls sich keine einheitliche Rechtsprechung herausbildet oder die Rechtsprechung nicht zu sachgerechten Ergebnissen gelangt.

---

[107] BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, BVerfGE 120, 274 = NJW 2008, 822 – Rn. 166 ff.

Die Abteilung Zivilrecht des 71. Deutschen Juristentages hat sich – wenn auch wenig repräsentativ mit 21:6:4 Stimmen – gegen eine Ergänzung von § 823 Abs. 1 BGB zum Schutz von digitalen Daten ausgesprochen.[108] Soweit auf dem Juristentag die Schaffung eines neuen Schutzgesetzes gefordert wurde, um über § 823 Abs. 2 BGB zu einer Haftung für fahrlässige Verletzungen zu gelangen, betrifft dies nicht die vorliegend zu klärende Frage, ob Daten als sonstiges Recht anzuerkennen sind. Der Vorschlag wird deshalb erst weiter unten in den zusammenfassenden Erwägungen erörtert (unter F. II.).

4. Zwischenergebnis

Mangels Erforderlichkeit besteht derzeit kein Regelungsbedarf hinsichtlich der Anerkennung von Daten oder eines Rechts am eigenen Datenbestand als sonstiges Recht i. S. v. § 823 Abs. 1 BGB. Dies gilt umso mehr, als dass es sich kaum in die hergebrachte (und bewährte) Systematik des § 823 Abs. 1 BGB einfügen würde.

II. Schutz der Daten gegen unberechtigten Zugriff

Zentraler Anknüpfungspunkt für die Bewertung des Regelungsbedarfs ist die Frage, ob ein hinreichender Schutz von Daten gegen unberechtigten Zugriff durch Dritte schon über die verschiedenen den Dateninhalt betreffenden Gesetze besteht (Datenschutzrecht, Urheberrecht etc.) oder ob sich hier für bestimmte Datenarten Schutzlücken ergeben.

1. Problemstellung

Rechtlicher Schutz von Daten durch ein absolutes Recht kann unterschiedliche Schutzrichtungen haben. Drei mögliche Schutzrichtungen sind hervorzuheben:[109]

Grundlegendste Schutzform ist der Integritätsschutz von Daten. Schutzgut ist die Unversehrtheit von Daten, die durch Verlust (Löschung) oder Verfälschung (Änderung) der Daten verletzt wird (nicht aber durch eine bloße Kopie, die den Bestand der kopierten Daten unberührt lässt).

Zweitens ist ein umfassend verstandener Geheimnisschutz zu erwähnen, der jeden fremden Zugriff verhindert. Insofern stößt das Recht allerdings an Grenzen. Datensicherheit ist zunächst ein technisches Problem. Praktisch jeder Datennutzer ist darauf bedacht, die von ihm erzeugten Daten mit mehr oder weniger aufwändigen technischen Maßnahmen gegen unbefugten Zugriff zu schützen. Damit kann nicht nur lesender Zugriff unterbunden werden, sondern auch Verletzungen

---

[108] Beschlüsse des 71. Deutschen Juristentages, Essen 2016, Abteilung Zivilrecht, These 28a, S. 10, http://www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf.

[109] Nach *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, S. 815 (821 ff.); vgl. ähnliche, wenn auch teilweise abweichende Klassifizierungen etwa bei *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (486); *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (140).

der Datenintegrität durch Löschung oder unbefugte Veränderung von Daten. Das Recht kann diesen tatsächlichen Schutz nicht ersetzen. Es kann den tatsächlichen Schutz aber flankieren und unbefugte Zugriffe sanktionieren.

Schließlich kann das Interesse an der Verwertung von Daten geschützt werden, indem man Daten einem Prätendenten exklusiv zuordnet und ihm bestimmte Verwertungsrechte zuweist. Wie im Immaterialgüterrecht schützt man damit die wirtschaftliche Verwertung von Daten. Daraus kann sich zugleich ein Schutz des Berechtigten bei unbefugten Verwertungshandlungen Dritter ergeben, etwa durch Begründung von Bereicherungs- und Schadensersatzansprüchen.

2. Schutz gegen unberechtigten Zugriff im geltenden Recht

Greift ein Dritter unbefugt auf Daten zu, kann dies für den Berechtigten ernste Folgen haben. Denkbar sind ganz unterschiedliche Fallkonstellationen. Es würde den Rahmen der vorliegenden Ausarbeitung sprengen, jede mögliche Fallkonstellation aufzugreifen und eine konkrete Bewertung nach geltendem Recht vorzunehmen. Die Arbeitsgruppe ist daher der allgemeinen Frage nachgegangen, ob bei unberechtigtem Datenzugriff ein Anspruch des Berechtigten auf Herausgabe (im Wege der [Rück-]Übertragung und nachfolgender Löschung bei dem Täter) und auf Schadensersatz besteht. Sie hat dabei vertragliche (a) und gesetzliche Ansprüche (b) in den Blick genommen, und zwar sowohl bei Daten, die auf einem eigenen Speichermedium abgelegt sind, als auch bei solchen, die bei einem Cloud-Betreiber oder sonst auf fremden Servern gespeichert sind.

a. Vertragliche Ansprüche

Eher unproblematisch sind Fälle, in denen der Berechtigte und der Täter vertraglich verbunden sind (bspw. bei unbefugtem Datenzugriff durch einen beauftragten IT-Dienstleister oder Zugriff eines Cloud-Providers auf gespeicherte Daten). In vielen Fällen werden Verträge ausdrücklich regeln, welche Ansprüche dem Berechtigten in solchen Fällen zustehen. Ist das nicht der Fall, greifen die Vorschriften des Schuldrechts ein, namentlich die §§ 280 ff. BGB über Schadensersatz bei Pflichtverletzungen.

Soweit Ansprüche Verschulden voraussetzen, kann die Annahme eines Mitverschuldens die Position des Berechtigten im Einzelfall verschlechtern. Unbefugte Zugriffe auf Daten lassen sich in vielen Fällen durch technische Maßnahmen verhindern oder jedenfalls wesentlich erschweren. Unterlässt ein Berechtigter solche Maßnahmen, kann dies nach § 254 BGB als Mitverschulden zu würdigen sein.[110]

Schwieriger sind Fälle mit mehreren Beteiligten zu beurteilen, wenn zwischen dem Berechtigten und dem Täter keine unmittelbare vertragliche Beziehung besteht. So liegt es etwa, wenn ein Cloudbetreiber sich eines Rechenzentrums bedient, das unbefugt auf die gespeicherten Daten eines Cloudnutzers zugreift. Im Einzelfall kann die Weitergabe der Daten an einen Dritten als Verletzung einer

---

[110] Vgl. (zu deliktsrechtlichen Ansprüchen) MüKo/*Wagner*, BGB, § 823 Rn. 165; BeckOGK/*Spindler*, BGB, § 823 Rn. 185.

vertraglichen Pflicht des Cloudbetreibers gegenüber dem Cloudnutzer zu beurteilen sein. Ist das nicht der Fall, sind die Grundsätze des Vertrages mit Schutzwirkungen zugunsten Dritter oder der Drittschadensliquidation in Betracht zu ziehen.[111] Besteht im Einzelfall kein vertraglicher Anspruch, kann der Berechtigte aus den nachfolgend anzusprechenden gesetzlichen Anspruchsgrundlagen vorgehen.

b. Gesetzliche Ansprüche

Für gesetzliche Ansprüche wegen unbefugten Zugriffs auf Daten gibt es unterschiedliche Ansatzpunkte. Daten sind mittelbar über das Eigentum am Speichermedium geschützt (1). Ferner bestehen unter mehreren Gesichtspunkten absolute Ansprüche ohne Bezug zum Speichermedium und zum Dateninhalt (2). Schließlich kann der Dateninhalt geschützt sein (3).

(1) Eigentumsschutz des Speichermediums

Speichermedien sind körperliche Gegenstände und damit Sachen (§ 90 BGB). Eigentum und Besitz am Speichermedium sind umfassend geschützt (u.a. §§ 823 Abs. 1, 858 ff., 903, 1004 BGB). Davon profitieren auch Daten, und zwar selbst dann, wenn der unbefugte Zugriff auf Daten keine körperliche Beeinträchtigung des Speicherträgers zur Folge hat. Es ist nämlich anerkannt, dass der unberechtigte Zugriff auf gespeicherte Daten zugleich das gemäß § 903 BGB universal geschützte Eigentum an dem Speichermedium verletzt.[112] Dem liegt der Gedanke zugrunde, dass der Eigentümer mit dem (körperlichen) Speichermedium „nach Belieben verfahren“ darf (§ 903 S. 1 BGB), dies aber nicht möglich ist, wenn ein Dritter unbefugt die darauf gespeicherten Daten gelöscht oder verändert hat.[113]

Liegen die Daten auf einem eigenen Speicher, steht das Speichermedium also im Eigentum (oder Besitz) des Berechtigten, besteht demnach ein umfassender Schutz. Ansprüche auf Herausgabe der Daten oder auf Schadensersatz wegen des unbefugten Zugriffs können auch dann auf die am Speichermedium bestehende dingliche Rechtsposition gestützt werden, wenn der Speicherträger physisch nicht verändert wurde.

Dieser Weg greift allerdings nicht, wenn Daten auf fremden Speichern abgelegt sind, etwa beim Cloud-Computing. Dann kommen jedoch - neben vertraglichen Ansprüchen - die nachfolgend angesprochenen absoluten Ansprüche ohne Bezug zum Speichermedium und zum Dateninhalt (2) sowie die auf den Dateninhalt gestützten Ansprüche in Betracht (3).

---

[111] Vgl. *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (296 − Fn. 107).

[112] Vgl. OLG Oldenburg, Verf. v. 3.11.2011 – 2 U 98/11, CR 2012, 77.

[113] Ähnlich *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (489).

(2) Absolute Rechte

Nach geltendem Recht bestehen an Daten als solchen (also unabhängig von der Rechtsbeziehung zum Speichermedium und vom Dateninhalt) nicht nur vertragliche - also relative - Rechte. Unter mehreren Gesichtspunkten sind Daten als solche auch vor dem Zugriff Dritter geschützt, die nicht Vertragspartner des Berechtigten sind. Hervorzuheben sind die zivilrechtlichen Folgen des oben bereits beschriebenen[114] strafrechtlichen Schutzes von Daten (a), der deliktsrechtliche Schutz (b) und der Schutz von Daten in der Insolvenz (c).

(a) §§ 202a ff., 303a StGB als Schutzgesetze i.S.v. § 823 Abs. 2 BGB

In den §§ 202a, 202b, 202c, 202d und 303a StGB finden sich Straftatbestände, die Daten unabhängig von einem Speichermedium und von ihrem Inhalt schützen. Nach § 202a Abs. 1 StGB wird bspw. mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft.

Bei den genannten Straftatbeständen handelt es sich nach wohl einhelliger Ansicht um Schutzgesetze i. S. v. § 823 Abs. 2 BGB. Der unbefugte Zugriff auf Daten kann deshalb zivilrechtliche Ansprüche des Verletzten gegen den Täter auf Schadensersatz und – über § 1004 BGB – Unterlassung begründen.[115]

(b) Deliktsrechtlicher Schutz

Ein absoluter, nicht nur gegenüber Vertragspartnern wirkender Schutz von Daten folgt aus § 826 BGB, dessen Tatbestandsvoraussetzungen allerdings eng sind.[116] Unabhängig vom Dateninhalt und von den Rechtsbeziehungen zum Speichermedium kann in dem unbefugten Zugriff auf Daten im Einzelfall eine sittenwidrige vorsätzliche Schädigung des Berechtigten liegen.

Eine Haftung des Täters nach § 823 Abs. 1 BGB kommt unter unterschiedlichen Gesichtspunkten in Betracht. Neben dem Eigentum (und berechtigten Besitz) am Speichermedium ist z. B. der eingerichtete und ausgeübte Geschäftsbetrieb geschützt (was beim unbefugten Zugriff auf Daten aber wohl nur mit Blick auf den Dateninhalt in Betracht kommt).[117] Entsprechendes gilt für den deliktsrechtlichen Schutz des allgemeinen Persönlichkeitsrechts. Was die Einordnung von Daten

---

[114] Siehe oben unter C.III.3.

[115] Vgl. OLG Naumburg, Urt. v. 27.8.2014 – 6 U 3/14, DAR 2015, 27 (zu einem Anspruch nach § 1004 Abs. 2 BGB i. V. m. § 823 Abs. 2 BGB i. V. m. §§ 202a, 202c StGB hinsichtlich der Daten, die bei der Geschwindigkeitsmessung mit einer Geschwindigkeitsmessanlage entstehen); OLG Celle, Urt. v. 22.12.2010 – 7 U 49/09, NJW-RR 2011, 1047 (zu einem Anspruch aus § 823 Abs. 2 BGB i. V. m. § 202a StGB wegen Kundendaten); Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (195 f.), der auf die Unbestimmtheit dieser Straftatbestände hinweist, soweit sie eine zivilrechtliche Zuordnung von Daten unterstellen.

[116] Siehe nur Palandt/*Sprau*, BGB, § 826 Rn. 3 ff.

[117] Zu den Anspruchsvoraussetzungen vgl. Palandt/*Sprau*, BGB, § 823 Rn. 133 ff.

oder eines Rechts am eigenen Datenbestand als sonstiges Recht i. S. v. § 823 Abs. 1 BGB betrifft, wird auf das oben zu I. Gesagte Bezug genommen.

(c) Schutz von Daten in der Insolvenz und bei Zwangsvollstreckung

Daten, die bei Dritten (etwa einem Cloudbetreiber) gespeichert sind, sind im Falle der Insolvenz regelmäßig durch ein Aussonderungsrecht des Berechtigten gemäß § 47 InsO vor dem (unbefugten) Zugriff des Insolvenzverwalters und der Gläubiger des Dritten geschützt. Entsprechendes gilt bei einer Einzelzwangsvollstreckung in solche Daten, der der Berechtigte mit der Drittwiderspruchsklage gemäß § 771 ZPO entgegentreten kann. Einzelheiten zu beiden Fällen werden nachfolgend unter III. erörtert.

(3) Schutz des Dateninhalts

Der Inhalt von Daten, also die in elektronischer Form dargestellte Information, genießt nach geltendem Recht vielfältigen Schutz unter ganz unterschiedlichen rechtlichen Gesichtspunkten. Das macht die Rechtslage unübersichtlich. Sie hängt davon ab, um welche Dateninhalte es jeweils geht und wie diese nach geltendem Recht gegen den unberechtigten Zugriff durch Dritte geschützt sind. In Betracht kommen insbesondere personenbezogene Daten (a), als Immaterialgüterrecht geschützte Daten (b) und Betriebs- und Geschäftsgeheimnisse (c).

(a) Personenbezogene Daten

Personenbezogene Daten unterliegen dem Recht auf informationelle Selbstbestimmung und dem darauf fußenden Datenschutzrecht. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, wenn eine gesetzliche Erlaubnis oder Anordnung besteht oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG). Die Einwilligung ist grundsätzlich frei widerruflich; bestimmten gesetzlich erlaubten Datenverarbeitungen kann der Betroffene widersprechen (vgl. § 28 Abs. 4 BDSG). Insgesamt genießen personenbezogene Daten einen weitgehenden Schutz, der einem unbefugten Zugriff durch Dritte entgegensteht.[118] Durch die EU-DSGVO sind weitere Schutzrichtungen hinzugetreten, etwa das Recht auf Vergessenwerden gemäß Art. 17 EU-DSGVO.[119]

Ungeachtet des verfassungs- und ordnungsrechtlichen Ursprungs des Datenschutzrechts strahlt der Schutz personenbezogener Daten in das Zivilrecht aus, u.a. über § 823 Abs. 2 BGB (Datenschutz als Schutzgesetz) und über den Schutz

---

[118] Vgl. *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (623 ff.).

[119] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1.

des allgemeinen Persönlichkeitsrechts nach § 823 Abs. 1 BGB.[120] Über § 1004 BGB kommen dabei auch Beseitigungs- und Unterlassungsansprüche in Betracht.

(b) Immaterialgüterrechte

Als weiterer großer Bereich sind diejenigen Daten zu nennen, an denen ein Immaterialgüterrecht besteht. Dabei ist zunächst das Urheberrecht zu erwähnen. Das Urheberrecht im subjektiven Sinne gewährt dem Werkschöpfer ein eigentumsähnliches Recht an seinem Geisteswerk, aufgrund dessen er insbesondere die Verbreitung kontrollieren kann. Nach § 2 Abs. 1 Nr. 7 UrhG gehören zu den geschützten Werken auch Darstellungen wissenschaftlicher oder technischer Art. Das Urheberrechtsgesetz (UrhG) schützt nicht nur Geistesschöpfungen, sondern in den §§ 70 ff. UrhG auch verwandte Leistungen geringerer Schöpfungskraft, u.a. Software (§§ 69a ff. UrhG).

Im vorliegenden Zusammenhang kommt dem Schutz von Datenbanken besondere Bedeutung zu. Das UrhG schützt Datenbanken unter zwei unterschiedlichen Aspekten. Zum einen genießen Datenbankwerke urheberrechtlichen Schutz nach § 4 Abs. 2 UrhG. Datenbankwerke sind nach dieser Vorschrift Sammelwerke, deren Elemente systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind. Die geschützte persönliche geistige Schöpfung liegt in der Auswahl und/oder Anordnung der einzelnen Elemente.[121] § 4 Abs. 2 UrhG schützt demnach zwar die Auswahl und Anordnung der einzelnen Elemente, nicht aber die einzelnen Elemente an sich. Geschützt sein kann ein unbefugter Zugriff auf die Struktur einer Datenbank, der im Einzelfall auch in der Übernahme aller oder vieler Elemente liegen kann. Nicht unter § 4 UrhG fällt aber der Zugriff auf einzelne Daten.[122]

Der zweite Ansatz, unter dem das UrhG Datenbanken schützt, ist der Investitionsschutz nach §§ 87a ff. UrhG. Datenbank im Sinne dieser Vorschriften ist die Sammlung unabhängiger Elemente, 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. Schutzgut ist nicht in erster Linie eine geistige Leistung, sondern eine Investition in (als solche nicht notwendigerweise schutzfähige) Datenbankinhalte. Dieses Schutzgut ist im Falle des Zugriffs auf

---

[120] Näher *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (619 f.).

[121] *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (293).

[122] Vgl. *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (621); *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (293).

digitale Daten eher berührt als der auf die geistige Schöpfung abstellende Datenbankschutz nach § 4 UrhG.[123]

Demnach bezieht sich der Schutz insoweit nicht auf die einzelnen Daten, sondern auf deren Sammlung in einer Datenbank. Nach § 87b UrhG hat der Datenbankhersteller das ausschließliche Recht, die Datenbank insgesamt oder in (wesentlichen) Teilen zu vervielfältigen, zu verbreiten und öffentlich wiederzugeben. Das kann je nach Lage des Einzelfalls einschlägig sein, bspw. für die im Rahmen der sog. Industrie 4.0 oder des Internets der Dinge automatisch erhobenen Daten oder für die bei Big-Data-Anwendungen gesammelten Daten.[124] Voraussetzungen hierfür sind jeweils insbesondere eine systematische und methodische Anordnung der Daten, eine wesentliche Investition und ein unbefugter Zugriff.[125]

Daneben kann der Dateninhalt auch durch andere Immaterialgüterrechte geschützt sein, etwa als Patent, Marke oder Design.

(c) Geschäfts- und Betriebsgeheimnisse

Innerbetriebliches Wissen, Know-how und sonstige nicht öffentlich zugängliche Informationen zählen zu den wichtigsten Vermögenswerten eines Unternehmens, deren unbefugte Weitergabe großen Schaden verursachen kann. Solche Inhalte werden deshalb im geltenden Recht unter mehreren Gesichtspunkten geschützt. Dieser Schutz gilt auch dann, wenn es um Geheimnisse in Gestalt digitaler Daten geht.[126]

Unter Geschäfts- oder Betriebsgeheimnis versteht man jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem Willen des Betriebsinhabers aufgrund eines berechtigten wirtschaftlichen Interesses geheim gehalten werden soll. Technisches Wissen wird als Betriebsgeheimnis, kaufmännisches als Geschäftsgeheimnis bezeichnet.[127]

---

[123] *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (293); *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (487).

[124] *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (622).

[125] Vgl. *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (487 f.).

[126] Eingehend, auch zum Geheimnisschutz über die deliktsrechtliche Fahrlässigkeitshaftung gemäß § 17 UWG, § 823 Abs. 1, Conrad/Grützmacher/*Gennen*, Recht der Daten und Datenbanken im Unternehmen, S. 155 ff.; *Zech*, Information als Schutzgegenstand, 2012, S. 230 ff.

[127] BGH, Urt. v. 27.4.2006 – I ZR 126/03, GRUR 2006, 1044 (1046); vgl. auch *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (622 f.); *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (291).

Das Gesetz gegen den unlauteren Wettbewerb (UWG) stellt den unbefugten Umgang mit Geschäfts- und Betriebsgeheimnissen unter verschiedenen Aspekten unter Strafe. Bspw. macht sich nach § 17 Abs. 2 Nr. 1 lit. a UWG strafbar, wer zum Zwecke des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, sich ein Geschäfts- oder Betriebsgeheimnis durch Anwendung technischer Mittel unbefugt verschafft oder sichert. Strafbar ist auch der Geheimnisverrat durch Beschäftigte, das Ausspähen von Geheimnissen durch Beschäftigte oder Dritte und die unbefugte Verwertung von Geheimnissen.

Diese Voraussetzungen dürften in vielen Fällen vorliegen, wenn unbefugt auf digitale Daten eines Unternehmens zugegriffen wird.[128] Problematisch kann unter anderem die fehlende Offenkundigkeit sein, wenn etwa Maschinendaten nicht nur bei einem Beteiligten gespeichert werden, sondern einem begrenzten Personenkreis zur Verfügung stehen.[129]

Da es sich bei den §§ 17 ff. UWG um Schutzgesetze handelt, stehen dem Geschädigten zivilrechtliche Ansprüche auf Schadensersatz, Unterlassung und Beseitigung zu, §§ 823 Abs. 2, 1004 BGB. Ferner kommen Ansprüche aus § 823 Abs. 1 BGB unter unterschiedlichen Gesichtspunkten in Betracht (insbesondere Verletzung des Eigentums am Unternehmen, Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb). Hat der Täter Gewinne erzielt, können Ansprüche auf Gewinnherausgabe bestehen wegen angemaßter Eigengeschäftsführung gemäß §§ 687 Abs. 1, 681, 667 BGB oder aus Eingriffskondiktion.[130]

Daneben sind Geheimnisse durch verschiedene Vorschriften im Gesellschafts- und Arbeitsrecht geschützt, häufig auch in vertraglichen Geheimhaltungsklauseln, und zwar gerade bei der Auslagerung von IT-Leistungen. Hervorzuheben ist zudem die EU-Know-how-Richtlinie vom 8. Juni 2016.[131] Die Richtlinie schützt Geschäftsgeheimnisse. Das sind nach Art. 2 Nr. 1 Informationen, die geheim sind (weil sie weder allgemein bekannt noch ohne Weiteres zugänglich sind), die deshalb von kommerziellem Wert sind und die Gegenstand von angemessenen Geheimhaltungsmaßnahmen durch den Berechtigten sind. Die Richtlinie ist bis zum 9. Juni 2018 umzusetzen (Art. 19 Abs. 1). Dabei müssen die Mitgliedstaaten gemäß Art. 4 unter anderem sicherstellen, dass die Inhaber von Geschäftsgeheimnissen bestimmte Maßnahmen, Verfahren und Rechtsbehelfe beantragen können,

---

[128] *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (622 f.).

[129] Vgl. *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (488 f.)

[130] Vgl. *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (623).

[131] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, ABl. L 157/1.

um einen rechtswidrigen Erwerb, eine rechtswidrige Nutzung oder eine rechtswidrige Offenlegung ihres Geschäftsgeheimnisses zu verhindern oder eine Entschädigung zu erlangen. Der Erwerb des Geschäftsgeheimnisses ohne Zustimmung des Berechtigten gilt unter anderem dann als rechtswidrig, wenn er durch unbefugten Zugang zu oder unbefugtes Kopieren von elektronischen Dokumenten erfolgt (Art. 4 Abs. 2 lit. a).

3. Zwischenergebnis

Die vorstehenden Ausführungen zeigen, dass digitale Daten unter verschiedensten rechtlichen Ansatzpunkten gegen den unbefugten Zugriff durch Dritte geschützt sind. Grob lassen sich unterscheiden der vertragliche und der gesetzliche (auch im Verhältnis zu fremden Dritten wirkende) Schutz, innerhalb des Letzteren der Eigentumsschutz des Speichermediums, der Schutz der Daten als solche und der Schutz des Dateninhalts. Insgesamt kann der Schutz von Daten im Zivilrecht als eine Art „Flickenteppich" bezeichnet werden, der sich aus vielen unterschiedlichen Teilen zusammensetzt, die in ihrer Gesamtheit gleichwohl ein offenbar hinreichend geschlossenes Schutzsystem bilden[132], da auch in der Literatur wesentliche Lücken des Integritäts- und Geheimnisschutzes nicht dargetan sind.

III. Gesamt- und Einzelzwangsvollstreckung gegen Eigentümer des Speichermediums

1. Problemstellung

Ständig wachsende Datenmengen und eine zunehmende Virtualisierung des Datenwesens haben zu einer rasanten Verbreitung des Cloud Computing geführt, also der Zurverfügungstellung skalierbarer IT-Infrastrukturen über ein Netzwerk. In der Praxis haben sich ganz unterschiedliche Formen von Cloud Computing etabliert, bei denen den gewerblichen und (zunehmend auch) privaten Cloudnutzern neben bloßer Speicherkapazität teilweise auch andere Leistungen angeboten werden (z. B. Datenverarbeitung, Zurverfügungstellung von Software, Aktualisierungen etc.).[133]

Die Unterscheidung verschiedener Erscheinungsformen von Cloud Computing kann im vorliegenden Zusammenhang dahinstehen. Relevant ist hier allein der Umstand, dass der Nutzer Daten auf fremde Server überträgt, was grundsätzlich bei allen Formen von Cloud Computing der Fall ist. Damit entfällt nämlich die Möglichkeit, Rechte an Daten mittelbar aus der Rechtsposition am Speichermedium abzuleiten, insbesondere aus dem Eigentum und Besitz des Berechtigten an der Speicherressource. Dem Cloudnutzer steht keine derartige Rechtsstellung am Speichermedium zu. Allerdings ergibt sich aus dem Cloud-Computing-Vertrag

---

[132] Dieses Bild verwendet *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (495).

[133] Vgl. *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063; Conrad/Grützmacher/*Lenzer*, Recht der Daten und Datenbanken im Unternehmen, S. 116 ff.; siehe hierzu auch die Ausführungen in Kapitel 2 unter D.

unproblematisch ein Anspruch des Nutzers auf Zugriff auf die in der Cloud hinterlegten Daten. Dabei kommt es nicht darauf an, ob die Daten im Einzelfall auf einem im Eigentum (oder Besitz) des Cloudbetreibers stehenden bestimmten (exklusiven) Server gespeichert sind oder gemeinsam mit den Daten anderer Kunden auf einer oder mehreren, möglicherweise an unterschiedlichen Orten vorgehaltenen Speicherressourcen abgelegt sind, wobei der Cloudbetreiber auch Dritte, etwa Rechenzentren, einschalten kann.[134]

Geht der Cloudbetreiber in die Insolvenz, kommt es zunächst auf die Ausübung des Wahlrechts des Insolvenzverwalters an.[135] Entscheidet er sich gemäß §§ 103 ff. InsO für die Fortführung des Vertrages, kann der Cloudnutzer die vertraglichen Ansprüche, die ihm bislang gegen den Schuldner (den Cloudbetreiber) zustanden, nunmehr gegen den Insolvenzverwalter geltend machen. Eine spezifische Gefährdung der in der Cloud abgelegten Daten besteht in diesem Fall nicht.[136]

Anders liegt es, wenn der Insolvenzverwalter die Erfüllung ablehnt. Der Cloudnutzer wird dann typischerweise ein Interesse daran haben, die abgelegten Daten zurückzubekommen, um sie entweder selbst zu speichern und zu verarbeiten oder um hiermit einen anderen Cloudbetreiber zu betrauen.[137] Vor diesem Hintergrund ist die Arbeitsgruppe der Frage nachgegangen, ob die Position des Cloudnutzers in diesem Fall hinreichend gesichert ist. Das kann - gerade im gewerblichen Bereich - von existentieller Bedeutung sein. Bereits eine vorübergehende Unterbrechung des Datenzugriffs kann zu hohen Schäden führen.

Bei der Einzelzwangsvollstreckung in Speichermedien stellen sich entsprechende Fragen, etwa wenn in den Server vollstreckt wird, auf dem Daten eines Cloudnutzers gespeichert sind. Auch hier hat der Cloudnutzer ein Interesse, weiterhin auf die Daten zugreifen zu können.

2. Grundsätze

Wer aufgrund eines dinglichen oder persönlichen Rechts geltend machen kann, dass ein Gegenstand nicht zur Insolvenzmasse gehört, ist nach § 47 InsO kein Insolvenzgläubiger. Er kann die Aussonderung des Gegenstands nach den außerhalb des Insolvenzverfahrens geltenden Regeln verlangen. Ein Aussonderungsrecht besteht, wenn die Berechtigung und die Verfügungsgewalt auseinanderfallen, wenn also die Person, der der auszusondernde Gegenstand von der Rechtsordnung zugewiesen ist (vorliegend also der Cloudnutzer hinsichtlich der abgelegten Daten), nicht auch die tatsächliche Verfügungsgewalt über den Gegenstand

---

[134] Näher *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (385); *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2064).

[135] Dazu *Bultmann*, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (993).

[136] Vgl. *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063.

[137] Näher *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2063 f.).

innehat (diese liegt vorliegend beim Cloudbetreiber als Insolvenzschuldner bzw. beim Insolvenzverwalter). Durch die Erfüllung des Aussonderungsrechts kommt der Insolvenzverwalter seiner Pflicht nach, die von ihm vorgefundene Ist-Masse zur Soll-Masse zu bereinigen und damit das erwähnte Auseinanderfallen der Berechtigung und der tatsächlichen Verfügungsgewalt zu beenden.[138]

Das Aussonderungsrecht nach § 47 InsO betrifft in erster Linie dingliche Rechte. Ein schuldrechtlicher Anspruch kann jedoch ebenfalls zur Aussonderung berechtigen, wenn der Gegenstand, auf den er sich bezieht, nicht zur Insolvenzmasse gehört (§ 47 S. 1 Var. 2 InsO). Hierfür kommt es entscheidend darauf an, welchem Vermögen der umstrittene Gegenstand nach Inhalt und Zweck der gesetzlichen Regelung haftungsrechtlich zuzuordnen ist. Diese Zuordnung wird in der Regel nach dinglichen Gesichtspunkten vorgenommen, weil das dingliche Recht im Grundsatz ein absolutes Herrschaftsrecht bezeichnet. Schuldrechtliche Ansprüche können aber bei einer den Normzweck beachtenden Betrachtungsweise zu einer von der dinglichen Rechtslage abweichenden Vermögenszuweisung führen, wenn der Gegenstand, dessen Aussonderung begehrt wird, mit Blick auf den schuldrechtlichen Anspruch als massefremd anzusehen ist.[139]

3. Rechtslage nach geltendem Recht

a. Rechtsprechung

Vorschriften, die speziell die Behandlung von digitalen Daten in der Insolvenz sowie in der Einzelzwangsvollstreckung regeln, gibt es (bisher) nicht. Überraschenderweise ergibt auch eine Recherche in der Rechtsprechung kaum Treffer. Hervorzuheben ist aber eine Entscheidung des OLG Düsseldorf aus dem Jahr 2012, deren Grundzüge nachfolgend skizziert seien:[140]

In dem der Entscheidung zugrunde liegenden Fall hatte ein Unternehmen einen Dienstleister mit der Versendung von Newslettern an Kunden beauftragt. Nach Eröffnung des Insolvenzverfahrens über das Vermögen des Dienstleisters verlangte das Unternehmen von dem Insolvenzverwalter die Herausgabe der E-Mail-Adressen, welche es dem Dienstleister für die Versendung der Newsletter überlassen hatte und welche dieser laufend gepflegt hatte.

Das OLG Düsseldorf hat einen gemäß § 47 InsO zur Aussonderung berechtigenden Anspruch aus §§ 667 Alt. 1, 675 BGB auf Herausgabe der E-Mail-Adressen bejaht. Es sei ein Geschäftsbesorgungsvertrag abgeschlossen worden. Der Dienstleister habe die E-Mail-Adressen zur Ausführung der Geschäftsbesorgung erhalten (§ 667 Alt. 1 BGB). Gegenständlich sei der Herausgabeanspruch gemäß § 667 Alt. 1 BGB nicht auf körperliche Gegenstände beschränkt, sondern umfasse auch immaterielle Güter. Dementsprechend müsse der Dienstleister nach § 667 Alt. 1

---

[138] HK-InsO/*Lohmann*, § 47 Rn. 1, 7; Schmidt/*Thole*, InsO, § 47 Rn. 3.
[139] BGH, Urt. v. 10.2.2011 – IX ZR 73/10, NJW 2011, 1282; HK-InsO/*Lohmann*, § 47 Rn. 16.
[140] OLG Düsseldorf, Urt. v. 27.9.2012 − I-6 U 241/11, CR 2012, 801.

BGB nach Beendigung der Geschäftsbesorgung auch ihm überlassene Kundendaten und das Recht herausgeben, diese Daten zu speichern und zu nutzen.

Bei einer Gesamtwürdigung aller Umstände sei, so das OLG Düsseldorf, zum einen festzustellen, dass die Kunden, die sich bei dem Newsletter an- oder abgemeldet hätten, im Rahmen ihres informationellen Selbstbestimmungsrechts und im Rahmen ihres sonstigen allgemeinen Persönlichkeitsrechts nur die Auftraggeberin und nicht den Dienstleister ermächtigt hätten, die E-Mail-Adressen zum Zweck des Newsletter-Versands zu speichern und zu nutzen. Für die Auftraggeberin seien diese, wenn auch von Seiten der Kunden jederzeit widerruflichen Ermächtigungen, ihre E-Mail-Adressen für den Newsletter-Versand zu speichern und zu nutzen, von erheblichem wirtschaftlichem Wert gewesen, weil sie auf diesem Wege ihre besonders interessierten Kunden gezielt habe bewerben können. Zum anderen habe die Auftraggeberin dem Dienstleister nur das von ihrer vorgenannten Rechtsstellung abgeleitete und nach dem Geschäftsbesorgungsvertrag jederzeit widerrufbare Recht eingeräumt, die E-Mail-Adressen insoweit zu speichern und zu nutzen, als es für die Durchführung des automatischen Newsletter-Versands notwendig gewesen sei. Die Herausgabe des Rechts zur Speicherung und Nutzung der Kundendaten erfolge dadurch, dass der Dienstleister der Auftraggeberin eine Kopie seiner Daten zukommen lasse und gleichzeitig die Daten im eigenen Bestand lösche.[141]

b. Aussonderungsrecht bei Cloud Computing

Die Entscheidung des OLG Düsseldorf,[142] die in der Literatur zustimmend zitiert wird,[143] fügt sich in die insolvenzrechtliche Dogmatik ein:[144]

Die Aussonderung kann auf dingliche oder auf persönliche, also schuldrechtliche Berechtigungen eines Dritten gestützt werden. Entscheidend ist, dass die Berechtigung dazu führt, dass der Gegenstand, dessen Aussonderung begehrt wird, als massefremd anzusehen ist. Daher schließen sich Aus- und Absonderung gegenseitig aus, denn die abgesonderte Befriedigung kann nur in Bezug auf massezu-

---

[141] Vgl. zur Herausgabe von Daten Conrad/Grützmacher/*Müller*, Recht der Daten und Datenbanken im Unternehmen, S. 313 ff. m. w. N.

[142] OLG Düsseldorf, Urt. v. 27.9.2012 − I-6 U 241/11, CR 2012, 801, vgl. soeben a..

[143] *Berger*, Immaterielle Wirtschaftsgüter in der Insolvenz, ZInsO 2013, 569 (571); Conrad/Grützmacher/*Czarnetzki/Röder*, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 340 ff.; HK-InsO/*Lohmann*, § 47 Rn. 5, 17; Schmidt/*Thole*, InsO, § 47 Rn. 62; Uhlenbruck/*Brinkmann*, InsO, § 47 Rn. 62; *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2064); *ders.*, Daten in der Cloud im Insolvenzfall - Ein internationaler Überblick, K u. R 2015, 448 (450); im Sinne des OLG Düsseldorf (wenn auch zeitlich früher) auch *Bultmann*, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (994); im Ergebnis ebenso MüKo/*Ganter*, InsO, § 47 Rn. 31a, 341.

[144] Der BGH hat (ausweislich der Verfahrensangaben bei juris) die gegen das Urteil des OLG Düsseldorf erhobene Nichtzulassungsbeschwerde zurückgewiesen (29.5.2013 - III ZR 322/12); so auch Conrad/Grützmacher/*Czarnetzki/Röder*, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 343.

gehörige Gegenstände verlangt werden. Für die Massezugehörigkeit ist eine haftungsrechtliche Betrachtungsweise maßgeblich, die danach fragt, für wessen Verbindlichkeiten der betreffende Gegenstand haftet. Haftet der Gegenstand nicht für die Verbindlichkeiten des Insolvenzschuldners, ist er massefremd und kann ausgesondert werden.[145]

Anerkannt ist, dass bloße schuldrechtliche Verschaffungsansprüche mangels haftungsrechtlicher Zuweisung grundsätzlich kein Aussonderungsrecht begründen, weil sie - wie bspw. der kaufvertragliche Übereignungsanspruch - auf eine Leistung aus der Masse gerichtet sind.[146] Anders kann es bei schuldrechtlichen Herausgabeansprüche liegen.[147] In Betracht kommt im vorliegenden Zusammenhang insbesondere ein in dem Cloud-Computing-Vertrag vereinbarter Anspruch des Cloudnutzers gegen den Cloudbetreiber auf Herausgabe der abgelegten Daten.[148]

Neben einem vertraglich ausdrücklich vereinbarten Herausgabeanspruch kann sich ein Aussonderungsrecht aus dem gesetzlichen Schuldrecht ergeben. Der o.g. Entscheidung des OLG Düsseldorf lag etwa ein Anspruch des Cloudnutzers als Geschäftsherr eines Geschäftsbesorgungsvertrages (§ 675 BGB) gegen den (insolventen) Cloudbetreiber als Geschäftsbesorger aus §§ 667 Alt. 1, 675 BGB zugrunde.[149] Ein solcher Anspruch ist regelmäßig gerichtet auf Herausgabe der Gegenstände, die der Geschäftsherr dem Geschäftsbesorger zur Ausführung des zu besorgenden Geschäfts übergeben hat.[150] Anders als die von dem Geschäftsbesorger aus der Geschäftsbesorgung erlangten Gegenstände (§§ 667 Alt. 2, 675 BGB) bleiben diejenigen Gegenstände, die dem Geschäftsbesorger zur Ausführung des Auftrags überlassen werden, jedenfalls dann in der Sphäre des Geschäftsherrn, wenn der Geschäftsführer sie lediglich zu einem eingegrenzten Zweck und nur mit beschränkten Befugnissen erhalten hat.[151]

Herausgabeansprüche, auf die das Aussonderungsbegehren gestützt werden kann, können sich – insbesondere mit Blick auf den Dateninhalt – ferner aus Immaterialgüterrechten, aus dem Datenschutzrecht und (über § 1004 BGB analog) aus den

---

[145] Uhlenbruck/*Brinkmann*, InsO, § 47 Rn. 9.
[146] Vgl. MüKo/*Ganter*, InsO, § 47 Rn. 347.
[147] Siehe nur MüKo/*Ganter*, InsO, § 47 Rn. 341 ff. m. w. N.
[148] *Bultmann*, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (994); *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2064, 2066).
[149] Liegt den vereinbarten Cloud-Diensten ein anderer Vertragstyp zugrunde – vgl. hierzu die Ausführungen in Kapitel 2 unter D. –, tritt ggf. ein anderer einschlägiger Herausgabeanspruch an die Stelle von §§ 667 Alt. 1, 675 BGB; eingehend zu materiell-rechtlichen Aspekten bei Ansprüchen auf Herausgabe von Daten Conrad/Grützmacher/*Müller*, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 313 ff.
[150] Vgl. *Bultmann*, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (994); MüKo/*Ganter*, InsO, § 47 Rn. 36, 340 f.; Uhlenbruck/*Brinkmann*, InsO, § 47 Rn. 9, 61 f.
[151] Uhlenbruck/*Brinkmann*, InsO, § 47 Rn. 62; MüKo/*Ganter*, InsO, § 47 Rn. 355; vgl. die Gesamtabwägung der Umstände des Einzelfalls durch das OLG Düsseldorf, Urt. v. 27.9.2012 − I-6 U 241/11, CR 2012, 801.

von § 823 Abs. 1 und 2 BGB geschützten Rechten/Rechtsgütern (u.a. allgemeines Persönlichkeitsrecht) und Straftatbeständen (etwa § 303a StGB) ergeben.[152]

Die Gesamtumstände beim Cloud Computing sprechen dafür, den Anspruch des Cloudnutzers gegen den Cloudbetreiber (auf welcher der vorgenannten Anspruchsgrundlagen er im Einzelfall auch beruhen mag) nicht als bloßen Verschaffungsanspruch, sondern als Herausgabeanspruch zu qualifizieren, auf dessen Grundlage das Aussonderungsrecht gemäß § 47 InsO geltend gemacht werden kann. Daten werden nämlich nicht Bestandteil des im Eigentum des Insolvenzschuldners (oder eines Dritten) stehenden Servers; vielmehr ist die Berechtigung an den Daten unabhängig vom Eigentum am Speichermedium zu klären.[153] Regelmäßig wird der Cloud-Computing-Vertrag so gestaltet sein, dass Daten nur zu eingeschränkten Zwecken (etwa zur Speicherung und Verarbeitung nach Maßgabe des Vertrages) übertragen werden und jederzeit zurückgefordert werden können, ohne dass der Cloudbetreiber sie zu eigenen Zwecken nutzen oder Dritten übertragen darf.[154] Der Cloudbetreiber erhält dabei nur eine dienende, mit sehr eingeschränkten Befugnissen verbundene Position, während der Cloudnutzer Herr der Daten bleibt. Dieser Vertragsgestaltung entspricht es, die in der Cloud abgelegten Daten der Haftungsmasse des Cloudnutzers (und nicht der Insolvenzmasse) zuzuordnen.[155]

c. Rechtslage bei Vertragsketten

Teilweise werden in der Literatur Defizite des Schutzes von Daten in der Insolvenz des Cloudbetreibers für den Fall gesehen, dass der Cloudbetreiber sich eines Dritten bedient, um die Daten zu speichern (bspw. eines Rechenzentrums).[156] Das erscheint keineswegs zwingend. Zwar besteht hier im Regelfall kein unmittelbarer Anspruch (insbesondere kein vertraglicher Anspruch) des Cloudnutzers gegen den Dritten. Zum einen kommt aber eine Auslegung des (vertraglichen) Herausgabeanspruchs des Cloudnutzers gegen den Cloudbetreiber dahingehend in Betracht, dass der Cloudnutzer vom Cloudbetreiber die Geltendmachung oder Abtretung von dessen Herausgabeanspruch gegen den Dritten verlangen kann. Zum anderen besteht ein vollstreckungsrechtlicher Weg: Der Cloudnutzer kann einen Herausgabetitel gegen den Cloudbetreiber bzw. den Insolvenzverwalter erwirken, bei dessen Vollstreckung ihm gemäß § 886 ZPO der Herausgabeanspruch des Cloudbetreibers gegen den Dritten überwiesen werden kann.[157] Entsprechend

---

[152] Näher *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2065); *Bultmann*, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (995).
[153] Vgl. BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.
[154] Zur Gestaltung schuldrechtlicher Zuordnungsklauseln in Cloud-Computing-Verträgen vgl. *Jülicher*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2066).
[155] Vgl. MüKo/*Ganter*, InsO, § 47 Rn. 355.
[156] So z.B. *Berger*, Immaterielle Wirtschaftsgüter in der Insolvenz, ZInsO 2013, 569 (572): Eine Anspruchsgrundlage bei Vertragsketten sei nicht ohne Weiteres ersichtlich.
[157] Vgl. MüKo/*Ganter*, InsO, § 47 Rn. 344 m. w. N.

liegt es, wenn bei einer solchen Vertragskette (Cloudnutzer-Cloudbetreiber-Dritter/Rechenzentrum) der Dritte insolvent wird.[158] Damit bietet das geltende Recht auch für Vertragsketten grundsätzlich taugliche Lösungsansätze.

d. Durchsetzung

Die Durchsetzung des Aussonderungsrechts wirft keine besonderen Schwierigkeiten auf. Der Anspruch auf Aussonderung ist gegen den Insolvenzverwalter als Partei kraft Amtes geltend zu machen. Er ist durch einstweilige Verfügung sicherbar, die im Einzelfall die Anordnung der Datenherausgabe im einstweiligen Verfügungsverfahren, also die Vorwegnahme der Hauptsache umfassen kann, etwa bei besonderer Dringlichkeit, wenn die Nichtherausgabe oder verzögerte Herausgabe erhebliche Schäden zur Folge hätte und einem Rechtsverlust gleichkäme.[159]

Die Zwangsvollstreckung des auf Herausgabe der Daten gerichteten Aussonderungsanspruchs wird regelmäßig gemäß § 888 ZPO auf Übertragung der Daten an den Cloudnutzer und Löschung beim Insolvenzverwalter bzw. dem Cloudbetreiber gerichtet sein.[160]

Praktische Schwierigkeiten können sich aus dem Umstand ergeben, dass die vom Cloudnutzer in der Cloud abgelegten Daten häufig nicht auf separaten physischen Ressourcen gespeichert werden, sondern aufgeteilt in mehrere Teile und zu Backup-Zwecken mehrfach vervielfältigt, weitgehend unstrukturiert organisiert und dezentral, häufig in ganz unterschiedlichen Ländern, abgelegt werden, wobei sich die Speicherorte im Zeitablauf ändern können.[161] Dieser technische Hintergrund kann die Durchsetzung des Anspruchs auf Aussonderung von Daten im Einzelfall zur Herausforderung machen. Auch insoweit sind indes (noch) keine konkreten Problemfälle bekannt geworden, die ein Eingreifen des Gesetzgebers geboten erscheinen lassen.

e. Einzelzwangsvollstreckung in Speichermedien

Wird im Wege der Einzelzwangsvollstreckung in den Server vollstreckt, auf dem Daten des Cloudnutzers gespeichert sind, hat der Cloudnutzer ein Interesse, weiterhin auf die Daten zugreifen zu können. Das geltende Recht verhilft dem Cloudnutzer hierzu grundsätzlich mit der Möglichkeit, Drittwiderspruchsklage gemäß § 771 ZPO zu erheben.

---

[158] Vgl. *Völzmann-Stickelbrock* auf dem Workshop des Justizministeriums NRW am 23.5.2016, Tagungsberichte bei *Christians,* Arbeitsgruppe „Digitaler Neustart im BGB“, AfP 2016, 334; *Liepin/Götz,* Braucht das BGB ein Update?, MMR-Aktuell 2016, 379185 (verfügbar bei beck-online).

[159] Vgl. *Bultmann*, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (996).

[160] Vgl. BGH NJW 1996, 2159 (2161); *Bultmann,* Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (996); *Jülicher,* Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2065 f.); eingehend Conrad/Grützmacher/*Müller,* Recht der Daten und Datenbanken im Unternehmen, 2014, S. 322 ff.

[161] Dazu BeckOGK/*Spindler,* BGB, § 823 Rn. 137; *Jülicher,* Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2064).

Behauptet ein Dritter, dass ihm an dem Gegenstand der Einzelzwangsvollstreckung ein die Veräußerung hinderndes Recht zustehe, so kann er gemäß § 771 ZPO der Zwangsvollstreckung im Wege der Drittwiderspruchsklage entgegentreten. Ansprüche aus schuldrechtlichen Verträgen genügen zwar auch insoweit grundsätzlich nicht. Auch hier sind jedoch Ausnahmen anerkannt, etwa wenn der Sicherungsnehmer im Verhältnis zum Sicherungsgeber nicht oder nur eingeschränkt berechtigt ist, das Sicherungsgut zu verwerten.[162]

Die Rechtslage gleicht weitgehend derjenigen bei § 47 InsO.[163] Schuldrechtliche Ansprüche begründen kein Widerspruchsrecht, soweit es sich um bloße Verschaffungsansprüche handelt. Anders liegt es jedoch, wenn der schuldrechtliche Anspruch Ausdruck der Nicht-Zugehörigkeit des Vollstreckungsgegenstands zum Schuldnervermögen ist. Ist der Gegenstand demnach dem Vermögen des Klägers zuzurechnen, gehört er nicht zu dem haftenden Vermögen des Vollstreckungsschuldners.[164] Maßgeblich sind mithin dieselben Grundsätze wie im Insolvenzrecht. Auf das hierzu Gesagte wird Bezug genommen.

Nach alledem kann der Cloudnutzer mit Hilfe der Drittwiderspruchsklage grundsätzlich durchsetzen, dass die Speichermedien (Server), auf denen seine Daten abgelegt sind, nicht im Wege der Einzelzwangsvollstreckung verwertet werden, bevor die Daten an ihn zurückübertragen (oder anderweitig gespeichert) und auf den zu verwertenden Speichern gelöscht wurden.

4. Kein aktueller Regelungsbedarf

Die Nutzung von Cloud-Computing-Angeboten durch Private und Unternehmen eröffnet große technische, gesellschaftliche und ökonomische Chancen. Das Zivilrecht sollte der Verbreitung des Cloud-Computing deshalb nicht entgegenstehen. Das wäre der Fall, wenn potentielle Cloudnutzer bei einer Insolvenz des Cloudbetreibers unangemessenen Risiken ausgesetzt wären und deshalb verbreitet Cloud-Anwendungen meiden und zu technisch und ökonomisch unterlegenen In-House-Lösungen greifen würden. Dann wäre zu prüfen, ob der Gesetzgeber dem etwa im Wege der Einführung eines absoluten Rechts an Daten oder durch andere gesetzgeberische Maßnahmen abhelfen könnte.

Derzeit ist indes nicht erkennbar, dass die Frage des Schutzes von Daten in der Insolvenz des Cloudbetreibers die Verbreitung des Cloud-Computing in nennenswerter Form hindern würde. Entsprechende Äußerungen von Verbänden der Anbieter- oder Nutzerseite oder von sonstigen Akteuren sind nicht ersichtlich. Vielmehr werden steigende Nutzerzahlen und Umsätze gemeldet.[165] Das mag auch

---

[162] BGH, Urt. v. 10.2.2011 – IX ZR 73/10, NJW 2011, 1282 m. w. N.
[163] Vgl. Schmidt/*Thole*, InsO, § 47 Rn. 4.
[164] Siehe nur MüKo/*Schmidt/Brinkmann*, ZPO, § 771 Rn. 39 f. m. w. N.
[165] Eingehend z.B. Cloud-Monitor 2016, abrufbar unter http://hub.klardenker.kpmg.de/cloud-monitor-2016?utm_campaign=Cloud-Monitor%202016&utm_source=AEM (letzter Abruf: 28.2.2017); siehe auch Pressemitteilung Bitkom e.V. vom 14.3.2017, „Nutzung von Cloud

damit zusammenhängen, dass die Beteiligten keinen entsprechenden tatsächlichen Fall (Insolvenz eines [größeren] Cloudbetreibers) im Blick haben und deshalb eher die technische Sicherheit des Cloud Computing und die Compliance als problembehaftete Themen ansehen.[166] Auch aus der juristischen Praxis sind keine Fälle bekannt, in der ein Cloudnutzer größere Schwierigkeiten gehabt hätte, Zugriff auf die in der Cloud abgelegten Daten zu bekommen. Dieser praktische Befund lässt sich auch damit erklären, dass das geltende Recht – wie oben im Einzelnen ausgeführt – mit dem Aussonderungsrecht gemäß § 47 InsO und der Drittwiderspruchsklage nach § 771 ZPO grundsätzlich taugliche Grundlagen für den Schutz digitaler Daten in der Insolvenz des Cloudbetreibers sowie bei der Einzelzwangsvollstreckung in Speichermedien bietet.

Dieses Ergebnis entspricht der Einschätzung der bei dem Workshop am 23. Mai 2016 im Justizministerium NRW angehörten Experten. Insbesondere Völzmann-Stickelbrock sah keine Schwierigkeiten, bei einer Insolvenz des Cloudbetreibers ein Aussonderungsrecht an Daten auf vertraglicher Grundlage anzunehmen, und zwar auch bei Vertragsketten, wenn also z. B. ein Cloudbetreiber die Daten in ein Rechenzentrum ausgelagert hat. Bereite die Annahme eines vertraglichen Anspruchs auf Herausgabe der Daten im Einzelfall Schwierigkeiten, könnten – so Völzmann-Stickelbrock – die Gerichte auf der Grundlage des geltenden Rechts helfen, angemessene Lösungen zu finden.[167]

5. Zwischenergebnis

Hinsichtlich des Schutzes von Daten in der Insolvenz des Cloudbetreibers bzw. bei der Einzelzwangsvollstreckung in das jeweilige Speichermedium besteht kein Regelungsbedarf. Aus heutiger Sicht sind keine Defizite feststellbar, die ein Eingreifen des Gesetzgebers erfordern.

Computing in Unternehmen boomt“, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Nutzung-von-Cloud-Computing-in-Unternehmen-boomt.html (letzter Abruf: 16.3.2017).

[166] Vgl. Cloud-Monitor 2016, abrufbar unter http://hub.klardenker.kpmg.de/cloud-monitor-2016?utm_campaign=Cloud-Monitor%202016&utm_source=AEM (letzter Abruf: 28.2.2017).

[167] *Völzmann-Stickelbrock* auf dem Workshop des Justizministeriums NRW am 23.5.2016, Tagungsberichte bei *Christians*, Arbeitsgruppe „Digitaler Neustart im BGB“, AfP 2016, 334; *Liepin/Götz*, Braucht das BGB ein Update?, MMR-Aktuell 2016, 379185 (verfügbar bei beck-online); so auch *Bultmann*, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (994 ff.); Conrad/Grützmacher/*Czarnetzki/Röder*, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 340 ff.; HK-InsO/*Lohmann*, § 47 Rn. 5; *Jülicher*, Daten in der Cloud im Insolvenzfall − Ein internationaler Überblick, K u. R 2015, 448 (450); *ders.*, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2066); Schmidt/*Thole*, InsO, § 47 Rn. 8; offen Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 40 f.; anders, jedenfalls „langfristig“, *Berger*, Immaterielle Wirtschaftsgüter in der Insolvenz, ZInsO 2013, 569 (572).

IV. Handel mit Daten

1. Problemstellung

Der Handel mit digitalen Inhalten (insbesondere Software und digitale kulturelle Güter in Gestalt von E-Books, Musik, Filmen etc.) entwickelt sich rasant. Verbraucher, die solche Güter digital und ohne verkörpertes Exemplar (etwa Buch, DVD etc.) online beziehen, meinen häufig, sie hätten einen Kaufvertrag abgeschlossen und Eigentum erworben. Entsprechend verhält es sich bei sonstigen Verträgen, mit denen Zugriff auf digitale Daten verschafft werden soll, bspw. im B2B-Bereich als Grundlage für Big-Data-Anwendungen.

Mit Blick auf den Gegenstand dieses Kapitels wird nachfolgend die Erfüllung derartiger Verträge näher betrachtet. Es wird der Frage nachgegangen, ob nach geltendem Recht Dateneigentum oder ein absolutes Recht an den betreffenden Daten übertragen wird (2.) bzw. ob dies gesetzlich geregelt werden sollte (3.).

2. Rechtslage nach geltendem Recht

Nach geltendem Recht besteht an Daten als solchen (also unabhängig von einem Datenträger und vom Dateninhalt) kein absolutes Recht. Über § 453 Abs. 1 BGB findet dennoch die maßgebliche Vorschrift in § 433 Abs. 1 BGB, nach der ein Verkäufer die Kaufsache zu übergeben und das Eigentum an der Kaufsache zu verschaffen hat, auf Daten als sonstige Gegenstände entsprechende Anwendung.[168] „Verkauft“ jemand Daten, hat er dem Käufer folgerichtig in Erfüllung des Kaufvertrages zwar nicht Besitz und Eigentum einzuräumen, was ihm nach dem Vorgesagten ohnehin rechtlich nicht möglich ist. Er hat dem Käufer aber Zugriff auf die Daten in dem vereinbarten Umfang zu verschaffen. Geschuldet ist damit die Verschaffung einer faktischen Position.

Werden Daten übertragen (beispielsweise als Dateianhang an einer E-Mail), ist dies nach geltendem Recht keine Verfügung, sondern ein faktischer Vorgang. Das geltende Recht stellt zwar keinen formalen Rahmen für die Übertragung von Daten auf einen Dritten zur Verfügung. Umgekehrt gibt es aber auch keine (zivil-)rechtlichen Hindernisse oder formale Vorgaben hierfür. Insbesondere genießt die Position des Empfängers gegenüber den übertragenen Daten grundsätzlich keinen geringeren Schutz als diejenige des Übertragenden.

Diese Grundsätze gelten auch für den entgeltlichen Download digitaler Güter im Internet, etwa von E-Books, Filmen oder Musikdateien. Auch solche Verträge werden – vorbehaltlich einer abweichenden Gestaltung im Einzelfall – als Kaufvertrag über einen sonstigen Gegenstand angesehen (§§ 433, 453 BGB).[169] Be-

---

[168] Näher *Hauck*, Gebrauchthandel mit digitalen Gütern, NJW 2014, 3616.
[169] Siehe nur Staudinger/*Beckmann*, BGB, § 453 Rn. 72 ff.

sonderheiten ergeben sich aus dem Dateninhalt, der meist urheberrechtlich geschützt sein wird.[170] Bei den im Internet als Massengeschäft angebotenen Downloads wird regelmäßig durch Allgemeine Geschäftsbedingungen bestimmt bzw. klargestellt, dass der Anbieter dem Verbraucher „nur" ein Nutzungsrecht zu verschaffen hat, wobei die Nutzung das Zugänglichmachen der Datei erfordert.[171] Hinsichtlich der vertragsrechtlichen Fragen, die sich in diesem Zusammenhang stellen, wird auf die Ausführungen in Kapitel 2 Bezug genommen.[172]

3. Regelungsbedarf

Der Handel mit Daten bietet für Unternehmen, aber auch für Verbraucher, neue Chancen. Aufgabe des Zivilrechts ist es, einen geeigneten Rechtsrahmen zur Verfügung zu stellen, der die Entwicklung des Datenhandels mindestens nicht behindert. Regelungsbedarf besteht, wenn sich solche Hindernisse aus dem Umstand ergeben, dass derzeit – wie soeben ausgeführt – kein absolutes Recht an den gehandelten Daten als solchen übertragen, sondern insoweit lediglich eine faktische Position verschafft werden kann.

Nachfolgend wird daher auf die Fragen eingegangen, ob ein absolutes Recht an Daten den Datenhandel erleichtern würde (a), ob ein gutgläubiger Erwerb von Daten in Betracht kommt (b) und ob der Handel mit Daten andere besondere Fragen der rechtlichen Zuordnung von Daten aufwirft (c).

a. Förderung des Handels mit Daten?

Regelungsbedarf könnte bestehen, wenn das Fehlen einer rechtlich grundierten absoluten Zuordnung von digitalen Daten sich negativ auf den Handel mit Daten auswirken würde. Das ist jedoch nicht ersichtlich. Entsprechende Äußerungen von Verbänden (sei es von Seiten der Wirtschaft oder der Verbraucher) oder sonstige Stimmen, die dies substantiiert fordern, liegen nicht vor.

Auch sonst ist nicht erkennbar, dass der Datenhandel durch Einführung eines absoluten Rechts an Daten gefördert werden könnte. Vielmehr dürfte das Fehlen

---

[170] Vgl. EuGH, Urt. v. 3.7.2012 – C-128/11, GRUR 2012, 904 − Rn. 38 ff.; BGH, Urt. v. 17.7.2013 – I ZR 129/08, NJW-RR 2014, 360, Rn. 33 ff., 42 ff.; OLG Hamm, Urt. v. 15.5.2014 – I-22 U 60/13, NJW 2014, 3659; näher *Kreuzer* (iRights.Law), Weiterveräußerungsfähigkeit von digitalen Gütern, http://www.verbraucherportal-bw.de/site/pbs-bw-new/get/documents/MLR.Verbraucherportal/Dokumente/Dokumente%20pdfs/Verbraucherschutz/Urheberrecht/15_10_20%20Studie%20Weiterver%C3%A4u%C3%9Ferungsf%C3%A4higkeit%20von%20digitalen%20G%C3%BCtern_Dr.%20Till%20Kreutzer.pdf.

[171] Vgl. OLG Köln, Urt. v. 26.2.2016 – 6 U 90/15, CR 2016, 458.

[172] Siehe dort etwa unter H.; Überblick zudem bei *Kreuzer* (iRights.Law), Weiterveräußerungsfähigkeit von digitalen Gütern, http://www.verbraucherportal-bw.de/site/pbs-bw-new/get/documents/MLR.Verbraucherportal/Dokumente/Dokumente%20pdfs/Verbraucherschutz/Urheberrecht/15_10_20%20Studie%20Weiterver%C3%A4u%C3%9Ferungsf%C3%A4higkeit%20von%20digitalen%20G%C3%BCtern_Dr.%20Till%20Kreutzer.pdf.

einer solchen Rechtsposition und die Einräumung einer bloßen faktischen Position an den betreffenden Daten unschädlich sein (oder den Handel durch die Flexibilität der Vertragserfüllung und niedrige Transaktionskosten sogar fördern, weil die Vertragserfüllung nicht formalisiert ist und es z. B. keiner Eintragung in ein Datenregister bedarf, wie es in der Literatur[173] vorgeschlagen wird).

Zwar bestehen durchaus offene Fragen im Bereich des Datenhandels. Nicht abschließend geklärt ist etwa, ob E-Books und andere in digitaler Form erworbene kulturelle Güter vom Erwerber weiterveräußert oder vererbt werden können. In diesem Zusammenhang (und für einen angemessenen Schutz der Rechte des Erwerbers) bedarf es jedoch nicht eines Dateneigentums oder eines sonstigen absoluten Rechts an Daten. Vielmehr handelt es sich in erster Linie um vertragsrechtliche und urheberrechtliche Fragen. Regelmäßig ergibt sich aus dem Vertrag (bzw. den diesem zugrunde liegenden Allgemeinen Geschäftsbedingungen), welche Befugnisse an den betroffenen Daten dem Erwerber eingeräumt werden sollen. Wird bspw. ausdrücklich nur ein befristetes persönliches Nutzungsrecht gewährt, kann die vertrags- sowie urheberrechtliche Zulässigkeit und Wirksamkeit der Abrede hinterfragt werden. Auf ein etwaiges absolutes Recht an den Daten kommt es dabei nicht entscheidend an: Bestünde ein derartiges Recht, würde es bei einer solchen Vertragsgestaltung wohl beim Anbieter verbleiben und nicht auf den Verbraucher übergehen.

Wird ein E-Book, eine Musikdatei oder Ähnliches dagegen ohne entsprechende Einschränkung verkauft und dem Käufer zugänglich gemacht, erwirbt dieser die Datei als Wirtschaftsgut, mit dem er faktisch nach Belieben verfahren kann – vorbehaltlich allerdings etwaiger sich aus dem Dateninhalt, etwa einem nicht erschöpften Urheberrecht, ergebender Einschränkungen.[174] Dasselbe gilt für den Handel mit Daten im B2B-Bereich. Es kommt mithin nicht auf ein absolutes Recht an den Daten an, sondern auf den Vertragsinhalt und das Urheberrecht.

Nach alledem ist nicht ersichtlich, dass die Schaffung eines absoluten Rechts an digitalen Daten den Datenhandel fördern könnte oder dass das Fehlen eines solchen Rechts sich negativ auf den Handel auswirken würde.

b. Kein gutgläubiger Erwerb von Daten

Zu klären ist, ob beim Handel mit Daten ein gutgläubiger Erwerb der Daten von einem Nichtberechtigten in Betracht kommt. Das ist de lege lata zu verneinen. Auch gegen die Schaffung einer solchen Möglichkeit bestehen Bedenken.

Das Eigentum an beweglichen Sachen und Rechte an Grundstücken können nach den §§ 932 ff., 892 f. BGB gutgläubig von einem Nichtberechtigten erworben

---

[173] *Zech*, Information als Schutzgegenstand, 2012, S. 437 ff.

[174] Vgl. *Hauck*, Gebrauchthandel mit digitalen Gütern, NJW 2014, 3616; EuGH, Urt. v. 3.7.2012 – C-128/11, GRUR 2012, 904 − Rn. 38 ff.; BGH, Urt. v. 17.7.2013 – I ZR 129/08, NJW-RR 2014, 360, Rn. 33 ff., 42 ff.; OLG Hamm, Urt. v. 15.5.2014 – I-22 U 60/13, NJW 2014, 3659.

werden. Grundlage des gutgläubigen Erwerbs ist jeweils ein Publizitätsmoment, und zwar bei beweglichen Sachen die Besitzübertragung und bei Rechten an Grundstücken die Eintragung im Grundbuch. Dabei handelt es sich um die für jeden Vertrauensschutz unerlässliche Rechtsscheingrundlage, die den Verlust des Eigentums beim Alteigentümer und den gutgläubigen Erwerb rechtfertigt.[175]

Ein gutgläubiger Erwerb von digitalen Daten erscheint bereits im Ansatz problematisch, weil eine vergleichbare Rechtsscheingrundlage fehlt. Daten haben andere technisch-naturwissenschaftliche Eigenschaften als körperliche Sachen. Sie können beliebig oft kopiert und verbreitet werden, ohne dass dies ihre Qualität beeinträchtigt (Nicht-Exklusivität). Sie können von beliebig vielen Personen gleichzeitig genutzt werden, ohne dass sich hierdurch technische Nachteile oder Konkurrenzen ergeben würden (Nicht-Rivalität).[176]

Mangels Körperlichkeit kann man Daten nicht besitzen.[177] Als Alternative zum Besitz, wie er bei beweglichen Sachen als Publizitätsmoment Bedeutung erlangt, könnte man auf den Zugriff auf Daten abstellen, also auf die tatsächliche Möglichkeit der Kenntnisnahme und des sonstigen Umgangs mit Daten, etwa durch den Besitz eines (körperlichen) Speichermediums oder die Kenntnis von Zugangsdaten.[178] Daten sind aber beliebig oft duplizierbar. Dem Innehaben von Daten kommt deshalb nicht dieselbe (und auch keine vergleichbare) Bedeutung als Rechtsscheinwirkung zu wie dem Besitz einer beweglichen Sache. Wesentliche, mit dem Besitz zusammenhängende, sachenrechtliche Prinzipien, wie Publizität und Gutglaubensschutz, sind nämlich auf Rivalität angewiesen.[179] Sind Daten aber nicht-rival, weil zur gleichen Zeit problemlos (ohne Rivalität) mehrere Personen auf sie zugreifen können, ist mangels eines geeigneten Publizitätsmoments ein gutgläubiger Erwerb ausgeschlossen. Mit anderen Worten: Wenn viele Personen gleichzeitig auf bestimmte Daten zugreifen können, kommt der Zugriffsmöglichkeit einer einzelnen Person sachenrechtlich nicht die Bedeutung zu, die einen gutgläubigen Erwerb rechtfertigt.

Der Besitz des Speichermediums, auf dem die betreffenden Daten abgelegt sind, genügt gleichfalls nicht als Publizitätsmoment. Die unkörperlichen Daten sind rechtlich von dem körperlichen Speichermedium zu trennen.[180] Daten lassen sich beliebig vervielfältigen. Mit der rechtlichen Zuweisung des Speichermediums werden nicht automatisch auch die darauf abgelegten Daten zugewiesen.[181] Die Berechtigung an den gespeicherten Inhalten folgt nämlich anderen Regeln als das

---

[175] Dazu Staudinger/*Seiler*, BGB, Eckpfeiler des Zivilrechts, 2014, Sachenrecht − Allgemeine Lehren, Rn. 65.
[176] Näher oben unter B. 2. a.
[177] *Zech*, Information als Schutzgegenstand, 2012, S. 119.
[178] Vgl. *Zech*, Information als Schutzgegenstand, 2012, S. 120.
[179] Näher *Zech*, Information als Schutzgegenstand, 2012, S. 277.
[180] BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109; vgl. *Zech*, Information als Schutzgegenstand, 2012, S. 336.
[181] Vgl. *Zech*, Information als Schutzgegenstand, 2012, S. 336.

Eigentum an dem Speichermedium.[182] Es besteht nach – soweit ersichtlich – allgemeiner Ansicht kein Gleichlauf der Rechte am Speichermedium und an den Daten. Nur bei einem solchen Gleichlauf könnte man aber annehmen, dass bei einem gutgläubigen Erwerb eines Speichermediums zugleich die darauf abgelegten Daten gutgläubig erworben werden.

Eine andere Beurteilung wäre ggf. dann angezeigt, wenn man ein Register für digitale Informationen einführen und ausschließliche Rechte an den dort angemeldeten Daten anerkennen würde. Das wird in der Literatur vorgeschlagen.[183] Einem solchen Register könnte bei entsprechender gesetzlicher Gestaltung – vergleichbar dem Grundbuch für Rechte an Grundstücken – eine hinreichende Publizität zukommen, um einen gutgläubigen Erwerb von Daten zu erlauben. Das erscheint allerdings kaum praktikabel. Daten sind ein Massenphänomen. Es wäre mit einem untragbaren Aufwand verbunden, jedes Datum und die jeweils berechtigte Person in ein Register einzutragen.[184]

Selbst wenn man einen gutgläubigen Erwerb von Daten für möglich hielte oder gesetzlich ausdrücklich vorsehen wollte, beträfe dies zunächst lediglich die Daten als solche. Unabhängig davon wäre das Schicksal etwaiger Rechte am Dateninhalt zu beurteilen. Der gutgläubige Erwerb bspw. einer urheberrechtlich geschützten E-Book-Datei brächte dem Erwerber wenig Nutzen, wenn er urheberrechtlich gehindert wäre, die Datei zu öffnen und das E-Book zu lesen. Entsprechendes gilt z. B. für personenbezogene Daten, da dem gutgläubigen Erwerber der bloßen Daten nicht zugleich eine datenschutzrechtliche Einwilligung zu deren Nutzung zugutekäme. Derartige am Inhalt des Datums bestehende Rechte müssten einem (etwa zu schaffenden) Recht am Datum als solchem aber vorgehen.[185]

c. Sonstige Erwägungen

Andere wesentliche Gesichtspunkte, die mit Blick auf den Handel mit Daten für die Schaffung eines absoluten Rechts an Daten sprechen könnten, sind nicht ersichtlich. Dieser Befund kann auch auf die besonderen technisch-naturwissenschaftlichen Eigenschaften von Daten zurückgeführt werden. Wie oben näher ausgeführt, sind Daten nicht-rival und nicht-exklusiv. Werden Daten nicht mit tatsächlichen oder technischen Mitteln (z. B. Verschluss des Speichermediums, Kennwortschutz) geheim gehalten, können sie beliebig oft kopiert und von einer Vielzahl von Interessenten gleichzeitig verwendet werden. Insofern unterscheiden Daten sich grundlegend von körperlichen Sachen, die nur einer Person (oder einer Personenmenge) zugeordnet sind.

---

[182] BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.
[183] *Zech*, Information als Schutzgegenstand, 2012, S. 437 ff.
[184] Ob ein solches Register unter Effizienzgesichtspunkten gerechtfertigt werden könnte, stellt auch *Zech*, Information als Schutzgegenstand, 2012, S. 440, in Frage.
[185] Näher *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, S. 815 (828); *Zech*, Information als Schutzgegenstand, 2012, S. 416 ff.

Wegen dieser spezifischen Eigenschaften kommt bei Daten technischen Schutzvorkehrungen eine herausgehobene Bedeutung zu. Gerade weil Daten technisch theoretisch ohne Weiteres für jedermann zugänglich sind, werden aufwändige Schutzmechanismen gegen unerwünschte Zugriffe installiert. Das gilt auch für den Handel mit Daten. Mittels technischer Vorkehrungen können bspw. E-Books oder Musikdateien effektiv bestimmten Nutzern zugeordnet werden (etwa über ein Zugriffssystem mit individueller Anmeldung und Kennwort). Unter dem Stichwort des Digital Rights Management (DRM) werden ganz unterschiedliche technische Zuordnungen diskutiert (z. B. digitale Signatur von Dateien, Kopierschutzsystem).[186] Hinzu kommt die IT-Sicherheit über Virenschutz, Firewalls etc. Diese technischen Systeme ersetzen zwar nicht rechtliche, an den Dateninhalt anknüpfende Zuordnungen etwa von Betriebs- und Geschäftsgeheimnissen. Wegen der spezifischen Eigenschaften von Daten ist der technische Schutz aber in besonderem Maße notwendig und effektiv.

Letztlich dürften technische Maßnahmen im Handel mit Daten eine befriedigende personelle Zuordnung ermöglichen. Auch deshalb ist derzeit nicht erkennbar, dass im Handel mit Daten ein Bedürfnis für eine stärkere rechtliche Zuordnung von Daten bestehen könnte.[187]

4. Zwischenergebnis

Der Handel mit Daten wirft keine besonderen Fragen der rechtlichen Zuordnung von Daten auf, die einer gesetzlichen Regelung zugeführt werden sollten. Es sind keine Anhaltspunkte dafür erkennbar, dass der Handel mit Daten durch ein absolutes Recht an Daten und die Möglichkeit eines gutgläubigen Erwerbs von Daten gefördert werden könnte und sollte.

V. Zuordnung automatisch generierter Daten

1. Problemstellung

Im Zuge der technischen Entwicklung gibt es immer mehr Sachverhalte, in denen Maschinen Daten selbst (jedenfalls ohne unmittelbare Mitwirkung eines Menschen) erzeugen. Hervorzuheben ist das sog. Internet der Dinge (Internet of Things, IoT), also die Ausbreitung des Internets auf physische Gegenstände, auf die aus der Ferne online zugegriffen werden kann und die ihre Umgebung vermessen und beeinflussen können. Beliebte Beispiele sind Haushaltsgegenstände, die entweder aus der Ferne gesteuert oder aufgrund bestimmter voreingestellter Parameter ohne unmittelbare Mitwirkung eines Menschen selbsttätig handeln,

---

[186] Vgl. Conrad/Grützmacher/*Meyer*, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 254 ff.; *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (492 f.).

[187] Ebenso unter dem Blickwinkel des Cloud Computing *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (385).

z. B. Lichter an- und ausschalten, die Heizung regeln oder Bestellungen von Lebensmitteln veranlassen. Im Straßenverkehr können vielfältige Daten aufgezeichnet und für verschiedenste Zwecke genutzt werden, etwa Daten über das Verkehrsaufkommen für Stauvorhersagen, Daten über das Fahrverhalten für eine individuelle Risikovorhersage und Bemessung von Versicherungstarifen sowie Unfalldatenspeicher für die Regulierung der Unfallschäden. Im industriellen Bereich führt die Möglichkeit der Vernetzung von Maschinen zu erheblichen Umbrüchen, die auch als „Industrie 4.0" bezeichnet werden. Die Angebots-, Auftrags-, Fertigungs- und Lieferzyklen können in neuartiger Weise integriert werden. Bspw. können Produkte mit geringerem Aufwand individualisiert, also auf die Bedürfnisse eines konkreten Käufers abgestimmt werden, Industrieanlagen können über Sensoren laufend überwacht und dadurch effektiver eingesetzt werden, Wartungen können vorausschauend geplant, Defekte und Produktionsausfälle minimiert werden.

Gemeinsam ist allen diesen Fällen – die Liste ließe sich beliebig verlängern[188] –, dass Daten nicht unmittelbar durch einen Menschen erzeugt werden, der faktisch auf die Daten zugreifen kann und dem sie zugeordnet werden können. Vielmehr kommen mehrere Beteiligte in Betracht, was an zwei Beispielen verdeutlicht sei:

- Moderne PKW sind mit einer Vielzahl von Sensoren ausgerüstet, die enorme Mengen von Daten erfassen. Diese Daten werden im Fahrzeug gespeichert oder automatisch von dem Fahrzeug an Dritte (regelmäßig an den Hersteller des Fahrzeugs) gesendet. Faktischen Zugriff auf diese Daten hat meist der Fahrzeughersteller. Denkbar wäre jedoch auch eine Zuweisung an einen anderen Beteiligten, etwa den Fahrer (dessen allgemeines Persönlichkeitsrecht betroffen sein kann), den Beifahrer und weitere Insassen (deren Stimmen oder Bilder aufgezeichnet sein können), den Halter, den Eigentümer, den Verkäufer des Fahrzeugs, einen Zulieferer der elektronischen Ausrüstung, die Werkstatt (die die Datenspeicher im Fahrzeug ausliest) und die Versicherung (die einen Unfall regulieren oder den Versicherungsbeitrag nach der Fahrweise berechnen möchte).[189]
- Entsprechendes gilt (ohne den Aspekt des Personenbezugs) für moderne Landmaschinen, die bspw. ihre genaue geografische Position kennen, laufend die Bodengüte ermitteln, ausgebrachte Mengen von Dünger, Pflanzenschutz, Saatgut usw. ermitteln und bei der Ernte kleinteilig Erträge messen.[190] Mit Hilfe dieser Daten können Landmaschinen autonom fahren und

---

[188] Weitere Beispiele bei *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS für Fezer, 2016, S. 815 (816 ff.).

[189] Vgl. *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 56; *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137; zur Verwendung von Fahrzeugdaten im Zivilprozess *Balzer/Nugel*, Das Auslesen von Fahrzeugdaten zur Unfallrekonstruktion im Zivilprozess, NJW 2016, 193.

[190] Beispiel nach *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137.

> die effektivste Route auf der zu bewirtschaftenden Fläche ermitteln, sie können z. B. die optimale Menge von Dünger kleinteilig ermitteln (etwa: mehr Dünger auf schattigeren Teilflächen) - und vieles mehr. Faktischen Zugriff auf die Daten hat regelmäßig der Hersteller der Landmaschine. Mit Hilfe der von der Landmaschine automatisch generierten Daten ist der Hersteller in der Lage, dem Landwirt (kostenpflichtige) Dienstleistungen anzubieten. In Betracht käme auch eine Zuweisung der Daten an andere Beteiligte, etwa den Eigentümer der Flächen oder deren Pächter, an den Landwirt, der sie bewirtschaftet, an den Eigentümer der Landmaschine (etwa einen Lohnunternehmer) oder an den Fahrzeugführer (der die automatische Aufzeichnung durch das Steuern der Landmaschine letztlich am unmittelbarsten veranlasst).[191]

Vor dem Hintergrund der vorstehenden Ausführungen stellt sich die Frage, ob es einer rechtlichen Zuordnung automatisch generierter Daten bedarf. Dies gälte auch für die Fälle, in denen die Daten – zweifellos – einer bestimmten Person faktisch zugeordnet werden können, da dieser Ansatz bei Maschinendaten möglicherweise zu unerwünschten Ergebnissen führt. Nach einem Blick auf die geltende Rechtslage (2.) wird daher zunächst noch einmal vertieft betrachtet, nach welchen Kriterien automatisch generierte Daten rechtlich zugeordnet werden könn(t)en (3.), bevor eine Aussage zum Regelungsbedarf getroffen wird (4.).

2. Geltendes Recht

Automatisch generierte Daten werden nach geltendem Recht – mangels einer die Zuordnung regelnden Norm – demjenigen zugeordnet, der faktisch auf sie zugreifen kann, der sie also z. B. speichern, verarbeiten, verkaufen oder löschen kann. Dies gilt allerdings nur vorbehaltlich etwaiger die Daten im Einzelfall betreffender Rechtspositionen. In Betracht kommen insoweit weniger die Rechtsverhältnisse am Speichermedium. Daten werden nämlich nicht Bestandteil des Speichers; vielmehr ist die Berechtigung an den Daten unabhängig vom Eigentum am Speichermedium zu klären.[192]

Die personelle Zuordnung kann sich aber aus dem Dateninhalt ergeben, etwa bei personenbezogenen Daten (Datenschutzrecht, allgemeines Persönlichkeitsrecht)[193], bei Immaterialgüterrechten (z. B. Urheberrecht) oder bei Daten, die Betriebs- oder Geschäftsgeheimnisse beinhalten. Ferner kann eine vertragliche Zuordnung Bedeutung erlangen, etwa ein Kauf von Daten, ein Lizenzvertrag oder

---

[191] Vgl. *Sahl*, Daten als Basis der digitalen Wirtschaft und Gesellschaft, RDV 2015, 236 (242): Theoretisch kämen bei nicht-personenbezogenen Maschinendaten fast alle Beteiligten in Betracht; ein nachvollziehbares Interesse habe fast jeder Beteiligte. Aus rechtlicher Perspektive gebe es jedenfalls keine zwingende Antwort.

[192] Vgl. BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.

[193] Vgl. *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (292 f.).

eine Abrede über die Nutzung personenbezogener Daten. Derartige Verträge gehen in der Praxis regelmäßig mit einer faktischen Zugriffsmöglichkeit auf die betreffenden Daten einher. Werden entsprechende Ausschließlichkeitsrechte in Erfüllung eines solchen Vertrages übertragen, kommt es zu einer Änderung der Güterzuordnung. Dagegen schaffen die zugrundeliegenden Verpflichtungsgeschäfte nur relative Ansprüche auf ein Tun oder Unterlassen. Sie bewirken mithin selbst keine Änderung der rechtlichen Zuordnung, deuten bei Daten, die nicht Gegenstand eines Ausschließlichkeitsrechts, sondern lediglich eine faktische Position sind, aber darauf hin, wem diese Position nach den Vorstellungen der Vertragsparteien zustehen soll.[194]

3. Möglichkeit einer rechtlichen Zuordnung

Denkbar sind unterschiedliche rechtliche Zuordnungskriterien.[195]

a. (Mittelbarer) Skripturakt

In Anlehnung an die Praxis im Strafrecht[196] könnte man auf einen gleichsam mittelbaren Skripturakt abstellen.[197] Werden bspw. in einem privaten sog. smart home automatisch Daten aufgezeichnet, hat dies zwar niemand unmittelbar veranlasst. Der Eigentümer und Bewohner des mit der smart-home-Anlage ausgestatteten Hauses, der die Anlage betreibt, der insbesondere die Parameter für die (automatische) Datenaufzeichnung eingestellt hat und der auf die aufgezeichneten Daten zugreifen kann, verursacht den Skripturakt jedoch gleichsam mittelbar. Er steht den Daten deshalb in einer wertenden Gesamtschau der Umstände des Einzelfalls näher als andere Beteiligte, etwa der Hersteller der Anlage oder der Elektriker, der sie installiert hat.

Denkbar sind jedoch auch viele Fälle, in denen eine Zuordnung nicht derart auf der Hand liegt.[198] In dem eingangs aufgeführten Beispiel moderner Landwirtschaftsmaschinen wäre am ehesten der Fahrer der Landmaschine als (mittelbarer) Skribent anzusehen, weil er die Maschine fährt, während (automatisch) Daten aufgezeichnet werden, womit er die Aufzeichnung – aus technisch-naturwissenschaftlicher Sicht – veranlasst. Der Fahrer der Landmaschine steht dem Vorgang aber wirtschaftlich möglicherweise eher fern, etwa wenn er die Landmaschine im

---

[194] *Zech*, Information als Schutzgegenstand, 2012, S. 113.

[195] Einen Überblick über den Meinungsstand gibt *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (486 ff.).

[196] Vgl. OLG Naumburg, Urt. v. 27.8.2014 – 6 U 3/14, DAR 2015, 27; OLG Nürnberg, Beschl. v. 23.1.2013 – 1 Ws 445/12, CR 2013, 212; BayObLG, Urt. v. 24.6.1993 − 5 St RR 5/93, CR 1993, 779 (780); Conrad/Grützmacher/*Hoeren*, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 306 ff.

[197] Zum sog. Skripturakt vgl. *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (487); Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 24 f.; *Zech*, Information als Schutzgegenstand, 2012, S. 388 ff.

[198] Kritisch *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (384).

Rahmen eines Nebenjobs bei einem Lohnunternehmer steuert. Selbst wenn man darauf abstellen wollte, wer von mehreren Beteiligten bei wertender Betrachtung als (mittelbarer) Skribent anzusehen ist, fällt eine klare Zuordnung in diesem Beispiel schwer. Insbesondere der Landwirt, der die Fläche bewirtschaftet und den Einsatz der Landmaschine beauftragt hat, der Lohnunternehmer, der die Landmaschine betreibt (und die Datenaufzeichnung möglicherweise als Zusatzleistung entgeltlich anbieten möchte), und der Hersteller der Maschine, der die Daten sammelt, auswertet und auf dieser Grundlage maßgeschneiderte Dienstleistungen anbietet, stehen den Daten nach den Gesamtumständen gleichermaßen nahe. Die Suche nach der Wesentlichkeit des Beeinflussungsmoments, auf die teilweise abgestellt wird,[199] hilft hier kaum weiter. *Becker* schlägt deshalb vor, die Daten grundsätzlich dem Hersteller der Maschine zuzuordnen, was allerdings nur eine faktische Zugriffsmöglichkeit rechtlich zementieren würde.[200]

Selbst unter wertender Betrachtung erscheint das Kriterium der technisch-naturwissenschaftlichen Veranlassung der Datenaufzeichnung als (mittelbarer) Skribent nicht in allen Fällen geeignet für eine hinreichend zuverlässige und vorhersehbare Zuordnung automatisch generierter Daten.

b. Verkehrsanschauung

Andere sehen in der Verkehrsanschauung das maßgebliche Zuordnungskriterium für Rechte an Daten, dem im Zweifel Vorrang gegenüber einer technisch-naturwissenschaftlichen Betrachtung zukomme.[201] Abzustellen ist danach auf denjenigen, der wirtschaftlich die Erzeugung der Daten, also das Codieren, veranlasst hat. Bei komplexen Maschinen ist dies nach Ansicht von *Zech*[202] regelmäßig der wirtschaftliche Betreiber, etwa der Halter eines Fahrzeugs oder der Unternehmensinhaber, der Produktionsmaschinen einsetzt. Dieser sorge dafür, dass die Aufnahme- bzw. Messvorrichtung unterhalten und effizient eingesetzt wird, und trage die dafür erforderlichen Aufwendungen. Für diese Lösung spricht der Grundgedanke von § 87a UrhG, der auf die wirtschaftliche Investition abstellt.[203]

---

[199] *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (488); Conrad/Grützmacher/*Hoeren*, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 310.

[200] *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, S. 815 (825).

[201] Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (200).

[202] *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (144).

[203] Dazu auch *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (292 f.).

Wie das soeben aufgeführte Beispiel zeigt, ermöglicht auch die Verkehrsanschauung keine zweifelsfreie Zuordnung, wenn – wie bei den in der modernen Landwirtschaft erhobenen Daten – die Daten aus Sicht der jeweiligen Verkehrskreise nicht nur einen Beteiligten betreffen, sondern gleichermaßen der Sphäre mehrerer Beteiligten zuzurechnen sind (z. B. Landwirt, Lohnunternehmer, Hersteller). Die Zuordnung zu einem Beteiligten für die Vielzahl aller denkbaren Einzelfälle generell-abstrakt zu regeln, erscheint vor diesem Hintergrund problematisch. Letztlich käme wohl nur eine generalklauselartige gesetzliche Zuordnung in Betracht. Es würde wohl lange dauern, bis sich in der Rechtsprechung eine Kasuistik herausbilden würde, die eine hinreichend vorhersehbare Zuordnung ermöglichen würde – eine auch unter dem Gesichtspunkt der Normenklarheit wenig befriedigende Lösung.

c. Sacheigentum

Diskutiert wird die Zuordnung anhand des Sacheigentums an dem Speichermedium, auf dem die Daten gespeichert sind.[204] Dieses Kriterium ist bereits aus tatsächlicher Sicht problematisch, weil automatisch generierte Daten in vielen Fällen mehrfach gespeichert werden.[205] Bei einem PKW können Sensordaten bspw. gespeichert werden in dem Fahrzeug, bei dem Telekommunikationsunternehmen, das Daten aus dem Fahrzeug automatisiert an den Hersteller sendet, bei dem Hersteller sowie bei einer Werkstatt, die die Fahrzeugspeicher ausliest. Jeder Beteiligte kann die Daten auch dezentral bei einem Cloudanbieter speichern (der dann Eigentümer des Speichers wäre, wenn er nicht seinerseits Speicher nutzt, die in fremdem Eigentum etwa eines Rechenzentrums stehen). Die Zuordnung der Daten an alle diese Beteiligten brächte wenig Klarheit. Betreibt ein anderer als der Eigentümer die Maschine (etwa ein Lohnunternehmer, der eine Landmaschine geleast hat), liegt eine Zuordnung der Daten an den Eigentümer eher fern.

Gegen die Maßgeblichkeit des Sacheigentums am Speichermedium spricht auch eine rechtliche Erwägung: Wie der BGH festgehalten hat, folgt die Berechtigung an den Inhalten anderen Regeln als das Eigentum an den Speichermedien.[206] Angesichts dessen erscheint es problematisch, ein absolutes Recht an Daten (das unabhängig von Rechten an Speichermedien personell zugeordnet werden soll) an das Eigentum an den Speicherressourcen zu knüpfen.[207] Hinzu kommt, dass Daten zunehmend nicht auf einem konkreten Datenträger gespeichert werden, sondern – bspw. beim Cloud Computing – dezentral an einer Vielzahl von teilweise weit

---

[204] Vgl. Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 24 f.

[205] *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (487).

[206] BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.

[207] *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (291 f.).

entfernten Orten, weshalb die exakte Bestimmung des körperlichen Speichermediums an Bedeutung verliert.[208]

d. Konkurrenz zu anderweitiger Zuordnung

Wie bereits oben (2.) erwähnt, können automatisch generierte Daten einer Person aufgrund ihres Inhalts (Datenschutzrecht, allgemeines Persönlichkeitsrecht, Immaterialgüterrechte, Betriebs- oder Geschäftsgeheimnisse) oder durch Abschluss von Verträgen (Datenkaufvertrag, Lizenzvertrag, Datennutzungsvertrag) zugeordnet sein. Würde man solche Daten nach anderen Kriterien rechtlich zuordnen (etwa an den mittelbaren Skribenten oder nach der Verkehrsanschauung), können sich Konkurrenzen ergeben. Der nach der Verkehrsanschauung oder nach der Veranlassung der Datenaufzeichnung als Berechtigter in Betracht Kommende muss nämlich nicht stets der gleiche sein, wie die nach einem Vertrag oder dem Dateninhalt berechtigte Person. Eine etwaige gesetzliche Vorschrift, die Kriterien für die Zuordnung von Daten bestimmt, müsste auch diese Konkurrenzfragen abstrakt und allgemein regeln. Das erscheint angesichts der Vielgestaltigkeit der in Betracht kommenden Fälle nicht unproblematisch.[209]

4. Regelungsbedarf

Vorstehend ist festgehalten worden, dass automatisch generierte Daten nach geltendem Recht regelmäßig demjenigen zugeordnet werden, der faktisch auf sie zugreifen kann, vorbehaltlich etwaiger aus dem Dateninhalt oder aus Verträgen resultierender abweichender Zuordnungen. Daran anknüpfend wird nachfolgend näher betrachtet, ob diese Zuordnung zu unerwünschten Ergebnissen führt (a.) und ob dies eine rechtlich grundierte Zuordnung notwendig macht (b.).

a. Unerwünschte Ergebnisse

Die grundsätzliche Zuordnung von automatisch generierten Daten an denjenigen, der faktisch auf sie zugreifen kann, kann vor allem dann zu unerwünschten Ergebnissen führen, wenn sie mit einer abweichenden, sich aus dem Dateninhalt ergebenden Zuordnung kollidiert (1) und wenn sie den Wettbewerb beschränkt (2).

(1) Kollision mit inhaltsbezogener Zuordnung

Ordnet man automatisch generierte Daten stets demjenigen zu, der faktisch auf sie zugreifen kann, führt dies in einigen Fällen zu Konflikten mit einer aus dem Dateninhalt abgeleiteten Befugnis an denselben Daten (vgl. oben 3. d.). Die von einem modernen PKW automatisch aufgezeichneten Daten weisen jedenfalls in weiten Teilen einen Personenbezug zum Fahrer auf. Nach Maßgabe der faktischen Zugriffsmöglichkeit sind diese Daten (regelmäßig) dem Fahrzeughersteller zuge-

---

[208] Vgl. *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (138).

[209] Eingehend zu konkurrierenden Ausschließlichkeitsrechten *Zech*, Information als Schutzgegenstand, 2012, S. 416 ff.

ordnet und nicht dem Fahrer, der typischerweise tatsächlich keine Zugriffsmöglichkeit hat. Gleichwohl ergeben sich aus dem Datenschutzrecht und dem allgemeinen Persönlichkeitsrecht (weitgehende) Rechte des Fahrers an diesen Daten. Bspw. ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dies gesetzlich erlaubt oder angeordnet ist oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG). Der Fahrzeughersteller ist somit zwar faktisch in der Lage, auf solche Daten zuzugreifen und nach Belieben mit ihnen umzugehen. Diese faktische Position ist rechtlich aber (eng) eingegrenzt. Entsprechendes gilt in vielen anderen Fällen, in denen anderen Personen als demjenigen, der faktisch auf die Daten zugreifen kann, Rechtspositionen an automatisch generierten Daten zustehen, bspw. weil Immaterialgüterrechte berührt sind oder weil die Daten Betriebs- oder Geschäftsgeheimnisse betreffen.

Unproblematisch erscheint demgegenüber der Gesichtspunkt einer abweichenden vertraglichen Regelung. Ergibt sich aus einem Vertrag über Daten eine andere personelle (Soll-)Zuordnung als die faktische (Ist-)Zuordnung, weist dies lediglich darauf hin, dass der Vertrag noch vollzogen werden muss, dem Erwerber also noch die tatsächliche Verfügungsbefugnis über die Daten in dem vereinbarten Umfang verschafft werden muss.

(2) Wettbewerbsbeschränkung

In vielen Fällen hat derjenige Beteiligte den faktischen Zugriff auf Daten, der unter allen Beteiligten über die größte Marktmacht verfügt. Sammeln sich große Datenmengen bei wenigen Großunternehmen (wie Kraftfahrzeug- oder Landmaschinenherstellern, aber auch IT-Unternehmen wie Google, Amazon, Microsoft usw.), kann dies negative Folgen für den Wettbewerb haben. Andere Unternehmen (insbesondere kleinere Unternehmen) können die Daten nicht nutzen und sind dadurch gehindert als Wettbewerber in bestehenden Märkten aufzutreten und aus den Daten neue Produkte zu entwickeln und damit neue Märkte zu schaffen.[210] Das zeigt sich etwa bei den in der modernen Landwirtschaft generierten Daten, mit deren Hilfe der Landmaschinenhersteller dem Landwirt maßgeschneiderte Dienstleistungen anbieten kann. Anderen Dienstleistern oder z. B. den Düngemittelherstellern ist ein Zugriff auf diese Daten und die Entwicklung konkurrierender oder zusätzlicher datenbasierter Angebote nur in dem Maße möglich, wie sie sich mit dem Landmaschinenhersteller, der allein über die Daten verfügt, über die Datennutzung einigen.

Die Monopolkommission[211] empfiehlt, die Verfügungsrechte im Rahmen der Datenschutzregelungen zu konkretisieren. Eine Vergabe von eindeutigen, absoluten Rechten, wo immer möglich, sei wettbewerbspolitisch zu befürworten. Dabei sei

---

[210] Vgl. *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, S. 815 (823 f.).

[211] Monopolkommission, Sondergutachten zu „Herausforderung digitale Märkte“, BT-Drs. 18/5080, Ziff. 88 f.

es aus ökonomischer Perspektive nicht eindeutig, welche Zuteilung der Verfügungsrechte zu dem effizientesten Marktgleichgewicht führe.

b. Vorteile einer rechtlich grundierten Zuordnung

Nach dem oben Gesagten ist eine Zuordnung automatisch generierter Daten allein an denjenigen, der faktisch auf sie zugreifen kann, nicht unproblematisch. Es erscheint jedoch zweifelhaft, ob dieser Befund eine rechtlich grundierte Zuordnung dieser Daten notwendig macht. Eine solche Zuordnung müsste, um in der Praxis handhabbar zu sein, automatisch generierte Daten generell-abstrakt nach einem für alle Fälle anzuwendenden Maßstab personell zuordnen. Das erscheint zum einen wegen der Vielgestaltigkeit der in Frage kommenden Sachverhalte kaum möglich, zumal die künftige technische Entwicklung nicht absehbar ist.[212] Zum anderen sind es auch rechtlich ganz unterschiedliche Belange, die in bestimmten Fällen gegen eine Zuordnung an denjenigen sprechen, der faktisch auf die Daten zugreifen kann (etwa abgeschlossene Verträge, Datenschutzrecht, Immaterialgüterrecht, allgemeines Persönlichkeitsrecht, Schutz von Betriebs- und Geschäftsgeheimnissen). Der Blick auf die in Betracht kommenden Zuordnungskriterien hat gezeigt, dass ein einheitliches, allen vorgenannten Maßgaben gerecht werdendes Kriterium für eine hinreichend klare gesetzliche Zuordnung von automatisch generierten Daten jedenfalls aus heutiger Sicht nicht erkennbar ist.[213] Allenfalls für konkrete, enge Fallgruppen könnte bewertet werden, wer als ausschließlich Berechtigter in Betracht kommt und welche weiteren Beteiligten und Konflikte berücksichtigt werden sollten.[214]

Beließe man es dagegen bei dem Grundsatz der faktischen Zuordnung, könnten im Einzelfall erforderliche Korrekturen zielgenau mit Hilfe des jeweils betroffenen Rechtsregimes vorgenommen werden. Verfügt bspw. ein PKW-Hersteller über personenbezogene Daten des Fahrers, bietet das Datenschutzrecht grundsätzlich geeignetere Instrumente, als sie eine abstrakt-generelle Zuordnung eines absoluten Rechts an den Daten ermöglichen würde. Entsprechendes gilt für die übrigen betroffenen Aspekte, etwa das Immaterialgüter- und das Wettbewerbsrecht. Das speziellere Recht erscheint auch jeweils passgenauer, um etwaige spezifische Problemlagen zu adressieren, die sich aus dem digitalen Wandel künftig ergeben könnten.

Ein solcher Weg profitiert im Übrigen von der Flexibilität des Vertragsrechts. Im Einzelfall zwischen den Beteiligten abgeschlossene Verträge können die Daten wesentlich genauer zuordnen, als dies mit einer allgemeinen gesetzlichen Zuordnung von automatisch generierten Daten möglich wäre. Soweit es insbesondere im B2C-Bereich zu unangemessenen Vertragsbedingungen kommt, bietet das AGB-Recht geeignete Gegenmittel. Ergeben sich im B2B-Bereich informatio-

---

[212] Vgl. *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 56 f.
[213] So auch *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 56.
[214] *Becker*, Rechte an Industrial Data und die DSM-Strategie, GRUR Newsletter 1/2016, S. 7.

nelle Asymmetrien oder ein Marktversagen, dürfte das Kartellrecht eher für Abhilfe sorgen können als die Schaffung eines absoluten (Zivil-)Rechts an automatisch generierten Daten.[215] Soweit ersichtlich, besteht insoweit – jedenfalls derzeit – allerdings kein vordringlicher Handlungsbedarf.[216] Wie beispielsweise die zunehmend intensive Zusammenarbeit von Automobilindustrie und Internetwirtschaft zeigt, besteht hierfür ein Markt.[217] Der Big-Data-Sektor wächst um 40 % pro Jahr und damit sieben Mal schneller als der IT-Markt insgesamt.[218] Sollten sich in einzelnen Bereichen Defizite ergeben, kann das Kartellrecht gezielt und sektorspezifisch gegensteuern, wie dies bspw. in dem (analogen) Kfz-Anschlussmarkt zum Schutz eines unabhängigen Marktes für Ersatzteile sowie Wartungs- und Reparaturleistungen geschehen ist.[219]

Dagegen ist nicht erkennbar, dass mit einer gesetzlichen Zuordnung eines absoluten Rechts an automatisch generierten Daten ein Anreiz für die Datenerfassung gegeben würde, dass die Aussicht auf ein Entgelt einen Anreiz für das Öffentlichmachen der Informationen bedeute und dass hierfür ein Markt geschaffen würde.[220] In einem funktionierenden Markt dürfte – wie oben ausgeführt – das freie Zusammenwirken der Beteiligten grundsätzlich zu besseren (vertraglich flexibel geregelten) Ergebnissen führen als eine pauschale und statische gesetzliche Festschreibung eines absoluten Rechts an Daten. Das gilt jedenfalls dann, wenn etwaigen Defiziten mit den geeigneten sachnächsten Instrumenten entgegengetreten wird (z. B. AGB-Recht, Datenschutzrecht, Wettbewerbsrecht, Kartellrecht).

---

[215] Näher *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (495).

[216] Eingehend *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (626 f.).

[217] Vgl. *Hornung/Goeble*, „Data Ownership" im vernetzten Automobil − Die rechtliche Analyse des wirtschaftlichen Werts von Automobildaten und ihr Beitrag zum besseren Verständnis der Informationsordnung, CR 2015, 265; siehe auch Große Ruse-Khan/Klass/von Lewinski/*Berberich*, Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 165 (205): „In welchem Maße ein Bedürfnis nach virtuellem Eigentum bestehen wird und insbesondere ob nicht technische Mechanismen zur Ressourcenzuweisung und -übertragung ein solches Recht praktisch entbehrlich machen, wird eine aus juristischer Sicht kaum zu beantwortende, rechtstatsächliche Frage sein."; *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (626), sieht in dem Anstieg der Investitionen im Bereich Big Data gerade einen Hinweis gegen die Annahme von Schutzlücken.

[218] So die Mitteilung der Europäischen Kommission vom 6.5.2015, Strategie für einen digitalen Binnenmarkt für Europa, COM (2015) 192 final, S. 16.

[219] Vgl. Verordnung (EU) Nr. 461/2010 der Kommission vom 27.5.2010, ABl. L 129/52.

[220] Abwägend *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (144 f.); *Sahl*, Daten als Basis der digitalen Wirtschaft und Gesellschaft, RDV 2015, 236 (242).

5. Zwischenergebnis

Für eine gesetzliche Zuordnung von automatisch generierten Daten besteht kein Bedarf. Das flexible Vertragsrecht ist einer abstrakt-generellen gesetzlichen Zuordnung überlegen. Das Wettbewerbsrecht und die den Dateninhalt betreffenden (bestehenden) Vorschriften (z. B. Datenschutzrecht, Immaterialgüterrechte) gewährleisten aus heutiger Sicht sachgerechte Einschränkungen der Befugnisse desjenigen, der faktisch auf automatisch generierte digitale Daten zugreifen kann; diese (speziellen) Rechtsbereiche kommen auch für die Korrektur etwaiger Fehlentwicklungen eher in Betracht als die pauschale Zuweisung eines absoluten Rechts.

VI. Zwangsvollstreckung in Datenbestände

1. Problemstellung

Ansprüche, die auf ein Tun oder Unterlassen in Bezug auf Daten gerichtet sind, unterliegen den allgemeinen Zwangsvollstreckungsregeln nach § 887 ZPO (vertretbare Handlungen) und § 888 ZPO (nicht vertretbare Handlungen). Beide Regelungen sind geeignet, die Besonderheiten von Daten angemessen zu erfassen. Der BGH hat unter Zugrundelegung dieser Vorschriften z. B. entschieden, dass Daten dadurch herausgegeben werden, dass der Schuldner dem Gläubiger eine Kopie der Daten überträgt und der Schuldner gleichzeitig die Daten im eigenen Bestand löscht.[221] Der Schaffung eines absoluten Rechts an Daten bedarf es insoweit nicht.[222]

Auch im Falle der Zwangsvollstreckung in das Speichermedium (bspw. in den Server eines Cloudproviders) sind die Rechte des Berechtigten an Daten hinreichend gewahrt. Im Ergebnis entspricht seine Rechtsposition derjenigen des Berechtigten an Daten bei der Insolvenz eines Cloudproviders – er kann sich auf einen Herausgabeanspruch z. B. aus § 667 BGB als ein die Veräußerung hinderndes Recht i. S. v. § 771 ZPO berufen.[223]

Eine andere Frage ist hingegen, ob Daten – über die anerkannte Pfändung von Software gemäß §§ 803 ff. ZPO[224] hinaus – als Zwangsvollstreckungsobjekt etwa wegen Geldforderungen (sowie als Beleihungsobjekt) in Betracht kommen sollten. Die generelle Zugriffsmöglichkeit fremder Dritter auf Daten als Wertgegenstand erscheint mit Blick auf den Dateninhalt (etwa personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse) problematisch. Die Arbeitsgruppe hat daher näher betrachtet, ob die Zwangsvollstreckung wegen einer Geldforderung in Datenbestände als Vermögensgegenstand Probleme aufwirft, die mit dem bisherigen Zwangsvollstreckungsrecht nicht sachgerecht gelöst werden können.

---

[221] BGH, Urt. v. 17.4.1996 – VIII ZR 5/95, NJW 1996, 2159 (2161).
[222] Vgl. zur Zwangsvollstreckung von Ansprüchen auf Herausgabe von Daten Conrad/Grützmacher/*Müller*, Recht der Daten und Datenbanken im Unternehmen, 2014, S. 322 ff.
[223] Vgl. MüKo/*Schmidt/Brinkmann*, ZPO, § 771 Rn. 40 m. w. N.
[224] Dazu MüKo/*Gruber*, ZPO, § 803 Rn. 27, § 808 Rn. 30 m. w. N.

2. Grundsätze

Geldforderungen sind darauf gerichtet, dass Geld in bestimmter Menge gezahlt wird. Die Zwangsvollstreckung wegen Geldforderungen ist in den §§ 803 bis 882a ZPO geregelt. Sie erfolgt in das bewegliche Vermögen durch Pfändung (§§ 803 ff. ZPO) und in das unbewegliche Vermögen durch Eintragung einer Zwangshypothek, durch Zwangsversteigerung oder durch Zwangsverwaltung (§§ 864 ff. ZPO).[225] Als bewegliches Vermögen gelten körperliche Sachen (§§ 808 ff. ZPO) und Forderungen (Geldforderungen – §§ 829 ff. ZPO, Herausgabeansprüche – §§ 846 ff. ZPO). Für die Zwangsvollstreckung in andere Vermögensrechte, die nicht Gegenstand der Zwangsvollstreckung in das unbewegliche Vermögen sind, gelten gemäß § 857 ZPO die §§ 829 bis 856 ZPO entsprechend.

§ 857 ZPO stellt eine Auffangnorm für die Zwangsvollstreckung wegen Geldforderungen in das bewegliche Vermögen dar, soweit dieses nicht den ausdrücklich geregelten Kategorien (namentlich den Geldforderungen und Herausgabeansprüchen) zugeordnet werden kann. Voraussetzung ist, dass es sich bei dem zu pfändenden Recht um ein Vermögensrecht handelt, das dem Haftungsverband des Schuldners zuzurechnen ist.[226] Das kommt in Betracht bei Rechten aller Art, die einen Vermögenswert derart verkörpern, dass die Pfandverwertung zur Befriedigung des Geldanspruchs des Gläubigers führen kann.[227] Nicht pfändbar sind dagegen personenrechtliche Ansprüche wie Namensrechte und bloße Befugnisse, deren Nutzung die Rechtsordnung zwar garantiert, die aber nicht als verkehrsfähige, pfändbare Rechte ausgestaltet sind (etwa ein Kündigungsrecht oder Anfechtungsrecht nach dem AnfG oder den §§ 129 ff. InsO).[228] Als gemäß § 857 ZPO pfändbar sind bspw. angesehen worden Anteilsrechte an einer Gesellschaft, beschränkt dingliche Rechte, Anwartschaftsrechte auf das Eigentum, Immaterialgüterrechte (Patentrechte, Markenrechte, Gebrauchs- und Geschmacksmuster sowie Urheberrechte mit den Beschränkungen der §§ 113 bis 119 UrhG) und die sog. Milchquote.[229]

§ 857 Abs. 1 i. V. m. § 851 Abs. 1 ZPO setzt eine zumindest eingeschränkte Übertragbarkeit des zu pfändenden Vermögensrechts voraus.[230] Diese hat der BGH bei Internet-Domains bejaht. Als Gegenstand der Pfändung ist dabei allerdings nicht die Domain oder der Domainname als solcher im Sinne eines absoluten Rechts angesehen worden, sondern die Gesamtheit der schuldrechtlichen Ansprüche, die

---

[225] Näher Thomas/Putzo/*Seiler*, ZPO, vor § 803 Rn. 1 f.
[226] Vgl. MüKo/*Smid*, ZPO, § 857 Rn. 7.
[227] BGH, Beschl. v. 20.12.2006 – VII ZB 92/05, NJW-RR 2007, 1219.
[228] BGH, Beschl. v. 20.12.2006 – VII ZB 92/05, NJW-RR 2007, 1219 m. w. N.
[229] Thomas/Putzo/*Seiler*, ZPO, § 857 Rn. 2 ff. m. w. N.
[230] Vgl. BGH, Beschl. v. 20.12.2006 – VII ZB 92/05, NJW-RR 2007, 1219.

dem Inhaber des Domainnamens gegenüber der Vergabestelle aus dem Registrierungsvertrag zustehen.[231] Die Verwertung der gepfändeten schuldrechtlichen Ansprüche kann durch Überweisung zum Schätzwert, durch Versteigerung im Internet oder durch freihändige Veräußerung erfolgen.[232]

3. Folgerungen für die Zwangsvollstreckung in Daten

Ergiebige Rechtsprechung oder Literatur zur Zwangsvollstreckung wegen Geldforderungen in Datenbestände ist nicht ersichtlich. Das deutet darauf hin, dass die Praxis insoweit keine besonderen Schwierigkeiten sieht, insbesondere keine Regelungslücken, die der Gesetzgeber schließen sollte. Dieser Befund mag auch wirtschaftliche Gründe haben: Die Zwangsvollstreckung aus einer Geldforderung in Daten kommt nur bei marktfähigen Daten in Betracht, deren Verwertung realistischerweise einen Erlös erwarten lässt, der die Kosten übersteigt. Das wird man bei den meisten digitalen Daten verneinen müssen.

Geht es dagegen (ausnahmsweise) um wertvolle Datenbestände, deren Verwertung einen nennenswerten Erlös erwarten lässt, gelangt man auf der Grundlage des geltenden Rechts zu sachgerechten Ergebnissen, indem man die oben skizzierten Grundsätze der Zwangsvollstreckung in Internet-Domains heranzieht.[233] Auch digitale Daten als solche sind indes wohl kein „anderes Vermögensrecht" i. S. v. § 857 Abs. 1 ZPO. Wie eingangs ausgeführt, kommt Daten (und zwar auch größeren Datenbeständen) keine etwa mit einem Patent-, Marken- oder Urheberrecht vergleichbare ausschließliche Stellung zu. Diese Rechte zeichnen sich dadurch aus, dass sie ihrem Inhaber einen Ausschließlichkeitsanspruch gewähren, der vom Gesetzgeber begründet worden ist und nicht durch Parteivereinbarung geschaffen werden kann. Digitale Daten sind dagegen (wenn man von ihrem Inhalt und dem Medium, auf dem sie gespeichert sind, absieht) lediglich eine flüchtige, beliebig vervielfältigbare, durch mehrere gleichzeitig nutzbare und ohne Weiteres löschbare tatsächliche Erscheinung. Die ausschließliche Stellung desjenigen, der Daten auf seinem Rechner vorhält, die er etwa durch Verschlüsselung vor dem Zugriff Dritter schützt, ist allein technisch bedingt. Eine derartige rein

---

[231] BGH, Beschl. v. 5.7.2005 – VII ZB 5/05, GRUR 2005, 969; BGH, Urt. v. 18.1.2012 – I ZR 187/10, BGHZ 192, 204 = NJW 2012, 2034; die Literatur stimmt dem – soweit ersichtlich − jedenfalls weit überwiegend zu, vgl. Staudinger/*Roth*, BGB, Neubearbeitung 2013, § 12 Rn. 100i; Zöller/*Stöber*, ZPO, § 857 Rn. 12c; BeckOK/*Riedel*, ZPO, § 857 Rn. 40 ff.; Musielak/Voit/*Becker*, ZPO, § 857 Rn. 13a; im Ergebnis auch MüKo/*Wagner*, BGB, § 823 Rn. 225; differenzierend *Berberich*, Absolute Rechte an der Nutzung einer Domain − eine zentrale Weichenstellung für die Rechtsentwicklung, WRP 2011, 543.

[232] Vgl. Zöller/*Stöber*, ZPO, § 857 Rn. 12c m. w. N.

[233] *Völzmann-Stickelbrock* auf dem Workshop des Justizministeriums NRW am 23.5.2016, Tagungsberichte bei *Christians*, Arbeitsgruppe „Digitaler Neustart im BGB", AfP 2016, 334; *Liepin/Götz*, Braucht das BGB ein Update?, MMR-Aktuell 2016, 379185 (verfügbar bei beck-online).

faktische Ausschließlichkeit begründet aber grundsätzlich kein absolutes Recht i. S. v. § 857 Abs. 1 ZPO.[234]

Bei Internet-Domains liegt es ähnlich. Anerkannt ist indes, wie oben ausgeführt, dass die Gesamtheit der Ansprüche, die dem Inhaber der Domain gegenüber der Vergabestelle zustehen und auf denen die Inhaberschaft an der Domain gründet, als „sonstiges Vermögensrecht" Gegenstand der Pfändung nach § 857 Abs. 1 ZPO ist. Dieser Gedanke kann auch für Daten fruchtbar gemacht werden: Wie vorstehend aufgezeigt wurde, ist der (berechtigte) Inhaber von Daten nach geltendem Recht durch eine Vielzahl unterschiedlicher Ansprüche geschützt. Es spricht viel dafür, dass die Gesamtheit dieser Ansprüche als „sonstiges Vermögensrecht" Gegenstand einer Pfändung nach § 857 Abs. 1 ZPO sein kann. Die Verwertung der gepfändeten Ansprüche kann – wie bei Internet-Domains – durch Überweisung zum Schätzwert, durch Versteigerung im Internet oder durch freihändige Veräußerung erfolgen.[235] Sie versetzt den Erwerber in dieselbe Position in Bezug auf die Daten, die zuvor der Schuldner innehatte. Wer als Drittschuldner anzusehen ist, richtet sich dabei nach den Umständen des Einzelfalls. Dies kann bei in einer Cloud abgelegten Daten bspw. der Cloud-Betreiber sein. Zu beachten ist, dass Daten aufgrund ihres Inhalts im Einzelfall nach allgemeinen Regeln unpfändbar sein können, etwa als Arbeitsmittel gemäß § 811 Abs. 1 Nr. 5 ZPO.[236]

Zu bemerken ist schließlich, dass es der vorstehend skizzierten Zwangsvollstreckung digitaler Daten nach Maßgabe von § 857 ZPO nicht bedarf, wenn die betreffenden Daten auf einem (körperlichen) Speichermedium abgelegt sind, das nach § 808 ZPO gepfändet werden kann,[237] oder wenn sie etwa gemäß §§ 87a ff. UrhG als Immaterialgüterrecht (ebenfalls gemäß § 857 ZPO) gepfändet werden können.

4. Zwischenergebnis

Die Zwangsvollstreckung in Datenbestände als Vermögensgegenstand bereitet keine besonderen Schwierigkeiten, die mit dem bisherigen Zwangsvollstreckungsrecht nicht sachgerecht gelöst werden können.

---

[234] Vgl. BGH, Beschl. v. 5.7.2005 – VII ZB 5/05, NJW 2005, 3353 f. (zu Internet-Domains).
[235] Vgl. Zöller/*Stöber*, ZPO, § 857 Rn. 12c m. w. N.
[236] LG Mönchengladbach, Beschl. v. 22.9.2004 – 5 T 445/04, MDR 2005, 118; Zöller/*Stöber*, ZPO, § 857 Rn. 12c.
[237] Vgl. zur Zwangsvollstreckung in Computer Musielak/Voit/*Becker*, ZPO, § 808 Rn. 24.

F. Zusammenfassende Erwägungen zum Regelungsbedarf

Anknüpfend an die vorstehende Analyse einzelner Fallgruppen wird nachfolgend zusammenfassend zur Frage des Regelungsbedarfs Stellung genommen (I.). Das Ergebnis dieser Gesamtbetrachtung wird sodann anhand des Meinungsbildes in der Fachliteratur (II.), der Praxis (III.) sowie auf europäischer Ebene (IV.) gewürdigt, bevor schließlich ein Blick auf die weitere Entwicklung gerichtet wird (V.).

I. Schlussfolgerungen aus der Analyse einzelner Fallgruppen

Bei der Beantwortung der Frage, ob ein absolutes Recht an Daten eingeführt werden sollte, kommt es nicht allein darauf an, ob ein solches Recht – aus welchen Gründen auch immer – irgendwie wünschenswert wäre. Beurteilungsmaßstab kann nicht ein allumfassender, jeden denkbaren Einzelfall erfassender Schutz von digitalen Daten sein. Nicht jede (noch so kleine) Schutzlücke rechtfertigt die Schaffung eines neuen absoluten Rechts an Daten. Eigentumsrechtliche Schutzrechtszuweisungen greifen nämlich in die Wettbewerbs- und Informationsfreiheit ein und bedürfen deshalb einer Rechtfertigung.

Die Rechtfertigung für die Schaffung exklusiver Rechte an Immaterialgütern liegt im Wesentlichen darin, dass zwar die Nutzungs-, Nachahmungs- und Übernahmefreiheit anderer Marktteilnehmer eingeschränkt wird, dies aber unumgänglich ist, um einerseits Anreize zur Schaffung neuer Werke und neuen Wissens zu setzen (weil die Ausschließlichkeitsrechte die Amortisation der zuvor getätigten Investitionen erlauben) und um andererseits den rechtlichen Rahmen für die Verbreitung vorhandener Werke und vorhandenen Wissens bereitzustellen.[238] Die Einführung eines Eigentumsrechts an Daten könnte gerechtfertigt sein, wenn es nachweislich wirtschaftliche, gesellschaftliche oder andere Vorteile für die Wohlfahrt gegenüber der geltenden Rechtslage verspräche. Das wäre der Fall, wenn das Fehlen exklusiver Rechte an Daten zur Folge hätte, dass gesellschaftlich wünschenswerte Investitionen in die Hervorbringung neuer Daten oder die Nutzung vorhandener Daten ausblieben, oder das geltende Schutzsystem andere ineffiziente Ergebnisse hervorbrächte.[239]

Daran gemessen, weist das geltende Recht - wenn man die Wertungen der vorliegenden Ausarbeitung teilt - derzeit keine Lücken auf, deren Schließung durch den Gesetzgeber geboten erscheint. Ein Dateneigentum oder ein anderes absolutes Recht an digitalen Daten kennt das geltende Recht zwar nicht. Daten genießen jedoch unter einer Vielzahl unterschiedlicher Ansatzpunkte rechtlichen Schutz. Das gilt nicht nur im vertraglichen Kontext. Auch gegenüber fremden Dritten

---

[238] Rehbinder/*Peukert*, Urheberrecht, Rn. 123 f., 759 ff.; *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (625).

[239] *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (625); *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (495).

kommen verschiedene Ansprüche in Betracht, in erster Linie mit Bezug zum Dateninhalt, aber auch unabhängig vom Dateninhalt aus dem Eigentum am Speichermedium und unabhängig hiervon unter anderem durch Einwirkung des strafrechtlichen Schutzes auf das Zivilrecht. Insgesamt kann der Schutz von Daten im Zivilrecht als eine Art „Flickenteppich“ bezeichnet werden, der sich aus vielen unterschiedlichen Teilen zusammensetzt, die zusammen ein – aus heutiger Sicht – hinreichend geschlossenes Schutzsystem bilden.[240] Ebenso wenig zeigen sich beim vorhandenen Rechtsrahmen für die Internetwirtschaft Defizite, die Anlass für gesetzgeberische Maßnahmen geben würden. Dies gilt insbesondere mit Blick auf den Handel von Daten sowie auf vollstreckungsrechtliche Fragestellungen. Folgerichtig besteht unter den gegebenen Umständen derzeit auch kein verfassungsrechtliches Gebot, ein absolutes Recht an Daten zu schaffen.

II. Einschätzungen der Wissenschaft

Dieser Befund wird im Wesentlichen bestätigt durch die herangezogene Literatur.[241] Nur vereinzelt wird die Schaffung eines absoluten Rechts an Daten (oder eine andere gesetzgeberische Maßnahme) vorgeschlagen.[242] Soweit dabei auf konkrete Schutzlücken verwiesen wird (was nur wenige Autoren tun), vermag dies jedenfalls keinen unmittelbaren Handlungsbedarf für den Gesetzgeber zu begründen. Einige Vorschläge, die bislang in diesem Kapitel mangels unmittelbaren Sachzusammenhangs noch nicht angesprochen wurden, sollen nachfolgend behandelt werden (1. bis 4.). Zudem wird ergänzend kurz auf die Stimmen in der Literatur eingegangen, die ausdrücklich vor (verfrühten) gesetzgeberischen Maßnahmen warnen (5.).

---

[240] Dieses Bild verwendet *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (495).

[241] Aus einer Vielzahl von Äußerungen seien die Folgenden hervorgehoben: Gegen gesetzgeberische Maßnahmen sprechen sich aus *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (626 f.); *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (495): „Voreilige gesetzgeberische Schritte sind zu vermeiden“, anders sehe dies nur bei (dinglichen) Herausgabeansprüchen aus; *Specht*, Ausschließlichkeitsrechte an Daten − Notwendigkeit, Schutzumfang, Alternativen − Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige Ausgestaltung, CR 2016, 288 (296), hält den geltenden Rechtsrahmen allgemein für nicht mehr zeitgemäß, sieht aber auch die Alternative, erhöhte Anforderungen an die technische Sicherheit zu stellen; abwartend auch Hoeren/*Hoeren/Völkel*, Big Data und Recht, 2014, S. 37 f.; *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (491).

[242] Vgl. etwa *Hoeren*, Dateneigentum, Versuch einer Anwendung von § 303a StGB im Zivilrecht, MMR 2013, 486 (491); *Zech*, „Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1160); lediglich betreffend dinglicher Herausgabeansprüche *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (492).

1. Erforderlichkeit eines neuen Schutzgesetzes

Faust[243] nimmt eine „erhebliche Schutzlücke“ an, aufgrund derer rational handelnde Personen auf die externe Speicherung von Daten verzichten könnten. Diese Lücke ergebe sich daraus, dass Daten nicht als sonstiges Recht i. S. v. § 823 Abs. 1 BGB geschützt seien und der Schutz gemäß § 823 Abs. 2 BGB in Verbindung mit der Strafnorm in § 303a StGB nur bei vorsätzlichem Handeln greife. Deshalb solle, so *Faust*, ein neues Schutzgesetz i. S. v. § 823 Abs. 2 BGB geschaffen werden, das auch fahrlässiges Handeln erfasse, und zwar im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, das dann umbenannt werden solle.[244] Auf dem Deutschen Juristentag 2016 hat dieser Vorschlag Zustimmung gefunden, wenngleich dieses Ergebnis (25:2:4 Stimmen) angesichts der geringen Zahl von Abstimmenden wenig repräsentativ ist.[245] Gegenstimmen hielten in der Diskussion auf dem Juristentag eine schrittweise Klärung durch die Rechtsprechung für ausreichend und vorzugswürdig.[246]

Dem Vorschlag von *Faust* ist vorerst nicht näherzutreten. Gegen ihn spricht zum einen, dass ohnehin ein eher beschränkter Kreis von Fällen in Rede steht. Es geht nur um Sachverhalte, in denen kein Eigentum am Datenträger besteht, kein Besitz am Datenträger vorliegt und kein vertraglicher Anspruch eingreift, und zwar auch nicht nach den Grundsätzen der Drittschadensliquidation. Darüber hinaus ist zu beachten, dass auch in diesen (wenigen) Fällen Daten nach geltendem Recht keineswegs schutzlos sind. Neben § 823 Abs. 2 BGB in Verbindung mit Strafnormen kommt eine Vielzahl anderer Anspruchsgrundlagen in Betracht, die auch nicht durchweg Vorsatz voraussetzen.[247] Bei betrieblichen Daten kann etwa ein Eingriff in den eingerichteten und ausgeübten Geschäftsbetrieb vorliegen,[248] bei privaten Daten kann das allgemeine Persönlichkeitsrecht berührt sein; beide Rechtsgüter sind nach § 823 Abs. 1 BGB als sonstige Rechte grundsätzlich auch gegen fahrlässige Verletzungen geschützt. Daneben können spezialgesetzliche, auf den Dateninhalt abstellende Ansprüche etwa nach dem UWG oder dem UrhG bestehen. Es kann daher mitnichten die Rede davon sein, dass die Rechtsordnung Daten nicht (hinreichend) schütze.

Im Übrigen fehlen Anhaltspunkte für die Annahme, rational handelnde Personen könnten (angesichts der vermeintlich erheblichen Schutzlücke) auf die externe

---

[243] *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 51.

[244] *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 57 ff.; zustimmend *Wendehorst*, Die Digitalisierung und das BGB, NJW 2016, 2609 (2613), die allerdings einen neuen deliktsrechtlichen Tatbestand außerhalb von § 823 BGB vorschlägt; ebenso zustimmend *Spindler*, Digitale Wirtschaft – analoges Recht: Braucht das BGB ein Update?, JZ 2016, 805 (814), der allerdings den Weg über den Schutz von Daten nach § 823 Abs. 1 BGB favorisiert (siehe oben E. I.3.).

[245] Beschlüsse des 71. Deutschen Juristentages, Essen 2016, Abteilung Zivilrecht, These 28b, S. 10, http://www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf.

[246] So etwa *Wagner*, eigene Mitschriften der Arbeitsgruppe.

[247] Vgl. oben E. II.

[248] *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (619).

Speicherung von Daten verzichten.[249] Faust belegt diese Annahme nicht. Statistische Daten über enorm wachsende Umsätze in den Bereichen Cloud Computing und Big-Data sprechen eher eine andere Sprache.[250] Äußerungen von Verbänden, die die Befürchtungen von Faust bestätigen, sind nicht ersichtlich.[251]

Hinzu kommt eine tatsächliche Erwägung: Ungeachtet der geltenden Rechtslage stehen jedem Einzelnen (und in besonderem Maße jedem Unternehmen) technische Selbstschutzmöglichkeiten offen. Dies gilt insbesondere für technische Vorkehrungen zum Schutz der eigenen Daten vor fahrlässigen Zugriffen.[252]

2. Schutzlücke bei Herausgabeansprüchen

Grützmacher[253] meint, mit Blick auf (dingliche) Herausgabeansprüche tue sich eine bereits heute klar erkennbare Lücke auf, und zwar in besonders drastischer Weise im Falle der Insolvenz des Dateninhabers und bei mehrstufigen Lieferverhältnissen. Das überzeugt zwar im Ausgangspunkt. Dennoch liegt insoweit aus heutiger Sicht keine Gesetzeslücke vor, die der Gesetzgeber aktuell schließen müsste. Wie oben[254] im Einzelnen ausgeführt wurde, gibt es durchaus taugliche Grundlagen für die Geltendmachung von Herausgabeansprüchen. Weder aus der Praxis noch aus Äußerungen von Verbänden ergeben sich derzeit konkrete Hinweise auf relevante Defizite des Rechtsrahmens.

3. Schaffung eines neuen Immaterialgüterrechts an Maschinendaten

Becker und *Zech* sprechen sich für die Schaffung eines neuen Immaterialgüterrechts an Maschinendaten aus.[255] Wünschenswert sei eine einheitliche europäische Regelung, die Vorbild für die Einführung eines Industriedatenschutzes in

---

[249] So die Begründung des Regelungsbedarfs bei *Faust*, Gutachten zum 71. Deutschen Juristentag, S. 52.

[250] *Becker*, Rechte an Industrial Data und die DSM-Strategie, GRUR Newsletter 01/2016, S. 7 (9); *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (618, 626); *Schapiro/Zdanowiecki*, Screen Scraping, MMR 2015, 497 (498).

[251] Vgl. unten III.

[252] Darauf weist zu Recht hin MüKo/*Wagner*, BGB, § 823 Rn. 165; die dogmatische Verortung der Selbstschutzmöglichkeiten als Ausprägung des Mitverschuldens (dazu BeckOGK/*Spindler*, BGB, § 823 Rn. 185) steht der wertenden Berücksichtigung bei der Frage nach einem Regelungsbedarf nicht entgegen; vgl. einschränkend zu den Grenzen des Selbstschutzes BVerfG, Urt. v. 27.2.2008 – 1 BvR 370/07, BVerfGE 120, 274 = NJW 2008, 822, Rn. 180; zum rechtlichen Schutz technischer Schutzmaßnahmen *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (492 ff.).

[253] *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (492, 495).

[254] Vgl. oben E., insbesondere unter II. und III.

[255] *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, 815 (816 ff.); *Zech*, Information als Schutzgegenstand, 2012, S. 423; *ders.*, Daten als Wirtschaftsgut − Überlegungen zu einem „Recht des Datenerzeugers", CR 2015, 137 (144 ff.).

anderen Teilen der Welt sein könne, der letztlich auch deutschen Unternehmen zugutekäme. Eine mögliche Schutzschwelle sei in Abstimmung mit dem Schutzumfang zu diskutieren.[256] In Betracht komme entweder ein breit gefasster Schutzgegenstand (z. B. für sämtliche Maschinendaten mit geringem Schutzumfang) oder ein großer Schutzumfang in Form breit gefasster Verwertungsrechte für ausgewählte Daten.[257] Zu erwägen sei, nur solche Daten zu schützen, die in einem (Online-)Register eingetragen sind.[258]

Einen aktuellen Regelungsbedarf für ein umfassendes, alle (Maschinen-)Daten erfassendes absolutes Recht sehen allerdings auch die Vertreter dieses Ansatzes nicht. Mögliche Schutzrechte müssten vielmehr induktiv entstehen, sie könnten nur schrittweise für bestimmte Daten in bestimmten Zusammenhängen eingeführt werden; insoweit könne in der näheren Zukunft vor allem das Richterrecht eine Rolle spielen.[259] Im Übrigen sei wegen der wirtschaftlichen Bedeutung und der enormen Auswirkungen eines absoluten Datennutzungsrechts eine breite gesellschaftliche Diskussion geboten.[260]

4. Weiterentwicklung des Schutzes personenbezogener Daten

Schließlich sind Vorschläge zu erwähnen, die vor allem personenbezogene Daten in den Blick nehmen und insoweit primär auf eine Weiterentwicklung des Datenschutzrechts abzielen. Vor dem Hintergrund des ökonomischen Werts personenbezogener Daten werden die Schaffung eines an das bestehende Urheberrecht angelehnte „Datennutzungsrechts“[261] sowie die Rechtskonstruktion eines „immaterialgüterrechtlichen Eigentumsrechts an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten“[262] diskutiert. Anders als die dem Prüfauftrag der Arbeitsgruppe geschuldete Perspektive in diesem Kapitel stellen diese Ansätze

---

[256] Kritisch dagegen *Dorner*, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (622): Ein sondergesetzlicher Schutz aller Daten würde der gesetzgeberischen Wertung widersprechen, wonach im Urheberrecht grundsätzlich nur der Ausdruck bzw. die Form einer Idee (das Werk), nicht aber die Idee selbst geschützt sei.

[257] *Becker*, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, 815 (824 ff.); *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem „Recht des Datenerzeugers", CR 2015, 137 (146).

[258] *Zech*, Daten als Wirtschaftsgut − Überlegungen zu einem „Recht des Datenerzeugers", CR 2015, 137 (146); *ders.*, Information als Schutzgegenstand, 2012, S. 437 ff.; vgl. Staudinger/*Seiler*, BGB, Eckpfeiler des Zivilrechts, 2014, Sachenrecht − Allgemeine Lehren, Rn. 62 (zum sachenrechtlichen Publizitätsgrundsatz).

[259] *Becker*, Rechte an Industrial Data und die DSM-Strategie, GRUR Newsletter 01/2016, S. 7 (11).

[260] *Zech*, „Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1160).

[261] *Zech*, „Industrie 4.0" − Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1154); *Wandtke*, Ökonomischer Wert von persönlichen Daten – Diskussion des „Warencharakters“ von Daten aus persönlichkeits- und urheberrechtlicher Sicht, MMR 2017, 6.

[262] *Fezer*, Theorie des immaterialgüterrechtlichen Eigentums an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten, MMR 2017, 3.

nicht auf die vom Dateninhalt unabhängige Rechtsposition am Datum als solchen ab, sondern sind fokussiert auf einen inhaltlichen Bezug der Daten zu einer bestimmten Person. Sie knüpfen damit an die (bisher noch) primär unter vertragsrechtlichen Aspekten geführte Diskussion an, ob und inwieweit die Hergabe personenbezogener Daten als Entgelt/Gegenleistung zu qualifizieren ist. Hierzu vertritt die Arbeitsgruppe die Auffassung, dass im allgemeinen Schuldrecht klarstellend geregelt werden sollte, dass eine vertragliche Gegenleistung (auch) in der Erteilung einer Einwilligung in die Verarbeitung personenbezogener Daten für kommerzielle Zwecke des Vertragspartners bestehen kann. Letztlich sieht die Arbeitsgruppe daher auch aus diesem Blickwinkel aktuell keinen Regelungsbedarf dafür, die Vertragskonzeption um einen eigentumsrechtlichen und/oder immaterialgüterrechtlichen Theorieansatz zum digitalen Datenrecht zu erweitern. Gleichwohl ist es geboten, die Weiterentwicklung des Datenschutzrechts als Alternativlösung stets im Blick zu halten, wenn sich der geltende Rechtsrahmen im Umgang mit (digitalen) Daten nicht mehr als ausreichend erweisen sollte. So wie sich die Frage des Regelungsbedarfs nur angemessen beantworten lässt, wenn man auch bestehende Immaterialgüterrechte (am Dateninhalt) berücksichtigt[263], kann auf die weitere Entwicklung der Digitalisierung möglicherweise auch (schon) dadurch angemessen reagiert werden, dass gezielt für bestimmte Dateninhalte eine neue Rahmenordnung geschaffen wird. Hierzu leisten die oben genannten Ansätze ggf. einen fruchtbaren Beitrag.

Entsprechendes gilt für den Vorschlag von *Schwartmann/Hentsch*[264], zur Anpassung des Datenschutzrechts an die digitale Welt anstelle der starren Einwilligungslösung des Datenschutzrechts eine datenschutzrechtliche Lizenz nach dem Muster des Urheberrechts einzuführen.

5. Risiken einer gesetzlichen Regelung

Mehrere Autoren warnen vor den Risiken, die mit einer gesetzlichen Regelung der Rechte an Daten zum jetzigen Zeitpunkt verbunden wären. *Grützmacher*[265] meint etwa, es solle „nicht vorzeitig nach dem Gesetzgeber gerufen werden, zu groß ist die Gefahr der verfehlten Monopolisierung von Informationen." *Grünberger*[266] warnt vor unangemessen hohen Transaktionskosten, wenn bei der Verwendung von Daten stets das Schutzobjekt, sein Inhaber und die geschützten Verwertungshandlungen identifiziert werden müssten. *Heymann*[267] hält die Konstruk-

---

[263] Siehe oben B.III.

[264] *Schwartmann/Hentsch*, Eigentum an Daten − Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV 2015, 221.

[265] *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (492).

[266] *Grünberger* auf dem Workshop des Justizministeriums NRW am 23.5.2016, Tagungsberichte bei *Christians*, Arbeitsgruppe „Digitaler Neustart im BGB", AfP 2016, 334; *Liepin/Götz*, Braucht das BGB ein Update?, MMR-Aktuell 2016, 379185 (verfügbar bei beck-online).

[267] *Heymann*, Der Schutz von Daten bei der Cloud Verarbeitung, CR 2015, 807 (809 ff.).

tion eines Dateneigentums für eine Sackgasse; allzu forsche generalisierende Lösungen verböten sich angesichts der Diversität der betroffenen Daten. *Heun/Assion*[268] sehen die Rechtspraxis in der Pflicht, die verschiedenen Fallkonstellationen zu bearbeiten. Die Schaffung eines neuartigen „Dateneigentums" sei hierfür nicht notwendig. Es handle sich keineswegs um eine Aufgabe, die reflexartig dem Gesetzgeber zugewiesen sei, bestehe doch eher ein „Zuviel" als ein „Zuwenig" an einschlägigem Recht. *Hoppen*[269] weist darauf hin, dass eine Sicherung von Eigentumsrechten an digitalen Daten technisch bedingt gar nicht sicher umsetzbar sei.

Auf dem 71. Deutschen Juristentag 2016 in Essen war die Frage, ob ein absolutes Recht an Daten geschaffen werden sollte, Gegenstand mehrerer Redebeiträge. Aktueller gesetzgeberischer Handlungsbedarf ist nicht benannt worden.[270] Dagegen zeigten verschiedene Wortbeiträge Gefahren auf, die mit einem solchen gesetzgeberischen Eingriff verbunden wären, etwa die Vermengung von Daten und Sachen[271], Schwierigkeiten der persönlichen Zuordnung und hohe Transaktionskosten[272], Ausschluss von heute nicht absehbaren Entwicklungen[273], Zerstörung des bei anderen Immaterialgüterrechten sorgfältig austarierten Gleichgewichts der Interessen[274] und Unmöglichkeit einer konsistenten Zuweisung bei zügiger laufender technischer Entwicklung[275].

Ein Beschluss ist auf dem Juristentag insoweit nicht gefasst worden. Im Zusammenhang mit vertragsrechtlichen Fragen hat die Abteilung Zivilrecht lediglich beschlossen,[276] der Gesetzgeber solle „prüfen, ob sich über die schuldrechtlichen Regelungen hinaus eine allgemeine Erweiterung des Sachbegriffs des § 90 BGB auf digitale Inhalte empfiehlt (mit Folgen für das Haftungs-, Sachen-, Zwangsvollstreckungs- und Insolvenzrecht)."[277] Eine Tendenz, welches Ergebnis diese Prüfung haben könnte oder sollte, ergibt sich aus dem Beschluss nicht.

III. Einschätzungen der Praxis

Überraschend wenige ober- und höchstrichterliche Entscheidungen beschäftigen sich mit den spezifischen Besonderheiten von digitalen Daten und ihrer Behandlung im Zivilrecht. Anhaltspunkte dafür, dass die Gerichte besondere Schwierigkeiten dabei haben, Sachverhalte aus der digitalen Welt mit dem vorhandenen

---

[268] *Heun/Assion*, Internet(recht) der Dinge − Zum Aufeinandertreffen von Sachen- und Informationsrecht, CR 2015, 812 (818).
[269] *Hoppen*, Sicherung von Eigentumsrechten an Daten, CR 2015, 802 (806).
[270] Eigene Mitschriften der Arbeitsgruppe.
[271] So etwa *Wendehorst*, eigene Mitschriften der Arbeitsgruppe.
[272] *Willems*, BDI, eigene Mitschriften der Arbeitsgruppe.
[273] So etwa *Raue*, eigene Mitschriften der Arbeitsgruppe.
[274] *Obergfell*, eigene Mitschriften der Arbeitsgruppe.
[275] *Wagner*, eigene Mitschriften der Arbeitsgruppe.
[276] Der Beschluss ist recht knapp mit 17:14:1 Stimmen ergangen.
[277] Beschlüsse des 71. Deutschen Juristentages, Essen 2016, Abteilung Zivilrecht, These 8c, S. 3, http://www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf.

rechtlichen Instrumentarium zu erfassen, fehlen. Diese Beobachtungen können als Hinweis darauf gedeutet werden, dass zum einen nicht viele Streitigkeiten betreffend die zivilrechtliche Behandlung von Daten jedenfalls zu den höheren Instanzen gelangen und es den Gerichten zum anderen grundsätzlich keine besonderen Probleme bereitet, solche Streitigkeiten auf der Grundlage des geltenden Zivilrechts zu entscheiden. Beides stützt die Ablehnung eines (aktuellen) Regelungsbedarfs.

Der *Deutsche Anwaltsverein* hat im November 2016 eine Stellungnahme zur Frage des „Eigentums" an Daten und Informationen veröffentlicht. Darin warnt er davor, dass eine zu frühe gesetzliche Regelung leicht zu praxisuntauglichen und/oder interessenwidrigen Lösungen kommen kann. Er empfiehlt daher, zunächst die weitere Diskussion abzuwarten, die Rechtslage auch in anderen EU-Mitgliedstaaten zu untersuchen und erst danach gesetzgeberische Lösungen zu entwickeln.[278]

Ähnlich liegt es mit Äußerungen der Interessenverbände auf Seiten der Wirtschaft und der Verbraucher. Eindeutige Positionierungen der Verbraucherverbände[279] wie auch der Verbände der Wirtschaft[280] für die Schaffung eines absoluten Rechts an Daten sind nicht ersichtlich. Namentlich der *Bundesverband der Deutschen Industrie* (BDI) hält die geltende Rechtslage für ausreichend, Probleme seien nicht bekannt.[281] Man solle vorsichtig mit der Rechtsetzung sein bei Sachverhalten, in denen durch Statuierung ausschließlicher Schutzrechte Monopole geschaffen würden. Das gelte vor allem für die Diskussion um ein allgemeines Recht an Daten; dieser Problemkreis sei noch zu wenig ausgeleuchtet und die Gefahr zu groß, faktische Zuordnungen durch gesetzliche Regelungen zu zementieren.[282]

---

[278] *DAV*, Stellungnahme zur Frage des „Eigentums" an Daten und Informationen, November 2016, S. 9 f.

[279] Vgl. − wenn auch nur auf persönliche Daten von Verbrauchern bezogen und daher wohl letztlich eher den Datenschutz betreffend − die Empfehlung des Sachverständigenrates für Verbraucherfragen beim BMJV, eine „rechtliche Sicherung der persönlichen Daten als Eigentum der Verbraucher" zu schaffen, in: Sachverständigenrat für Verbraucherfragen, Verbraucher in der Digitalen Welt − Verbraucherpolitische Empfehlungen, Januar 2016, S. 1, http://www.svr-verbraucherfragen.de/wp-content/uploads/2016/01/Verbraucher-in-der-Digitalen-Welt-Verbraucherpolitische-Empfehlungen.pdf.

[280] Zurückhaltend etwa Gutachten von *Noerr LLP* im Auftrag des BDI, Digitalisierte Wirtschaft/Industrie 4.0, November 2015, S. 14 f., 28 f., http://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf.

[281] So etwa *Willems*, BDI, auf dem 71. Deutschen Juristentag, Essen 2016, eigene Mitschriften der Arbeitsgruppe. In den BDI-Notizen zum Wirtschaftsrecht, Juni 2016, wird *Axel Voss*, MdEP, CDU, mit der Äußerung zitiert: „Persönlich halte ich die Debatte um eine künftige Definition von Dateneigentum für brandgefährlich!"

[282] Vgl. Gutachten von *Noerr LLP* im Auftrag des BDI, Digitalisierte Wirtschaft/Industrie 4.0, November 2015, S. 14 f., http://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf.

Eine gesetzliche Regelung sei derzeit verfrüht. Sollte sich die Verteilung der Datennutzung durch privatautonome Instrumente als unzureichend erweisen, könne zu einem späteren Zeitpunkt nachgebessert werden. Monopolisierungstendenzen könne zudem bereits durch den bestehenden Rechtsrahmen - namentlich durch das Kartellrecht - entgegengewirkt werden.[283]

IV. Bestrebungen auf europäischer Ebene

Auch die EU-Kommission hat das Thema „Dateneigentum“ in jüngster Zeit in verschiedenen Papieren angesprochen, ohne indes konkrete regulatorische Maßnahmen zu ergreifen. Im Rahmen der im Mai 2015 vorgestellten Strategie für den digitalen Binnenmarkt hat die Europäische Kommission am 10. Januar 2017 allerdings erste Konzepte für die Schaffung einer europäischen Datenwirtschaft vorgelegt. Neben der Feststellung, dass in der EU ein Binnenmarkt für Daten nicht bestehe und das darin liegende Potenzial nicht hinreichend ausgeschöpft werde, erhebt die Kommission in ihrer Mitteilung insbesondere den Befund, dass es erhebliche Rechtsunsicherheiten in Bezug auf nicht personenbezogene, maschinengenerierte digitale Daten gebe. Zum einen würden die geltenden europäischen Haftungsvorschriften den aktuellen Datenprodukten und -diensten nicht mehr gerecht. Zum anderen ergäben sich auch im Zusammenhang mit dem Zugang, der Übermittlung und der Übertragbarkeit von nicht-personenbezogenen Daten erhebliche Probleme, die eine großflächige Nutzung erschwerten. Daran anknüpfend will die Kommission für eine Erhöhung der Rechtssicherheit in Haftungsfragen sorgen, um ein besseres Investitions- und Innovationsklima für das Internet der Dinge und autonome Systeme zu schaffen.

Zur Vorbereitung legislativer Schritte möchte sich die Kommission zunächst ein Bild von den ökonomischen und rechtlichen Auswirkungen verschaffen. Sie hat deshalb zeitgleich öffentliche Konsultationen zur Schaffung der europäischen Datenwirtschaft sowie zur Bewertung der Richtlinie über die Haftung für fehlerhafte Produkte eingeleitet. Die Ergebnisse sollen in eine im Laufe des Jahres 2017 geplante Initiative der Kommission zur europäischen Datenwirtschaft einfließen. Mit strukturierten Dialogen wird die Kommission zudem mit Mitgliedstaaten und Interessenvertretern die Verhältnismäßigkeit von Datenlokalisierungsvorschriften diskutieren und weitere Fakten zu Auswirkungen auf Unternehmen und Einrichtungen der öffentlichen Hand zusammentragen.

Ob die gegenwärtigen Initiativen in die Begründung eines „europäischen Dateneigentums“ münden, ist ungewiss. Sie verdeutlichen jedoch, dass die EU-Kommission auf unterschiedlichen Ebenen das Ziel verfolgt, den freien Fluss nicht-personenbezogener Daten im Binnenmarkt zu fördern und nationale Vorgaben

---

[283] BDI/*Noerr*, Industrie 4.0 − Rechtliche Herausforderungen der Digitalisierung, Ein Beitrag zum politischen Diskurs, November 2015, S. 12, https://www.noerr.com/~/media/Noerr/PressAndPublications/Brochures/studien/Rechtliche-Herausforderungen-Digitalisierung-Industrie-40.pdf.

obsolet zu machen. Auch wenn derzeit noch keine regulatorischen Schritte in diesem Zusammenhang abzusehen sind, könnte die Kommission nationalen Alleingängen daher eher kritisch gegenüberstehen, namentlich der Schaffung eines absoluten Rechts an Daten im nationalen Recht, das notwendigerweise Auswirkungen auf den freien Datenverkehr im Binnenmarkt hätte.[284]

V. Ausblick

Derzeit besteht kein Bedarf für die Schaffung eines absoluten Rechts an Daten oder andere, Daten rechtlich zuweisende gesetzgeberische Maßnahmen.

Diese Einschätzung kann sich allerdings ändern. Die IT-Technik und die Internetwirtschaft entwickeln sich mit rasender Geschwindigkeit. Immer wieder gibt es neue Anwendungen, die häufig ganz spezifische Fragestellungen zum Umgang mit Daten aufwerfen. Es ist ohne Weiteres denkbar, dass sich z. B. aus der Rechtsprechungspraxis, von Seiten der Verbraucher- und Wirtschaftsverbände oder aus der Rechtswissenschaft Hinweise darauf ergeben, dass das geltende Recht nicht mehr genügt. Auch vor dem Hintergrund der soeben erwähnten Aktivitäten der EU-Kommission kann sich Handlungsbedarf ergeben. Nach alledem erscheint es geboten, das Thema „Dateneigentum“ auch weiterhin intensiv im Blick zu behalten. Dabei kann sich künftig ein Regelungsbedarf für ein umfassendes absolutes Recht an Daten ergeben, möglicherweise aber auch (nur) das Bedürfnis, Einzelfragen zu regeln oder sachlich begrenzte Lücken zu schließen, bspw. nur bestimmte Kategorien von Daten ausschließlich zuzuweisen oder nur begrenzte Befugnisse gesetzlich einzuräumen.

Auch die Entwicklung der Wettbewerbsverhältnisse sollte beobachtet werden. Es gilt, eine verfehlte Monopolisierung von Daten zu verhindern.[285] Idealerweise bildet sich zwar für Daten, die ein einzelnes Unternehmen erhoben hat und auf die es faktisch allein zugreifen kann, ein Markt, wenn andere Akteure ein (wirtschaftliches) Interesse an der Verarbeitung dieser Daten haben und einen entsprechend hohen Preis bieten. Dennoch drohen Fehlentwicklungen, namentlich wenn marktbeherrschende Unternehmen nur unzureichend zur Weitergabe von Daten bereit sind und damit die Entstehung oder das Erstarken neuer Märkte und neuer Wettbewerber verhindern. Das Bundeskartellamt weist in einem Arbeitspapier aus dem Juni 2016 auf die Gefahr von Marktzutrittsschranken durch exklusive Datenherrschaft marktmächtiger Unternehmen hin.[286] Im März 2016 hat das Bundeskartellamt ein Verfahren gegen Facebook wegen des Verdachts eröffnet, dass

---

[284] Vgl. *Becker*, Rechte an Industrial Data und die DSM-Strategie, GRUR Newsletter 01/2016, S. 7 (11).

[285] Dazu oben E. V. 4. a. (2).

[286] Bundeskartellamt, Arbeitspapier „Marktmacht von Plattformen und Netzwerken“, Ergebnisse und Handlungsempfehlungen, Juni 2016, S. 4, http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht-Kurzzusammenfassung.pdf?__blob=publicationFile&v=2.

durch die Ausgestaltung von Vertragsbedingungen zur Verwendung von Nutzerdaten eine mögliche marktbeherrschende Stellung auf dem Markt für soziale Netzwerke missbraucht worden sein könnte.[287]

Aus heutiger Sicht dürfte es schwierig sein, eine verfehlte Monopolisierung von Daten mit Mitteln des Zivilrechts zu verhindern. Umgekehrt birgt die ausschließliche Zuordnung digitaler Daten durch Schaffung eines absoluten Rechts aber gerade das Risiko, eine unerwünschte Konzentration von Informationen mit rechtlichen Mitteln zu ermöglichen und zu verfestigen.[288] Es bleibt abzuwarten, wie sich der nationale und internationale Datenverkehr entwickelt und inwieweit das Kartellrecht in der Lage sein wird, bei einem Marktversagen, insbesondere bei einer verfehlten Monopolisierung von Daten, effektiv gegenzusteuern.

G. Ergebnis

Ausgehend von der Fragestellung der Konferenz der Justizministerinnen und Justizminister ist festzuhalten, dass es keiner gesetzlichen Bestimmung der Rechtsqualität von Daten bedarf. Ein Dateneigentum oder ein anderes absolutes Recht an digitalen Daten kennt das geltende Recht zwar nicht. Daten genießen jedoch unter einer Vielzahl unterschiedlicher Ansatzpunkte rechtlichen Schutz. Insgesamt kann dieser Schutz von Daten im Zivilrecht als eine Art „Flickenteppich" bezeichnet werden, der sich aus vielen unterschiedlichen Teilen zusammensetzt, die zusammen ein – aus heutiger Sicht – hinreichend geschlossenes Schutzsystem bilden. Auch mit Blick auf den Handel von Daten oder die Zwangsvollstreckung in Speichermedien bzw. Datenbestände bestehen keine Lücken im geltenden Recht, deren Schließung durch den Gesetzgeber geboten ist.

---

[287] Bundeskartellamt, Pressemitteilung vom 2.3.2016, http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html.

[288] *Grützmacher*, Dateneigentum − ein Flickenteppich − Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (492); *Grünberger* auf dem Workshop des Justizministeriums NRW am 23.5.2016, Tagungsberichte bei *Christians*, Arbeitsgruppe „Digitaler Neustart im BGB", AfP 2016, 334; *Liepin/Götz*, Braucht das BGB ein Update?, MMR-Aktuell 2016, 379185 (verfügbar bei beck-online); vgl. auch entsprechende Vorschläge des BDI in: BDI/*Noerr*, Industrie 4.0 − Rechtliche Herausforderungen der Digitalisierung, Ein Beitrag zum politischen Diskurs, November 2015, S. 12, https://www.noerr.com/~/media/Noerr/PressAndPublications/Brochures/studien/Rechtliche-Herausforderungen-Digitalisierung-Industrie-40.pdf.

Kapitel 2: Digitales Vertragsrecht

A. Vorbemerkung

Ausgehend von der Beschlussfassung der Justizministerinnen und Justizminister hat sich die Arbeitsgruppe eingehend mit Fragen befasst, welche die Digitalisierung im Bereich des Vertragsrechts aufwirft.

Der als Überschrift gewählte Begriff „Digitales Vertragsrecht“ hat dabei Symbolcharakter. Einerseits ist er neu. Das hat er mit den unter vertragsrechtlichen Aspekten behandelten Phänomenen gemeinsam. Andererseits wird er (trotz der für einen solchen Begriff unvermeidlichen Unschärfe) von denjenigen, die sich mit vertragsrechtlichen Fragen der Digitalisierung befassen, wie selbstverständlich verwendet oder jedenfalls akzeptiert. Die darin zum Ausdruck kommende Aufgeschlossenheit spiegelt sich in dem Bestreben wider, für „digitale Verträge“ ausgewogene und belastbare rechtliche Rahmenbedingungen zu gewährleisten.

Die Arbeitsgruppe hat sich bei ihrer Beschäftigung mit der Thematik zum einen Fragen gewidmet, die sich aus einem zunehmend autonomen Agieren von Gegenständen und Produkten ergeben. Zum anderen ist sie Fragen nachgegangen, die Verträge über digitale Leistungen und im Kontext mit ihnen stehende neue Formen der Gegenleistung aufwerfen. Soweit dies im Zusammenhang mit den einzelnen digitalen Phänomenen geboten erschien, hat sich die Arbeitsgruppe über die rein vertragsrechtlichen Aspekte hinaus mit weiteren rechtlichen Gesichtspunkten befasst.

Kennzeichnend für den Themenkomplex „Digitales Vertragsrecht“ ist das breite Spektrum an digitalen Phänomenen, die vertragsrechtliche Fragen aufwerfen. Die Arbeitsgruppe hat dem dadurch Rechnung getragen, dass sie sich – entsprechend den exemplarisch im Beschluss der Justizministerinnen und Justizminister genannten Erscheinungsformen der Digitalisierung – praktisch besonders bedeutsamen Phänomenen gewidmet hat. Bezugspunkt war dabei dem Prüfungsauftrag entsprechend das geltende nationale Recht, mit dem sich die Arbeitsgruppe unter Auswertung von Rechtsprechung und Literatur im Einzelnen befasst hat. Soweit der Kontext dafür Anlass bot, hat die Arbeitsgruppe die neueren Rechtsentwicklungen auf europäischer Ebene in ihre Betrachtungen miteinbezogen.

Einer Auseinandersetzung mit Fragen des Vertragsschlusses durch Roboter (B.) und haftungsrechtlichen Fragen im Internet der Dinge (C.) schließen sich Ausführungen zu schuldrechtlichen Aspekten – insbesondere der vertragstypologischen Einordnung – des Cloud Computing (D.), des Streaming (E.) und sozialer Netzwerke (F.) an. Am Beispiel der sozialen Netzwerke wird sodann das Phänomen des „Bezahlens mit Daten“ näher untersucht (G.). Die folgenden Darstellungen widmen sich dem Erwerb digitaler Inhalte im Wege des Downloads (H.), dem WAP-Billing als missbrauchsanfälliger Form der Abrechnung digitaler Leistungen und Zahlungswegen im Internet (I.) sowie virtuellen Währungen (J.). Die

Ausführungen zu den einzelnen Unterthemen schließen jeweils mit einer Zusammenfassung der Ergebnisse bzw. Handlungsempfehlungen für den Gesetzgeber.

In allen untersuchten Bereichen ist die Arbeitsgruppe zu dem Ergebnis gelangt, dass es keinen Anlass gibt, zur Bewältigung bürgerlich-rechtlicher Fragestellungen völlig neue Wege zu gehen. In einzelnen Punkten hat die Prüfung aber ergeben, dass es durchaus Anlass für ein gesetzgeberisches Tätigwerden gibt.

B. Vertragsschluss durch Roboter

I. Untersuchungsgegenstand

Unter dem „*Internet der Dinge*“ ist allgemein die Verknüpfung von „intelligenten Gegenständen“ zu verstehen, die in einer internetähnlichen Struktur unmittelbar miteinander – ggf. auch mit menschlichen Teilnehmern – kommunizieren. Ziel der Kommunikation zwischen diesen intelligenten Gegenständen oder Dingen (sog. „*Smart Products*“) ist es, automatisierte, unmerkliche Unterstützungsleistungen für die Anwendung im Privat- oder Geschäftsbereich, der Logistik und der industriellen Produktion zu erbringen. Dies geschieht insbesondere durch die Bereitstellung und den Austausch von vorhandenen oder unmittelbar beim Teilnehmer erhobenen Informationen.

Mit der voranschreitenden Vernetzung von Produktionsanlagen, Fertigungsstätten und Maschinen (sog. „*Industrie 4.0*“) bieten sich der verarbeitenden Industrie und anderen Geschäftsbereichen wie der Logistik und dem Transportwesen neue Möglichkeiten der Prozessoptimierung und Kostenreduzierung. Aber auch im privaten Bereich spielen „Smart Products“ eine immer größere Rolle. Dabei handelt es sich um Produkte, bei denen zum reinen Produktnutzen ein Zusatznutzen durch die Fähigkeit zum Sammeln und Übermitteln von Daten entsteht. Diese Daten können das Produkt ebenfalls befähigen, autonom Aktionen auszuführen. Auch durch die externe Steuerung über eine App wird ein Produkt „smart“. Mit sog. „*Smart Services*“ haben Unternehmen in einer vernetzten Industrie 4.0 neue Möglichkeiten zur Kundenbindung oder auch zur vereinfachten Bedienung von Maschinen und Geräten. Hinter dem Begriff „Smart Services“ stehen digitale Dienstleistungen, die über das Internet mit den unternehmenseigenen oder fremden Wertschöpfungsketten verbunden sind. Sie ermöglichen daten- und dienstbasierte Geschäftsmodelle, wie bspw. Sharing-Dienste.

Im Internet der Dinge wird grundsätzlich ein Grad an Vernetzung angestrebt, der Bestellungen im Onlineshop, die Produktion der angeforderten Ware „nach Be-

darf“ sowie die autonome Vergabe des Logistikauftrages unmittelbar computergesteuert ermöglicht, ohne dass der Mensch noch selbst eingreift.[289] Erscheinungsformen des „*Internets der Dinge*“ sind, soweit sie im hier behandelten Zusammenhang interessieren, insbesondere

- der individualisierte, d. h. vom Besteller jederzeit zu beeinflussende Produktionsprozess,
- die vorausschauende Wartung von Maschinen (Predictive Maintenance),
- von Smart Products automatisiert generierte Bestellungen von Waren (z. B.: Kühlschrank bestellt selbständig),
- der Einsatz intelligenter Transportmittel („InBin“ vom Fraunhofer-Institut für Materialfluss und Logistik, autonome Flugobjekte) und die Vernetzung unterschiedlicher Logistikkomponenten.

Das in der Entwicklungsphase befindliche „*Brain-Machine-Interface*“ (übersetzt: Gehirn-Maschine-Schnittstelle), das eine unmittelbare Kommunikation des Menschen mit einem Rechner mittels spezieller Übertragungswege ermöglichen soll, wird im Folgenden wegen der noch nicht hinreichend spezifizierten Anwendungen außer Betracht gelassen; zivilrechtliche Fragestellungen sind insoweit ohnehin (derzeit) nicht erkennbar.

Die verschiedenen Erscheinungsformen des Internets der Dinge werfen zahlreiche rechtliche Fragestellungen auf.[290] Eine davon ist diejenige, ob im Rahmen der Kommunikation zwischen Computern oder Maschinen (M2M) wirksame Verträge geschlossen werden können.

---

[289] *Wulf/Burgenmeister*, Industrie 4.0 in der Logistik – Rechtliche Hürden beim Einsatz neuer Vernetzungs-Technologien, Anwendungsbeispiele und Lösungswege zu sechs zentralen Bereichen der Logistik, CR 2015, 404 (406).

[290] Neben den hier behandelten Rechtsbereichen können insbesondere auch die Folgenden betroffen sein: Soweit der mit der Vernetzung einhergehende Datenfluss personenbezogene Daten betrifft, ist das Datenschutzrecht tangiert. Bei der Speicherung und ggf. Zusammenführung der Datenbestände (Big Data) stellt sich die Frage, wer die Eigentumsrechte innehat oder ob Urheberrechte tangiert sind. Werden beim Predictive Maintenance im Rahmen einer sensorischen Auswertung von Daten auch Mitarbeiterdaten erfasst, sind das individuelle und kollektive Arbeitsrecht betroffen. Kommt es zum Einsatz privater (Liefer-)Fahrzeuge oder Drohnen als besonderer Form intelligenter Transportmittel, finden die Regelungen des Straßenverkehrsrechts und des Luftverkehrsrechts Anwendung.

II. Maschinell ausgelöste Erklärungen als Willenserklärungen

Zu klären ist zunächst, ob die von Maschinen ausgelösten Erklärungen als Willenserklärungen i. S. d. §§ 116 ff. BGB zu behandeln sind und wem sie zuzurechnen sind.

Die Willenserklärung ist ein notwendiger Bestandteil jeden Rechtsgeschäfts.[291] Das Gesetz geht davon aus, dass ein Vertrag durch korrespondierende Willenserklärungen (Antrag und Annahme, §§ 145 ff. BGB) zustande kommt. Eine Willenserklärung ist die Äußerung eines auf die Herbeiführung einer Rechtswirkung gerichteten Willens. Sie bringt einen Rechtsfolgewillen zum Ausdruck, d. h. einen Willen, der auf den Eintritt einer privaten Rechtsfolge (Begründung, inhaltliche Änderung oder Beendigung eines privaten Rechtsverhältnisses) gerichtet ist.[292]

1. Einfach automatisierte Willenserklärungen

Der Einsatz von automatischen Einrichtungen zur Herbeiführung von Rechtsgeschäften ist im Grundsatz kein neues Phänomen des Computer- und Internetzeitalters. Auch schon vor Inkrafttreten des BGB gab es Waren- und Dienstleistungsautomaten, bei denen man sich mit der Vorstellung behalf, der Automat speichere gewissermaßen fertige Willenserklärungen „ad incertas personas“.[293]

Im Computerzeitalter muss diese Vorstellung weiterentwickelt werden, da hier schwerlich noch davon gesprochen werden kann, der Verwender der automatischen Systeme treffe Einzelentscheidungen schon im Vorfeld „auf Vorrat“. Der Verwender bedient sich stattdessen eines Computerprogramms, das die Willenserklärung nach Maßgabe der Programmvorgaben erzeugt. Letztlich lässt sich damit aber auch diese Erklärung wieder auf den Willen desjenigen zurückführen, der sich des Computerprogramms bedient um damit „seine“ Willenserklärung zu erzeugen.

Entsprechend diesem Grundgedanken erkennt der BGH[294] die automatisiert erstellte Willenserklärung als echte Willenserklärung an, die nicht dem Computersystem, sondern der Person (oder dem Unternehmen) zuzurechnen ist, die das Computersystem als Kommunikationsmittel nutzt. Auch in der Literatur[295] wird ganz überwiegend die Auffassung vertreten, dass Computererklärungen der das

---

[291] *Köhler*, BGB Allgemeiner Teil, § 5 Rn. 5; *Wolf/Neuner*, Allgemeiner Teil des Bürgerlichen Rechts, § 28 Rn. 2.

[292] *Köhler*, BGB Allgemeiner Teil, § 6 Rn. 1; Palandt/*Ellenberger*, BGB, Einf v § 116, Rn. 1.

[293] Hierzu instruktiv *Köhler*, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen, AcP 182 (1982), 126 (132).

[294] Vgl. BGH, Urt. v. 16.10.2012 − X ZR 37/12, NJW 2013, 598 − Rn. 19.

[295] *Cornelius*, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353 (355, 358); *Faust*, Bürgerliches Gesetzbuch Allgemeiner Teil, § 2 Rn. 5; Soergel/*Hefermehl*, BGB, Vor § 116 Rn. 30; *Köhler*, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen, AcP 182 (1982), 126 (134); *ders.*, BGB Allgemeiner Teil, § 6 Rn. 8; *Mehrings*, Vertragsabschluß im Internet, Eine neue Herausforderung für das "alte" BGB, MMR 1998, 30 (33); MüKo/ *Säcker*, BGB, Einl. Rn. 185; Staudinger/*Singer*, Vorbem zu §§ 116 ff. Rn. 57; *Wolf/Neuner*, Allgemeiner Teil des Bürgerlichen Rechts, § 31 Rn. 10.

Computersystem nutzenden Person unmittelbar als deren eigene Willenserklärung zuzurechnen sind, weil sie sich letztlich auf den Willen dieser Person zurückführen lassen. Andere Erklärungsmodelle (etwa Stellvertretung oder Botenschaft durch das Computersystem, Blanketterklärung und sonstige arbeitsteilig hergestellte Willenserklärungen oder das Angebot ad incertas personas) spiegeln die Interessenlage im Fall der Computererklärung dagegen nicht angemessen wider.[296]

In diesem Bereich besteht aufgrund der allgemeinen Anerkennung automatisiert erstellter Erklärungen als Willenserklärungen i. S. d. BGB kein Regelungsbedarf.

2. Automatisierte Willenserklärungen eines sog. Softwareagenten

In der Literatur[297] ist vereinzelt (ohne Benennung der rechtlichen Konsequenzen) die Auffassung vertreten worden, beim Einsatz sog. Softwareagenten könne künftig eine Zurechnung als Willenserklärung des Nutzers eines sog. Softwareagenten möglicherweise ausgeschlossen sein, wenn sich deren Grad an Autonomie des Softwaresystems künftig weiter steigert. Sog. Softwareagenten sind Computerprogramme, die ohne menschlichen Einfluss auf der Grundlage ihrer eigenen Lernprozesse und Wissenserkenntnisse *eigenständig* Problemlösungen erstellen, die nicht programmtechnisch über Funktionen vorgegeben sind.[298] Sie sind damit *autonome Systeme*.[299]

Gegen eine solche Sonderbehandlung von Erklärungen durch sog. Softwareagenten spricht jedoch, dass sich auch bei noch so gesteigerter Autonomie des Systems dessen Einsatz nach wie vor auf den Willen der dahinterstehenden (natürlichen oder juristischen) Person zurückführen lässt und in diesem willentlichen Einsatz das entscheidende Zurechnungsmoment liegt, welches die Behandlung der Erklärung als Willenserklärung dieser Person rechtfertigt. Auch ein noch so autonom agierendes System kann letztlich nur innerhalb der von dem Verwender dieses Systems vorgegebenen Zielvorgaben handeln, der damit im Ergebnis die Kon-

---

[296] Vgl. zu diesen alternativen Erklärungsmodellen *Sorge*, Softwareagenten, Vertragsschluss, Vertragsstrafe, S. 24 f. m. w. N. Ablehnend zu einer Konstruktion mittels Botenschaft und Stellvertretung durch das Computersystem etwa auch Soergel/*Hefermehl*, BGB, Vor § 116 Rn. 30.

[297] *Sorge*, Softwareagenten, Vertragsschluss, Vertragsstrafe, S. 42.

[298] *Cornelius*, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353 f.; *Müller-Hengstenberg*/*Kirn*, Intelligente (Software-)Agenten: Eine neue Herausforderung unseres Rechtssystems? Rechtliche Konsequenzen der "Verselbstständigung" technischer Systeme, MMR 2014, 307 (309).

[299] Der Begriff „autonome Systeme“ ist bisher nicht endgültig definiert. Im Weiteren wird – wie überwiegend – darunter eine weiterentwickelte Softwareanwendung verstanden, bei der an die Stelle vorgegebener Abläufe und manueller Rekonfiguration maschinelles Lernen und algorithmische Handlungsplanung auf der Basis von Nutzer- und Umgebungsdaten sowie Informationen unterschiedlicher Systemwelten und digitaler Dienste tritt (vgl. Zwischenbericht des Fachforums Autonome Systeme im Hightech-Forum).

trolle behält und daher auch – im Rahmen der allgemeinen Regeln der Rechtsgeschäftslehre – die Verantwortung für dieses System zu tragen hat, indem er sich diese Erklärungen als „seine“ Erklärungen zurechnen lassen muss.[300]

Die Notwendigkeit eigenständiger rechtsgeschäftlicher Regeln für Willenserklärungen von sog. Softwareagenten ist somit im Hinblick auf die Zurechnung dieser Erklärungen „als Willenserklärungen“ nicht ersichtlich.

III. Zugang von Erklärungen, die von Maschinen in Empfang genommen und autonom weiterverarbeitet werden

Eine empfangsbedürftige Willenserklärung unter Abwesenden wird in dem Zeitpunkt wirksam, in dem sie dem Empfänger zugeht, § 130 Abs. 1 S. 1 BGB. Zugegangen ist die Willenserklärung, wenn sie so in den Bereich des Empfängers gelangt ist, dass dieser unter normalen Verhältnissen die Möglichkeit hat, vom Inhalt der Erklärung Kenntnis zu nehmen.[301] Zum Bereich des Empfängers gehören auch die von ihm zur Entgegennahme von Erklärungen bereit gehaltenen Einrichtungen, wie Briefkasten, E-Mail-Postfach oder Posteingangsserver.[302] Bei der Nutzung elektronischer Kommunikationsmittel bestehen insoweit keine Besonderheiten.[303]

Bei der Verwendung eines sog. Softwareagenten auf Empfängerseite ist eine Willenserklärung dann zugegangen, wenn diese die Schnittstelle zum Softwareagenten erreicht hat, sodass dieser unter Zugrundelegung normaler Verhältnisse die Möglichkeit der Verarbeitung hat. Der Empfänger verzichtet in diesem Fall regelmäßig schon antizipiert durch die Programmierung oder den Einsatz des Softwareagenten darauf, von seiner Möglichkeit der Kenntnisnahme Gebrauch zu machen.[304] Ob im Falle der Kommunikation mit einem Softwareagenten die Willenserklärung unter An- oder Abwesenden abgegeben wird, ist ein eher akademisches

---

[300] Gegen jede Sonderbehandlung von Erklärungen, die durch Einsatz von Softwareagenten zustandekommen, daher auch *Cornelius*, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353 (355); Staudinger/*Singer*, BGB, Vorbem zu §§ 116 Rn. 57.

[301] *Faust*, Bürgerliches Gesetzbuch Allgemeiner Teil, § 2 Rn. 22; *Köhler*, BGB Allgemeiner Teil, § 6 Rn. 13; *Wolf/Neuner*, Allgemeiner Teil des Bürgerlichen Rechts, § 33 Rn. 12 a.E.

[302] *Faust*, Bürgerliches Gesetzbuch Allgemeiner Teil, § 2 Rn. 32 f.; *Köhler*, BGB Allgemeiner Teil § 6 Rn. 14 (Briefkasten), 18 (elektronische Kommunikationssysteme); *Wolf/Neuner*, Allgemeiner Teil des Bürgerlichen Rechts, § 33 Rn. 15.

[303] *Köhler*, BGB Allgemeiner Teil, § 6 Rn. 18.

[304] Vgl. *Cornelius*, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353 (356); *Sorge*, Softwareagenten, Vertragsschluss, Vertragsstrafe, S. 31 mit Hinweis auf Ausnahmefälle. *Cornelius* spricht in diesem Zusammenhang von einer Modifikation der Empfangstheorie. Dies überzeugt jedoch nicht. Es verhält sich hier nicht anders, als würde ein Empfänger seinen Briefkasten mit einem Aktenvernichter koppeln, der eingehende Post umgehend zerstört, bevor sie gelesen werden kann. Da er jederzeit die Möglichkeit hat, den Aktenvernichter zu deaktivieren, hat er auch im Sinne der allgemeinen Zugangsdefinition die „Möglichkeit der Kenntnisnahme“. So auch hier: Der Empfänger hat sich lediglich antizipiert entschieden, von seiner Möglichkeit zur Kenntnisnahme durch organisatorische Vorkehrungen seiner Sphäre (Programmierung des Softwareagenten) keinen Gebrauch zu machen.

Problem und wird in der Praxis der vollautomatisierten Bestellverfahren mittels Computererklärung wohl kaum eine Rolle spielen,[305] sodass hier nicht weiter darauf eingegangen werden muss.

IV. Anwendbare Auslegungsgrundsätze

Von besonderer Bedeutung ist die Frage, welche Auslegungsgrundsätze gelten, wenn bei der Abgabe und dem Empfang von Willenserklärungen elektronische Kommunikationsmittel genutzt werden.

Für die Auslegung von unter Einsatz von Computersystemen abgegebenen und empfangenen elektronischen Willenserklärungen gelten nach einhelliger Auffassung[306] die allgemeinen Auslegungsgrundsätze (§§ 133, 157 BGB). Der BGH[307] hat die Geltung dieser Grundsätze jüngst dahingehend konkretisiert, dass dabei nicht auf die automatisierte Reaktion des Computersystems abzustellen ist, dessen sich eine Vertragspartei bedient. Der Inhalt der Erklärung sei nicht danach zu bestimmen, wie das automatisierte System sie voraussichtlich deuten und verarbeiten werde, sondern danach, wie sie der dahinterstehende menschliche Adressat nach Treu und Glauben und der Verkehrssitte verstehen dürfe. Diese Auffassung hat in der Lehre weitgehend Zustimmung erfahren[308] und darf heute als gesichert angesehen werden.

Diese Auslegungsgrundsätze dürften auch dann eingreifen, wenn bei der Abgabe oder dem Empfang einer Willenserklärung ein sog. Softwareagent beteiligt ist. Es ist nicht ersichtlich, warum die im Rahmen der Ziel- und Programmvorgaben des Verwenders bestehende größere Autonomie des sog. Softwareagenten den Auslegungsmaßstab beeinflussen sollte.

V. Anfechtung von maschinell ausgelösten Willenserklärungen

Fraglich ist ferner, unter welchen Voraussetzungen eine Anfechtung von maschinell ausgelösten Willenserklärungen möglich ist.

Rechtsprechung und Lehre haben sich bereits eingehend mit der Frage beschäftigt, in welchem Umfang und in welchen Fällen die Anfechtung von Willenserklärungen möglich ist, die unter Einsatz von elektronischen Hilfsmitteln übermittelt werden oder zustande gekommen sind. Dabei haben sich folgende Differenzierungen herausgebildet:

---

[305] Vgl. *Sorge*, Softwareagenten, Vertragsschluss, Vertragsstrafe, S. 32; *Mehrings*, Vertragsabschluß im Internet, Eine neue Herausforderung für das "alte" BGB, MMR 1998, 30 (33); *Cornelius*, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353 (357).
[306] Siehe nur MüKo/*Busche*, BGB, § 133 Rn. 12.
[307] BGH, Urt. v. 16.10.2012 − X ZR 37/12, NJW 2013, 598 − Rn. 17, 19.
[308] Siehe etwa MüKo/*Busche*, BGB, § 133 Rn. 12; *Faust*, Bürgerliches Gesetzbuch Allgemeiner Teil, § 2 Rn. 11; Jauernig/*Mansel*, BGB, § 133 Rn. 11; kritisch allein *Sutschet*, Anforderungen an die Rechtsgeschäftslehre im Internet, NJW 2014, 1041 (1046).

1. Eingabe- und Bedienungsfehler bei elektronisch übermittelten Willenserklärungen

Die Willenserklärung ist anfechtbar, wenn der Fehler der Willenserklärung auf einem Eingabe- oder Bedienungsfehler (Vertippen, Verschreiben o.ä.) desjenigen beruht, der sich des technischen Systems lediglich zur Übermittlung der Willenserklärung bedient (§ 119 Abs. 1 Alt. 2 BGB).[309] Gemeint ist etwa der einfache Fall, in dem der Anwender sich beim Abfassen einer E-Mail verschreibt oder vertippt.

2. Übermittlungsfehler aufgrund fehlerhafter Übermittlungssoftware

Willenserklärungen, die nicht dem Willen des Erklärenden entsprechen, weil sie aufgrund eines unerkannten Softwarefehlers bei der Übermittlung ihrem Inhalt nach verfälscht werden, sind ebenfalls anfechtbar.[310] Derartige Verfälschungen des ursprünglich richtig Erklärten auf dem Weg zum Empfänger durch eine unerkannt fehlerhafte Software, die den Datentransfer stört, ist ebenfalls als Irrtum in der Erklärungshandlung (§ 119 Abs. 1 Alt. 2 BGB) anzusehen. Denn es besteht kein Unterschied, ob sich der Erklärende selbst verschreibt, vertippt, durch seinen Boten die Erklärung verfälscht wird (§ 120 BGB) oder ob die Abweichung vom gewollten Erklärungstatbestand auf dem weiteren Weg zum Empfänger eintritt.[311]

3. Fehler bei elektronisch generierten Willenserklärungen auf der Ebene der Datenverarbeitung

Schwieriger zu beurteilen sind solche Fehler, die bei Willenserklärungen auftreten können, bei denen die von dem Fehler unmittelbar betroffene Softwarekomponente nicht lediglich zur Datenübermittlung eingesetzt wird (Datentransfer), sondern auch schon zur Generierung der Willenserklärung selbst anhand bestimmter vom Verwender eingegebener Daten (Datenverarbeitung). Liegt der Fehler im Bereich der Datenverarbeitung und Generierung der Willenserklärung bedarf es der Abgrenzung, ob der Fehler einer der Irrtumskategorien der §§ 119 f. BGB zuzuordnen oder vielmehr ein bloßer Motivirrtum ist, der im System des geltenden Irrtumsrechts gerade nicht zur Anfechtung berechtigt.[312] Insoweit kommt es darauf an, ob der konkrete Anlass für den Fehler angesichts des arbeitsteiligen Zusammenwirkens des Verwenders mit der Datenverarbeitungssoftware wertungsmäßig der Willensbildung zuzuordnen ist (dann: unbeachtlicher Motivirrtum) oder der Äußerung des bereits fertig gebildeten Willens (dann: Geschäftsirrtum im Sinne einer der Kategorien der §§ 119 f. BGB).[313]

---

[309] OLG Köln, Urt. v. 20.1.2001 – 9 U 173/99, NVersZ 2001, 351 (352); MüKo/*Säcker*, BGB, Einl. Rn. 188; Staudinger/*Singer*, BGB, § 119 Rn. 35.
[310] BGH, Urt. v. 26.1.2005 – VIII ZR 79/04, NJW 2005, 976 (977); OLG Frankfurt/Main, Urt. v. 20.11.2001 – 9 U 94/02 (zitiert nach juris); *Faust*, Bürgerliches Gesetzbuch Allgemeiner Teil, Rn. 23 (Fall 14a); MüKo/*Säcker*, BGB, Einl. Rn. 191.
[311] BGH, Urt. v. 26.1.2005 – VIII ZR 79/04, NJW 2005, 976 (977).
[312] MüKo/*Säcker*, BGB, Einl. Rn. 189.
[313] MüKo/*Säcker*, BGB, Einl. Rn. 190.

Die denkbaren Fallkonstellationen und Möglichkeiten lassen sich an dieser Stelle nicht abschließend darstellen.[314] Es werden nur einige Beispiele aufgezeigt:

Beruht der Fehler der Willenserklärung etwa darauf, dass der Verwender in den Datenverarbeitungsvorgang Daten eingibt, über die er sich falsche Vorstellungen macht, handelt es sich um einen unbeachtlichen Motivirrtum, der nicht zur Anfechtung berechtigt.[315] So etwa, wenn der Verkäufer eine veraltete Einkaufspreisliste in sein Warenwirtschaftssystem eingibt und die Software hieraus unzutreffende Verkaufspreise errechnet. Dann handelt es sich um einen Kalkulationsirrtum bei der Preisberechnung, der als bloßer Motivirrtum bei der Willensbildung eine Anfechtung nicht ermöglicht.[316]

Beruht der Fehler hingegen etwa darauf, dass der Verwender sich bei der Eingabe eines Datums in den Datenverarbeitungsvorgang vertippt, das dann nach den Programmvorgaben *unverändert in die von der Software erzeugte Willenserklärung* eingeht, dann handelt es sich wertungsmäßig eher um einen Fall, der dem Erklärungsirrtum gleichsteht, da der Wille dann in diesem Punkt durch den Verwender bereits abschließend gebildet war und lediglich aufgrund des Erklärungsirrtums unzutreffend in den Datenverarbeitungsvorgang eingespeist wurde (§ 119 Abs. 1 Alt. 2 BGB).[317]

4. Gesamtschau

Nach alledem ist davon auszugehen, dass sich die Irrtumsfälle anhand der im Gesetz in den §§ 119 ff. BGB enthaltenen Irrtumskategorien auch bei elektronischen Willenserklärungen entscheiden lassen. Es ist zwar denkbar, dass mitunter Grenzfälle auftreten, bei denen die konkrete Zuordnung schwer fällt.[318] Dies ist jedoch keine Besonderheit gerade von Willensmängeln bei elektronisch übermittelten oder generierten Willenserklärungen, sondern eine Folge der Differenzierung des Gesetzes zwischen den zur Anfechtung berechtigenden Geschäftsirrtümern (§§ 119 f. BGB) einerseits und dem grundsätzlich nicht zur Anfechtung berechtigenden bloßen Motivirrtum andererseits.[319] Die mitunter in Grenzfällen schwie-

---

[314] Siehe die weiter ausdifferenzierenden Darstellungen bei *Köhler*, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen, AcP 182 (1982), 126 (135 ff.); MüKo/*Säcker*, BGB, Einl. Rn. 190 ff; Staudinger/*Singer*, BGB, § 119 Rn. 35 f.

[315] Palandt/*Ellenberger*, BGB, § 119 Rn. 10; MüKo/*Säcker*, BGB, Einl. Rn. 193; Staudinger/*Singer*, BGB, § 119 Rn. 37.

[316] Dazu *Faust*, Bürgerliches Gesetzbuch Allgemeiner Teil, § 21 Rn. 21, 23 (Fall 14b); MüKo/*Säcker*, BGB, Einl. Rn. 193 a.E.

[317] *Köhler*, Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen, AcP 182 (1982), 126 (136); Staudinger/*Singer*, BGB, § 119 Rn. 36.

[318] Vgl. etwa Beispielsfälle 14c und 14d bei *Faust*, Bürgerliches Gesetzbuch Allgemeiner Teil, § 21 Rn. 21, 23.

[319] Zu der Unterscheidung von Geschäfts- und Motivirrtum im Irrtumsrecht des BGB siehe etwa schon die eingehende Kritik bei *Titze*, Vom sogenannten Motivirrtum, FS für Ernst Heymann, 1940, Bd. 2, S. 70 ff. Aus heutiger Sicht hierzu die Einordnung durch Staudinger/*Singer*, BGB,

rige Unterscheidung verschiedener Irrtumskategorien führt auch in anderen Lebensbereichen zu Abgrenzungsfragen, die bspw. unter den Schlagworten des Rechts(folge)irrtums[320] und des Kalkulationsirrtums[321] seit jeher geführt werden. Es besteht aber, solange nicht das Irrtumsrecht insgesamt reformiert werden soll, kein Anlass, speziell mit Blick auf elektronische Willenserklärungen Sonderregeln zu schaffen und dabei von der allgemeinen Systematik des Irrtumsrechts abzuweichen.

VI. Empfehlung

Im Hinblick auf das Zustandekommen eines wirksamen Vertrages (Zurechnung von Willenserklärungen, Abgabe und Zugang, Auslegungsgrundsätze und Anfechtung irrtumsbehafteter Erklärungen) kann kein Regelungsbedarf festgestellt werden in Bezug auf Rechtsgeschäfte, die unter Einsatz moderner digitaler Technologien zustande kommen. Die gesetzlichen Regelungen des BGB zur Rechtsgeschäftslehre sind hinreichend abstrakt gehalten, um auch die Phänomene der modernen Kommunikations- und Datenverarbeitungstechnologien zu bewältigen.

Praktische Problemkonstellationen, in denen die bestehenden Regelungen nicht zu sachgerechten Ergebnissen führen, sind bislang nicht bekannt geworden. Bei der Gesetzesanwendung mögen die modernen Technologien mitunter neue Rechtsanwendungsfragen aufwerfen. Die Rechtsprechung ist aber – wie bspw. die jüngste Rechtsprechung des BGH[322] zur Auslegung elektronischer Willenserklärungen belegt – ohne Weiteres dazu in der Lage, derartige offene Rechtsfragen verlässlich zu beantworten und auf diesem Wege das abstrakte gesetzliche Regelungsmodell der Rechtsgeschäftslehre des Bürgerlichen Gesetzbuches systemkonform zu konkretisieren. Vorauseilende punktuelle Einzelfallregelungen, die unüberschaubare Ausstrahlungseffekte bei der systematischen Auslegung der gesetzlichen Regeln und eine Einschränkung der Rechtsprechung bei der systemkonformen Konkretisierung des bestehenden Regelgefüges zur Folge haben könnten, empfehlen sich dagegen nicht.

Es besteht kein Anlass, die allgemeinen Vorschriften des BGB zur Rechtsgeschäftslehre um Bestimmungen zu ergänzen, die sich ausdrücklich auf automatisierte Willenserklärungen beziehen.

---

§ 119 Rn. 3 ff., der ebenfalls auf die Abgrenzungsprobleme hinweist, die aus der gesetzlichen Unterscheidung resultieren.

[320] Siehe hierzu die umfangreichen Nachweise und Ausführungen bei MüKo/*Armbrüster*, BGB, § 119 Rn. 81 ff.

[321] Siehe hierzu die umfangreichen Nachweise und Ausführungen bei MüKo/*Armbrüster*, BGB, 119 Rn. 85 ff.

[322] BGH, Urt. v. 16.10.2012 − X ZR 37/12, NJW 2013, 598, Rn. 17, 19.

C. Haftungsrechtliche Fragen im Internet der Dinge

I. Untersuchungsgegenstand

Im Zusammenhang mit dem „Internet der Dinge“[323] sind verschiedene Fallkonstellationen denkbar, in denen es zu Schäden kommen und sich deshalb die Frage stellen kann, welche Haftung das Gesetz vorsehen sollte. Beispielhaft seien die beiden folgenden Sachverhalte[324] genannt:

- *Smart Products*[325] verursachen Schäden beim Käufer (z. B. selbstfahrender Rasenmäher),
- *autonome Systeme*[326] treffen nicht vorhersehbare eigenständige Entscheidungen, die zu schadensverursachenden Fehlleistungen in autonomen Produktions- und Prozessabläufen führen.

Es ist der Frage nachzugehen, ob eine Haftungslücke für den Fall besteht, dass erworbene „Smart Products“ oder autonome Systeme einen Sachmangel aufweisen oder ihr Betrieb zu einem Schaden an sonstigen Rechtsgütern führt. Dabei kann zwischen der vertraglichen Haftung (dazu unter II.) und der außervertraglichen Haftung (dazu unter III.) unterschieden werden.

II. Vertragliche Haftung

Was die vertragliche Ebene angeht, so sieht das Gesetz sowohl verschuldensunabhängige Mängelrechte (Nacherfüllung, Minderung, Rücktritt) als auch solche Rechte vor, die ein Vertretenmüssen voraussetzen (Schadensersatz, Ersatz vergeblicher Aufwendungen).

1. Verschuldensunabhängige Rechte

Im Hinblick auf die verschuldensunabhängigen Rechte, die dem Käufer wegen eines *Mangels am Produkt* zustehen (vgl. § 437 Nr. 1 u. 2 BGB), ergeben sich bei dem Erwerb von Smart Products oder autonomen Systemen nach hiesiger Einschätzung keine besonderen Probleme im Vergleich zu analogen Sachverhalten. Auch wenn mitunter schwierige Rechtsfragen oder Fragen der Darlegungs- und Beweislast zu klären sind – bspw. bei schadhafter Software[327] – ist insoweit derzeit kein Regelungsbedarf des Gesetzgebers erkennbar. Es ist nicht ersichtlich, weshalb die hier betrachteten Besonderheiten des Produkts es erfordern, dass die verschuldensunabhängigen Rechte insoweit abweichend ausgestaltet werden.

---

[323] Zum Begriff Kap. 2., B. I.
[324] Der Themenkomplex „Big Data“ wird von der hiesigen Aufgabenstellung nicht umfasst.
[325] Zum Begriff Kap. 2, B. I.
[326] Zum Begriff Kap. 2, B. I.
[327] Dazu BGH, Urt. v. 5.6.2014 − VII ZR 276/13, MMR 2014, 591.

2. Anspruch auf Schadensersatz oder Ersatz vergeblicher Aufwendungen

Der Anspruch auf Schadensersatz aus §§ 437 Nr. 3, 280 Abs. 1 BGB (ggf. i. V. m. § 281 BGB) setzt ein Vertretenmüssen voraus. Das gilt (selbstverständlich) auch dann, wenn es um mangelhafte Smart Products oder fehlerhafte autonome Systeme geht. Die für die Haftung erforderliche Pflichtverletzung kann zwar darin liegen, dass der Verkäufer seine Pflicht zur mangelfreien Leistung verletzt. Ein Anspruch des Käufers wird in diesen Fällen gleichwohl nicht selten am fehlenden Vertretenmüssen scheitern. Der Verkäufer, der nur Zwischenhändler ist, ist kein Hersteller, und der Hersteller ist auch nicht sein Erfüllungsgehilfe i. S. v. § 278 BGB. Er kennt den Mangel meist nicht und muss ihn auch nicht kennen. Den Zwischenhändler trifft nämlich gegenüber dem Käufer[328] hinsichtlich der Kaufsache grundsätzlich keine Untersuchungspflicht. Dies ist jedoch keine Besonderheit der hier interessierenden Fälle. Auch ist nicht ersichtlich, weshalb bei der Veräußerung von Smart Products oder autonomen Systemen strengere Anforderungen an den Zwischenhändler gestellt werden sollten als sonst. Vor diesem Hintergrund ist nicht erkennbar, dass der Gesetzgeber insoweit tätig werden sollte. Nichts anderes gilt für mögliche Ansprüche des Käufers aus §§ 437 Nr. 3, 311a BGB oder §§ 437 Nr. 3, 284 BGB.

3. Besonderheiten beim Einsatz von direkter M2M-Kommunikation?

Beim Einsatz von direkter *M2M-Kommunikation*[329], insbesondere im Bereich der voranschreitenden Vernetzung von Produktionsanlagen, Fertigungsstätten und Logistik („Industrie 4.0“), stellt sich die Frage, wer für mögliche Fehler und Ausfälle haftet, in besonderer Weise. Dabei wird man zwischen der Haftung für fehlerhafte Datenquellen und Datenerzeugung einerseits und Fehlern in der Datenübermittlung andererseits unterscheiden müssen. Bei der Begründung eines Haftungsanspruchs können sich Schwierigkeiten hinsichtlich der Kausalität der Schädigungshandlung und dem eingetretenen Schaden sowie dem Vertretenmüssen ergeben. In vernetzten und komplexen Wertschöpfungsketten ist kaum vorhersehbar, wie sich einzelne Fehler auswirken werden. Daneben lassen sich die Schadensfolgen nur schwer abschätzen. Ein weiteres Problem tritt auf, wenn Fehler in einer nachträglichen Analyse nicht mehr reproduzierbar und rückverfolgbar sind. Im Ergebnis werden Darlegung und Beweis von Haftungstatbeständen schwierig, potentielle Haftungsrisiken sind kaum abzuschätzen. Es bleibt jedoch die weitere Entwicklung abzuwarten, ob vertragliche Vereinbarungen der an der Wertschöpfungskette Beteiligten die auftretenden tatsächlichen Probleme interessengerecht lösen können. Derzeit gibt es jedenfalls noch keinen hinreichenden Anlass dafür, dass der Gesetzgeber insoweit tätig wird.

---

[328] § 377 HGB betrifft das Verhältnis zum (vorangehenden) Verkäufer.
[329] Zum Begriff unter 2. Kap., B. I. a. E.

III. Außervertragliche Haftung

1. Allgemeines Deliktsrecht

Im allgemeinen Deliktsrecht kann zwischen dem Anspruch aus § 823 Abs. 1 BGB und demjenigen aus § 823 Abs. 2 BGB unterschieden werden.

a. Anspruch aus § 823 Abs. 1 BGB

Die Deliktshaftung nach § 823 Abs. 1 BGB setzt neben der Verletzung eines dort genannten Rechtsguts stets ein Verschulden voraus. Grundsätzlich dürfte das im Deliktsrecht geltende Verschuldensprinzip einen sachgerechten Haftungsgrund bilden.

Für Schäden, die durch die Nutzung eines Produkts entstehen, haftet der *Hersteller* im Rahmen der deliktsrechtlichen Produzentenhaftung nach § 823 Abs. 1 BGB, wenn er die ihn treffende Verkehrssicherungspflicht verletzt hat. Es gilt das Prinzip, dass derjenige, der eine Gefahrenquelle eröffnet oder beherrscht, für diese verantwortlich ist. Dabei kann es sich um Konstruktions-, Fabrikations- oder Materialfehler sowie Informationsfehler handeln. Auch eine unzureichende Produktbeobachtung in der praktischen Anwendung führt zu einer deliktischen Haftung des Herstellers. Er hat durch organisatorische Maßnahmen für die Produktüberwachung und im Einzelfall für geeignete Maßnahmen zur Gefahrabwendung einschließlich des Rückrufs der gefährlichen Produkte zu sorgen. Die Pflichten des Herstellers bei der Fertigung von Robotern werfen keine besonderen Rechtsfragen gegenüber der allgemeinen Produkthaftung und der für sie entwickelten Pflichten auf.[330] Dadurch, dass die Ursache der Fehlerquelle zunehmend technisch bedingt sein wird, findet gleichzeitig eine Verlagerung der Sorgfaltspflichten vom Nutzer auf den Hersteller statt.

Der Einsatz autonomer Systeme stellt aber auch den *Betreiber* vor gesteigerte Sorgfaltsanforderungen. Er hat sicherzustellen, dass etwaige Fehlfunktionen möglichst rechtzeitig erkannt werden und dafür Sorge zu tragen, dass sie sich nicht schädigend auswirken. Dabei ist grundsätzlich davon auszugehen, dass mit zunehmender Automatisierung die an den Betreiber autonomer Systeme zu stellenden Sorgfaltsanforderungen nicht mehr in erster Linie an die konkrete Handlung, sondern immer mehr an die Überwachung anknüpfen werden.[331]

---

[330] *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (769).

[331] *Horner/Kaulartz*, Haftung 4.0 − Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7 (8).

b. Anspruch aus § 823 Abs. 2 BGB

Unabhängig von einem Anspruch aus § 823 Abs. 1 BGB kann für den *Hersteller* eine Haftung infolge Schutzgesetzverletzung nach § 823 Abs. 2 BGB bestehen. Insbesondere beim Produktsicherheitsgesetz (ProdSG) handelt es sich um ein Schutzgesetz. Ein Anspruch des Produktbenutzers besteht aufgrund des eingeschränkten Schutzbereichs des ProdSG jedoch nur für die Schutzgüter Leben und Gesundheit. Bei fehlerhaften Medizinprodukten mit Softwaresteuerung können zudem die Vorschriften des Medizinproduktegesetzes (MPG) als Schutzgesetz zur Anwendung kommen.

2. Produkthaftung

Das Produkthaftungsgesetz (ProdHaftG) regelt die Haftung des Herstellers für Folgeschäden, die der bestimmungsgemäße Verbraucher oder sonstige Personen durch die Benutzung des fehlerhaften Produkts erleiden.[332] Es handelt sich dabei um eine verschuldensunabhängige Gefährdungshaftung (§ 1 Abs. 1 ProdHaftG), die einen Haftungshöchstbetrag bei Tod oder Körperverletzung (§ 10 ProdHaftG) und eine Selbstbeteiligung bei Sachschäden (§ 11 ProdHaftG) bestimmt. Der Anspruchsteller muss „lediglich“ nachweisen, dass ein Fehler des Produkts vorlag und daraus ein kausaler Schaden entstanden ist, § 1 Abs. 4 ProdHaftG.

Bei der Verursachung eines Schadens an der Gesundheit oder dem Körper durch ein fehlerhaftes Produkt oder System besteht die Haftung des Herstellers unabhängig davon, ob der Schaden bei einem gewerblichen Käufer, dem Endabnehmer oder einem Dritten eingetreten ist. § 1 Abs. 1 S. 2 ProdHaftG erfasst dagegen nur den Sachschaden, der einem privaten Endverbraucher oder einem unbeteiligten Dritten entstanden ist. Gewerblich genutzte Sachen erhalten insoweit keinen Schutz.

Für unvermeidbare Entwicklungsfehler ist die Haftung nach § 1 Abs. 2 Nr. 5 ProdHaftG ausgeschlossen, wenn der Produktfehler zum Zeitpunkt des Inverkehrbringens bei Einhaltung des Stands der Wissenschaft und Technik für den Hersteller nicht erkennbar war, wobei die Beweislast insoweit den Hersteller trifft. Technische Normen können zwar einen Mindeststandard bilden, deren Einhaltung genügt aber nicht, wenn die technische Entwicklung darüber hinausgegangen ist.[333]

Nach § 15 Abs. 2 ProdHaftG bleibt die verschuldensabhängige Haftung des Produzenten gemäß §§ 823 ff. BGB unberührt.

---

[332] Palandt/*Bassenge*, BGB, ProdhaftG, Einf. Rn. 1.
[333] Vgl. *Jänich*, Rechtsprobleme des autonomen Fahrens, NZV 2015, 313.

3. Haftungslücken beim Betrieb von autonomen Systemen

Es sind Sachverhalte denkbar, in denen *autonome Systeme* Aktionen vornehmen, die zum Zeitpunkt der Herstellung und Inbetriebnahme nicht vorhersehbar waren und dadurch Schäden verursachen. Problematisch sind die Fälle, in denen der Hersteller die im Verkehr erforderliche Sorgfalt beachtet hat, beim Betrieb jedoch Schäden eintreten. In diesen Fällen trifft den Hersteller kein Verschulden. In Betracht kommt dann nur eine Haftung des Betreibers, wenn dieser beim Einsatz des Systems mangelhafte Sorgfalt walten lässt.[334] Offen ist bislang der hierfür anzulegende Maßstab, denn je „autonomer" ein System (eine Software) durch entsprechende Programmierung zu entscheiden in die Lage versetzt wird, desto „unvorhersehbarer" werden die erzielten Ergebnisse. Ab einem gewissen Grad der Komplexität ist es theoretisch für Mensch und Maschine nicht mehr möglich, die Eigenschaften eines Algorithmus oder dessen Korrektheit formal zu beweisen oder zu garantieren. Eine Abschätzung des Risikos, das von solchen Systemen ausgeht, wird kaum noch möglich sein.[335] In dieser „Eigenständigkeit" des Systems liegt ja gerade der (wirtschaftliche) Sinn des Einsatzes.

Ein Anspruch gegen den Hersteller aus Produkthaftung ist nach derzeitigem Recht gemäß § 1 Abs. 2 Nr. 5 ProdHaftG ausgeschlossen, wenn ein unvermeidbarer Entwicklungsfehler vorliegt. Davon dürfte auszugehen sein, wenn das autonome System trotz Anwendung aller im Verkehr erforderlichen Sorgfalt unvorhersehbare Entscheidungen trifft, die einen Schaden verursachen. Soweit keine andere Gefährdungshaftung eingreift, die dieses Risiko mitumfasst (bspw. im Bereich des autonomen Fahrens die Halterhaftung des § 7 StVG), besteht eine Haftungslücke. Für autonom handelnde Systeme zeichnet sich mithin für das Haftungsrecht eine Regelungsnotwendigkeit ab.

4. Verteilung des Haftungsrisikos

Kernfrage dürfte sein, wem ein etwaiges Fehlverhalten autonomer Systeme zugerechnet werden kann und wie Risiken im Zusammenhang mit der Herstellung und Nutzung autonomer Systeme interessengerecht verteilt werden können.[336] Bei der Verteilung der Haftung nach der Verantwortlichkeit für Risikosphären, die die Verletzung einer Handlungspflicht oder einen Fehler nicht voraussetzt, handelt es sich um das Haftungsmodell der sog. Kausalhaftung. Eine Kausalhaftung in diesem Sinne wird insbesondere in der ökonomischen Diskussion vertreten und auch als „enge" Gefährdungshaftung bezeichnet.[337] Als Grundlage der Kausalhaftung

---

[334] *Bräutigam/Klindt*, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137 (1139).

[335] *Reichwald/Pfisterer*, Autonomie und Intelligenz im Internet der Dinge − Möglichkeiten und Grenzen autonomer Handlungen, CR 2016, 208 (212).

[336] Dazu *Horner/Kaulartz*, Haftung 4.0 − Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7.

[337] *Borges*, Haftung für selbstfahrende Autos − Warum eine Kausalhaftung für selbstfahrende Autos gesetzlich geregelt werden sollte, CR 2016, 272 (278); *Deutsch*, Das neue System der

wird neben dem wesentlichen Gesichtspunkt der (abstrakten) Beherrschbarkeit des Risikos auch das Einstehenmüssen für geschaffene Gefahren genannt. Das beruht auf der Erwägung, dass derjenige, der die Gefahr schafft, sie am besten beherrschen kann, und sei es durch Unterlassen. Ferner kommt der Gedanke zum Tragen, dass derjenige, der den Vorteil aus einer Aktivität zieht, auch deren Nachteile tragen soll.[338] Für die Schadenszurechnung kommen mithin Hersteller und Betreiber[339] in Betracht:

Zunächst scheidet eine Haftung der *Maschine* selbst – ggf. auch neben einer (gesamtschuldnerischen) Haftung von Hersteller und/oder Betreiber – nach überzeugender Auffassung[340] aus. Gegen eine spezielle Roboterhaftung[341] ist zunächst anzuführen, dass ein schadensursächliches Ereignis nur einem Rechtsträger zugerechnet werden kann. Hinzu kommt: Auch wenn es sich bei autonomen Systemen um hochkomplexe und anpassungsfähige – allerdings auch störanfällige – Einheiten handelt, sind deren Aktivitäten letztlich doch immer auf den Akt der Programmierung zurückzuführen.[342] Damit verbleibt es nach wie vor beim Anknüpfungspunkt des menschlichen Handelns, sei es als Setzen einer Gefahrenquelle im Sinne der Gefährdungshaftung, sei es im Sinne einer verschuldensabhängigen Haftung wie im allgemeinen Deliktsrecht.[343] Eine Roboterhaftung würde zudem eine Haftungsmasse voraussetzen. Würden Roboter mit einer Haftungsmasse ausgestattet, hätte dies den Nachteil, dass viel Haftungsmasse ohne konkreten Schaden gebunden wäre, jeweils aber nur eine limitierte individuelle Haftungsmasse zur Verfügung stünde.[344]

Durch das Inverkehrbringen des autonomen Systems schafft der *Hersteller* eine Gefahrenquelle. Verwirklicht sich das in dem autonomen System immanente Gefährdungsrisiko, ist an eine Herstellerhaftung zu denken. Demgemäß wird für den Bereich des autonomen Fahrens teilweise vertreten, eine gesetzliche Kausalhaftung des Kfz-Herstellers für Schäden einzuführen, die durch den Betrieb von Kfz

---

Gefährdungshaftungen − Gefährdungshaftung, erweiterte Gefährdungshaftung und Kausal-Vermutungshaftung, NJW 1992, 73 (75).

338 *Borges*, Haftung für selbstfahrende Autos − Warum eine Kausalhaftung für selbstfahrende Autos gesetzlich geregelt werden sollte, CR 2016, 272 (278).

339 Der Begriff „Betreiber" soll in diesem Kontext vergleichbar mit dem des Halters nach § 7 StVG zu verstehen sein.

340 *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (774).

341 Vgl. dazu Hilgendorf/*Hanisch*, Robotik im Kontext von Recht und Moral, S. 46 f.; siehe auch *Schirmer*, Rechtsfähige Roboter, JZ 2016, 660.

342 *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (767).

343 *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (767).

344 Hilgendorf/*Hanisch*, Robotik im Kontext von Recht und Moral, S. 40.

bei aktivierter autonomer Fahrzeugsteuerung verursacht werden.[345] Zur Begründung wird ausgeführt, der Hersteller sei im Vergleich zum Fahrzeugführer, der ja nicht mehr fahre, sondern nur noch Passagier sei, besser in der Lage, Schadensrisiken zu begrenzen. Dies gelte jedoch nur, soweit es um die spezifischen Risiken der autonomen Steuerung[346] gehe.[347] Gegen eine volle Risikozuweisung an den Hersteller werden teilweise ökonomische Gründe angeführt. Dies würde zu einer Verteuerung der Produkte führen, die deren Unverkäuflichkeit zur Folge haben könnten, wodurch im Ergebnis der Fortschritt bei der Entwicklung automatisierter Vorgänge gehemmt würde.[348]

Soweit teilweise eine Reduzierung der Haftung für den Hersteller diskutiert wird,[349] ist dies abzulehnen. Aus ökonomischer Sicht wäre das deshalb nicht überzeugend, weil anderenfalls die Anreize, sichere Technologien zu schaffen, verringert würden.

Die Entscheidung des *Betreibers* zum Betrieb des autonomen Systems ist unmittelbar kausal für das Entstehen des Gefährdungsrisikos. Zudem zieht er den wirtschaftlichen Nutzen aus dem Betrieb. Auch darin liegt ein sachgerechter Anknüpfungspunkt für die Haftung.

5. Lösungsmöglichkeiten zur Beseitigung der Haftungslücke

Im Folgenden werden vier Lösungsansätze aufgezeigt, die darauf abzielen, die herausgearbeitete Haftungslücke im Bereich der außervertraglichen Haftung zu beseitigen.

---

[345] *Borges*, Haftung für selbstfahrende Autos − Warum eine Kausalhaftung für selbstfahrende Autos gesetzlich geregelt werden sollte, CR 2016, 272 (280).

[346] In diesem Sinne hat der schwedische Kfz-Hersteller Volvo bereits in einer Pressemitteilung im Oktober 2015 erklärt, er wolle bei Unfällen mit seinen selbstfahrenden Fahrzeugen künftig die volle Haftung übernehmen.

[347] *Borges*, Haftung für selbstfahrende Autos − Warum eine Kausalhaftung für selbstfahrende Autos gesetzlich geregelt werden sollte, CR 2016, 272 (279).

[348] *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (775).

[349] Vgl. *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (774).

a. *Lösungsansatz 1:* Schaffung eines neuen Gefährdungshaftungstatbestandes zu Lasten des Betreibers

Stimmen in der Literatur[350] erwägen eine Schließung der aufgezeigten Haftungslücke durch Schaffung eines neuen Gefährdungshaftungstatbestandes *zu Lasten des Betreibers*. Die Gefährdungshaftung war und ist seit jeher das Mittel, die Risiken einer zwar sozial erwünschten (und damit rechtmäßigen), aber gefährlichen Technologie bei demjenigen zu internalisieren, der über den Einsatz der Technologie entscheidet.[351] Diese Lösung bewegt sich in der Struktur des bestehenden Haftungssystems. Denkbar ist eine Betreiberhaftung im Sinne einer Gefährdungshaftung für bestimmte automatisch betriebene Geräte nach dem Vorbild der Halterhaftung nach dem Straßenverkehrsgesetz oder der Tierhalterhaftung. Dem Geschädigten ist nicht zuzumuten, die Ursache des Fehlers eines autonomen Systems zu ermitteln, um dann zielgerichtet gegen den Verantwortlichen des Fehlers vorzugehen. Er soll sich an den Betreiber (Nutzer) halten können. Zugleich bleibt dem Betreiber unbenommen, den Hersteller in Regress zu nehmen. Sind auch die Voraussetzungen einer Herstellerhaftung erfüllt, würden Hersteller und Betreiber dem geschädigten Dritten gemäß § 840 BGB als Gesamtschuldner haften. Es würde ferner der Gesamtschuldnerausgleich nach § 426 BGB gelten.

Nicht außer Betracht zu lassen ist der *ökonomische Effekt*, den die Einführung einer Gefährdungshaftung haben kann. Sie steuert mittelbar das Aktivitätsniveau des Handelnden und könnte sich innovationshemmend auswirken. Durch den Gefährdungshaftungstatbestand wächst das persönlich zu tragende wirtschaftliche Risiko des Betreibers deutlich an. Folge ist, dass er nicht nur den Grad seiner anzuwendenden Sorgfalt, sondern auch seine Aktivität von einer Kosten-Nutzen-Analyse abhängig macht.[352] Wenn er dadurch von Tätigkeiten abgehalten wird, die nach seiner Einschätzung zu riskant sind, ist dies nach hier vertretener Auffassung allerdings nicht negativ zu bewerten. Darüber hinaus geht die Gefährdungshaftung typischerweise mit Haftungshöchstsummen einher, wodurch eine gewisse Sozialisierung der Risiken im Interesse der Innovation billigend in Kauf genommen wird.[353]

---

[350] *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766; *Horner/Kaulartz*, Haftung 4.0 − Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7 (13).

[351] *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (775).

[352] *Horner/Kaulartz*, Haftung 4.0 − Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7 (13).

[353] *Spindler*, Roboter, Automation, künstliche Intelligenz, selbst-steuernde Kfz – Braucht das Recht neue Haftungskategorien? Eine kritische Analyse möglicher Haftungsgrundlagen für autonome Steuerungen, CR 2015, 766 (775).

Zu erwägen ist, die Gefährdungshaftung unter Umständen mit der Einführung einer entsprechenden *Versicherungspflicht* des Betreibers zu verbinden. Mit Blick auf die Gefährdungshaftungstatbestände nach § 7 StVG und § 833 BGB ist auch für den Gefährdungshaftungstatbestand für die Nutzung autonomer Systeme an eine Abschwächung der Risikoverteilung zu denken. Im Straßenverkehr besteht eine Versicherungspflicht nach § 1 PflVG. Dem Geschädigten steht gegen die Kfz-Haftpflichtversicherung gemäß § 115 Abs. 1 S.1 Nr. 1 VVG ein Direktanspruch zu. Dabei haften Halter und Versicherer gemäß § 115 Abs. 1 S. 4 VVG als Gesamtschuldner. Im Bereich der Tierhalterhaftung fällt die dahingehende Gesetzgebungskompetenz in den Bereich der Landesgesetzgebung. Die meisten Bundesländer haben sich – mit Abstufungen im Detail – auch hier für eine Versicherungspflicht entschieden. Mit Blick auf das Schadensrisiko und die potentielle Schadenshöhe scheint eine Versicherungspflicht auch hier naheliegend, soweit hierfür ein Gemeinwohlinteresse besteht. Das dürfte der Fall sein, wenn das autonome System signifikante Schäden verursachen kann. Maßgebend kann dabei auch die Frage sein, ob das Haftungsrisiko einen Privaten oder ein Unternehmen trifft.

b. *Lösungsansatz 2:* Verschärfung der Haftung des Herstellers

Die Lösung kann auch in der Erweiterung der *Haftung des Herstellers* gesucht werden. Insoweit ist an die Verschärfung der Produkthaftung für autonome Systeme – evtl. abhängig von einem bestimmten Grad der Autonomie – zu denken. Dabei kann insbesondere erwogen werden, die Haftungslücke durch eine nationale Regelung auf der Grundlage von Art. 15 Abs. 1 lit. b) der Produkthaftungsrichtlinie zu schließen, wonach auch sog. Entwicklungsrisiken der verschuldensunabhängigen Produkthaftung unterworfen werden können. Weitergehende nationale Regelungen müssten in jedem Fall den durch die Produkthaftungsrichtlinie gesetzten Rahmen beachten.

c. *Lösungsansatz 3:* Entwicklung eines neuen Haftungsregimes

Losgelöst von der bestehenden Struktur der außervertraglichen Haftung wäre auch die Entwicklung spezieller Haftungsregelungen für autonome Systeme denkbar, die den Hersteller oder sämtliche Akteure, die an der Entwicklung und Herstellung des autonomen Systems beteiligt sind, jedenfalls im Außenverhältnis zu einer gesamtschuldnerischen Haftung – ggf. zusammen mit dem Betreiber – verpflichten.[354] Ein solches Haftungsregime würde dem Umstand Rechnung tragen, dass sich in der Produktions- und Lieferkette bei digitaler Vernetzung einzelne Bearbeitungsschritte oftmals nicht mehr eindeutig voneinander abgrenzen lassen werden.

---

[354] Denkbar wäre zudem die Bildung eines Haftungsfonds, den Geschädigte im Falle einer Haftungslücke in Anspruch nehmen könnten.

d. *Lösungsansatz 4:* Europäische Lösung

Eine europäische Lösung erscheint deshalb erwägenswert, weil sich die Haftungsfragen im Internet der Dinge nicht auf eine nationale Ebene begrenzen lassen. In ihrer Mitteilung[355] an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Digitalisierung der europäischen Industrie – Die Chancen des digitalen Binnenmarkts in vollem Umfang nutzen" stellt die Kommission ihre Planung wie folgt dar:

> *„Prüfung der rechtlichen Rahmenbedingungen für autonome Systeme und IoT-Anwendungen, insbesondere Sicherheits- und Haftungsregelungen sowie die rechtlichen Voraussetzungen, um Praxistests in großem Maßstab zu ermöglichen".*

In diesem Sinne hat der Rechtsausschuss des Europäischen Parlaments unter dem 27. Januar 2017 seinen Bericht vorgestellt, der eine Entschließung des Europäischen Parlaments mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich der Robotik (2015/2103(INL)) beinhaltet. Diesen hat das Europäische Parlament am 16. Februar 2017 angenommen. In dem Bericht wird insbesondere die Auffassung vertreten, die zivilrechtliche Haftung von Robotern sei eine Frage von entscheidender Bedeutung, mit der man sich auf europäischer Ebene befassen müsse.[356] Die Kommission wird aufgefordert, dem Europäischen Parlament „einen Vorschlag für ein Rechtsinstrument über rechtliche Fragen im Zusammenhang mit der für die nächsten 10 - 15 Jahre vorhersehbaren Entwicklung von Robotik und künstlicher Intelligenz zu unterbreiten."[357] Als mögliche Lösung für die komplexe Frage, wem die Verantwortung für Schäden zuzuordnen ist, die von zunehmend autonomeren Robotern verursacht werden, wird in dem Bericht eine „verschuldensunabhängige" Haftung erwogen, wobei die Verantwortung des „Lehrers" des Roboters umso höher anzusetzen sein soll, je größer dessen Lernfähigkeit oder Autonomie sei und je länger seine „Ausbildung" bereits andauerte. Ferner wird eine obligatorische Versicherungsregelung vorgeschlagen, nach der ein Hersteller dazu verpflichtet werden soll, für jeden autonomen Roboter, den er produziert, eine Versicherung abzuschließen. Dabei wird erwogen, dieses Versicherungssystem durch einen Fonds zu ergänzen.[358]

---

[355] COM(2016) 180 final.
[356] 2015/2103(INL), Rn. 49.
[357] 2015/2103(INL), Rn. 51.
[358] 2015/2103(INL), Rn. 58.

IV. Empfehlungen

Im Hinblick auf die außervertragliche Haftung besteht ein Regelungsbedarf. Zwar scheint das geltende Haftungsregime derzeit noch ausreichend zu sein. Jedenfalls sind bislang keine Fälle bekannt geworden, die nach dem geltenden Recht zu untragbaren Ergebnissen geführt hätten. Da jedoch der Grad der Selbständigkeit von autonomen Systemen weiter steigen wird und dadurch – wie gezeigt – Haftungslücken auftreten werden, sollten diese – bereits heute – geschlossen werden.

Zur Beseitigung der Haftungslücke kommen die oben aufgezeigten vier Lösungsansätze in Betracht. Die Entscheidung darüber, welcher Lösungsansatz bevorzugt wird, hängt maßgeblich auch von wirtschaftspolitischen Erwägungen ab. Aus diesem Grunde stehen die Lösungsansätze nicht in einem strengen Alternativverhältnis, sondern können ggf. miteinander kombiniert werden.

In Bezug auf die Haftung aus Verträgen, die von Robotern geschlossen werden, besteht kein Regelungsbedarf des Gesetzgebers. Dasselbe gilt für die vertragliche Haftung in dem Fall, dass erworbene Smart Products oder autonome Systeme einen Sachmangel aufweisen.

Eine Haftungslücke beim Einsatz autonomer Systeme (wie Robotern) droht jedoch im außervertraglichen Bereich. Falls die insoweit notwendigen Lösungen nicht in angemessener Zeit auf europäischer Ebene gefunden werden können, sollte der nationale Gesetzgeber tätig werden. Insoweit kommt insbesondere eine stärkere Betreiberhaftung oder eine verschärfte Herstellerhaftung in Betracht. Auch eine kumulative Haftungserweiterung ist denkbar. Auf welche Weise die Haftung im Einzelnen auszugestalten ist, muss einer gesonderten Prüfung vorbehalten werden, bei der auch versicherungsrechtliche und wirtschaftspolitische Fragen zu berücksichtigen sind.

D. Cloud Computing

I. Technische Grundlagen und ökonomische Bedeutung

1. Allgemeines

Die Entwicklung der Informationstechnologie hat vielfältige Ansätze der Leistungstiefengestaltung in der IT hervorgebracht, sowohl in Bezug auf die erbrachte Leistung selbst als auch hinsichtlich deren Erbringung in Form komplexer, häufig globaler Wertschöpfungsketten.[359] Die Zeiten, in denen Unternehmen eigene IT-Abteilungen unterhielten und von Anwendungsentwicklung bis zur Rechnerwartung alles selbst übernahmen, scheinen vorüber zu sein.[360] Auch der private Nutzer ist dazu übergegangen, vermehrt webbasierte Dienste in Anspruch zu nehmen.

Abhängig von der konkreten Ausgestaltung wird die Auslagerung von Informationstechnologie und Informationssystemen entweder als (traditionelles) IT-Outsourcing oder als „Cloud Computing“ bezeichnet. Insbesondere für das Cloud Computing fehlt es indes an einer allgemeingültigen Definition.[361] Der Dachverband der digitalen Wirtschaft, Bitkom e.V., verwendet folgende Begriffsbestimmungen:

IT-Outsourcing bezeichnet die Übernahme der Verantwortung für den Betrieb von IT-Systemen und des damit verbundenen IT-Managements auf partnerschaftlicher Basis und auf der Grundlage vereinbarter Leistungen und Service Level Agreements (SLA – Dienstgütevereinbarungen). *Cloud Computing* ist eine Form der bedarfsgerechten und flexiblen Nutzung von IT-Leistungen. Diese werden in Echtzeit als Service über das Internet bereitgestellt und nach Nutzung abgerechnet. Damit ermöglicht Cloud Computing den Nutzern eine Umverteilung von Investitions- zu Betriebsaufwand. Die IT-Leistungen können sich auf Anwendungen, Plattformen für Anwendungsentwicklungen und -betrieb bzw. Basisinfrastruktur beziehen.[362]

Ein weiterer Vorschlag zur Definition von Cloud Computing findet sich bei *Wicker*[363]:

> *„Cloud Computing ist ein auf Visualisierung basierendes IT-Bereitstellungsmodell, bei dem sowohl Ressourcen in Form von Infrastruktur als auch Entwicklungen, Entwicklungsplattformen und Daten als verteilter*

---

[359] Vgl. Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 4.
[360] Vgl. Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 5.
[361] Zu den verschiedenen Ansätzen: Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 2 Rn. 27 ff.
[362] Beschreibung des AK Cloud Computing & Outsourcing, abrufbar unter https://www.bitkom.org/Bitkom/Organisation/Gremien/Cloud-Computing-Outsourcing.html.
[363] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen − Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (783).

Dienst über das Internet durch einen oder mehrere Leistungserbringer bereitgestellt werden, wobei diese Dienste nach Bedarf flexibel skalierbar und verbrauchsabhängig abgerechnet werden können."

Die nachfolgenden Ausführungen beschränken sich auf das entgeltliche Cloud Computing.[364]

2. Technische Grundlagen

a. Charakteristische Eigenschaften

Die vorstehenden Definitionen von Cloud Computing lassen sich anhand der in der Literatur identifizierten charakteristischen Eigenschaften konkretisieren. Zu diesen auch „Designprinzipien" genannten Eigenschaften gehören insbesondere:

(1.) Zugriff über ein Netzwerk

Cloud Services werden über ein Netzwerk (z. B. das Internet) bereitgestellt und ermöglichen dem Nutzer einen Zugriff über standardisierte Schnittstellen.

(2.) Ressourcenbündelung

Cloud-Anbieter bündeln ihre Ressourcen und stellen sie ihren Kunden über ein mandantenfähiges System zur Verfügung. Mandantenfähigkeit bedeutet in diesem Zusammenhang, dass mehrere „Mandanten" auf denselben Server oder dasselbe Software-System zugreifen können, ohne jedoch gegenseitigen Einblick in ihre Daten, Benutzerverwaltung oder Ähnliches zu haben.

(3.) Skalierbarkeit

Die Ressourcenbündelung bedingt zwar ein geringes Maß an individueller Anpassungsmöglichkeit. Auf der anderen Seite versetzt sie den Anbieter jedoch in die Lage, dem Kunden je nach Bedarf „flexibel skalierbar" Ressourcen zur Verfügung zu stellen. Obwohl die Ressourcen prinzipiell begrenzt sind, wird dem Kunden so das Gefühl unendlicher Rechenkapazität gegeben.

(4.) Virtualisierung

Cloud-Ressourcen sind virtualisierte Ressourcen. Dies bedeutet, dass logische Systeme von der physischen Implementierung und Infrastruktur (bspw. Hardware) abstrahiert werden.[365]

Cloud Computing ist aus technischer Sicht keine wirkliche Neuerung. Es handelt sich vielmehr um eine Mischung aus alten und neuen IT-Konzepten,

---

[364] Wegen der rechtlichen Einordnung von „Daten als Entgelt" wird auf die Ausführungen unter G. Bezug genommen.

[365] Vgl. Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 32; *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen − Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (783).

die verschiedene Softwarelösungen zusammenführen und eine globale Nutzbarkeit bieten.[366] Ausschlaggebend für den Erfolg des Cloud Computing scheint unter anderem die kostengünstige Entwicklung sehr spezialisierter Geschäftsmodelle zu sein, bei denen mit nahezu unbegrenzten IT-Ressourcen von verschiedenen Orten aus auf die angebotenen Leistungen zugegriffen werden kann.[367]

b. Differenzierung von Cloud Services nach dem potentiellen Nutzerkreis

In Abhängigkeit vom potentiellen Nutzerkreis wird bei der Art des Bezugs von Cloud Services üblicherweise zwischen vier Modellen unterschieden:

(1) Private Cloud

Private Clouds zeichnen sich dadurch aus, dass exklusiv ein vorab festgelegter Nutzerkreis Zugriff auf die bereitgestellten IT-Services hat. Management und Betrieb werden innerhalb eines Unternehmens oder einer gemeinsamen Organisation (sog. Shared Service Center) abgewickelt. Hierbei handelt es sich um (teil-)autonome Organisationseinheiten, die nutzerorientiert die operativen Einheiten eines unternehmensinternen Nutzerkreises mit unterstützenden und generischen Leistungen beliefern. Der Zugang zur Private Cloud erfolgt in der Regel über ein Intranet beziehungsweise ein Virtual Private Network (VPN).[368]

Vorteil der Private Cloud ist, dass sich die IT-Ressourcen, die für die Bereitstellung der angebotenen Services genutzt werden, unter der direkten Kontrolle des Kunden befinden. Zudem können die Serviceangebote individuell auf die Anforderungen des Unternehmens/des Nutzerkreises angepasst werden.

(2) Public Cloud

Public Clouds richten sich hingegen an einen offenen Nutzerkreis. Die Nutzer teilen sich die vorhandenen Ressourcen wie Rechenleistung oder Speicherplatz, die von dem (unabhängigen) Betreiber, zumeist einem IT-Dienstleister, bereitgestellt werden. Sie wissen dabei grundsätzlich nicht, welche weiteren Personen ihre Daten in der Cloud des Anbieters gespeichert haben. Auch eine Lokalisierung der genutzten Ressource ist in der Regel unmöglich.[369]

Wesentlicher Vorteil der Public Cloud ist die Möglichkeit des Anbieters, durch die Standardisierung des Serviceangebotes und die damit einhergehende Ressour-

---

[366] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (361).
[367] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (361).
[368] Vgl. Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 37 f. − VPN = Virtuelles privates, in sich geschlossenes Kommunikationsnetz, das ein bestehendes Kommunikationsnetz (ausschließlich) als Transportmedium verwendet (Bsp.: Heimarbeitsplatz), Quelle: www.wikipedia.de.
[369] Vgl. Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 44.

cenbündelung eine bessere Auslastung des Systems zu erzielen. Neben Größenvorteilen der Public Cloud kann dies zu einer spürbaren Kostenreduzierung führen. Dies gilt jedenfalls dann, wenn der Bedarf des Nutzers starken Schwankungen unterworfen ist und deshalb ein effizienter Eigenbetrieb nur schwer zu realisieren ist.

(3) Hybrid Cloud

Die Hybrid Cloud ist eine Kombination aus Private und Public Cloud. Dabei wird die private Cloud-Infrastruktur des Nutzers mit der öffentlichen Cloud-Infrastruktur eines externen Public Cloud-Anbieters verbunden. Reichen die Rechen- oder Speicherkapazitäten der Private Cloud nicht aus, kann der Nutzer über gemeinsame, standardisierte oder auch proprietäre Schnittstellen auf die Public Cloud zugreifen. Der Vorteil dieses Modells ist, dass sich das Unternehmen entscheiden kann, sensible Daten und Anwendungen im Kontrollbereich der eigenen Organisation zu belassen, um in Zeiten, in denen mit einem erhöhten Ressourcenbedarf zu rechnen ist, weniger kritische Daten und Anwendungen in die Public Cloud verschieben zu können.[370]

(4) Community Cloud

Die Community Cloud stellt eine Erweiterung des Private-Cloud-Konzeptes dar. Cloud Services werden – wie in der Private Cloud – ausschließlich einem geschlossenen Benutzerkreis zur Verfügung gestellt. Ähnlich einer Einkaufsgemeinschaft setzt sich dieser Benutzerkreis jedoch aus unterschiedlichen, wirtschaftlich und rechtlich unabhängigen Personen zusammen.[371] Community Clouds werden bevorzugt von Unternehmen oder Organisationen genutzt, die aus derselben Branche stammen und ihre jeweiligen Private Clouds miteinander zu einer Community Cloud verbinden.[372]

c. Datenübertragung / Schnittstellen

Um die Nutzung von Cloud Services durch unterschiedliche, räumlich verteilte Nutzer gewährleisten zu können, ist eine einheitliche (d. h. standardisierte) Kommunikation eine notwendige Voraussetzung. Üblicherweise kommen heutzutage Internet-Techniken (WWW-Server, Browser, TCP/IP etc.) zum Einsatz, und zwar unabhängig davon, ob die Kommunikation zwischen Nutzer und Cloud-Betreiber über das Internet (Public Clouds), über das Intranet des Nutzers (v.a. Private Clouds) oder aber über ein sog. Extranet (Erweiterung des Intranets eines Nutzers um Lieferanten, Kunden etc.) stattfindet.[373]

---

[370] Vgl. Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 50.
[371] Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 49.
[372] *Alexander Plaum*, Im siebten Himmel der IT: Was Sie schon immer über die Cloud wissen wollten, abrufbar unter http://community.oreilly.de/blog/2012/04/25/im-siebten-himmel-der-it-was-sie-schon-immer-uber-die-cloud-wissen-wollten/ (letzter Abruf: 28.2.2017).
[373] Vgl. Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 51 ff.

Neben einer standardisierten Kommunikation ist die Kompatibilität der am Datenaustausch beteiligten Systeme wichtig. Darunter versteht man die Möglichkeit des Austausches jeder Art von Daten zwischen den Systemen des Cloud-Anbieters und denen des Nutzers. Hierzu müssen einheitliche Schnittstellen zwischen den Systemen definiert und formale Zusicherungen vorhanden sein. Dies gilt beim Cloud Computing vor allem auch mit Blick auf die Kombination von Cloud Services von unterschiedlichen Anbietern. Wenn Leistungen untereinander nicht kombinierbar sind, weil Schnittstellen unterschiedlich definiert sind, wird das Konzept ad absurdum geführt. Ungeachtet dessen hat sich bis heute noch kein einheitlicher Standard durchgesetzt.[374]

3. Servicemodelle im Cloud Computing

Neben der Betrachtung des (potentiellen) Nutzerkreises hat sich am Markt eine weitere Klassifizierung etabliert, die sich nach Art bzw. Umfang der Cloud Services richtet. Die vorhandenen Geschäftsmodelle („Servicemodelle“) werden grob in vier Modelle unterteilt:[375]

a. „Infrastructure as a Service“ [IaaS]

   Kurzbeschreibung: Bedarfsabhängige Bereitstellung von IT-Ressourcen, insbesondere Rechen-, Speicher-, Kommunikations- und andere Basisressourcen.

Die Dienste ermöglichen es einem Nutzer, *selbst* beliebige Software zu installieren und auszuführen oder Daten zu speichern, ohne die dafür notwendigen Hardwareressourcen direkt zu steuern und zu kontrollieren. Zugriff auf diese virtuellen Services erhält er über breitbandige Netze. Abgerechnet wird nach der tatsächlichen Nutzung oder einem Flat-Tarif. Typische IaaS-Angebote umfassen die Rechner-Hardware, das Netzwerk mit seinen Firewalls und Routern, benutzerspezifische virtualisierte Plattformen und die Dienstgütevereinbarungen (SLA). Die physische Infrastruktur sowie die im Rahmen des Cloud Services genutzten Software-Lizenzen bleiben Eigentum des Cloud-Anbieters und werden lediglich für eine gewisse Zeit zur Nutzung überlassen. Infrastrukturanbieter stellen also die zum Betrieb der Anwendungen benötigen Computing- und Speicherlösungen (das technische „Rückgrat“) bereit, während in Abgrenzung hierzu Serviceanbieter im Rahmen von SaaS-Anwendungen (siehe nachfolgend) Dienstleistungen/Anwendungen betreiben, die einen Wert für ihre Kunden generieren. Dabei greifen sie ggf. auf die Infrastruktur von Infrastrukturanbietern zurück.

b. „Platform as a Service“ [PaaS]

   Kurzbeschreibung: Bereitstellung einer (Entwicklungs-)Plattform.

---

[374] Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 1 Rn. 59 ff.

[375] Vgl. zur Unterteilung: Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 2 Rn. 15; Trusted Cloud (ein Projekt des BMWi): Leitfaden Nr. 3 − Vertragsgestaltung beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), dort S. 14.

Services der Plattformebene ermöglichen es dem Nutzer, mit Hilfe vom Anbieter zur Verfügung gestellter Laufzeit- und Programmierumgebungen zugekaufte oder selbst erstellte Applikationen in der Cloud auszuführen. Folgerichtig sind vor allem Software-Architekten und Anwendungsentwickler die primäre Zielgruppe dieses Angebots.

c. „Software as a Service“ [SaaS]

Kurzbeschreibung: Bereitstellung von (Anwendungs-)Software zur Nutzung.

Der Anbieter stellt dem Nutzer über das Internet eine unmittelbar einsatzbereite Geschäftsanwendung (vollwertige Applikation) zur Verfügung, wobei eine Vielzahl von Nutzern (Mandanten) die gleiche Installation nutzt. Der Betrieb der Software inklusive Wartung, Aktualisierung, Fehlerbehebung und notwendiger Lizensierung von Soft- und Hardware erfolgt vollständig durch den jeweiligen Dienstleister und liegt nicht im Verantwortungsbereich des Nutzers.[376] Die Nutzer können lediglich einzelne Aspekte der Anwendung konfigurieren und so an ihren individuellen Bedarf anpassen.

Vor allem bei hoch komplexen Programmen, bei denen eine umfangreiche Einrichtung des Programms für den jeweiligen Kunden notwendig ist, um sie sinnvoll nutzen zu können, kommt es oft vor, dass letztendlich das konkrete Programmpaket nur einem einzigen Kunden zur Verfügung gestellt wird.[377]

Darüber hinaus gibt es auch Fälle, in denen das Programm doch auf dem Rechner des Kunden (und nicht auf dem des Dienstleisters) abläuft, also zumindest vorübergehend dort geladen wird.[378]

Dem Angebotsspektrum sind keine Grenzen gesetzt. Als Beispiele werden Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.[379]

d. „Business Process as a Service“ [BPaaS]

Kurzbeschreibung: Durchführung von Geschäftsprozessen durch Cloud Computing.

Der Anbieter setzt Software ein, um die vom Kunden vorgegebenen Prozesse durchzuführen bzw. den dadurch beabsichtigten Erfolg herbeizuführen. Zu denken ist etwa an die Erstellung von Gehaltsabrechnungen für Mitarbeiter, die Beschaffung und die Auftragsvergabe sowie die Versendung von E-Mail-Newslettern. Dem Kunden wird dabei nicht eine Software aus der Cloud zur Nutzung zur

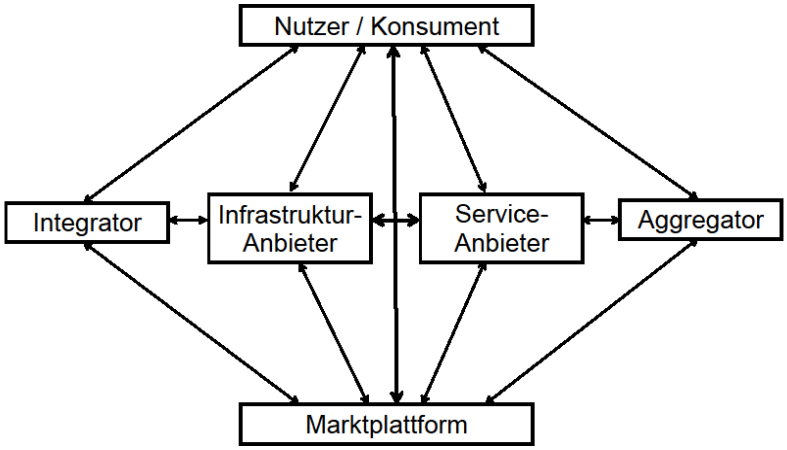
---

[376] Vgl. Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 2 Rn. 32.
[377] Hoeren/Sieber/Holznagel/*Redeker*, Handbuch Multimedia-Recht, Teil 12, Rn. 376.
[378] Hoeren/Sieber/Holznagel/*Redeker*, Handbuch Multimedia-Recht, Teil 12, Rn. 377.
[379] Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 144.

Verfügung gestellt, sondern diese vom Anbieter selbst eingesetzt, um eine vom Kunden definierte Leistung zu erbringen.[380]

4. Akteure (Wertschöpfungsstrukturen)

Das Cloud Computing hat nicht nur mehrere Geschäftsmodelle hervorgebracht, sondern auch neue Wertschöpfungsstrukturen mit unterschiedlichen Akteuren. Die maßgeblichen Akteure und ihre wechselseitigen Beziehungen lassen sich in einer Grafik vereinfacht wie folgt darstellen:



Für die einzelnen Rollen (die teilweise auch kumulativ von einer Person eingenommen werden können) gilt in Anlehnung an die Ausführungen bei Borges/Meents[381] zudem Folgendes:

a. Nutzer / Konsument

Der Konsument (auch als „Kunde“ bezeichnet) kauft Dienstleistungen mittels unterschiedlicher Distributionskanäle, etwa direkt vom Serviceanbieter oder mittels einer Marktplattform.

b. Infrastrukturanbieter

Infrastrukturanbieter stellen die zum Betrieb von Anwendungen benötigten Computing- und Speicherlösungen bereit. Sie bilden somit das „technische Rückgrat“.

c. Serviceanbieter

Serviceanbieter (auch als „Inhaltsanbieter“ oder „Hersteller“ bezeichnet) entwickeln und betreiben Dienstleistungen/Anwendungen, die Wert für ihre Kunden generieren. Dabei greifen sie ggf. auf die Infrastruktur von Infrastrukturanbietern zurück.

---

[380] Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 148.
[381] Borges/Meents/*Krcmar*, Rechtshandbuch Cloud Computing, § 2 Rn. 35 ff.

d. Aggregatoren

Aggregatoren können als spezielle Form eines Serviceanbieters betrachtet werden. Sie bieten durch Aufbereitung und Zusammenstellung neue Dienstleistungen auf Basis der Kombination bereits existierender Dienstleistungen oder Teilen von existierenden Dienstleistungen an. Dementsprechend sind sie beides: Konsument (aus der Perspektive eines Serviceanbieters) und ein Serviceanbieter (aus der Sicht ihrer Kunden).

e. Integratoren

Integratoren nehmen die Anbindung von (neuen) Cloud Services an individuelle Kundensysteme und bestehende Datensammlungen vor. Daneben bieten sie bei Bedarf weiterführende Trainings oder Kundensupport an.

f. Marktplattform-Betreiber

Betreiber einer Marktplattform stellen eine Umgebung bereit, auf der Cloud-Dienstleistungen (IaaS, PaaS, SaaS und/oder BPaaS) gehandelt werden.

5. Ökonomische Bedeutung / Marktentwicklung

Der „Digitalverband“ Bitkom hat im Auftrag der KPMG AG Wirtschaftsprüfungsgesellschaft Anfang 2017 zum sechsten Mal den sog. Cloud-Monitor vorgestellt, der sich mit der Cloud-Nutzung in deutschen Unternehmen befasst.[382] Nach den Ergebnissen dieser Studie, bei der 554 Unternehmen ab 20 Mitarbeitern befragt wurden, setzen mittlerweile zwei von drei Unternehmen (65 Prozent) in Deutschland Cloud Computing ein. Im Vergleich zum Vorjahr ist der Anteil der Cloud-Nutzer in Unternehmen damit von 54 Prozent um 11 Prozentpunkte gestiegen. Im Jahr 2014 waren es erst 44 Prozent. Cloud Computing hat sich damit durchgesetzt und sich innerhalb weniger Jahre zur Basis-Technologie der Digitalisierung entwickelt.

Die zentralen Erkenntnisse fasst die Studie wie folgt zusammen:

Die Cloud-Nutzung in der deutschen Wirtschaft legt erneut kräftig zu, wobei kleine und mittlere Unternehmen bei der Cloud-Nutzung mit den großen gleichziehen.

Insbesondere die Serviceangebote zu Sicherheitslösungen in der Public Cloud sind stärker gefragt. Die deutliche Mehrheit der Unternehmen hält die eigenen Daten in der Public Cloud für sicher. Tatsächlich gibt es auch mehr Sicherheitsvorfälle in den internen IT-Systemen als in der Public Cloud. Allerdings überwachen nicht alle Unternehmen die Public-Cloud-Nutzung und viele verfügen noch nicht über ein umfassendes Sicherheitsmanagement für die Cloud.

---

[382] Zusammenfassung des Cloud-Monitors 2017, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Nutzung-von-Cloud-Computing-in-Unternehmen-boomt.html (letzter Abruf: 30.3.2017); der vollständige Bericht Cloud-Monitor 2017 wird erst im Mai 2017 veröffentlicht.

Wie schon im Cloud-Monitor 2016[383] prognostiziert und durch eine aktuelle Analyse der International Data Corporation (IDC), weltweit führender Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation, bestätigt[384], ist der Cloud-Markt in den letzten Jahren enorm gewachsen und wird weiter wachsen. Die IDC rechnet bei Public-Cloud-Services für 2017 mit einem Umsatzanstieg von über 24 Prozent gegenüber dem Vorjahr, was einem Volumen von 122,5 Milliarden Dollar entspräche. Bis zum Jahr 2020 sei eine durchschnittliche jährliche Zuwachsrate von über 21 Prozent zu erwarten. Der Cloud-Markt würde damit fast sieben Mal so schnell zulegen wie die durchschnittlichen IT-Ausgaben der Unternehmen weltweit. Insbesondere Softwaredienste aus den Bereichen Customer-Relationship-Management (CRM) und Enterprise-Resource-Management (ERM), aber auch Server- und Storage-Services sind beliebt.
Immer weniger Unternehmen können es sich leisten, die Vorteile einer Cloud-Lösung nicht zu nutzen. Unternehmen, die das Potenzial von Cloud Computing nicht ausschöpfen, laufen Gefahr, im Zuge der digitalen Transformation ins Hintertreffen zu geraten. Cloud Computing ist oftmals ein geeignetes und sogar notwendiges Mittel, um die mit anderen Megatrends wie Big Data und Mobility verbundenen Chancen für das eigene Unternehmen zu nutzen.

II. Schuldrechtliche Einordnung des Rechtsverhältnisses zwischen Anbieter und Nutzer

Die praktischen Fragestellungen, die sich im Zusammenhang mit Cloud Computing ergeben, betreffen in erster Linie Art, Umfang und Abwicklung des jeweiligen Cloud Services. Es ergeben sich hieraus neben zivilrechtlichen Aspekten Berührungspunkte zu zahlreichen Rechtsdisziplinen wie etwa

- Datenschutzrecht,[385]
- Urheberrecht,
- Steuerrecht (u.a. bei steuerrechtlich relevanten Daten, §§ 146 ff. AO),[386]

---

[383] Vgl. Cloud-Monitor 2016, abrufbar unter http://hub.klardenker.kpmg.de/cloud-monitor-2016?utm_campaign=Cloud-Monitor%202016&utm_source=AEM, S. 33 (zuletzt abgerufen am 28.2.2017).
[384] Computerwoche 2017-10-11 vom 6.3.2017, S. 6 f.
[385] Siehe hierzu *Hoeren*, in: Skriptum IT-Vertragsrecht, abrufbar unter https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien (Stand Oktober 2016; letzter Abruf: 28.2.2017), S. 364 ff.
[386] Siehe hierzu *Hoeren*, in: Skriptum IT-Vertragsrecht, abrufbar unter https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien (Stand Oktober 2016; letzter Abruf: 28.2.2017), S. 370 ff.

- Arbeitsrecht (u.a. Mitwirkungspflichten nach Betriebsverfassungsgesetz),[387]
- Strafrecht.

Nachfolgend wird mit Blick auf die Vorgaben der Arbeitsgruppe indes nur auf schuldrechtliche Themen/Fragestellungen eingegangen und dabei im Wege eines Problemaufrisses ein besonderes Augenmerk auf die schuldrechtlichen Beziehungen zwischen Anbieter und Nutzer gelegt, denen typischerweise ein – entgeltlicher – (Cloud Computing-)Vertrag zugrunde liegt.

1. Vorbemerkung zur Einordnung auf europäischer Ebene

a. Richtlinienvorschlag der Europäischen Kommission

Der Vorschlag der EU-Kommission für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte [COM(2015) 634 final] erfasst nach Art. 2 RL-E – von wenigen Ausnahmen abgesehen (vgl. Art. 3 Ziff. 4. - 6. RL-E) – alle entgeltlichen Verträge über die Bereitstellung von

a) Daten, die in digitaler Form hergestellt und bereitgestellt werden, darunter Video- und Audioinhalte, Anwendungen, digitale Spiele, sonstige Software;

b) Dienstleistungen, die die Erstellung, Verarbeitung oder Speicherung von Daten in digitaler Form ermöglichen, wenn diese Daten vom Verbraucher bereitgestellt werden; und

c) Dienstleistungen, die die gemeinsame Nutzung der von anderen Nutzern dieser Dienstleistungen in digitaler Form bereitgestellten Daten und sonstige Interaktionen mit diesen Daten ermöglichen.

Folgerichtig fallen auch Vereinbarungen über Cloud-Services grundsätzlich in den Anwendungsbereich der Richtlinie, was in Erwägungsgrund 11 ergänzend klargestellt wird.

Der Richtlinienvorschlag wird gegenwärtig kontrovers diskutiert.[388] Ein zentraler Streitpunkt ist dabei der Verzicht auf eine bestimmte Vertragstypologie. Zwar enthält der Richtlinienvorschlag (zwangsläufig) auch Differenzierungen. So gibt es etwa Sonderregelungen betreffend digitaler Inhalte, die „im Laufe eines Zeitraums bereitgestellt werden“. Die Kommission hat aber ausdrücklich von einer Vertragstypenqualifizierung abgesehen. Der Vorschlag knüpft dementsprechend

---

[387] Siehe hierzu *Hoeren*, in: Skriptum IT-Vertragsrecht, abrufbar unter https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien (Stand Oktober 2016; letzter Abruf: 28.2.2017), S. 372 f.

[388] Siehe hierzu bspw. die Stellungnahme des Bundesrates: BR-Drs. 168/16 (B) sowie die verschiedenen Stellungnahmen aus Anlass der öffentlichen Anhörung im AfRechtVer am 10.5.2016.

rechtssystematisch nicht bei den die verschiedenen Vertragstypen kennzeichnenden Pflichten, sondern vornehmlich daran an, dass ein Vertrag „die Bereitstellung digitaler Inhalte“ zum Gegenstand hat. Der Bundesrat hat sich in den Ziffern 5. und 6. der BR-Drs. 168/16 (B) zu diesem Punkt auszugsweise wie folgt geäußert:

> *„5. Der Bundesrat weist zudem darauf hin, dass ein Vertrag nicht dadurch geprägt wird, auf welches Gut er sich bezieht, sondern dadurch, was mit diesem Gut geschehen soll und welchen wechselseitigen Leistungspflichten sich die Vertragsparteien unterwerfen. Insofern begegnet es grundlegenden Bedenken, dass die vorgeschlagene Richtlinie rechtssystematisch nicht bei den die verschiedenen Vertragstypen kennzeichnenden Pflichten, sondern daran anknüpft, dass ein Vertrag die Bereitstellung digitaler Inhalte zum Gegenstand hat. Damit werden nicht nur Verträge über die dauernde und über die zeitweilige Überlassung standardisierter digitaler Inhalte im Ansatz denselben Regelungen unterworfen, sondern diese Regelungen sollen auch für Verträge über individuell erstellte digitale Inhalte und über Dienstleistungen im Zusammenhang mit digitalen Inhalten gelten. Für verschiedene Vertragstypen – Kaufverträge, Mietverträge, Dienstverträge, Werkverträge und andere Verträge – mit ganz unterschiedlichen Hauptleistungspflichten des Anbieters werden einheitliche Regelungen geschaffen, die nicht auf das jeweils anders ausgestaltete Pflichtengefüge abgestimmt sind. […]*
>
> *6. Grundlegende Probleme sieht der Bundesrat auch mit Blick auf die Umsetzung der vorgeschlagenen Richtlinie in nationales Recht. Das zweite Buch des Bürgerlichen Gesetzbuchs (Recht der Schuldverhältnisse) ist nach Vertragstypen strukturiert und differenziert vom Ansatz her im Wesentlichen gerade nicht nach dem Gegenstand, auf den sich das Vertragsverhältnis bezieht. Eine Umsetzung der vorgeschlagenen Richtlinie durch Schaffung eines Abschnitts, der sich auf die Bereitstellung digitaler Inhalte bezieht, würde sich daher in keiner Weise in die Systematik des BGB einfügen. […]“*

Entgegen früheren Planungen hat die Ratsarbeitsgruppe Zivilrecht (Vertragsrecht) bisher noch keine (partielle) allgemeine Ausrichtung zum Richtlinienentwurf vereinbart. Für das vorliegende Arbeitspapier ist er dennoch vor allem unter zwei Aspekten von besonderer Bedeutung:

Die beabsichtigte Vollharmonisierung würde dazu führen, dass der nationale Gesetzgeber bei der Richtlinienumsetzung nur dort über einen eigenen Spielraum verfügt, wo die Richtlinie einen solchen ausdrücklich eröffnet (Bsp.: Art. 14 Abs. 2 RL-E) oder selbst keine konkrete Regelung trifft (Bsp.: B2B-Verträge). Ausgeschlossen wären demzufolge im Anwendungsbereich der Richtlinie nach gegenwärtigem Stand bspw. – mit Ausnahme von Schadensersatzansprüchen – ergänzende/abweichende Regelungen hinsichtlich der konkreten Ausgestaltung

von Gewährleistungsansprüchen (Abhilfe bei nicht erfolgter Bereitstellung oder Vertragswidrigkeit, vgl. Art. 11 ff. RL-E.).

Fraglich ist, ob die vorgeschlagene Richtlinie (auch) für Cloud Computing-Dienste ein tragfähiges Konzept für einen angemessenen Rechtsrahmen bereitstellt (und damit ggfs. auch außerhalb ihres Anwendungsbereichs ein Vorbild für den nationalen Gesetzgeber sein kann). Dies gilt insbesondere mit Blick darauf, dass die erfassten Verträge eben keinem bestimmten Vertragstyp zugeordnet und erst recht keine neuen Vertragstypen definiert werden. Dabei ist kritisch zu hinterfragen, ob damit zugleich ein Verzicht auf gesetzliche Leitbilder (i. S. v. § 307 Abs. 2 BGB) verbunden ist und deshalb - abseits der nationalen Klauselverbote in §§ 308, 309 BGB - etwaige Leistungsbeschreibungen der Anbieter grundsätzlich Vertragsinhalt werden, soweit sie nur hinreichend transparent i. S. v. Art. 6 RL-E sind.

b. Mitteilung und Konsultationen zur Schaffung einer Europäischen Datenwirtschaft

Als (weiteren) Teil ihrer Strategie für einen Digitalen Binnenmarkt hat die Europäische Kommission am 11. Januar 2017 politische und rechtliche Konzepte vorgestellt, um die „Datenwirtschaft voranzubringen".[389] In der Mitteilung zur Schaffung einer Europäischen Datenwirtschaft[390] erhebt die Kommission den Befund, dass in der EU ein Binnenmarkt für Daten nicht bestehe und das darin liegende Potenzial nicht hinreichend ausgeschöpft werde. Ein freier Datenfluss zwischen Standorten, über Grenzen hinweg und innerhalb eines einheitlichen Datenraums sei nicht möglich. Ursache seien rechtliche und technische Hindernisse, die der Verfügbarkeit und der Nutzung von Daten entgegenstünden. In diesem Zusammenhang stellt die Kommission auch Überlegungen zum Cloud Computing an, etwa unter dem Aspekt der Datenübertragbarkeit zwischen verschiedenen Anbietern. Im Wesentlichen geht es ihr aber zunächst darum, sich ein Bild von den ökonomischen und rechtlichen Auswirkungen zu verschaffen. Zu diesem Zweck hat sie zeitgleich die öffentliche Konsultation zur Schaffung der europäischen Datenwirtschaft sowie die öffentliche Konsultation zur Bewertung der Richtlinie über die Haftung für fehlerhafte Produkte eingeleitet. Die Ergebnisse dieser Konsultationen sollen neben anderen Erkenntnisquellen in eine im Laufe des Jahres 2017 geplante Initiative der Kommission zur europäischen Datenwirtschaft einfließen. Dementsprechend hat die Kommission bisher keine weiteren, über den oben genannten Richtlinienvorschlag für die Bereitstellung digitaler Inhalte hinausgehenden Handlungsempfehlungen ausgesprochen.

---

[389] Pressemitteilung der Europäischen Kommission vom 10.1.2017, abrufbar unter http://europa.eu/rapid/press-release_IP-17-5_de.htm (letzter Abruf: 22.2.2017).

[390] Communication on Building a European Data Economy {SWD(2017) 2 final}, abrufbar unter https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy (letzter Abruf: 22.2.2017).

c. Einordnung von Cloud-Diensten nach der Rom I-VO

Da Cloud-Anbieter und Cloud-Nutzer oft aus unterschiedlichen Ländern interagieren und sich auch die genutzte Hardware häufig an einem vom Anbieter und Nutzer entfernten Standort befindet, stellt sich bei rechtlichen Auseinandersetzungen die Vorfrage, welches Recht materiell berufen ist, um die Streitigkeit zu klären.

Auf europäischer Ebene werden Cloud Computing-Verträge in aller Regel als Dienstverträge nach Art. 4 Abs. 1 lit. b Rom I-VO einzuordnen sein, da der Begriff der Dienstleistung dort wesentlich weiter ausgelegt wird als etwa der Dienstleistungsbegriff des BGB. Für die Frage, welches Recht anwendbar ist, kann die Einordnung aber letztlich dahinstehen. Ist der jeweilige Vertrag als Dienstvertrag i. S. d. Art. 4 Abs. 1 lit. b Rom I-VO einzuordnen, so ist das Recht des gewöhnlichen Aufenthaltsortes des Dienstleisters anwendbar. Lehnt man dies ab, weil man den Cloud-Vertrag als gemischten Vertrag ansieht, wie es im deutschen Recht auch vertreten wird, dann bestimmt sich das anwendbare Recht nach Art. 4 Abs. 2 Rom I-VO, der ebenfalls auf das Recht am gewöhnlichen Aufenthaltsort des Dienstleisters verweist.[391] Wenn der Cloud Nutzer ein Verbraucher ist (B2C), gilt die Besonderheit, dass nach Art. 6 Abs. 1 Rom I-VO das Recht des Staates Anwendung findet, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat.[392]

2. Vertragliche Pflichten / Schuldrechtliche Einordnung

Die bisherigen Ausführungen haben verdeutlicht, dass es vielfältige Arten von Cloud Services gibt, denen eine einheitliche Definition kaum gerecht werden kann. Ratsam aus Sicht beider Parteien eines Vertrages über Cloud Services ist daher eine differenzierte vertragliche Abbildung der konkreten Leistungspflichten und Risikozuordnungen[393]. Zur Bewertung der rechtlichen Rahmenbedingungen für das Cloud Computing nach der gegenwärtigen Rechtslage und zur Ermittlung eines etwaigen Handlungsbedarfs des Gesetzgebers ist darüber hinaus aber auch in den Blick zu nehmen, welche Regelungen das Bürgerliche Gesetzbuch bereits vorsieht und ob bzw. unter welchen Umständen die Vertragsparteien hiervon abweichen können[394].

Die Komplexität und Vielgestaltigkeit der verfügbaren Cloud Services sowie die Vielzahl rechtlicher Fragestellungen, die sich bereits bei einfachstrukturierten Fallkonstellationen ergeben, steht einer vollständigen Aufarbeitung des Themas Cloud Computing unter den gegebenen Umständen entgegen. Die Arbeitsgruppe

---

[391] Borges/Meents/*Borges*, Rechtshandbuch Cloud Computing, § 3 Rn. 17.
[392] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (369).
[393] Vgl. Trusted Cloud: Leitfaden Nr. 3 − Vertragsgestaltung beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), S. 9; siehe hierzu auch unter 1.
[394] Siehe hierzu unter b).

hat sich daher darauf verständigt, zunächst abgrenzbare Ausschnitte auf einen gesetzgeberischen Handlungsbedarf zu untersuchen.

Gegenstände der nachfolgenden Untersuchungen sind daher mit Blick auf die Rechtsbeziehung zwischen Nutzer und (Komplett-)Anbieter und Dienste in einer Public Cloud:

→ Vereinbarungen über „Infrastructure as a Service“[395]

→ Vereinbarungen über „Software as a Service“

→ Vereinbarungen über „Business Process as a Service“

a. Regelungsinhalte

Wichtige Regelungsinhalte bei Verträgen über Cloud Services sind:

- Anwendbares Recht
- Gerichtsstand
- Konkrete Leistungsbeschreibung, einschließlich Qualität der zu erbringenden Leistung
- Einräumung urheber- und patentrechtlicher Nutzungsrechte und Freistellung von etwaigen Ansprüchen Dritter
- Geheimhaltung, Datensicherheit und Datenschutz
- Beachtung von branchenspezifischen regulatorischen Vorgaben (bspw. bei Banken)
- IT-Compliance und IT-Notfallplanung
- Berichtswesen (Monitoring und Reporting)
- Zulässigkeit des Einsatzes von Subunternehmern
- Mitwirkungspflichten des Nutzers
- Rechtsfolgen bei Abweichungen von der vereinbarten Leistung
- Voraussetzungen für Vertragsanpassungen/-änderungen während der Vertragslaufzeit
- Kündigungsmodalitäten (insbesondere Gründe und Fristen)
- Haftungsfragen
- Rechte und Pflichten nach Beendigung des Vertrages[396]

---

[395] Sogenanntes Single Vendor-Modell, vgl. Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 5.

[396] Vgl. Trusted Cloud: Leitfaden Nr. 3 − Vertragsgestaltung beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), S. 32 f.

b. Vertragstypologische Einordnung

(1) Ausgangspunkt

Den Vertragstyp „Cloud Computing“ gibt es nicht. Die anzuwendenden gesetzlichen Vorschriften richten sich daher grundsätzlich danach, wie Verträge über Cloud Services bzw. bestimmte (Teil-)Leistungen in die vorhandene Vertragstypologie des BGB einzuordnen sind. Bereits die aufgezeigte Vielfalt von Cloud Services – insbesondere IaaS, SaaS und BPaaS – deutet dabei auf die Schwierigkeiten hin, abseits von der Beurteilung des konkreten Einzelfalls eine solche Einordnung (allgemeingültig) vorzunehmen. Hinzu kommt aber noch, dass sich selbst hinsichtlich „einfach strukturierter“ Vertragsbeziehungen bisher keine einheitliche Rechtsprechungs- und Literaturmeinung herausgebildet hat.[397]

Cloud Computing-Verträge sind in der Regel Dauerschuldverhältnisse. Die physische Infrastruktur sowie die im Rahmen des Cloud Services genutzten Software-Lizenzen bleiben Eigentum des Cloud-Anbieters (oder dessen Erfüllungsgehilfen) und werden lediglich für eine gewisse Zeit zur Nutzung überlassen.[398] Von dem IT-Outsourcing unterscheidet sich Cloud Computing, insbesondere IaaS, durch die flexiblere Zuordnung physikalischer Ressourcen und die daraus folgende Skalierbarkeit der Leistungen.[399]

Als Vertragstypen des BGB werden zur Anwendung auf Cloud Computing-Verträge, ggf. auch in Form typengemischter oder zusammengesetzter Verträge, allgemein das Werkvertrags-, Dienstleistungs- und Mietvertragsrecht diskutiert.

Eine besondere Notwendigkeit der vertraglichen Einordnung von Cloud Services in die Vertragstypologie ergibt sich bereits aus ihrer Funktion, Lücken im Rahmen der Auslegung bestehender Parteivereinbarungen zu schließen. Darüber hinaus ist die Zuordnung zu einem bestimmten Vertragstyp aber auch von Bedeutung für

- das Auffinden des richtigen Mängelgewährleistungsrechts[400],
- die Identifizierung vertraglich unabdingbarer Rechte und Pflichten (Bsp.: Unabdingbarkeit des Rechts zur außerordentlichen Kündigung nach § 543 Abs. 1 BGB),
- die Identifizierung des gesetzlichen Leitbildes i. S. v. § 307 Abs. 2 BGB im Rahmen einer etwaigen AGB-Kontrolle.[401]

---

[397] Vgl. Trusted Cloud: Leitfaden Nr. 3 − Vertragsgestaltung beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), S. 16 f.
[398] Borges/Meents/*Krcmar,* Rechtshandbuch Cloud Computing, § 2 Rn. 20.
[399] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (783).
[400] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (783).
[401] Vgl. Borges/*Meents,* Rechtshandbuch Cloud Computing, § 4 Rn. 38.

Daneben gilt es, die gesetzlichen Vorgaben zur Inhaltskontrolle von Allgemeinen Geschäftsbedingungen im Blick zu halten. Anbieter von Cloud Services sind in der Regel bemüht, ihre zumeist standardisierten Leistungen (s. o.) in gleichartiger Weise anbieten zu wollen. Sie bedienen sich zu diesem Zweck vorformulierter Vertragsbedingungen, die ggf. an §§ 305 bis 310 BGB zu messen sind.[402] Praxisrelevant und rechtlich problematisch zugleich sind vor allem Klauseln, die folgende Aspekte betreffen:

- Einschränkung der (mietvertraglichen) Erhaltungspflicht;
- Beschränkung und Veränderung des Leistungsgegenstandes;
- Bestätigung der erhaltenen Leistung als vertragsgemäße Leistung;
- Pflicht zur Übernahme von Updates;
- Preisbeschreibende Klauseln;
- Vertragsdauer;
- Voraussetzung und Umfang von Gewährleistungsansprüchen
- Haftungsfragen.[403]

(2) Typengemischte/Zusammengesetzte Verträge

Cloud Computing-Verträge enthalten in der Regel mehrere unterschiedliche Leistungen, die dann in einem typengemischten Vertrag zusammengefasst sind. Die vertragstypologische Einordnung hängt deswegen stark davon ab, welche Leistungen im konkreten vertraglichen Verhältnis vereinbart worden sind.[404] Letztlich sind drei verschiedene Fallkonstellationen zu unterscheiden:

→ Liegt der Schwerpunkt auf einer bestimmten Hauptleistung, die dem Vertrag sein rechtliches und wirtschaftliches Gepräge gibt, und stellen die weiteren Leistungspflichten bloße Nebenabreden dar, setzt sich das Recht der Hauptleistung grundsätzlich durch.

→ Hat der Anbieter mehrere „selbstständige Leistungen“ zu erbringen (Bsp.: Überlassung von Speicherplatz und Hotlineservice), handelt es sich um einen sog. zusammengesetzten Vertrag, bei dem jeder Vertragsteil nach dem

---

[402] Vgl. Trusted Cloud: Leitfaden Nr. 3 − Vertragsgestaltung beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), S. 10.

[403] Vgl. Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 232 ff.; zum letzten Punkt auch *Wicker*, Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787.

[404] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (366).

Recht des auf ihn zutreffenden Vertragstypus zu beurteilen ist, soweit dies nicht im Widerspruch zum Gesamtvertrag steht.[405]

→ Werden die einzelnen Elemente eines Vertrages zu einem eigenen Vertragstyp „verschmolzen", handelt es sich um einen sog. typengemischten Vertrag, bei dem ggf. jede einzelne Pflicht gesondert zu bewerten ist. Nach höchstrichterlicher Rechtsprechung sind in diesen Fällen zumindest bei der Frage von Leistungsstörungen die Regelungen des gesetzlich ausgestalteten Vertragstyps für das zu klärende Rechtsproblem heranzuziehen, der am besten passt.[406]

(3) ASP-Urteil des BGH

Hilfestellung bei der vertragsrechtlichen Einordnung bietet zunächst das sog. ASP-Urteil des BGH aus 2006.[407] Der Entscheidung lag folgende Vertragskonstellation zugrunde:

Die Parteien waren durch einen sog. ASP-Vertrag (Application Service Providing/Bereitstellung von Softwareanwendungen und damit verbundenen Dienstleistungen) verbunden. Hiernach stellte der Anbieter (Kläger) dem Nutzer (Beklagten) auf einem zentralen Server installierte Buchhaltungs- und Warenwirtschaftssoftware zur Nutzung über das Internet zur Verfügung. Der Vertrag umfasste die „Miete der Software incl. Programmpflege, kostenlose Programmupdates, Nutzung bis zu 500 MB Datenvolumen/User, tägliche Datensicherung, Hotlineservice".

Der BGH bestätigte in der genannten Entscheidung die Vorinstanz, auf den zwischen den Parteien abgeschlossenen Vertrag, soweit er auf die unentgeltliche Überlassung von Standardsoftware gerichtet war, Mietvertragsrecht anzuwenden. Bei derartigen ASP-Verträgen stehe die Gewährung der Online-Nutzung von Software für eine begrenzte Zeit im Mittelpunkt der vertraglichen Pflichten. Es liege deshalb nahe, als Rechtsgrundlage für die vertraglichen Ansprüche einen Mietvertrag, der die entgeltliche Gebrauchsüberlassung einer beweglichen oder unbeweglichen Sache zum Gegenstand habe, anzunehmen.

Darüber hinaus ist nach der Auffassung des BGH auch die – im vorliegenden Fall darüber hinaus vereinbarte – Zurverfügungstellung von Speicherkapazitäten auf dem Server des Anbieters zur Speicherung der vom Nutzer im Rahmen der Softwarennutzung eingegebenen Daten mietvertraglich zu qualifizieren.

---

[405] Vgl. dazu auch die nachfolgend erörterte ASP-Entscheidung des BGH, Urt. v. 15.11.2006 − XII ZR 120/04.

[406] Vgl. Trusted Cloud: Leitfaden Nr. 10 − Haftungsrisiken beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf 28.2.2017), dort S. 8; *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (784); siehe hierzu auch die Übersicht bei Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 63.

[407] BGH, Urt. v. 15.11.2006 − XII ZR 120/04.

Zu den übrigen Leistungen führt der Senat hingegen Folgendes aus:

> *„Der Anwendung von Mietvertragsrecht auf die Softwareüberlassung steht auch nicht entgegen, dass in dem ASP-Vertrag weitere Leistungen wie Programmpflege, Programmupdates, Datensicherung, Hotlineservice und Einweisung in die Software vereinbart worden sind, die anderen Vertragstypen (Dienst- oder Werkvertrag) zugeordnet werden können. Insoweit handelt es sich bei dem ASP-Vertrag um einen zusammengesetzten Vertrag, bei dem jeder Vertragsteil nach dem Recht des auf ihn zutreffenden Vertragstypus zu beurteilen ist."*

In der Literatur ist das ASP-Urteil des BGH nicht unwidersprochen geblieben. Gegen die Einordnung als Mietvertrag ist insbesondere eingewandt worden, dass dem Nutzer bei ASP-Verträgen keine Möglichkeit zum tatsächlichen Zutritt zu einer Sache eingeräumt, sondern nur eine bloße Nutzungsmöglichkeit geboten werde.[408]

(4) Literaturmeinungen

Während es insgesamt wenig Rechtsprechung zu Cloud Computing-Verträgen und deren rechtlicher Einordnung gibt, hat sich in der Literatur ein Meinungsbild verfestigt, welches – wohl auch mit Blick auf die eindeutige Positionierung des BGH – in Anlehnung an die ASP-Rechtsprechung auf Cloud Services regelmäßig die Anwendung von Mietrecht vertritt.[409] Nur vereinzelt wird stattdessen (bisher) die Auffassung vertreten, dass Cloud Computing-Verträge eher dem Dienst- oder Werkvertragsrecht unterfallen.[410] Insgesamt ist aber festzustellen, dass einhellig die Auffassung vorzuherrschen scheint, dass es angesichts der vielfältigen Möglichkeiten der Gestaltung des konkreten Cloud Computing-Vertrages schwer fällt, einen Vertrag insgesamt einem bestimmten Vertragstyp zuzuordnen. Vielmehr ist jeder Vertrag im Einzelfall hinsichtlich der vereinbarten Leistungen zu untersuchen, um eine der Vertragsgestaltung und dem Parteiwillen angemessene Einordnung – ggf. auch einzelner Teilleistungen – in die vorhandene Vertragstypologie

---

[408] *Hoeren*, in: Skriptum IT-Vertragsrecht, abrufbar unter https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien (Stand Oktober 2016; letzter Abruf 28.2.2017), dort S. 360.

[409] Vgl. Trusted Cloud: Leitfaden Nr. 3 − Vertragsgestaltung beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), S. 17; für eine mietrechtliche Einordnung im Übrigen auch: LG Mannheim, Urt. v. 7.12.2010 − Az.: 11 O 273/10; Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 45 ff.; *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (785); *Faust*, Digitale Wirtschaft − Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, S. 33 f.; *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (365 f.); Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 152 ff.

[410] Hoeren/Sieber/Holznagel/*Redeker*, Handbuch Multimedia-Recht, Teil 12, Rn. 386 ff.; *Kirn/Müller-Hengstenberg*, Überfordert die digitale Welt der Industrie 4.0 die Vertragstypen des BGB?, NJW 2017, 433 (437 f.).

des BGB vorzunehmen zu können. Sind Gegenstand des Vertrages über Cloud Services mehrere voneinander trennbare Leistungen, sodass es sich um einen typengemischten Vertrag handelt, kann dieser nicht allein einem Vertragstyp zugeordnet werden. Nach höchstrichterlicher Rechtsprechung sind in diesen Fällen zumindest bei der Frage von Leistungsstörungen die Regelungen des gesetzlich ausgestalteten Vertragstyps für das zu klärende Rechtsproblem heranzuziehen, der am besten passt.[411]

Es wird schließlich von keiner Seite die Ansicht vertreten, dass ein neuer Vertragstypus für den Bereich des Cloud Computing geschaffen werden müsse.

III. Vertragstypologische Einordnung der verschiedenen Businessmodelle

Vor dem Hintergrund der bisherigen Ausführungen sollen nunmehr die im Rahmen des Arbeitsgruppenauftrags konkret zu untersuchenden Servicemodelle des Cloud Computings hinsichtlich der Leistungsbeziehung zwischen Anbieter und Nutzer einer näheren Betrachtung unterzogen werden. Soweit möglich sollen die jeweiligen „Reinformen“ bzw. die Fälle, in denen eine den Vertrag prägende Hauptleistung zu ermitteln ist, in die vorhandenen Vertragstypen des BGB eingeordnet werden, um daran anknüpfend erste Anhaltspunkte für ggf. auftretende rechtliche Probleme oder Lücken aufzudecken.

1. IaaS (Infrastructure as a Service)

Mit Blick auf die im BGB normierten Vertragstypen kommt bei näherer Betrachtung nur die Anwendung von Mietrecht oder Dienstvertragsrecht in Betracht. Eine Anwendung von Werkvertragsrecht auf reine IaaS-Dienste scheidet hingegen in der Regel aus, da der Anbieter keinen Erfolg i. S. d. § 631 BGB schuldet. Zu den Grundprinzipien des Cloud Computing gehören nämlich die Ressourcenbündelung durch den Cloud-Anbieter und die Skalierbarkeit des Ressourcenabrufs durch den Nutzer. Daraus folgt für IaaS-Verträge, dass der Nutzer lediglich die Möglichkeit erhält, im vertraglich vereinbarten Umfang die jeweilige Infrastruktur zu nutzen. Eine individuelle Lösung für jeden einzelnen Nutzer, d. h. eine konkret zuzuordnende Leistung im Sinne eines vom Werkunternehmer herzustellenden Werkes, ist hingegen gerade nicht Vertragsgegenstand. Der Anbieter kann vielmehr die Skalierung seiner Ressourcen flexibel ausgestalten. Etwas anderes gilt allenfalls dann, wenn eine individuell angepasste Leistung Vertragsgegenstand ist. In diesen Fällen kann die Vertragsbeziehung ausnahmsweise werkvertragliche Züge aufweisen.

---

[411] Vgl. Trusted Cloud: Leitfaden Nr. 10 − Haftungsrisiken beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), dort S. 8;.*Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (784); siehe hierzu auch die Übersicht bei Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 63.

Nach der gegenwärtigen Rechtslage dürfte national auf IaaS-Verträge Mietrecht anzuwenden sein, auch wenn Deutschland insoweit im europäischen Kontext einen Sonderweg gehen würde, da in anderen EU-Mitgliedsstaaten derartige Verträge als Dienstverträge klassifiziert werden. Bei einem Dienstvertrag nach deutschem Recht ist grundsätzlich nur ein Bemühen geschuldet, was der Bedeutung des Cloud Computing-Vertrags nicht gerecht wird, da der Cloud-Anbieter im Rahmen seiner Leistungen zumindest eine gewisse Art Erfolg schuldet: nämlich den, dass der Cloud Nutzer die bereit gestellte Infrastruktur letztlich auch tatsächlich in Gebrauch nehmen kann und der Anbieter sich nicht nur – ggf. erfolglos – um die Überlassung von Speicherplatz bemüht.

Nach § 535 Abs. 1 BGB genügt es für die Annahme eines Mietvertrages, dass der Vermieter dem Mieter den Gebrauch der Mietsache überlässt. Ohne abweichende Vereinbarung muss er ihm insbesondere keinen Besitz an der Mietsache einräumen. Ausreichend für die Anwendung von Mietrecht kann demzufolge bereits sein, wenn dem Mieter ein Online-Zugang zur Mietsache gewährt wird.[412] Diese Voraussetzungen sind bei einem IaaS-Vertrag im Ergebnis als erfüllt anzusehen. Sein Kern liegt in der Verschaffung der Nutzungsmöglichkeit von IT-Ressourcen, die dem Nutzer zeitweise über das Internet zur Verfügung gestellt werden und die er nutzungsabhängig vergüten muss.[413]

Zumindest im Ergebnis ist es deshalb gerechtfertigt, eine vertragstypologische Einordnung von IaaS-Verträgen als Mietverträge i. S. v. § 535 BGB vorzunehmen, wofür sich letztlich auch das überwiegende Schrifttum (vornehmlich ganz allgemein für Cloud Computing-Verträge) ausspricht.[414] Im Übrigen ist mit Blick auf die oben genannte ASP-Rechtsprechung des BGH zu vermuten, dass sich die Rechtsprechung dem bei Fortgeltung der bestehenden Rechtslage anschließen wird. Bisher ist allerdings kein Urteil öffentlich geworden, das sich vertieft mit dieser Problematik befasst hat.

2. SaaS (Software as a Service)

a. Vorbemerkung: Urheberrechtliche Einordnung

Die Nutzung von SaaS wirft zwangsläufig auch urheberrechtliche Fragen auf. Dies gilt insbesondere für die Abgrenzung und die Zurechnung urheberrechtlich relevanter Handlungen. Zugleich ist die urheberrechtliche Bewertung aber auch

---

[412] Vgl. BGH, Urt. v. 15.11.2006 − XII ZR 120/04, unter Hinweis auf das Urteil vom 28.10.1992 − XII ZR 92/91 − zur Nutzung der Kapazitäten eines Großrechners über „Fernzugang“.

[413] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 46.

[414] *Faust*, Digitale Wirtschaft − Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, S. 33; a.A. *Kirn/Müller-Hengstenberg*, Überfordert die digitale Welt der Industrie 4.0 die Vertragstypen des BGB?, NJW 2017, 433 (437 f.).

ein wichtiger Aspekt bei der vertragsrechtlichen Einordnung von Vereinbarungen über SaaS.[415]

(1) Zugang zur SaaS in der Cloud

Für etwaige auf dem Rechner des Nutzers lokal installierte Software, die ihm den Zugriff auf die Cloud-Services und damit auf die SaaS erst ermöglicht (Browser, Client-Software des Anbieters oder Applet), benötigt er entsprechende Rechte.[416] Bei der Speicherung von der SaaS vorgeschalteter Zugangssoftware auf dem Nutzer-Rechner handelt es sich nämlich um eine Vervielfältigung, für die es nach § 69c Nr. 1 UrhG der Zustimmung seitens des Rechteinhabers des Programms bedarf. Dieses Nutzungsrecht betreffend den Zugang zur Cloud ist jedoch abgekoppelt von den Rechten betreffend die eigentliche Nutzung der angebotenen SaaS selbst. Ist es Teil der Vereinbarung, handelt es sich folgerichtig um eine (vertragliche) Zusatzleistung, die nicht den SaaS-Dienst an sich betrifft.

(2) Urheberrechtlich relevante Inhalte innerhalb von SaaS

Urheberrechtlich relevant werden kann ferner das Hoch- und Herunterladen von Inhalten in oder aus der betreffenden Anwendung, die als SaaS genutzt wird, etwa bei Fotos von Ansprechpartnern, wenn ein Kontaktdatenbankmanagement Gegenstand der SaaS ist. Hier stellen sich jedoch keine spezifisch die SaaS betreffenden urheberrechtlichen Fragen betreffend das Verhältnis zwischen Anbieter und Nutzer. Der Nutzer muss für den Inhalt, den er in die SaaS innerhalb der Cloud hochlädt, die Rechte besitzen, ohne dass den Anbieter eine Kontroll- oder Überwachungspflicht träfe. Die Vervielfältigung im Arbeitsspeicher des Nutzers zur Betrachtung von (z. B. vom Anbieter hochgeladenen) Inhalten, an denen Urheberrechte Dritter bestehen, sind von der Schranke des § 44a UrhG gedeckt.[417]

(3) Nutzung von SaaS innerhalb der Cloud

Grundsätzlich keiner besonderen Zustimmung durch den Rechteinhaber bedarf hingegen die Nutzung der bereitgestellten SaaS durch den Nutzer. Folgerichtig muss der Anbieter dem Nutzer auch in der Regel keine Nutzungsrechte an der bereitgestellten SaaS übertragen, um den SaaS-Vertrag zu erfüllen.

- Schon die Voraussetzungen einer Vervielfältigung i. S. v. § 69c Nr. 1 UrhG sind auf Seiten des Nutzers üblicherweise nicht gegeben.

  Bei der Nutzung der eigentlichen SaaS werden Teile der Software zwar „auf Veranlassung des Nutzers“ in den Arbeitsspeicher des Anbieter-Servers geladen und damit vervielfältigt i. S. d. § 69c Nr. 1 UrhG.[418] Der BGH

---

[415] Vgl. *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3.
[416] Hilber/*Paul/Niemann*, Handbuch Cloud Computing, Teil 3, Rn. 85.
[417] Hilber/*Paul/Niemann*, Handbuch Cloud Computing, Teil 3, Rn. 128.
[418] Hilber/*Paul/Niemann*, Handbuch Cloud Computing, Teil 3, Rn. 91; Wandtke/Bullinger/*Grützmacher*, Praxiskommentar zum Urheberrecht, § 69c Rn. 5.

stellt jedoch eine rein technische Betrachtung an, nach der derjenige vervielfältigt, der die körperliche Festlegung technisch bewerkstelligt und kontrolliert.[419] Dies zugrunde gelegt ist es in aller Regel der Anbieter, dem die Vervielfältigung zuzurechnen ist, nicht der Nutzer. Letzterer hat standardmäßig keine Kontrolle darüber, welche Software-Teile gespeichert werden und vor allem, wo die Speicherung konkret stattfindet. Wenn dies ausnahmsweise anders sein sollte, wäre die Vervielfältigung aber ohnehin auch von § 69d Abs. 1 UrhG gedeckt, da es sich insoweit um eine bestimmungsgemäße Nutzung der SaaS innerhalb der Cloud handelt.[420]

- Soweit während der Nutzung Speicherungen im Browser-Cache, im Cache der Client-Software und/oder im Arbeitsspeicher des Nutzers zum Zwecke der Darstellung der Inhalte stattfinden, handelt es sich ebenfalls nicht um urheberrechtlich relevante Vervielfältigungshandlungen des Nutzers.[421] Der Gegenstand dieser Vervielfältigungen ist nicht „die Software" in dem Sinne, dass ein Programmcode an den Nutzerrechner übertragen würde, sondern lediglich die Benutzeroberfläche. Diese genießt nach der Rechtsprechung des Europäischen Gerichtshofs (EuGH) keinen Schutz nach den §§ 69a ff. UrhG.[422] Für einen Schutz nach § 2 UrhG dürfte es der im Browser-Cache oder Arbeitsspeicher des Nutzers vervielfältigten Benutzeroberfläche zudem im Regelfall an der Schöpfungshöhe fehlen.[423]

- Die Erstellung von Backups im Rahmen von SaaS wird, wie oben dargestellt, durch den Anbieter innerhalb seiner Infrastruktur und nicht durch den Nutzer vorgenommen. Einer Nutzungsrechteeinräumung gegenüber dem Nutzer bedarf es daher nicht. Diese Vervielfältigungshandlung seitens des Anbieters ist von § 69d Abs. 2 UrhG gedeckt.[424]

- Eine Verbreitung der Software nach § 69c Nr. 3 UrhG findet bei SaaS-Diensten nicht statt, da die Vorschrift lediglich Software in körperlicher Form (auf einem Datenträger oder als Download[425]) erfasst.[426]

---

[419] BGH, Urt. v. 22.4.2009 − I ZR 216/06, CR 2009, 598.
[420] Vgl. Hilber/*Paul/Niemann*, Handbuch Cloud Computing, Teil 3, Rn. 141.
[421] Für Browser-Caching EuGH, Urt. v. 5.6.2015 − Rs. C 360/13, CR 2014, 594; für die Speicherung im Arbeitsspeicher Wandtke/Bullinger/*Grützmacher*, Praxiskommentar zum Urheberrecht, § 69c Rn. 5.
[422] EuGH, Urt. v. 22.12.2010 − Rs. C-393/09, CR 2011, 221; vgl. zum Meinungsstand Wandtke/Bullinger/*Grützmacher*, Praxiskommentar zum Urheberrecht, § 69a Rn. 14.
[423] Hilber/*Paul/Niemann*, Handbuch Cloud Computing, Teil 3, Rn. 97.
[424] Hilber/*Paul/Niemann*, Handbuch Cloud Computing, Teil 3, Rn. 147 f.
[425] Vgl. hierzu EuGH, Urt. v. 3.7.2012 − Rs. C 128/11, CR 2012, 498 (Usedsoft).
[426] Wandtke/Bullinger/*Grützmacher*, Praxiskommentar zum Urheberrecht, § 69c Rn. 34 ff.

b. Vertragstypologische Einordnung

Die schon zur vertragstypologischen Einordnung von IaaS-Verträgen herangezogenen Grundsätze, die der BGH in seiner ASP-Entscheidung aufgestellt hat, lassen sich auch auf die Cloud-Leistung SaaS übertragen: Der Nutzer greift über Datenleitungen auf die auf den Systemen des Anbieters installierte Software zu, um sie über seinen Client-Rechner für eine bestimmte Zeit zu nutzen.[427] Dies bedeutet in letzter Konsequenz, dass auch auf diese Vertragsbeziehungen Mietvertragsrecht anzuwenden ist.

Als problematisch erweist sich – analog zur ASP-Entscheidung – zwar, dass das Mietrecht des BGB nach dem Wortlaut des § 535 Abs. 1 BGB von der Miete einer Sache (§ 90 BGB) ausgeht. Der BGH hat jedoch bereits mehrfach entschieden, dass eine auf einem Datenträger verkörperte Standardsoftware wie eine bewegliche Sache zu behandeln ist. Er zieht insofern den Vergleich zu einem Buch, das als Ergebnis einer schöpferischen Geistestätigkeit allein wegen seines Inhalts, nicht wegen seines Informationsträgers, dem Papier, erworben wird. Die Software befindet sich bei SaaS zwar schwer lokalisierbar in der Cloud, dennoch ist sie irgendwo auf einem Datenträger verkörpert. Durch ein Steuerungsprogramm werden die virtuellen Komponenten einer physischen Ressource zugeordnet, sodass die Voraussetzungen der Körperlichkeit der Sache letztlich erfüllt sind.[428] Da der Mietvertrag zudem keine Besitzverschaffung, sondern lediglich eine Gebrauchsüberlassung voraussetzt, ist es unerheblich, dass der Nutzer lediglich Zugang und nicht alleinige Verfügungsgewalt erhält.[429]

Soweit vereinzelt vertreten wird, dass (auch „reine“) SaaS-Verträge dienstvertraglich einzuordnen sind, da als Leistung geschuldet werde, dass das zur Nutzung überlassene Programm auch ordnungsgemäß abläuft und der Nutzer nur das Programm, nicht aber seine konkrete Verkörperung nutzen wolle (weshalb man nicht von einer Sachmiete ausgehen könne)[430], wird dem zu Recht entgegengehalten, dass dies nicht zielführend ist. Beim Dienstvertrag wird grundsätzlich keinerlei Art von Erfolg, sondern lediglich ein Bemühen hinsichtlich der Leistungserbringung geschuldet. Dies entspricht aber in der Regel nicht dem erkennbaren Interesse des Cloud-Nutzers, der die Leistung des Anbieters tatsächlich – ordnungsgemäß – nutzen können will.[431] Nach dem allgemeinen Verständnis von Cloud-Services sollte der Anbieter zudem grundsätzlich jederzeit in der Lage sein, die vom Nutzer gewünschten Ressourcen zur Verfügung zu stellen, da die Cloud schließlich nur virtuell existiert. Der Cloud-Anbieter ist keinen Einschränkungen

---

[427] Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 152.
[428] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 47.
[429] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (786).
[430] Hoeren/Sieber/Holznagel/*Redeker*, Handbuch Multimedia-Recht, Teil 12, Rn. 387, 391.
[431] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (784); Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 53.

unterworfen, da er selbst stets neue Ressourcen nutzbar machen kann. Dies spricht ebenfalls gegen die Annahme, dass sich der Anbieter bei SaaS-Verträgen lediglich darum „bemühen“ muss, die geschuldete Leistung zu erbringen.[432]

Trotz der vorstehend beschriebenen Erfolgsorientierung wird in der Regel auch nicht in Betracht kommen, auf reine SaaS-Verträge Werkvertragsrecht anzuwenden. Der Anbieter stellt üblicherweise kein nutzerspezifisches Werk her, sondern stellt „lediglich“ eine standardisierte Leistung für mehrere Cloud-Nutzer zur Verfügung. Eine werkvertragliche Einordnung würde zudem zu sehr auf eine aktive Tätigkeit des Cloud-Anbieters abstellen. Dieser ist jedoch stattdessen nur verpflichtet, die Services zum Abruf bereitzuhalten. Weitergehende Tätigkeiten schuldet der Cloud-Anbieter in der Regel nicht.[433] Daher kann allenfalls in Einzelfällen, in denen der Cloud-Anbieter dem Nutzer eine an dessen konkrete Bedürfnisse angepasste IT-Leistung oder die Herstellung einer individuellen Software schuldet, von einem werkvertraglichen Charakter auszugehen sein.[434]

Klarzustellen ist, dass die vorstehenden Ausführungen nur eingeschränkt auf Zusatzleistungen im Rahmen eines Cloud Computing-Vertrages übertragen werden können. Dies gilt etwa für die Vereinbarung von Support- oder Beratungsleistungen.[435] Hier kommt durchaus – etwa über die Grundsätze des zusammengesetzten Vertrages – auch die Anwendung von Dienstvertragsrecht in Betracht. Entsprechendes gilt für die Zurverfügungstellung des Clienten, die werkvertraglichen Charakter haben kann. Bei diesen Leistungen handelt es sich aber nicht um Cloud-Services im eigentlichen Sinn, sondern eben um Zusatzvereinbarungen.[436]

3. BPaaS (Business Process as a Service)

Die wesentliche Leistung bei Cloud-Diensten des Business Process as a Service besteht zumeist in einer einmaligen oder wiederholten Rechenleistung, bei der es aus Sicht des Nutzers darauf ankommt, eine richtige Berechnung als Ergebnis des Datenverarbeitungsprozesses zu erhalten. Hierbei ist wohl davon auszugehen, dass ein konkreter Erfolg mit der Folge geschuldet wird, dass eine Vereinbarung

---

[432] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR, 2012, 783 (784); ebenso Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 53.

[433] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 54; *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (786).

[434] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 54; *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (786).

[435] Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 167.

[436] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (784), siehe hierzu auch die Definitionen des Cloud Computing unter D. I. 1.

mit werkvertraglichem Charakter vorliegt und damit grundsätzlich Werkvertragsrecht nach §§ 631 ff. BGB zur Anwendung kommt.[437] Es handelt sich dann nämlich nicht um den Fall, dass der Anbieter die Software an den Nutzer „vermietet", sondern er nutzt diese selbst, um das geschuldete Ergebnis herbeizuführen. Das setzt voraus, dass der Nutzer keinen (vollen) Zugriff auf die Software hat und damit den von ihm angestrebten Erfolg nicht selbst herbeiführen könnte.[438] Letzteres wäre ein Fall des klassischen SaaS.

Ebenfalls als Werkvertrag ist einzustufen, wenn es der Anbieter gemäß dem genannten Beispiel übernimmt, E-Mail-Newsletter zu versenden oder sonstige Leistungen zu erbringen, die aus Sicht des Nutzers einen messbaren Erfolg voraussetzen, weil die eingekauften Leistungen für ihn ansonsten nutzlos wären.[439]

4. Einordnung übriger Vertragsleistungen

Wie bereits angesprochen, haben Cloud Computing-Verträge regelmäßig neben der Bereitstellung von Software und/oder Hardware weitere Leistungen zum Gegenstand, die für sich betrachtet je nach Art der Leistung und Ausgestaltung im Einzelfall dienst- oder werkvertraglich einzuordnen sind. Sofern der Schwerpunkt des Vertrages in einer typischerweise mietvertraglich einzuordnenden IT-Leistung besteht und die Zusatzleistungen als mietvertragliche Nebenleistungen qualifiziert werden können, ist der gesamte Vertrag einheitlich nach Mietrecht zu beurteilen. Etwas anderes gilt jedoch, wenn sich die Leistungen nicht als mietvertragliche Nebenpflichten qualifizieren lassen. Dann sind sie separat vertragstypologisch einzuordnen, und zwar je nach Einzelfallanalyse.[440]

5. Erleichterung vertragstypologischer Zuordnung durch Einfügung eines „§ 453 Abs. 1 BGB" ins Mietrecht

Die wesentliche Kritik an der vertragstypologischen Einordnung von Cloud Computing-Vereinbarungen als Mietvertrag zielt darauf ab, dass nach § 535 Abs. 1 BGB nur körperliche Sachen Gegenstand eines Mietvertrages sein können, eine Sachqualität (§ 90 BGB) des Vertragsgegenstandes beim Cloud Computing jedoch abgelehnt wird. Diesem Ansatz kann man mit den Grundsätzen der bereits angeführten Rechtsprechung des BGH zur Qualifizierung von Software als Sache begegnen. Die vertragstypologische Einordnung ließe sich jedoch erleichtern, wenn eine dem § 453 Abs. 1 BGB[441] entsprechende Regelung ins Mietrecht eingefügt wird, mit der klargestellt wird, dass die Vorschriften über die Miete einer

---

[437] So auch Kompentenzzentrum Trusted Cloud, Leitfaden Nr. 10, - Haftungsrisiken beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), Rn. 14.
[438] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 61.
[439] Vgl. dazu insgesamt Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 164 f.
[440] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 57 ff.
[441] § 453 Abs. 1 BGB lautet: „Die Vorschriften über den Kauf von Sachen finden auf den Kauf von Rechten und sonstigen Gegenständen entsprechende Anwendung."

Sache auch für die Miete sonstiger Gegenstände entsprechende Anwendung finden.[442] Dann käme es auf die Abgrenzung zwischen „unkörperlichen“ und verkörperten Datenmengen nicht mehr an. Insbesondere mit Blick auf Lizenzverträge sind insoweit allerdings Friktionen mit dem Urheberrecht zu vermeiden, etwa indem die Regelung nur sonstige Gegenstände – und nicht auch Rechte – erfasst.

6. Zwischenergebnis

Die überwiegenden Gründe sprechen dafür, mit der mehrheitlichen Auffassung in der Literatur die hier in Rede stehenden Vertragsbeziehungen IaaS und SaaS grundsätzlich als Mietvertrag einzuordnen, während es sich bei BPaaS-Verträgen üblicherweise um Werkverträge handeln dürfte.

Gleichwohl hängt die Einordnung im Einzelfall angesichts der Komplexität und der Vielgestaltigkeit von Cloud Computing-Verträgen stets davon ab, welcher Leistungsgegenstand bzw. welche Leistungsgegenstände konkret dem jeweiligen Vertrag zugrunde liegen. Zudem ist danach zu differenzieren, ob „nur“ eine Hauptleistung vereinbart ist (ggf. flankierend durch unselbstständige Nebenpflichten) oder verschiedene Leistungspflichten gleichwertig nebeneinander stehen, die jeweils einem auf sie passenden Vertragstypus zuzuordnen sind.

Vor diesem Hintergrund wird nachfolgend unter verschiedenen Aspekten erörtert, welche Folgen sich aus der (unterschiedlichen) vertragstypologischen Einordnung ergeben können und welche Probleme ggf. daraus erwachsen. Dies dient dazu, etwaigen gesetzgeberischen Handlungsbedarf auszuloten. Zugleich wird damit – auch mit Blick auf die insoweit fehlende Rechtsprechung – insbesondere den kritischen Stimmen in der Literatur Rechnung getragen, die eine Anwendbarkeit des Mietrechts/Werkvertragsrechts ablehnen und stattdessen Cloud Computing-Verträge dem Dienstvertragsrecht unterwerfen wollen.

IV. Untersuchung einzelner Aspekte unter Zugrundelegung einer vertragstypologischen Einordnung als Miet-, Dienst- oder Werkvertrag

1. Pflichten der Vertragsparteien

Welche rechtlichen Pflichten die Vertragsparteien – vorbehaltlich einer abweichenden Vereinbarung – kraft Gesetzes treffen, hängt von der vertragstypologischen Einordnung des konkret geschuldeten Cloud Service ab.

a. Mietvertrag

Die Hauptleistungspflicht des Cloud-Anbieters (Vermieters) besteht bei Anwendung von Mietvertragsrecht darin, dem Cloud-Nutzer (Mieter) den Cloud Service

---

[442] *Faust*, Digitale Wirtschaft − Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, S. 34; ob das Mietrecht einen geeigneten Rechtsrahmen bietet, wird unter IV. erörtert.

während der Dauer des Vertrages in einem zum vertragsgemäßen Gebrauch geeigneten Zustand „bereitzustellen“ (Grundsatz der ständigen Verfügbarkeit).[443] Der Cloud-Anbieter schuldet die Möglichkeit der Inanspruchnahme des Service. Die Übergabepflicht des Cloud-Anbieters ist erst erfüllt, wenn der Cloud-Nutzer die Leistungen vertragsgemäß in Anspruch nehmen kann.[444]

Der Cloud-Anbieter kann und muss allerdings keinen Einfluss auf die Internetverfügbarkeit des Cloud-Nutzers nehmen. Die Verfügbarkeit des Internets fällt in die eigene Risikosphäre des Cloud-Nutzers. Die Verantwortlichkeit des Cloud-Anbieters beginnt erst, wenn der Cloud-Nutzer auf sein Angebot zugreift.[445]

Gemäß § 535 Abs. 1 S. 2 BGB hat der Cloud-Anbieter den Cloud Service zudem während der gesamten Vertragslaufzeit in einem vertragsgemäßen Zustand zu erhalten. Der Cloud-Nutzer hat nämlich ein Interesse daran, die Services permanent fehlerfrei nutzen zu können. Eine solche dauerhafte Verfügbarkeit kann aber auf der anderen Seite aufgrund zeitweise notweniger Wartungsarbeiten eingeschränkt werden, weshalb die Parteien oftmals vertraglich – individuell oder über AGBs – Verfügbarkeitsquoten festlegen (z. B. 95%), um so zu erwartende Systemunterbrechungen zu berücksichtigen.[446] Für den Fall erforderlicher Wartungsleistungen für die Sicherstellung der Funktionsfähigkeit ist der Cloud-Anbieter durch die mietrechtlichen Vorschriften bereits ausreichend abgesichert. Die Umstände, die dem Cloud-Nutzer im Zusammenhang mit der Instandhaltung entstehen, fallen nicht unter das Gebot der ständigen Verfügbarkeit, sodass ein dadurch begründeter Ausfall vom Nutzer hingenommen werden muss.[447]

In der Literatur wird die Frage nicht einheitlich beantwortet, ob zur Erhaltungspflicht des Cloud-Anbieters auch die Durchführung von Modernisierungs- oder Aktualisierungsmaßnahmen gehört.[448]

Weiterhin wird im Zusammenhang mit der Erhaltungspflicht die Frage aufgeworfen, ob und inwieweit der Abschluss eines separaten Pflegevertrages im Sinne einer weiteren Hauptleistungspflicht sinnvoll oder notwendig ist. Typische Regelungsinhalte eines solchen Pflegevertrags sind die Beseitigung von Fehlern, die Fortentwicklung der bereitgestellten Software, die Pflicht, jeweils den aktuellen Standard bereitzustellen sowie die Verpflichtung zur Einrichtung einer Hotline.

---

[443] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (716); Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 71.

[444] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 73.

[445] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (787).

[446] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 76.

[447] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (787).

[448] Zustimmend Hoeren/Sieber/Holznagel/*Redeker*, Handbuch Multimedia-Recht, Teil 12, Rn. 408; verneinend Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 77, der grds. nur eine technische Leistung auf dem Stand des Vertragsschlusses für geschuldet erachtet.

Während einige der Leistungen eines solchen Pflegevertrages wohl von der mietvertraglichen Erhaltungspflicht umfasst sind – und somit auch nicht extra vergütet werden müssten –, gehen andere Leistungen darüber hinaus und sind dann auch ggf. eher dienst- oder werkvertraglich einzuordnen.[449]

Auch den Cloud-Nutzer treffen vertragliche Pflichten: Neben der Hauptleistungspflicht, die in der Zahlung der vereinbarten Vergütung besteht, hat der Cloud-Nutzer zahlreiche Mitwirkungspflichten, die es dem Cloud-Anbieter erst ermöglichen, seinen Vertrag ordnungsgemäß zu erfüllen.[450] Abgesehen von der Auswahl einer seinen Bedürfnissen entsprechenden Cloud-Lösung und der Mitteilung ggf. vorhandener Sicherheitsvorkehrungen oder technischer Besonderheiten, muss er bspw. die Daten in einer verarbeitungsfähigen Form übermitteln, seine Firewall und den Virenschutz auf dem Stand der Technik erhalten sowie Login-Informationen nebst Passwörtern geheim halten.[451] Soweit diese Pflichten nicht bereits vertraglich geregelt sind, lassen sie sich aus §§ 241, 242 BGB herleiten.[452] Zudem muss er Fehler unverzüglich anzeigen, § 536c Abs. 1 BGB.[453]

Aus Sicht der Vertragsparteien ist es zudem sinnvoll, eine Funktionsprüfung zu vereinbaren, da dem Mietrecht eine Abnahmepflicht fremd ist. Angesichts der soeben beschriebenen Pflichten des Nutzers dürfte auch eine entsprechende Klausel in Allgemeinen Geschäftsbedingungen zulässig sein.[454]

b. Dienstvertrag

Der Cloud-Anbieter hat bei einem dienstvertraglich einzuordnenden Cloud-Service lediglich mit Blick auf den versprochenen Service tätig zu werden, ohne dass ein definierter Leistungserfolg geschuldet ist. Dies entspricht jedoch – wie bereits ausgeführt – bei den üblichen Cloud Computing-Verträgen nicht den Interessen des Cloud-Nutzers, der die bereitgestellten Dienste letztlich auch tatsächlich nutzen will und nicht nur ein - ggf. erfolgloses - Bemühen des Cloud-Anbieters erwartet.

c. Werkvertrag

Beim Werkvertrag schuldet der Cloud-Anbieter die Herstellung des versprochenen Werks, mithin einen Erfolg, welcher von den Vertragsparteien vertraglich festzulegen ist.[455] Da Cloud-Leistungen in der Regel standardisiert sind und nicht auf den einzelnen Nutzer „zugeschnitten“ werden, kommt eine werkvertragliche

---

[449] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 80.
[450] Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 214.
[451] Kompetenzzentrum Trusted Cloud Leitfaden Nr. 3 − Vertragsgestaltung beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), Rn. 58 ff.
[452] Kompetenzzentrum Trusted Cloud, Leitfaden Nr. 10 − Haftungsrisiken beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), Rn. 66.
[453] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 69.
[454] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 75.
[455] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 82.

Einordnung i. S. d. Herstellung eines bestimmten Werks nur ausnahmsweise – wie bspw. für den Bereich des BPaaS – in Betracht.

d. Vertragsänderungen/-anpassungen

Ein Problemfeld eröffnet sich noch in Bezug auf die Frage, ob und inwieweit während der Vertragslaufzeit Vertragsanpassungen oder -änderungen vorgenommen werden können. Insbesondere die technische Fortentwicklung des Angebotes kann ein Interesse des Anbieters begründen, auf eine Änderung der geschuldeten Leistungen hinwirken zu können. Stimmt der Nutzer einer solchen Änderung im konkreten Einzelfall nicht zu, bedarf es hierfür eines einseitigen Änderungsrechts. Ein solches Recht ist im Mietrecht bisher nicht vorgesehen. Der Richtlinienentwurf der EU-Kommission „Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte" [COM(2015) 634 final] sieht in Art. 15 ein solches Änderungsrecht vor. Danach soll der Anbieter unter bestimmten Voraussetzungen seine vertraglich geschuldete Leistung (einseitig) ändern dürfen. Der Nutzer erhält im Gegenzug ein außerordentliches Kündigungsrecht. Allerdings ist hierfür eine Voraussetzung in Art. 15 RL, dass die Parteien die Möglichkeit vereinbart haben, dass der Anbieter den Vertrag einseitig ändern darf. Insofern enthält der Richtlinienvorschlag keine wesentliche Neuerung zum deutschen Recht. Einigen sich die Parteien auf einen Änderungsvorbehalt, darf der Anbieter in den vertraglich vereinbarten Grenzen eine Änderung des Vertrages herbeiführen. Für die Bestimmung der geänderten Leistung gilt § 315 BGB. Grenzen für die formularmäßige Vereinbarung eines einseitigen Änderungsvorbehalts setzt § 308 Nr. 4 BGB. Danach ist die Vereinbarung eines Rechts des Verwenders, die versprochene Leistung zu ändern oder von ihr abzuweichen, in Allgemeinen Geschäftsbedingungen unwirksam, wenn nicht diese unter Berücksichtigung der Interessen des Verwenders für den anderen Vertragsteil zumutbar ist.

2. Leistungsstörungen

Wie bei jedem Vertrag stellt sich auch beim Cloud Computing die Frage, wie mit Leistungsstörungen umzugehen ist. Dies gilt auch mit Blick auf mögliche Schäden, zu denen es beim Cloud Computing kommen kann. Insbesondere Verfügbarkeitslücken, Datenverlust und Sicherheitslücken können beim Cloud-Nutzer zu erheblichen finanziellen Nachteilen führen.[456]

Verfügbarkeitslücken können den Cloud-Nutzer selbst dann schädigen, wenn sie nur temporär sind. Dies ist insbesondere der Fall, wenn ein Nutzer in seinem Geschäft von der ständigen Nutzung der IT abhängt und dadurch Gewinnausfälle i. S. d. § 252 BGB entstehen.[457]

---

[456] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (716).

[457] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (715).

Sicherheitslücken (Schutz vor unberechtigtem Zugriff/Datensicherheit/Sicherheitsmanagement: Firewall, Verschlüsselung, Authentifikation/Geheimhaltung, Datensicherheit und Datenschutz) können beim Cloud-Nutzer einen Schaden hervorrufen, etwa indem sie Unbefugten ermöglichen, in schlecht gesicherte Cloud-Server einzudringen und auf Daten des Nutzers zuzugreifen. Werden diese Daten Dritten zugänglich gemacht, könnte Unternehmens-Knowhow abfließen, der Nutzer Ansprüchen Dritter ausgesetzt sein oder gar sein Bild in der Öffentlichkeit geschädigt werden.[458]

Steigt ein Unternehmen vollständig auf die Cloud-Nutzung um und hält keine eigenen IT-Ressourcen mehr vor, gehört der Verlust der Daten in der Cloud zu den verhängnisvollsten Ereignissen. Hierzu kann es ausreichen, dass die Daten beschädigt werden und daher nicht mehr ausgelesen werden können. Typisches Beispiel ist aber auch die Zerstörung des Cloud-Servers einschließlich der darauf gespeicherten Daten.[459]

Je nach vertragstypologischer Einordnung der geschuldeten Leistung können unterschiedliche Gewährleistungsrechte zur Anwendung kommen.

a. Mietrecht

Gemäß § 535 Abs. 1 S. 2 BGB hat der Vermieter dem Mieter die Mietsache in einem zum vertragsgemäßen Gebrauch geeigneten Zustand zu überlassen und sie während der Mietzeit in diesem Zustand zu erhalten. Verletzt der Cloud-Anbieter diese Pflicht, stehen dem Cloud-Nutzer die mietvertraglichen Gewährleistungsrechte zu.[460] Er schuldet gemäß § 536 BGB nur eine geminderte Miete (Vergütung), kann unter den Voraussetzungen von § 536a Abs. 1 BGB Schadenersatz verlangen und ggf. gemäß § 543 BGB den Vertrag kündigen.

Voraussetzung ist das Vorliegen eines Sach- oder Rechtsmangels, der die Tauglichkeit der Mietsache zum vertragsgemäßen Gebrauch aufhebt oder nicht nur unerheblich mindert (§ 536 Abs. 1 BGB). Hat der geschuldete Cloud-Service die Bereitstellung von Software zum Gegenstand, ist zwischen anfänglichen Mängeln, die bereits bei der Bereitstellung des Service vorliegen, und nachträglichen Mängeln zu unterscheiden. Software-Mängel sind typischerweise anfängliche Mängel, die sich erst nach Vertragsschluss zeigen.[461] Nachträgliche Mängel können bspw. durch Änderungen (z. B. durch Parametrisierung), durch neue Softwareversionen oder durch Änderungen der Umgebungsbedingungen, wie z. B. Gesetzesänderungen oder Währungsumstellungen, entstehen.

---

[458] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (715).
[459] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (715).
[460] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 85.
[461] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 87.

Ein nachträglicher Mangel kommt auch dann in Betracht, wenn der gebuchte Cloud-Service nicht mehr im vereinbarten Umfang verfügbar ist. Zur Feststellung, ob diese Nichtverfügbarkeit einen Mangel darstellt, sind einerseits vertraglich vereinbarte Verfügbarkeitsquoten zu berücksichtigen und andererseits in die Betrachtung einzubeziehen, dass Ausfallzeiten wegen Instandhaltung nicht unter das Gebot der ständigen Verfügbarkeit fallen (s. o.).

Ein Rechtsmangel liegt vor, wenn der Cloud-Nutzer die Services aufgrund des Rechts eines Dritten ganz oder teilweise nicht nutzen kann (z. B. Urheberrechte, Patente, Marken- und Titelschutzrechte).[462]

Der Cloud-Nutzer hat den Mangel unverzüglich anzuzeigen. Unterlässt er dies, läuft er Gefahr, seine Gewährleistungsansprüche zu verlieren.

Soweit ein Mangel bereits vor Vertragsschluss oder vor erstmaliger Annahme der Mietsache vorgelegen haben sollte, sind die Rechte des Nutzers nach § 536b BGB ausgeschlossen, wenn er den Mangel kannte oder aufgrund von grober Fahrlässigkeit nicht kannte. Diese Konstellation dürfte aber oftmals keine Anwendung finden, da der Nutzer im Gegensatz zum Mieter einer haptischen Sache keinen Einblick in die Geschäftsvorgänge des Cloud-Anbieters haben wird.

Der Cloud-Anbieter hat den Mangel zu beseitigen. Zwar kennt das Mietrecht grundsätzlich keine Nachlieferung. Bei Softwareverträgen ist es aber üblich, dass im Falle eines Mangels neue Softwarestände geliefert werden.[463] Für die Dauer der Mangelbeseitigung – wobei fraglich ist, binnen welcher Zeitspanne diese zu erfolgen hat – steht dem Cloud-Nutzer ein Zurückbehaltungsrecht bezüglich der restlichen Vergütung gemäß § 320 BGB zu.[464]

Nach § 536a BGB hat der Cloud-Anbieter dem Cloud-Nutzer sämtliche Schäden zu ersetzen, die auf einem Mangel beruhen, den der Cloud-Anbieter zu vertreten hat. Dies sind vor allem kurzfristige Kosten für Ersatzbeschaffung von IT, der Verlust des Datenbestandes selbst und Folgeschäden wie der Gewinnausfall des Cloud-Nutzers.[465] Eine Vermögenseinbuße durch Datenverlust ist vom Tatrichter zu schätzen.[466] § 249 Abs. 2 S. 1 BGB umfasst hierbei auch die Herstellungskosten für einen gelöschten Datensatz.[467]

Soweit der Mangel nicht bereits bei Vertragsschluss vorlag, sondern erst im Nachhinein entstanden ist, haftet der Cloud-Anbieter nach § 276 Abs. 1 BGB für Vorsatz und Fahrlässigkeit und nach § 278 Abs. 1 BGB für seine Subunternehmer als

---

[462] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 88.
[463] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 90.
[464] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 92.
[465] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (716).
[466] BGH, Urt. v. 9.12.2008 − VI ZR 173/07, Leitsatz.
[467] BGH, Urt. v. 9.12.2008 − VI ZR 173/07, Leitsatz.

Erfüllungsgehilfen.[468] Grundsätzlich obliegt zwar die Beweislast für die Voraussetzungen des Schadensersatzanspruchs dem Cloud-Nutzer, doch trifft die Beweislast des Vertretenmüssens den Cloud-Anbieter als Vermieter.[469] Den Cloud-Anbieter trifft demnach ein hohes Risiko.[470]

Auch mit Blick auf die verschuldensunabhängige Haftung für anfängliche Mängel gemäß § 536a Abs. 1 Alt. 1 BGB trifft den Cloud-Anbieter ein hohes Risiko. Diese Haftung gilt nämlich auch dann, wenn der Mangel den Parteien bei Vertragsschluss nicht bekannt ist, sondern sich erst später offenbart, bspw. wenn der Cloud-Anbieter Drittsoftware einsetzt, auf deren Fehleranfälligkeit er keinerlei Einfluss hat.[471] Sinn und Zweck des Cloud Computing ist es aber, die Daten in die Obhut des Anbieters zu geben. Das hier beschriebene Risiko ist dem Anbieter daher grundsätzlich zuzumuten.

Im Falle der Nichterreichbarkeit des Cloud-Service kann einzelvertraglich oder über AGB bereits im Vorfeld Klarheit darüber geschaffen werden, wie eine mögliche Haftung, insbesondere bspw. pauschalierter Schadensersatz, ausfallen soll.[472] Die Vertragspartner können aber individualvertraglich weitgehende Haftungsbeschränkungen vereinbaren, solange diese nicht gänzlich hinter das gesetzliche Leitbild des Mietrechts zurückfallen.[473] Da aber im Rahmen des Cloud Computing individualvertragliche Vereinbarungen eher die Ausnahme darstellen, dürfte im Ergebnis diese Frage stets in den AGB der Anbieter angesprochen werden.[474] Insofern stellt sich hier die Aufgabe einer AGB-Kontrolle, wobei zum einen zu prüfen wäre, ob und, wenn ja, in welchem Umfang die Vereinbarung einer Nichterreichbarkeit zulässig sein könnte, und zum anderen, ob und, wenn ja, in welchem Umfang eine Pauschalierung des Schadenersatzes möglich wäre.

Bei Vorliegen eines wichtigen Grundes steht es jeder Partei frei, das Vertragsverhältnis außerordentlich zu kündigen (§ 543 Abs. 1 S. 1 BGB). Ein wichtiger Grund kann aus Sicht des Cloud-Nutzers vor allem die vollständige oder teilweise Nichtgewährung, die nicht rechtzeitige Gewährung sowie der nachträgliche Entzug der Nutzungsmöglichkeit des Cloud-Service sein. Ein Verschulden ist nicht erforderlich.[475]

---

[468] A.A. wohl *Kirn/Müller-Hengstenberg,* Überfordert die digitale Welt der Industrie 4.0 die Vertragstypen des BGB?, NJW 2017, 433 (436).
[469] BGH in st. Rspr., u.a. NJW 2000, 2344; NJW 2009, 142.
[470] So auch *Wicker,* Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (716).
[471] Borges/*Meents,* Rechtshandbuch Cloud Computing, § 4 Rn. 94, 114.
[472] *Wicker,* Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (787).
[473] *Wicker,* Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787 (787).
[474] *Wicker,* Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787 (787).
[475] Borges/*Meents,* Rechtshandbuch Cloud Computing, § 4 Rn. 98.

Der im Mietrecht grundsätzlich verankerte Anspruch des Cloud-Nutzers auf Selbstbehebung des Mangels und anschließende Geltendmachung des Ersatzes der hierzu erforderlichen Aufwendungen dürfte beim Cloud Computing keine wesentliche Relevanz haben, da das Recht zur Selbstvornahme in der Regel technische Schwierigkeiten bereiten dürfte, da der Cloud-Nutzer üblicherweise keinen Zugriff auf die Verwaltung der Systeme hat.[476]

b. Dienstvertragsrecht

Sind Cloud Services dem Dienstvertragsrecht zuzuordnen, schuldet der Cloud-Anbieter die Erbringung der vertraglich zugesagten Leistung (§ 611 Abs. 1 BGB). Bei Leistungsstörungen haftet er allein nach den allgemeinen Vorschriften (§§ 280 ff. und §§ 323 ff. BGB). Schadensersatz hat er demnach nur zu leisten, wenn er die Leistungsstörung zu vertreten hat (§ 280 Abs. 1 S. 2 BGB). Das Dienstvertragsrecht kennt keine speziellen Mängelrechte, insbesondere kein Minderungsrecht.

Bei Nichtleistung wirkt sich dies im Ergebnis jedoch nicht in relevanter Weise aus, denn die Vergütung ist grundsätzlich erst nach Leistungserbringung geschuldet (§ 614 BGB), sodass der Cloud-Nutzer keine Vergütung zahlen muss, wenn der Cloud-Anbieter die Leistung nicht erbringt. Darüber hinaus kann der Vertrag von jeder Vertragspartei aus wichtigem Grund gekündigt werden.[477]

Hingegen wirkt sich mit Blick auf eine etwaige Schlechtleistung (zum Nachteil des Nutzers) aus, dass im Dienstvertragsrecht kein besonderes Leistungsstörungsrecht normiert ist. Anders als im Mietrecht gibt es etwa keine Regelung, wonach sich im Falle einer Schlechtleistung die geschuldete Gegenleistung grundsätzlich verschuldensunabhängig mindert. Den Vertragsparteien wird daher angeraten, den Umfang der konkreten Cloud-Leistungen in qualitativer und quantitativer Hinsicht detailliert zu beschreiben, um so Pflichtverletzungen feststellen zu können. Selbst dann kann es aber für den Nutzer mühsam und aufwendig sein, den konkreten und kausal durch den Service-Level-Verstoß verursachten Schaden zu beweisen. Als Lösung werden hierzu die Vereinbarung von Schadenspauschalen diskutiert oder auch die Einbehaltung oder Minderung der Vergütung (ggf. als pauschalierte Minderung). Individualvertraglich ist dies jedenfalls aushandelbar.[478] Die Lösung einer pauschalierten Minderung böte dem Nutzer zudem den Vorteil, ggf. zusätzlich einen Schaden geltend machen zu können. Soweit eine pauschalierte Minderung in AGBs geregelt ist, ist deren Zulässigkeit mit Blick auf § 307 Abs. 1 BGB noch nicht geklärt. Unter der Annahme, dass die AGBs vom Cloud-Anbieter als Verwender vorgelegt werden, dürften einer pauschalierten Minderung als für den Nutzer vorteilhafter Regelung aber wohl keine Bedenken entgegenstehen.[479]

---

[476] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 102.
[477] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 104.
[478] Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 225.
[479] Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 225 (Fn. 1).

Vor diesem Hintergrund ist nachvollziehbar, dass der 71. Deutsche Juristentag für das Dienstvertragsrecht die Einführung eines Minderungsrechts gefordert hat.[480] Mit Blick auf das Cloud Computing wird dies jedoch nur relevant, wenn man – entgegen des hier vertretenen Ansatzes – Dienstvertragsrecht auf entsprechenden Vereinbarungen anwendet.

c. Werkvertragsrecht

Beim Werkvertrag hat der Cloud-Anbieter die vertraglich vereinbarte Leistung frei von Sach- und Rechtsmängeln herzustellen (§ 633 Abs. 1 BGB). Verletzt er diese Pflicht, stehen dem Cloud-Nutzer die werkvertraglichen Gewährleistungsrechte zu (§§ 634 ff. BGB), die allerdings erst ab Abnahme des Werks geltend gemacht werden können (§ 640 BGB). Bis zu diesem Zeitpunkt hat der Cloud-Nutzer einen Erfüllungsanspruch auf Herstellung des versprochenen mangelfreien Werks, sodass der Cloud-Anbieter nach den allgemeinen Vorschriften (§§ 280 ff. und §§ 323 ff. BGB) haftet. Ferner ist der Cloud-Nutzer berechtigt, den Vertrag bis zur Vollendung des Werks jederzeit zu kündigen (§ 649 BGB), wobei der Cloud-Anbieter die vereinbarte Vergütung verlangen kann.

Es ist fraglich, ob die werkvertraglichen Mängelrechte grundsätzlich dem Interesse des Cloud-Nutzers entsprechen. Er könnte Nacherfüllung (§ 634 Nr. 1 i. V. m. § 635 BGB) verlangen, vom Vertrag zurücktreten (§ 634 Nr. 3, 1. Alt. i. V. m. §§ 636, 323 und § 326 Abs. 5 BGB), die Vergütung mindern (§ 634 Nr. 3, 2. Alt. i. V. m. § 638 BGB) oder Schadensersatz (§ 634 Nr. 4, 1. Alt. i. V. m. §§ 636, 280, 281, 283 und § 311a BGB) bzw. Aufwendungsersatz (§ 634 Nr. 3, 2. Alt. i. V. m. § 284 BGB) verlangen.

Der Rücktritt, der grundsätzlich auf Verträge mit einem einmaligen Leistungsaustausch ausgerichtet ist, erscheint bei auf Dauer angelegten Cloud Computing-Verträgen nicht sinnvoll. Eine Kündigungsmöglichkeit wäre deshalb insoweit passender. Eine solche kommt nur nach § 314 Abs. 1 BGB bei Vorliegen eines wichtigen Grundes in Betracht, wobei ggf. die Regelung des § 314 Abs. 2 S. 1 BGB zu beachten ist (im Falle einer Verletzung einer Vertragspflicht ist die Kündigung erst nach Ablauf einer zur Abhilfe bestimmten Frist oder nach erfolgloser Abmahnung zulässig).[481]

Die Bemessung der Höhe einer Minderung oder eines Schadensersatzanspruchs bereitet selbst bei unstreitigen Leistungsstörungen der Cloud Services Schwierigkeiten. Schließlich dürfte – BPaaS-Vereinbarungen ausgenommen – das Recht zur Selbstvornahme nach einer erfolglosen Fristsetzung zur Nacherfüllung in der Regel wenig sinnvoll bis unmöglich sein, da der Cloud-Nutzer keinen Zugriff auf die dafür benötigte Infrastruktur hat. Es bestünde die Möglichkeit, das Selbstvornahmerecht vertraglich auszuschließen, da eine vertragliche Einschränkung der Mängelrechte grundsätzlich zulässig ist, soweit der Unternehmer den Mangel

---

[480] Ziffer A. IV. 22. d. des Beschluss der zivilrechtlichen Abteilung, abrufbar unter http://www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf (letzter Abruf: 22.2.2017).
[481] Borges/*Meents,* Rechtshandbuch Cloud Computing, § 4 Rn. 84.

nicht arglistig verschwiegen oder eine Garantie für die Beschaffenheit des Werks übernommen hat (§ 639 BGB).[482]

Zusammenfassend ist festzustellen, dass die Anwendung des werkvertraglichen Gewährleistungsrechts für „typische“ Cloud Computing-Verträge schon wegen deren Dauerschuldcharakter nur bedingt sinnvoll erscheint. Soweit die vertraglich geschuldete Leistung jedoch auf einen konkreten Erfolg ausgerichtet ist (wie etwa bei BPaaS-Diensten), führen die werkvertraglichen Gewährleistungsvorschriften zu einem angemessenen Interessenausgleich.

3. Haftung

Bei der Nutzung von Cloud Computing-Leistungen können dem Cloud-Nutzer durch verschiedene Szenarien erhebliche finanzielle Nachteile drohen, sei es bspw. durch den Verlust der gespeicherten Daten oder den vorübergehenden Ausfall der Verfügbarkeit der zugesagten Leistungen.

a. Haftungsbeschränkung in AGB

Ausgangspunkt für Haftungsfragen sind für gewöhnlich die gesetzlich normierten Grundlagen. Im Rahmen des Cloud Computing werden diese aber in der Regel durch Standard-Vertragsklauseln des Cloud-Anbieters ersetzt bzw. modifiziert, die naturgemäß häufig anbieterfreundlich ausgestaltet sind und dem Nutzer wenig Wahlfreiheit belassen.[483] Die Anbieter versuchen dadurch, ihre Haftung für Schäden soweit wie möglich auszuschließen oder zumindest Haftungsobergrenzen in den Vertrag einzuziehen.[484] Insofern wird bei Haftungsfragen im Streitfall in der Regel eine AGB-Kontrolle durchzuführen sein.

Eine vollkommene Freizeichnung von Schäden aufgrund der Verletzung einer vertragswesentlichen Kardinalspflicht ist aber ausgeschlossen.[485] Solche Kardinalpflichten dürften bei Cloud Computing-Verträgen die Datensicherheit und die Datenverfügbarkeit sein. Ein vollständiger Haftungsausschluss für fahrlässigen Datenverlust, fahrlässige Datenbeschädigung oder die Nichtverfügbarkeit von Daten dürfte daher unzulässig sein.[486] Da die Haftungsbeschränkungen mithin

---

[482] Vgl. zu allem Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 108 f., 116.
[483] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (370).
[484] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (370); *Wicker*, Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787 (787).
[485] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (374).
[486] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (375); *Wicker*, Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787 (788).

zum Schutz des Verbrauchers eingeschränkt sind, sind häufig haftungsbeschränkende AGB unwirksam.[487]

Insofern bleibt zu prüfen, ob eine Haftungsbegrenzung nach Schadensarten, also z. B. für Folgeschäden wie Gewinnausfall, wirksam ausgeschlossen werden kann. Eine Haftungsfreizeichnung dürfte hierbei nicht in Betracht kommen, da eine solche den Cloud-Nutzer unangemessen benachteiligen würde und deshalb nach § 307 Abs. 1 S. 1 und Abs. 2 BGB unwirksam ist. Für den Cloud-Anbieter ist aber eine Begrenzung auf typischerweise vorhersehbare Schäden trotz der Verletzung einer wesentlichen Pflicht nach § 307 Abs. 2 Nr. 2 BGB durch einfaches fahrlässiges Verhalten möglich.[488] Die Problematik liegt hier aber darin festzustellen, welche Pflichten wesentlich und welche Schäden typisch sind. Problematisch ist die Frage der Haftungsbegrenzung für den Cloud-Anbieter insofern, als dass er keine Kenntnis über die Art und Wertigkeit der in der von ihm zur Verfügung gestellten Cloud eingestellten Daten hat.

Fraglich ist, ob angesichts der durch das AGB-Recht eingeschränkten Möglichkeiten einer gerechten Risikoverteilung zwischen den Vertragsparteien eine Änderung des AGB-Rechts diskussionswürdig ist. Dies gilt insbesondere vor dem Hintergrund, dass internationale Cloud-Angebote hinsichtlich des AGB-Rechts häufig größere Freiräume bieten. Teilweise wird in der Literatur gefordert, die gesetzlichen Regelungen dahingehend zu präzisieren, dass bei einer Inhaltskontrolle das Motivationsgefälle zwischen den Parteien, das bei einem Vertragsschluss unter Einbeziehung einseitig vorformulierter Klauseln typischerweise zu beobachten ist, stärker Berücksichtigung findet.[489]

Es dürfte hingegen sinnvoller sein, angesichts zukünftiger Entwicklungen im Bereich des Cloud Computing zunächst einmal die Entwicklung der Rechtsprechung insoweit abzuwarten. Abgesehen davon können auch bei Verwendung von AGB praxisnahe Lösungen eine interessengerechte Risikoverteilung gewährleisten, wie sich aus den folgenden Ausführungen zum Mitverschulden des Cloud-Nutzers ergibt.

b. Mitverschulden des Nutzers

Die Datensicherung fällt grundsätzlich in den Risikobereich des Cloud-Nutzers. Die Nichterfüllung der eigenen Pflicht zur Datensicherung kann daher im Rahmen eines Mitverschuldens nach § 254 BGB Berücksichtigung finden.[490] Hierbei ist

---

[487] *Wicker*, Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787 (787), unter Verweis auf LG Berlin, MMR 2014, 563, das die Unwirksamkeit von AGB von Google festgestellt hat.

[488] *Wicker*, Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787 (788).

[489] Vgl. *Wicker*, Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787 (789).

[490] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (718).

indes zu berücksichtigen, dass es das Geschäftsmodell des Cloud Computing ist, IT-Ressourcen auf Dritte auszulagern. Neben der weltweiten Verfügbarkeit bietet gerade die Einsparung von Speicherplatz einen Anreiz, Cloud Computing-Verträge abzuschließen. Das Erfordernis einer täglichen Datensicherung ließe das Geschäftsmodell daher weitgehend ins Leere laufen.[491] Auf der anderen Seite lässt sich aber argumentieren, dass Cloud Computing lediglich die Bereitstellung von IT-Ressourcen von Kauf auf Miete per Internet verschiebt, sodass es keine Kollision bedeutet, den Cloud-Nutzer zur Verwendung weiterer IT-Ressourcen zu verpflichten. Auch beim Kauf eines PC muss der Nutzer mithilfe weiterer Speichermedien eine Backup-Strategie haben.[492]

c. Haftung des Cloud-Nutzers

Während – mit Ausnahme der Vergütung – die vertragliche Hauptleistung naturgemäß vom Anbieter erbracht wird, sind dem Nutzer typischerweise vertragliche Mitwirkungs- und Nebenpflichten auferlegt, deren Verletzung Schadensersatzansprüche des Anbieters begründen können. Sie ergeben sich aus dem konkreten Inhalt der Parteivereinbarung oder werden aus allgemeinen Grundsätzen (§§ 241, 242, 280 BGB) hergeleitet. Ein denkbares Szenario ist etwa die (unbewusste) Installation von Schadsoftware durch den Nutzer, die eine Betriebsstörung der vom Anbieter bereitgestellten Cloud verursacht.[493]

d. Durchsetzbarkeit

Während der Cloud-Anbieter für seine fehlende Verantwortung für Schäden beweispflichtig ist, muss der Cloud-Nutzer beweisen, dass ein Mangel, eine Pflichtverletzung oder eine Rechtsgutsverletzung vorlag und jeweils auch mit hinreichender Kausalität zu einem Schaden geführt hat. Die Feststellung des Schadensverlaufs und der Beweis der Kausalität können aber mit erheblichen Schwierigkeiten verbunden sein, da sich sämtliche diesbezüglichen Informationen im Herrschaftsbereich des Cloud-Anbieters befinden.[494] Dem Cloud-Anbieter wird demnach eine erweiterte Darlegungslast zukommen. Problematisch bleibt aber die Pflicht des Cloud-Nutzers, einen Schaden konkret darzulegen und zu beweisen. An dieser Hürde dürften viele Schadenersatzansprüche scheitern.[495] Welchen Wert hatten z. B. die unwiederbringlich gelöschten Urlaubsfotos des Nutzers?

---

[491] *Boehm*, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (379).

[492] *Wicker*, Haftungsbegrenzung des Cloud-Anbieters trotz AGB-Recht? Relevante Haftungsfragen in der Cloud, MMR 2014, 787 (790).

[493] Vgl. Kompetenzzentrum Trusted Cloud, Leitfaden Nr. 10 − Haftungsrisiken beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), S. 23 ff. − auch zu Haftungstatbeständen im Verhältnis zu Dritten.

[494] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (717).

[495] *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (717).

4. Laufzeit / Beendigung

Wie auch bei der Frage nach den Hauptleistungspflichten und den Gewährleistungsregeln kommt es auch für die Frage der Beendigung des Cloud Computing-Vertrages auf die typologische Einordnung des konkreten Vertrages an.

a. Mietrecht

Im Falle der Anwendung mietrechtlicher Regelungen gilt hinsichtlich der Beendigung von Verträgen über Cloud Services grundsätzlich Folgendes:

- Ist der Vertrag befristet, endet er mit Ablauf der vereinbarten Frist (§ 542 Abs. 2 BGB).
- Vereinbaren die Parteien keine Frist, kann jede Partei mit der gesetzlichen Kündigungsfrist nach § 580a BGB kündigen (§ 542 Abs. 1 BGB).
- Liegen die Voraussetzungen des § 543 BGB vor, besteht ein Recht zur außerordentlichen Kündigung. Dazu müsste einer der Gründe des Katalogs aus § 543 BGB vorliegen oder eine Tatsache aus dem Risikobereich des Cloud-Nutzers das Festhalten am Vertrag für den Cloud-Anbieter unzumutbar machen.
- Weitere Beendigungstatbestände sind der Abschluss eines Aufhebungsvertrages (§ 311 BGB), der Eintritt einer zuvor vereinbarten Bedingung, Rücktritt (§ 346 BGB), Unmöglichkeit, Anfechtung und Wegfall der Geschäftsgrundlage (§ 313 BGB).[496]

Der Tod einer Vertragspartei führt hingegen nicht zur Beendigung eines Vertrages über Cloud Services. Hier dürfte vielmehr der erbrechtliche Grundsatz der Universalsukzession (§ 1922 BGB) gelten.

Als problematisch erweist sich die Frage der Kündigungsfrist:

Soll ein Cloud Computing-Vertrag beendet werden, dürfte der Nutzer ein erhebliches Interesse daran haben, einen gewissen Zeitrahmen zur Verfügung gestellt zu bekommen, um einen neuen Vertragspartner zu suchen. Zum einen wäre es ihm nicht zuzumuten, von heute auf morgen den Markt zu recherchieren und einen passenden neuen Anbieter zu finden. Zum anderen sollte er auch nicht die Gefahr von Imageeinbußen oder Gewinneinbrüchen tragen müssen, wenn er auf seine Daten nicht mehr zugreifen kann. Die Kündigungsvorschriften des gewerblichen Mietrechts bieten nach der geltenden Rechtslage in dieser Konstellation den besten Schutz, da die Kündigungsfrist des § 580a Abs. 2 BGB von drei Monaten dieses Risiko am besten abzufangen vermag. Falls die Parteien durch eine kürzere Frist hinreichend geschützt sein würden, wäre auch eine solche nach

---

[496] Vgl. Palandt/*Weidenkaff*, BGB, § 542 Rn. 1 ff.

§ 580a Abs. 1 BGB möglich.[497] Kritisch ist jedoch zu sehen, dass diese Regelungen auf Cloud Computing-Verträge allenfalls analog anzuwenden sein dürften und sich insofern möglicherweise auch eine analoge Anwendung der deutlich kürzeren Fristen in § 580a Abs. 3 BGB rechtfertigen ließe. Aufgrund der fundamentalen Bedeutung eines Kündigungsrechts sollte aber das Gesetz für alle Konstellationen klare Regelungen vorhalten. Soweit ersichtlich, ist von den Gerichten bisher noch nicht entschieden worden, ob und inwieweit eine entsprechende Anwendung von § 580a BGB zulässig ist.

Eine Einordnung der jeweiligen Cloud-Leistung unter die einzelnen Regelungen des § 580a BGB ist selbst bei einer formularvertraglich vereinbarten Kündigungsfrist erforderlich, da nach § 307 BGB der Ausschluss des ordentlichen Kündigungsrechts zu Lasten des Mieters ebenso unzulässig ist wie eine Verkürzung der gesetzlich vorgesehenen Frist.[498]

Es bedarf daher einer gesetzlichen Klarstellung zur anwendbaren Kündigungsfrist. Diese könnte sich ggf. an den Regelungen in Art. 16 Abs. 1 und 2 RL-E[499] orientieren, der sich hinsichtlich B2C-Verträgen mit dem Kündigungsrecht des Verbrauchers befasst.

b. Dienstvertrag

Dienstvertraglich einzuordnende Cloud Services können nach Maßgabe der §§ 621 ff. BGB durch jede Vertragspartei gekündigt werden, wenn die Vertragsdauer weder bestimmt noch aus der Beschaffenheit oder dem Zweck der Dienste zu entnehmen ist (§ 620 Abs. 2 BGB). Je nach Bemessung der Vergütung kann die Kündigungsfrist einen Tag bis zu sechs Wochen betragen (§ 621 BGB).

Sämtliche Regelungen können vertraglich abbedungen werden. Bei Verbraucherverträgen (und auch im Verhältnis zwischen Unternehmern) ist allerdings § 309 Nr. 9 BGB zu beachten.

Bei befristeten Dienstverträgen kommt vor Laufzeitende nur eine außerordentliche Kündigung nach §§ 626, 627 BGB in Betracht. Dieses Recht ist auch nicht dispositiv.

---

[497] Vgl. dazu auch *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (787); Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 217.

[498] Hilber/*Intveen/Hilber/Rabus*, Handbuch Cloud Computing, Teil 2, Rn. 360; Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 217.

[499] Diese lauten: Abs.1: „Sollen die digitalen Inhalte dem Vertrag zufolge unbefristet bereitgestellt werden oder beträgt die erstmalige Laufzeit des Vertrags oder betragen dessen Verlängerungen zusammengenommen mehr als 12 Monate, ist der Verbraucher berechtigt, den Vertrag jederzeit nach Ablauf des ersten 12-Monats-Zeitraums zu beenden.“ Abs. 2: „Der Verbraucher übt sein Recht auf Vertragsbeendigung durch eine auf beliebige Weise abgegebene Mitteilung an den Anbieter aus. Die Beendigung des Vertrags wird 14 Tage nach Eingang der Mitteilung wirksam.“

Ein Rücktrittsrecht wird mit dem Zeitpunkt der Überlassung der dienstvertraglich geschuldeten Leistung durch das Kündigungsrecht ersetzt.

c. Werkvertrag

Werkvertraglich einzuordnende Cloud Services können jederzeit vom Cloud-Nutzer bis zur Vollendung des Werks gekündigt werden (§ 649 S. 1 BGB), wobei auch diese Regelung abdingbar ist.

Der BGH hat die Anwendbarkeit von § 649 S. 1 BGB im Falle eines Internet-System-Vertrages (bei einer Mindestvertragslaufzeit von 36 Monaten) bejaht.[500] Er hat die in Rechtsprechung und Literatur vertretene Auffassung, nach der bei Werkverträgen mit fortgesetzter Erbringung von Werkleistungen für unbestimmte Dauer § 649 S. 1 BGB keine Anwendung finden solle und stattdessen die Möglichkeit einer ordentlichen Kündigung unter Einhaltung einer angemessenen Kündigungsfrist bestehe, für *nicht unbedenklich* gehalten, wenn dadurch das Kündigungsrecht nach § 649 S. 1 BGB ausgeschlossen würde. Denn dieses könne nur ausgeschlossen werden, wenn der Unternehmer über die Realisierung seines Vergütungsanspruchs hinaus ein berechtigtes Interesse an der Ausführung der Vertragsleistung habe und dieses Interesse durch eine jederzeitige freie Kündigung in einer ihm nicht zumutbaren Weise beeinträchtigt werden würde. Nach Ansicht des BGH soll daher weder die Vereinbarung einer Mindestlaufzeit noch die Festlegung eines (allein) außerordentlichen Kündigungsrechts durch die Parteien ausreichen, um die Rechte des Nutzers nach § 649 S. 1 BGB auszuschließen.

Im Gegensatz zu miet- oder dienstvertraglich einzuordnenden Cloud Services kann bei Anwendung werkvertraglicher Regelungen - neben der Kündigung nach § 314 Abs. 1 BGB - auch während der Vertragsdurchführung der Rücktritt vom Vertrag erklärt werden, wenn der Cloud Service mangelhaft ist (§§ 634 Nr. 3, 636, 323 bzw. § 326 Abs. 5 BGB).[501] Die Wirkungen des Rücktrittsrechts sind bei langfristigen Cloud Computing-Verträgen allerdings ungeeignet und entsprechen nicht den Parteiinteressen. Erklärt eine Partei den Rücktritt vom Vertrag, wandelt sich der Vertrag in ein Rückgewährschuldverhältnis (§ 346 BGB) um. Der Cloud-Nutzer ist verpflichtet, die empfangenen Leistungen zurückzugewähren und die gezogenen Nutzungen herauszugeben, wozu er in der Regel nicht in der Lage sein wird, sodass er dem Cloud-Anbieter Wertersatz zu leisten hat (§ 346 Abs. 1, 2 BGB). Der Cloud-Anbieter ist wiederum verpflichtet, dem Cloud-Nutzer die gezahlte Vergütung zurückzuerstatten. Abgesehen davon, dass sich der Cloud-Anbieter diesem Risiko nicht wird aussetzen wollen, lässt sich die Rückabwicklung in der Praxis kaum realisieren. Dem Interesse der Vertragsparteien entspricht daher allein eine Vertragsbeendigung mit ex-nunc-Wirkung, bei der Leistungen, die bereits abgeschlossen sind, nicht erfasst werden. Ein Rücktrittsrecht ist nur für

---

[500] BGH, Urt. v. 4.3.2010 − III ZR 79/09, CR 2010, 331.
[501] Borges/*Meents,* Rechtshandbuch Cloud Computing, § 4 Rn. 224.

den Zeitraum nach Vertragsschluss, aber vor Erbringung der ersten geschuldeten Leistung sinnvoll.[502]

5. Rechte und Pflichten nach Beendigung des Vertrages

Endet der Vertrag, stellt sich die Frage, welche wechselseitigen Rechte und Pflichten zum Vertragsende bzw. nachvertraglich bestehen, soweit diese nicht ausdrücklich vertraglich vereinbart wurden. Für den Nutzer ist ggf. eine ganze Reihe von Maßnahmen von besonderem Interesse:

- (Rechtzeitige) Herausgabe der Datenbestände in geeigneten Formaten;
- Vermittlung von Know-How durch den Anbieter;
- Einräumung von urheberrechtlichen Nutzungsrechten an der Software;
- Migrationsunterstützung (insbesondere beim Anbieterwechsel).[503]

Das besondere Vertragsrecht enthält insoweit keine konkreten Regelungen. Hier sollen mit der Migrationsunterstützung und der Datenherausgabe zwei Problemfelder näher untersucht werden.

a. Migrationsunterstützung

Die Pflicht des alten Cloud-Anbieters, den Nutzer bei der Migration der Daten auf einen neuen Cloud-Anbieter zu unterstützen, ist als vertragliche Nebenpflicht nach § 241 Abs. 2 BGB einzuordnen. Die Pflicht, eine bereits erbrachte Leistung auf einen Dritten zu übertragen und damit „am Leben zu erhalten", wird allgemein als Leistungssicherungspflicht bezeichnet. Die Leistungssicherungspflicht, die nach den Umständen des Einzelfalls zu bestimmen ist, ist dabei die Pflicht, alles zu tun, um den eingetretenen Leistungserfolg zu sichern und alles zu unterlassen, was die Position der anderen Partei schmälert oder entwertet. Voraussetzung für das Bestehen einer solchen Pflicht ist danach, dass die Risiken/Probleme für den Anbieter erkennbar sind, er ferner die Möglichkeit hat, die Verwirklichung der Risiken zu verhindern oder zumindest zu verringern und dass die vertraglichen Regelungen der Annahme einer Leistungssicherungspflicht nicht entgegenstehen. Daneben wird man aber auch – ebenso wie bei der Begründung von Beratungspflichten – eine Interessenabwägung vornehmen müssen.[504]

Wichtig für den Cloud-Nutzer ist es, dass ihm bei einer Vertragsbeendigung die Cloud Services nicht sofort vom Anbieter entzogen werden, sondern er Zeit hat, sich einen neuen Anbieter zu suchen. Anderenfalls liefe er ggf. Gefahr, erhebliche Schäden zu erleiden. Daher ist der Cloud-Anbieter ggf. verpflichtet, während ei-

---

[502] Borges/*Meents,* Rechtshandbuch Cloud Computing, § 4 Rn. 224.
[503] Vgl. Kompetenzzentrum Trusted Cloud Leitfaden Nr. 3 − Vertragsgestaltung beim Cloud Computing, abrufbar unter www.trusted-cloud.de (letzter Abruf: 28.2.2017), S. 28.
[504] *Schuster/Hunzinger,* Vor- und nachvertragliche Pflichten beim IT-Vertrag − Teil II: Nachvertragliche Pflichten, CR 2015, 277 (278).

ner Übergangsphase seine Leistung weiter zu erbringen. Dies stellt sich bei ergänzender Vertragsauslegung als Nebenpflicht dar.[505] Diese Problematik korrespondiert mit der oben dargestellten Länge der Kündigungsfrist.

Zusammenfassend kann also festgehalten werden, dass der Cloud-Anbieter die Pflicht hat, für den Fall der Beendigung der Vertragsbeziehung einen reibungslosen Übergang auf ein Fremdsystem zu ermöglichen.[506]

Der Umfang der erforderlichen Migrationsunterstützung ist dabei letztlich einzelfallabhängig. So kann der Cloud-Anbieter auch verpflichtet sind, dem Cloud-Nutzer etwa eine Dokumentation des Know-hows zur Verfügung zu stellen, z. B. in Form von Prozessbeschreibungen, damit entweder der Cloud-Nutzer selbst oder der neue Anbieter leistungsfähig sind.[507]

b. Datenherausgabe

Während der Umfang der nachvertraglichen Pflichten – bei fehlender Absprache der Vertragsparteien – überwiegend davon abhängen dürfte, was im Einzelfall noch als vertragliche Nebenpflicht i. S. d. § 241 BGB anzusehen ist, spricht vieles dafür, dass der Anbieter bei Beendigung des Vertrages regelmäßig die Herausgabe der Datenbestände schuldet.

Es stellt sich die Frage, welche Rechte der Nutzer an den beim Anbieter gespeicherten Daten hat (1) und nach welcher Norm der Nutzer mit Ablauf des Vertrages die Herausgabe der Daten verlangen kann (2). Ferner ist fraglich, inwieweit ggf. Zurückbehaltungsrechte des Nutzers und/oder des Anbieters bestehen (3).

(1) Rechte an Daten

Hinsichtlich der Frage, wer welche Rechte an den Daten hat (auch mit Blick auf das Sonderproblem der Insolvenz des Cloud-Betreibers), wird auf die Ausführungen in Kapitel 1 – Dateneigentum – Bezug genommen.

(2) Herausgabe der Daten

Die Herausgabepflicht des Anbieters ergibt sich bei einer entsprechenden vertraglichen Regelung aus dem Vertrag.[508]

Fehlt eine solche Regelung, werden für die Herausgabepflicht verschiedene Anspruchsgrundlagen diskutiert: § 667 BGB i. V. m. § 675 BGB, § 539 Abs. 2 BGB, § 242 BGB oder § 241 Abs. 2 BGB.[509]

---

[505] Hilber/*Intveen/Hilber/Rabus,* Handbuch Cloud Computing, Teil 2, Rn. 380.
[506] So auch OLG München, Urt. v. 22.4.1999 − 6 U 1657/99, CR 1999, 484 (485).
[507] Borges/*Meents,* Rechtshandbuch Cloud Computing, § 4 Rn. 229.
[508] Unabhängig davon können entsprechende Ansprüche in Bezug auf personenbezogene Daten aus datenschutzrechtlichen Gesichtspunkten bestehen.
[509] Vgl. *Schuster/Hunzinger,* Vor- und nachvertragliche Pflichten beim IT-Vertrag − Teil II: Nachvertragliche Pflichten, CR 2015, 277 (279 ff.) − auch zur Frage eines etwaigen Zurückbehaltungsrechts des Anbieters.

- Nach Maßgabe der obigen Ausführungen wird ein Cloud-Computing-Vertrag oftmals dem Miet-, Dienst- oder Werkvertragsrecht zuzuordnen sein. In diesen Fällen kommt ein Anspruch des Nutzers aus § 667 i. V. m. § 675 BGB nicht in Betracht. Gleichwohl sind Fälle sind denkbar, in denen die Vertragsbeziehung zwischen Cloud-Nutzer und Cloud-Betreiber dem Recht des Geschäftsbesorgungsvertrages i. S. v. § 675 Abs. 1 BGB unterliegt, weil es sich bei der Leistungspflicht des Cloudbetreibers im Kern um eine entgeltliche Verwaltung fremden Vermögens handelt. Dann besteht ein entsprechender Herausgabeanspruch.[510]

- Das Wegnahmerecht aus § 539 Abs. 2 BGB hilft hingegen in keinem Fall weiter, da diese Norm nur eine Duldungspflicht konstituiert, aber keine aktive Herausgabepflicht des Cloud-Anbieters begründet.

- Letztlich ergibt sich die Herausgabepflicht daher durch ergänzende Vertragsauslegung. Dies folgt aus den Interessen der Vertragsparteien, insbesondere dem Interesse des Nutzers als „Herr der Daten“, vom Anbieter jederzeit – also grundsätzlich auch vor Vertragskündigung (dann hergeleitet aus § 242 BGB), insbesondere aber nach Vertragsbeendigung – die Herausgabe der Daten verlangen zu können.

  Nach Vertragskündigung besteht eine Nebenpflicht aus § 241 Abs. 2 BGB, die Daten herauszugeben, und zwar in einem Format, das dem Anbieter selbst ohne größeren Aufwand zur Verfügung steht (Rechtsgedanke des § 243 Abs. 1 BGB). Nützt das dem Anbieter zur Verfügung stehende Datenformat dem Nutzer nichts, kann über eine ergänzende Vertragsauslegung hergeleitet werden, dass der Anbieter gegen Zahlung einer entsprechenden Vergütung zu einer ggf. zeitintensiven Konvertierung der Daten und/oder zur Schaffung einer entsprechenden Schnittstelle verpflichtet ist.

  Die Herausgabe von Daten erfolgt im Wege der Übertragung (Kopie) an den Berechtigten und Löschung beim Datenbesitzer. Es wird insoweit Bezug genommen auf die Ausführungen in Kapitel 1 „Dateneigentum“.[511]

(3) Zurückbehaltungsrechte

Besteht Streit über die fehlende Erbringung (vermeintlich) geschuldeter Leistungen, kann sich die Frage nach der Möglichkeit der Ausübung von Zurückbehaltungsrechten stellen.

Ein solches lässt sich wohl nicht aus § 320 BGB herleiten, da Vergütung und Datenherausgabe nicht in einem Synallagma stehen. Ein Zurückbehaltungsrecht kann sich aber bei Vorliegen der Voraussetzungen aus § 273 BGB ergeben. Problematisch ist insoweit in erster Linie, wann der Anspruch auf Herausgabe der

---

[510] OLG Düsseldorf, Urt. v. 27.9.2012 − 6 U 241/11, CR 2012, 801.
[511] Siehe Kapitel 1 „Dateneigentum“, Abschnitt D. I. 3. und E. II. 2.

Daten fällig wird. Wird die Datenherausgabe als Nebenpflicht nach § 241 Abs. 2 BGB nach einer Kündigung verlangt, tritt Fälligkeit mit Zugang der Kündigung ein. Wird die Herausgabe jedoch im laufenden Vertragsverhältnis oder die Bereitstellung in einem konvertierten Datenformat verlangt und damit auf die ergänzende Vertragsauslegung nach § 242 BGB gestützt, kann eine Fälligkeit nicht sofort eintreten, sondern muss nach den Umständen (§ 271 Abs. 1 BGB) bestimmt werden.

Die Ausübung des Zurückbehaltungsrechts kann nach Treu und Glauben ausgeschlossen sein, bspw. wenn die zurückbehaltene Leistung besonders wertvoll ist und dieser eine verhältnismäßig geringfügige Leistung entgegensteht. Bei Cloud Computing-Verträgen kann dies also dazu führen, dass die Daten wegen einer ausstehenden Vergütung dann nicht zurückbehalten werden dürfen, wenn diese eine existentielle Bedeutung für den Nutzer haben, z. B. wenn dann die Ausübung des Geschäfts faktisch nicht mehr möglich wäre.[512]

V. Ergebnisse

Die Prüfungen der Arbeitsgruppe haben ergeben, dass bislang eine klare Tendenz zu erkennen ist, auf Cloud Computing-Verträge mietrechtliche Vorschriften anzuwenden, was nach obigen Ausführungen insgesamt auch gerechtfertigt erscheint. Das Mietrecht bietet überwiegend gute Lösungen für bei Cloud Computing-Verträgen auftretende Probleme. Soweit die Arbeitsgruppen Lücken im Mietrecht ausgemacht hat, können diese durch Klarstellungen und ergänzende Regelungen (s. dazu im Folgenden) geschlossen werden.

Die Prüfung hat nämlich auch ergeben, dass die vorhandenen Regelungen an einigen Stellen Schwachstellen hinsichtlich sachgerechter und angemessener Lösungen von Problemen im Bereich von Cloud Computing-Verträgen aufweisen, die Anlass für gesetzgeberische Maßnahmen geben:

Das Mietrecht des BGB geht von der Miete einer Sache aus. Es sollte daher durch eine dem § 453 Abs. 1 BGB vergleichbare Regelung im Mietrecht klargestellt werden, dass das Mietrecht auch auf andere („sonstige“) Gegenstände als auf Sachen Anwendung finden kann.

Die verschiedenen Kündigungsfristen des § 580a BGB entsprechen je nach Einzelfall nicht den Interessen der Cloud Computing-Vertragsparteien. Folgerichtig sollte zumindest klargestellt werden, welche Fristen des § 580a BGB einschlägig sind. Ggf. ist der Fristenkatalog zu erweitern.

---

[512] *Schuster/Hunzinger*, Vor- und nachvertragliche Pflichten beim IT-Vertrag − Teil II: Nachvertragliche Pflichten, CR 2015, 277 (283 f.).

Ein Anspruch des Nutzers gegen den Anbieter auf Rückgabe von Daten nach Vertragsbeendigung lässt sich bisher nur über eine ergänzende Vertragsauslegung bzw. als nachvertragliche Nebenpflicht herleiten. Ein solcher Anspruch sollte aber gesetzlich klar verankert sein.

Passt man auf diese Weise das Mietrecht an, ist für die untersuchten Vertragsbeziehungen (vorerst) ein angemessener Rechtsrahmen gewährleistet. Soweit dennoch Lücken verbleiben sollten, könnte es der Privatautonomie der Parteien überlassen bleiben, die für ihren Vertrag passenden Regelungen zu finden. Hierfür spricht auch, dass insoweit bisher weder von Wirtschafts- noch von Verbraucherseite unzureichende Regelungen moniert worden sind. Schließlich sollte der Rechtsprechung vorbehalten und ihr auch zugetraut werden, die neuen Sachverhalte unter die vorhandenen Normen zu subsumieren und so einer sachgerechten Lösung zuzuführen.[513]

Gleichwohl weist die Arbeitsgruppe an dieser Stelle noch einmal ausdrücklich darauf hin, dass wegen der Komplexität und Vielgestaltigkeit der verfügbaren Cloud Services sowie der Vielzahl rechtlicher Fallgestaltungen nur ausgesuchte Aspekte einer vertieften Prüfung unterzogen wurden.[514] Zudem ist zu erwarten, dass die Initiativen der EU-Kommission zum Digitalen Binnenmarkt und zur freien Datenwirtschaft weiter Konturen annehmen werden. Daran anknüpfend empfiehlt die Arbeitsgruppe, zumindest mittelfristig, eine umfassende Prüfung – ggf. unter Fortsetzung der Arbeitsgruppe – der rechtlichen Fragestellungen im Zusammenhang mit Cloud Computing vorzunehmen.

---

[513] Vgl. *Faust*, Digitale Wirtschaft − Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, S. 59.
[514] Siehe D. III. 2.

E. Streaming

I. Technische Grundlagen

Streaming bezeichnet das Abspielen von Multimediadateien schon während des Downloads, d. h. die Dateien „strömen“ konstant zum Nutzer. Im Unterschied zu einem gewöhnlichen Download werden die Daten jedoch nur temporär auf dem Computer des Nutzers gespeichert und nach Abschluss des Vorgangs (automatisch) verworfen. Dies bedeutet, dass der Nutzer – abgesehen von der Verwendung rechtswidriger Umgehungstechniken (sog. „Rippen“) – nicht in den Besitz einer für ihn autonom nutzbaren Mediendatei kommt.[515]

Es handelt sich beim Streaming nicht um eine festgelegte Methode, sondern um einen Sammelbegriff verschiedener Techniken. Dabei wird generell zwischen zwei Arten des Streaming unterschieden, dem On-Demand Streaming und dem Live-Streaming. Regelmäßig besteht der Streaming-Vorgang aus drei Schritten:

(1.) Codierung in ein versendbares Format

Die Video- und Audiodaten werden zunächst vom Anbieter mit einer Encoder-Software (in Ausnahmefällen durch eine sog. Encoderbox) in ein passendes Format umgewandelt. Teilweise werden sie auch komprimiert, um in das Netzwerk eingespeist werden zu können.

(2.) Weiterleitung über Streaming Server

Nach der Codierung/Komprimierung werden die Daten auf einem Streaming Server hinterlegt. Im Falle des Live-Streams können die Daten auch direkt vom Encoder an den Nutzer weitergeleitet werden – der Server dient dann ggf. (nur) als zwischengeschalteter Verteiler.

(3.) Empfang des Streams durch Client

Der Datenstrom wird vom Server an die sog. Clients (Nutzer) gesendet und dort mit Hilfe einer speziellen Software wiedergegeben.[516]

Ein – vor allem aus urheberrechtlicher Sicht – wesentlicher Aspekt ist beim Streaming, dass es stets zu einer (temporären) Speicherung der Daten auf dem Zielrechner kommt. Sie ist integraler und wesentlicher Bestandteil des technischen Verfahrens, auch wenn der Nutzer – anders als beim Download – ohne rechtswidrige Umgehungstechniken nicht in den Besitz einer für ihn autonom nutzbaren Mediendatei gelangt. Unterschiedlich und abhängig von der Form des

---

[515] Vgl. *Galetzka/Stamer*, Streaming − aktuelle Entwicklungen in Recht und Praxis, MMR 2014, 292.

[516] Vgl. Skript „Streaming“ des Regionalen Rechenzentrum der Universität Köln, S. 15, abrufbar unter https://rrzk.uni-koeln.de/fileadmin/zustaendigkeiten/multimedia/Streaming.pdf (letzter Abruf: 1.2.2017).

Streaming sowie den Softwareeinstellungen sind nur die Größe der gespeicherten Segmente sowie Dauer und der Ort der Speicherung.

II. Ökonomische Bedeutung/Marktentwicklung

Das (legale) Streaming bietet einige Vorteile gegenüber anderen Verwertungs- bzw. Nutzungsarten.

Aus Sicht der Anbieter bzw. der Verwerter von urheberrechtlich geschützten Werken liegt der wesentliche Vorteil in der Steuerbarkeit der Werkverwertung. Dies zeigt sich insbesondere im Vergleich zu Download-Angeboten. Zwar kann der Anbieter bei beiden Verwertungsarten mehrere hundert oder sogar tausend Nutzer gleichzeitig mit entsprechenden Inhalten versorgen. Beim Streaming hat er jedoch eine viel bessere Kontrollmöglichkeit über die weiteren Verbreitungswege des Werkes.

Aus Nutzersicht kann sich hingegen vor allem Folgendes als vorteilhaft erweisen:

- Ohne die für einen (vollständigen) Download ggf. erforderliche Wartezeit kommt der Nutzer sofort, überall und jederzeit in den „Genuss“ des Werkes;
- Mit Ausnahme einer etwaigen Zwischenspeicherung werden keine Speicherkapazitäten des Nutzers in Anspruch genommen;
- Der Nutzer hat größere Auswahlmöglichkeiten durch die Vielfalt der Datenbanken für Musik-, Film- oder Videostreaming.

Das Geschäft mit Streaming boomt. Allein die Umsätze in Deutschland mit Video-On-Demand werden in diesem Jahr voraussichtlich auf 945 Millionen Euro steigen, das ist ein Plus von 18 Prozent gegenüber 2016. Mehr als drei Viertel der Internetnutzer über 14 Jahren schauen Videos per Stream. Dabei setzen die Anbieter auf verschiedene Geschäftsmodelle, um mit Video-Streaming Geld zu verdienen. Etwa 434 Millionen Euro erzielen kostenfreie, werbefinanzierte Angebote wie Vimeo, YouTube oder auch die Webseiten der privaten Fernsehsender. Kostenpflichtige Video-Angebote bringen 2017 voraussichtlich Umsätze von 511 Millionen Euro. Dazu zählen Portale mit unbegrenzt vielen Filmen oder Serien gegen eine monatliche Grundgebühr sowie Dienste, bei denen der Nutzer für einzelne Videos zahlt. Beispiele für solche kostenpflichtigen Video-Streaming-Plattformen sind Amazon Video, Apple iTunes, Google Play, Maxdome, Netflix, Sky Go oder Watchever.[517]

Auch Audio-Streaming wächst rasant. In Deutschland hört jeder dritte Internetnutzer ab 14 Jahren (44 Prozent) Musik per Streaming. Bei den Über-65-Jährigen sind es immerhin noch 24 Prozent, die Dienste wie Spotify, Deezer, Soundcloud

---

[517] Pressemitteilung Bitkom e.V. vom 16.1.2017, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/Umsatz-mit-Video-Streaming-knapp-an-der-Milliardengrenze.html (letzter Abruf: 16.3.2017).

& Co in Anspruch nehmen. Die Nutzer können dabei auf verschiedene Formen von Musik-Streaming-Diensten zurückgreifen, die sich zwischenzeitlich etabliert haben. Bei einigen besteht ein direkter Zugriff auf Millionen von Titeln. Andere funktionieren wie ein personalisiertes Radio, dem der Hörer ein Musikgenre oder bestimmte Künstler vorgibt und anschließend nur Titel aus diesem Bereich zu hören bekommt. Zudem gibt es Streaming-Dienste, bei denen Musiker ihre Stücke selbst hochladen und so ihren Fans zur Verfügung stellen können.[518]

III. Vertragsrechtliche Einordnung von Live-Streaming

Der hier nachzugehenden Frage, ob das geltende Vertragsrecht gesetzliche Rahmenbedingungen bereitstellt, die Gewähr für einen rechtssicheren Umgang mit Streaming-Verträgen sowie einen angemessenen Ausgleich zwischen den Vertragsparteien bieten, ist eine vertragsrechtliche Einordnung der entsprechenden Vertragsverhältnisse voranzustellen. Hierbei sind Live-Streaming und On-Demand-Streaming getrennt voneinander zu behandeln.

1. Technische Darstellung – „faktische Leistung des Anbieters an den Nutzer“

Als Live-Streaming bezeichnet man ein Streaming-Angebot, das vom Anbieter in Echtzeit bereitgestellt wird, wie z. B. die parallele Übertragung eines laufenden Fußballspiels. Die beim Anbieter über Video- bzw. Audiokanäle eingehenden Daten werden in Echtzeit komprimiert, encodiert und in das Netzwerk eingespeist. Dort steht der Stream zu einer bestimmten Zeit (zum sofortigen Abruf) bereit.[519] Die zeitversetzte bzw. nochmalige Wiedergabe oder Vor- bzw. Zurückspulen des Streams sind grundsätzlich nicht möglich.

Haben beliebig viele Empfänger auf den Stream Zugriff, handelt es sich um ein sog. Multicast, das mit einer Fernseh- oder Radioausstrahlung vergleichbar ist.[520] Teilweise werden Rundfunksendungen parallel zu ihrer Ausstrahlung im Fernsehen oder Radio auch über die Internetseiten der Sender als Live-Streams ausgestrahlt. In diesem Fall spricht man von „Simulcasts“.[521]

---

[518] Pressemitteilung Bitkom e.V. vom 9.3.2017, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/ Musik-Streaming-in-Deutschland-waechst-seit-fuenf-Jahren.html (letzter Abruf: 16.3.2017).

[519] Vgl. Skript „Streaming“ des Regionalen Rechenzentrum der Universität Köln, S. 7, abrufbar unter https://rrzk.uni-koeln.de/fileadmin/zustaendigkeiten/multimedia/Streaming.pdf (letzter Abruf: 1.2.2017); *Koch*, Der Content bleibt im Netz − gesicherte Werkverwertung durch Streaming-Verfahren, GRUR 2010, 574.

[520] *Galetzka/Stamer*, Streaming − aktuelle Entwicklungen in Recht und Praxis, MMR 2014, 292; *Koch*, Der Content bleibt im Netz − gesicherte Werkverwertung durch Streaming-Verfahren, GRUR 2010, 574.

[521] Vgl. *Bortloff*, Internationale Lizensierung von Internet-Simulcasts durch die Tonträgerindustrie, GRUR Int 2003, 669.

2. Einordnung des Rechtsverhältnisses zwischen Anbieter und Nutzer in die vorhandene Vertragstypologie des BGB

a. Vorbemerkung

Abhängig vom konkreten Inhalt des jeweiligen Angebotes können für das Live-Streaming die Vorschriften des Rundfunkstaatsvertrages und/oder des Telemediengesetzes gelten.[522] Darauf ist jedoch vorliegend nicht näher einzugehen, da sich hieraus allenfalls regulatorische Vorgaben für den Anbieter ergeben, die das vertragsrechtliche Verhältnis zwischen Anbieter und Nutzer grundsätzlich unberührt lassen.

Eine Anwendung des Telekommunikationsgesetzes (und der darin vorgesehenen Kundenschutzvorschriften) kommt für das Live-Streaming hingegen nicht in Betracht. Beim Live-Streaming handelt es sich um einen sog. Inhaltsdienst, der – anders als die Voraussetzung für Telekommunikationsdienste nach § 3 Nr. 24 TKG – nicht „ganz oder überwiegend" in der Übertragung von Signalen über Telekommunikationsnetze besteht.[523]

b. Urheberrechtliche Vorbetrachtung (rechtliche Natur der Leistung des Anbieters)

Die Werkverwertung über Streaming-Plattformen wirft zahlreiche Rechtsfragen auf, welche zumindest vordergründig vor allem die urheberrechtliche Einordnung und deren Folgen für die praktische Handhabung betreffen. Beispielhaft sind hier zu nennen:

- Art und Umfang der Betroffenheit von Verwertungsrechten;
- Art und Umfang erforderlicher Lizenzen zur Bereitstellung eines Streaming-Angebotes;
- Unterscheidung „legaler" und „illegaler" Streaming-Angebote;
- Konsequenzen der Nutzung „illegaler" Streaming-Plattformen.

Eine rechtliche Bewertung des Streamings erfolgte in Rechtsprechung und rechtswissenschaftlicher Literatur dementsprechend bisher nahezu ausnahmslos im Zusammenhang mit urheberrechtlichen Fragestellungen. Nicht zuletzt die auch in

---

[522] *Bauer/v. Einem*, Handy-TV − Eine neue Herausforderung für die Rundfunkregulierung?, MMR 2007, 423.

[523] Vgl. *Kühling/Schall*, WhatsApp, Skype & Co. − OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts, CR 2015, 641.

der Öffentlichkeit viel diskutierten Fälle von kino.to[524] und Redtube[525] haben dafür gesorgt, dass sich zahlreiche Publikationen damit befasst haben, wie der Betrieb eines Streaming-Portals und insbesondere die Nutzung von (illegalen) Streaming-Angeboten urheberrechtlich einzuordnen sind.[526]

Auch für die vertragliche Einordnung von Vereinbarungen über Streaming-Dienste bietet es sich an, die durch eine Werkverwertung mittels Streaming betroffenen Regelungen im Urheberrecht in den Blick zu nehmen. Zwar richtet sich der Vertragsinhalt und damit auch dessen vertragsrechtliche Einordnung allein nach dem (übereinstimmenden) Willen der Vertragsparteien (§§ 133, 157 BGB). Das Urheberrecht ist in diesem Zusammenhang aber nicht nur für die Frage relevant, ob der Anbieter die versprochene Leistung auch tatsächlich vertragsgemäß erfüllen kann. Die urheberrechtliche Bewertung, welche (Nutzungs-)Rechte der Anbieter dem Nutzer beim Streaming in der Regel verschaffen muss, damit dieser berechtigterweise in den „Werkgenuss" kommen kann, ist zugleich ein wichtiger Aspekt bei der Frage, um welchen Vertragstyp es sich typischerweise bei einer Vereinbarung über die einzelnen Streaming-Angebote handelt.[527]

Ausgangspunkt der urheberrechtlichen Betrachtung ist der Umstand, dass beim Streaming zwar nicht das gesamte Werk auf einmal auf dem Gerät des Benutzers verkörpert wird. Es werden jedoch diejenigen (minimalen) Werkteile, die gerade zur Wiedergabe erforderlich sind, physisch auf dem Benutzergerät gespeichert und (erst) unmittelbar danach automatisch wieder gelöscht. Beim Streaming handelt es sich folgerichtig nicht bloß um einen rezeptiven – urheberrechtlich grundsätzlich irrelevanten[528] – Werkgenuss, sondern bei der gebotenen objektiven Betrachtung um einen Eingriff in das Vervielfältigungsrecht (§ 16 UrhG). [529] Daran ändert auch der Umstand nichts, dass es dem durchschnittlichen Benutzer nicht

---

[524] Die Betreiber von kino.to hatten Internetnutzern Zugriff auf mehrere Zehntausend Kinofilme, Serien und Dokumentationen ermöglicht, die ohne Zustimmung der Rechteinhaber im Internet verfügbar gemacht worden waren. Sie wurden in 2011/2012 zu mehrjährigen Haftstrafen verurteilt, ebenso wie der Betreiber einer „Nachfolgeplattform" (kinox.to).

[525] Einige Kammern des LG Köln hatten Ende 2013 Anträgen auf Herausgabe von Namen und Anschriften zu IP-Adressen stattgegeben, die damit begründet wurden, dass die Nutzer der IP-Adressen Pornofilme über die Streaming-Plattform angesehen hatten. Soweit dagegen Rechtsmittel eingelegt wurden, wurden die Entscheidungen später aufgehoben.

[526] Vgl. nur *Galetzka/Stamer*, Streaming − aktuelle Entwicklungen in Recht und Praxis, MMR 2014, 292.

[527] Vgl. *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3.

[528] BGH, Urt. v. 20.1.1994 – I ZR 267/91, NJW 1994, 1216; Urt. v. 4.10.1990 – I ZR 139/89, NJW 1991, 1231; *Marly*, Bildschirmkopien, Cache-Kopien und Streaming als urheberrechtliche Herausforderung, EuZW 2014, 616; *Ensthaler*, Streaming und Urheberrechtsverletzungen, NJW 2014, 1553 (1554).

[529] *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3 (6); *Marly*, Bildschirmkopien, Cache-Kopien und Streaming als urheberrechtliche Herausforderung, EuZW 2014, 616 (618); *Ensthaler*, Streaming und Urheberrechtsverletzungen, NJW 2014, 1553 (1554).

bekannt sein dürfte, dass der zur Wiedergabe nötige Puffer und damit die Größe der auf seinem Gerät abgespeicherten Teile veränderbar ist, denn auf die konkrete Größe des vom jeweiligen Nutzer abgespeicherten Teils kann es im Ergebnis nicht ankommen. Dies hätte nämlich zur Folge, dass es allein der Disposition des Nutzers unterliegt, ob eine Vervielfältigung vorliegt oder nicht, was eine objektive Klärung verhindert und erhebliche Nachweisprobleme mit sich bringt.[530]

Gleichwohl bedarf es mit Blick auf die Schrankenregelung des § 44a Nr. 2 UrhG im Ergebnis keiner Einräumung von Nutzungsrechten durch den Streaming-Anbieter.

Die Schrankenregelung des § 44a Nr. 2 UrhG verfolgt das Ziel, den allein rezeptiven Werkgenuss, der in der analogen Welt nicht urheberrechtlich geschützt ist, auch in der digitalen Welt in gleicher Weise gemeinfrei zu halten, indem sie das in § 16 UrhG (zu) weit gefasste Vervielfältigungsrecht für vorübergehende Vervielfältigungen einschränkt.[531] Unter fünf kumulativen Voraussetzungen sind hiernach Vervielfältigungshandlungen erlaubt. Die Vervielfältigungen müssen als integraler und wesentlicher Bestandteil eines technischen Verfahrens vorübergehend sowie flüchtig oder begleitend sein. Ihr alleiniger Zweck muss eine rechtmäßige Nutzung des Werkes sein und sie dürfen keine eigenständige wirtschaftliche Bedeutung haben (d. h. keine neuen Nutzungsmöglichkeiten eröffnen). Diese Voraussetzungen sind beim Streaming von „legalen Inhalten“ nach herrschender Auffassung allesamt gegeben.[532]

Aus urheberrechtlicher Sicht als problematisch erweisen sich lediglich solche Streaming-Angebote, bei denen der Anbieter über keine Berechtigung verfügt, das Werk zu verbreiten bzw. zu vervielfältigen. Äußerst umstritten ist insoweit die Auslegung des Merkmals der „rechtmäßigen Nutzung“ in § 44a Nr. 2 UrhG. Teilweise wird vertreten, dass die Schranke nur greift, wenn eine (auch konkludent erteilbare[533]) Erlaubnis zur Vervielfältigung seitens des Rechteinhabers vorliegt oder die Vervielfältigung durch sonstige Schranken gedeckt ist. Nach anderer Ansicht genügt in Anlehnung an § 53 Abs. 1 S. 1 UrhG hingegen, dass auf der Serverseite des Anbieters keine offensichtlich rechtswidrig hergestellte Kopie abrufbar ist. Schließlich wird unter Bezugnahme auf die Entscheidung des EuGH „FAPL/Murphy“ auch vertreten, dass die Anwendung des § 44a Nr. 2 UrhG un-

---

[530] *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3 (6).

[531] Vgl. *Ensthaler*, Streaming und Urheberrechtsverletzungen, NJW 2014, 1553 (1554).

[532] *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3 (6); *Marly*, Bildschirmkopien, Cache-Kopien und Streaming als urheberrechtliche Herausforderung, EuZW 2014, 616 (619) − auf die abweichende, vereinzelt gebliebene Auffassung von *Ensthaler*, wonach stets − vergleichbar dem „Blättern in einem Buch“ − nur eine Orientierung über die angebotenen Inhalte zulässig sein soll, wird an dieser Stelle nicht weiter eingegangen.

[533] BGH, Urt. v. 29.4.2010 – I ZR 69/08, NJW 2010, 2731; Urt. v. 19.10.2011 – I ZR 140/10, NJW 2012, 1886.

abhängig von der Rechtmäßigkeit der Vorlage zu betrachten ist und es ausschließlich auf die Rechtmäßigkeit der Nutzung ankommt.[534] Letztlich ist dieser Meinungsstreit über die Auslegung des § 44a Nr. 2 UrhG für die hier allein zu beantwortende Frage, welche Rechte dem Nutzer vom Anbieter eines Streaming-Dienstes eingeräumt werden müssen, aber nicht zu entscheiden.

Verfügt der Anbieter über keine vom Rechteinhaber eingeräumten Nutzungsrechte, sondern sind die Inhalte illegal (unter Verletzung von § 19a UrhG) auf die Plattform gelangt, kann er dem Streaming-Nutzer auch keine irgendwie gearteten Nutzungsrechte an den Inhalten einräumen. Sind die Inhalte demgegenüber mit ausdrücklicher oder konkludenter Zustimmung seitens des Rechteinhabers auf die Plattform gelangt, ist das Streaming durch die Schranke des § 44a Nr. 2 UrhG gedeckt. Daraus folgt, dass der Anbieter in keinem Fall verpflichtet ist, dem Benutzer ein urheberrechtliches Nutzungsrecht einzuräumen. Seine „Pflicht" besteht allenfalls darin, selbst über die für das Streaming-Angebot erforderlichen Nutzungsrechte zu verfügen und damit die Voraussetzungen des § 44a Nr. 2 UrhG zu schaffen.[535]

Die vorstehenden Überlegungen gelten im Übrigen entsprechend für die Schranke des § 53 Abs. 1 S. 1 UrhG, die Vervielfältigungen zum privaten Gebrauch gestattet.

Zusammenfassend ist also Folgendes festzuhalten:

Zur Erfüllung eines Vertrages über Streaming-Dienste bedarf es grundsätzlich keiner Einräumung eines urheberrechtlichen Nutzungsrechts durch den Anbieter gegenüber dem Nutzer.[536]

c. Vertragsrechtliche Einordnung

Den Vertragstyp „Streaming" gibt es nicht. Die anzuwendenden schuldrechtlichen Vorschriften richten sich daher grundsätzlich danach, wie Verträge über Streaming-Dienste in die vorhandene Vertragstypologie des BGB einzuordnen sind. In Betracht kommen insbesondere folgende Vertragstypen/Vertragsarten:

- Mietvertrag (§§ 535ff. BGB);
- Dienstvertrag (§§ 611ff. BGB);
- Werkvertrag (§§ 631ff. BGB);
- Typengemische Verträge (siehe dazu auch unter Ziffer IV.).

---

[534] Vgl. zum Meinungsstand *Galetzka/Stamer*, Streaming − aktuelle Entwicklungen in Recht und Praxis, MMR 2014, 292.
[535] Vgl. *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3 (6).
[536] So auch *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3 (6).

(1) Höchstrichterliche Entscheidungen

Bisher liegen keine höchstrichterlichen Entscheidungen zur vertragsrechtlichen Einordnung von Streaming-Verträgen vor. Zwei Entscheidungen des BGH geben jedoch insoweit zumindest Hilfestellung:

(a) ASP[537]-Urteil vom 15. November 2006[538]

Der BGH bestätigt in dem oben genannten Urteil die Vorinstanz, auf einen Vertrag Mietvertragsrecht anzuwenden, soweit dieser auf die entgeltliche Überlassung von Standardsoftware über das Internet gerichtet ist. Bei derartigen (ASP-)Verträgen stehe die Gewährung der Online-Nutzung von Software für eine begrenzte Zeit im Mittelpunkt der vertraglichen Pflichten. Es liege deshalb nahe, als Rechtsgrundlage für die vertraglichen Ansprüche einen Mietvertrag, der die entgeltliche Gebrauchsüberlassung einer beweglichen oder unbeweglichen Sache zum Gegenstand habe, anzunehmen. Wegen der weiteren Einzelheiten der Entscheidung wird auf die diesbezüglichen Ausführungen im Unterkapitel „Cloud Computing“ Bezug genommen.[539]

In der Literatur ist das ASP-Urteil des BGH nicht unwidersprochen geblieben. Gegen die Einordnung als Mietvertrag ist insbesondere eingewandt worden, dass dem Nutzer bei ASP-Verträgen keine Möglichkeit zum tatsächlichen Zutritt zu einer Sache eingeräumt, sondern nur eine bloße Nutzungsmöglichkeit geboten werde.[540]

(b) Pay-TV

Der BGH hat mit Urteil vom 15. November 2007 – wenn auch ohne vertiefte Begründung – zum wiederholten Male entschieden, dass es sich bei einem Abonnentenvertrag über Bezahlfernsehen, d. h. einem Vertrag über die Bereitstellung bestimmter „Programmpakete“, um einen Dienstvertrag handelt.[541]

(2) Vertragsrechtliche Einordnung eines entgeltlichen Vertrages über Live-Streaming

Anknüpfend an die Vorüberlegungen zur faktischen und (urheber-)rechtlichen Leistung des Anbieters schuldet der Anbieter bei Verträgen über Live-Streaming typischerweise folgende (Haupt-)Leistung:

---

[537] ASP = Application Service Providing/Bereitstellung von Softwareanwendungen und damit verbundenen Dienstleistungen.
[538] BGH, Urt. v. 15.11.2006 – XII ZR 120/04, NZM 2007, 379.
[539] Siehe unter D. II. 1. B. (3).
[540] *Hoeren*, Skriptum IT-Vertragsrecht, S. 374, abrufbar unter https://www.uni-muenster.de/Jura.itm/hoeren/lehre/materialien (Stand: April 2017; letzter Abruf: 2.5.2017).
[541] BGH, Urt. v. 15.11.2007 – III ZR 247/06, MMR 2008, 159; Urt. v. 13.3.2003 – I ZR 290/00, MMR 2003, 527.

Einspeisung von in einem bestimmten Format encodierten/komprimierten Video-/Audiosignalen in ein Netzwerk (das Internet), um dem Nutzer zu ermöglichen, die Video-/Audiosignale *zu einem bestimmten Zeitpunkt* (in Echtzeit) per Streaming zu konsumieren.

Bei einem entgeltlichen Live-Streaming Vertrag handelt es sich demzufolge grundsätzlich um einen Dienstvertrag. Im Mittelpunkt des Vertrages steht – wie beim konventionellen Pay-TV – das Versprechen des Anbieters, die Voraussetzungen für eine hinsichtlich des einzelnen Video-/Audiosignals auf einen bestimmten Zeitpunkt beschränkte Datenübertragung zu schaffen. Insbesondere diese zeitliche Beschränkung der Datenübertragung (des Streams) steht zugleich der Annahme eines Mietvertrages entgegen. Der Nutzer hat – anders als bei der genannten ASP-Entscheidung des BGH – gerade keinen Anspruch darauf, dass ihm für einen bestimmten Zeitraum der Zugang zur Online-Nutzung ausgewählter Daten oder Programme ermöglicht wird. Er hat nur die Wahl, ob er den vom Anbieter in das Netzwerk eingespeisten Stream konsumiert oder nicht.

(3) Vertragsrechtliche Einordnung eines unentgeltlichen Vertrages über Live-Streaming

Stellt der Anbieter den Live-Stream unentgeltlich zur Verfügung, ist zunächst eine Abgrenzung zu einem reinen Gefälligkeitsverhältnis vorzunehmen. Maßgeblich ist insoweit, ob die Parteien den für einen Vertragsschluss erforderlichen Rechtsbindungswillen haben. Fehlt ein solcher Wille, bestehen wechselseitig weder Erfüllungs- noch Aufwendungsersatzansprüche.

Verfügen Anbieter und Nutzer indes über den erforderlichen Rechtsbindungswillen, kommt zwischen ihnen ein (Gefälligkeits-)Vertrag in Form eines Auftrages gemäß § 662 BGB zustande. Dies folgt in logischer Konsequenz der Einordnung des entgeltlichen Vertrages über Live-Streaming als Dienstvertrag, da die (Un-)Entgeltlichkeit das zentrale Unterscheidungskriterium zwischen Dienstvertrag und Auftrag darstellt.[542] Die oben näher bezeichnete Hauptleistungspflicht, Einspeisung von encodierten/komprimierten Video-/Audiosignalen in ein Netzwerk, um zu einem bestimmten Zeitpunkt deren Streaming zu ermöglichen, bleibt unverändert, allein die Vergütungspflicht fällt weg.

Der Begriff der Geschäftsbesorgung in § 662 BGB ist im Übrigen denkbar weit zu verstehen. Gegenstand eines Auftragsverhältnisses können Dienste jeder Art sein.[543] Entscheidend ist, dass es sich um ein für den Auftragnehmer fremdes Geschäft im Rechtskreis des Auftraggebers handelt. Es genügt, wenn ein Interesse des Auftraggebers gefördert wird.[544] Dies ist bei der Bereitstellung der Inhalte zum Abruf per Streaming ersichtlich der Fall.

---

[542] Vgl. Schulze/*Schreiber*, BGB, § 611 Rn. 7; Palandt/*Sprau*, BGB, § 662 Rn. 6; Palandt/*Weidenkaff*, BGB, § 611 Rn. 27.
[543] MüKo/*Müller-Glöge*, BGB, § 611 Rn. 34.
[544] BGH, Urt. v. 17.10.1991 – III ZR 352/89, NJW-RR 1992, 560.

Ungeachtet dessen, dass sich die vertragsrechtliche Einordnung grundsätzlich nach den Hauptleistungspflichten richtet, stehen auch die übrigen gesetzlichen Regelungen zum Auftrag – hier insbesondere §§ 664 ff. BGB – einer entsprechenden Einordnung nicht entgegen.

Nach § 664 Abs. 1 S. 1 BGB ist die Geschäftsbesorgung zwar „im Zweifel" unübertragbar, während es dem Nutzer in aller Regel gleichgültig sein dürfte, wer den Stream bereitstellt. Gerade weil es sich aber um eine bloße Zweifelsregelung handelt, ist eine Abweichung im gesetzlichen Leitbild bereits angelegt.

Unerheblich ist auch, dass der Anbieter in aller Regel den Zeitpunkt für die Abrufbarkeit des Streams vorgibt, während es dem typischen Bild des Auftrages entspricht, dass Vorgaben zur Durchführung des Auftrages (Weisungen) vom Auftraggeber ausgehen (vgl. etwa § 665 BGB). Die vertragliche Vereinbarung des Zeitpunktes, in dem der Stream abrufbar zur Verfügung steht, ist Teil der Konkretisierung des Auftragsverhältnisses, binnen dessen der Nutzer ggf. Weisungen erteilen kann.

Schließlich kommt es für die Einordnung des Vertragsverhältnisses als Auftrag nicht darauf an, ob der Anbieter bei der Ausführung des Streaming-Vertrages etwas erlangt, was er nach § 667 BGB herausgeben könnte. Bei einer Vielzahl von klassischen Geschäften, die dem Auftragsrecht unterworfen sind, erlangt der Auftragnehmer nichts (z. B. Botengänge). Vor diesem Hintergrund kann auch dahinstehen, ob der Anbieter nach Ende des Vertragsverhältnisses bestimmte Daten des Nutzers „herausgeben" muss.

IV. Vertragsrechtliche Einordnung von On-Demand-Streaming

1. Technische Darstellung – „faktische Leistung des Anbieters an den Nutzer"

Beim On-Demand-Streaming kann der Nutzer auf einem Server gespeicherte Daten individuell an Orten und zu Zeiten seiner Wahl (per Link) abrufen. Sie werden dann über eine Punkt-zu-Punkt-Verbindung (sog. Unicast) an den Client übertragen. Der Nutzer kann grundsätzlich die Wiedergabe jederzeit anhalten, vor- und zurückspulen.[545]

Man unterscheidet das On-Demand-Streaming weiterhin in das True-On-Demand-Streaming und den Progressive Download. Beim Progressive Download wird eine Datei vollständig von einem Server heruntergeladen. Die (Zwischen-) Speicherung erfolgt dabei im Arbeitsspeicher oder auf der Festplatte. Das Abspielen der gestreamten Datei beginnt während des laufenden Downloads. Beim True-On-Demand-Streaming erfolgt hingegen keine vollständige Speicherung der Ziel-

---

[545] Vgl. *Galetzka/Stamer*, Streaming − aktuelle Entwicklungen in Recht und Praxis, MMR 2014, 292; *Koch*, Der Content bleibt im Netz − gesicherte Werkverwertung durch Streaming-Verfahren, GRUR 2010, 574.

datei, sondern es werden lediglich fortwährend Zwischenspeicherungen vorgenommen. Das Abrufen eines Videos auf der Plattform Youtube stellt ein typisches Beispiel für True-On-Demand-Streaming dar.[546]

2. Einordnung des Rechtsverhältnisses zwischen Anbieter und Nutzer

a. Urheberrechtliche Vorbetrachtung (rechtliche Natur der Leistung des Anbieters)

Auf die Ausführungen unter Ziffer III. 2. b) wird Bezug genommen. Hiernach bedarf es auch zur Erfüllung eines Vertrages über On-Demand-Streaming-Dienste grundsätzlich keiner Einräumung eines urheberrechtlichen Nutzungsrechts durch den Anbieter gegenüber dem Nutzer.[547]

Mit Blick auf die technischen Gegebenheiten schuldet der Anbieter bei Verträgen über On-Demand-Streaming folgerichtig typischerweise folgende (Haupt-) Leistungen:

> Verschaffung und Bereithaltung des Netzwerkzugangs zu encodierten (ggf. auch komprimierten) Video-/Audiosignalen, die auf einem Server hinterlegt sind, damit der Nutzer die Video-/Audiosignale *über eine gewisse Dauer* per Streaming konsumieren kann.[548]

Obwohl die Speicherung der Daten auf dem Server ein notwendiger Schritt beim On-Demand-Streaming ist, wird man sie nicht als Teil der Hauptleistung auffassen können. Für den „Gebrauch" des Werkes ist völlig unerheblich, wo die Daten hinterlegt sind. Im Übrigen dürfte es in der Regel auch so sein, dass der Anbieter auf fremde Server (Infrastruktur) zurückgreift.

b. Vertragstypologische Einordnung

Die vertragstypologische Einordnung von On-Demand-Streaming bereitet Probleme, und zwar insbesondere mit Blick auf die notwendige Abgrenzung von Dienst- und Mietvertrag.

Der Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte [COM(2015) 634 final], auf die nachfolgend noch näher einzugehen sein wird, ist ungeeignet, die vorstehende Problematik aufzulösen. Zwar erfasst der Richtlinienvorschlag durch die weite Definition von „digitalen Inhalten" in Art. 2 Nr. 1 RL-E auch Verträge über Streaming-Dienste. Die Richtlinie lässt jedoch bewusst offen, um welche (nationalen) Vertragstypen es sich bei Verträgen über

---

[546] Vgl. *Galetzka/Stamer*, Streaming − aktuelle Entwicklungen in Recht und Praxis, MMR 2014, 292.
[547] Vgl. *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3 (6).
[548] Zum Cloud Computing allgemein *Zech*, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3.

die Bereitstellung digitaler Inhalte handelt, wie in der Richtlinienbegründung ausdrücklich klargestellt wird (S. 7).

Letztlich ist eine differenzierte Betrachtung erforderlich:

(1) Einzelwerke im On-Demand-Streaming

Das „Entleihen" einer (Film-)DVD gegen Entgelt (etwa aus einer Videothek) unterfällt unstreitig dem Mietrecht. Fraglich ist deshalb zunächst, ob dies auch für On-Demand-Streaming-Verträge gilt, die nur ein konkretes Werk (wie etwa einen bestimmten Film) zum Gegenstand haben.

Nach § 535 Abs. 1 BGB genügt es für die Annahme eines Mietvertrages, dass der Vermieter dem Mieter den Gebrauch der Mietsache überlässt. Ohne abweichende Vereinbarung muss er ihm insbesondere keinen Besitz an der Mietsache einräumen. Ausreichend für die Anwendung von Mietrecht kann demzufolge bereits sein, wenn dem Mieter ein Online-Zugang zur Mietsache gewährt wird.[549] Diese Voraussetzungen sind bei einem On-Demand-Streaming-Vertrag als erfüllt anzusehen. Sein Kern liegt entsprechend der oben wiedergegebenen Definition der Hauptleistungspflicht des Anbieters in der Verschaffung der Nutzungsmöglichkeit von Daten, die dem Nutzer zeitweise über das Internet zur Verfügung gestellt werden und die er nutzungsabhängig vergüten muss.[550] Der On-Demand-Streaming-Vertrag entspricht daher seinem Wesen nach einem Mietvertrag.

Als problematisch erweist sich – analog zur ASP-Entscheidung – zwar, dass das Mietrecht des BGB nach dem Wortlaut des § 535 Abs. 1 BGB von der Miete einer Sache (§ 90 BGB) ausgeht. Der BGH hat jedoch bereits mehrfach entschieden, dass eine auf einem Datenträger verkörperte Standardsoftware wie eine bewegliche Sache zu behandeln ist. Er zieht insofern den Vergleich zu einem Buch, das als Ergebnis einer schöpferischen Geistestätigkeit allein wegen seines Inhalts, nicht wegen seines Informationsträgers, dem Papier, erworben wird. Zwar erfolgt beim On-Demand-Streaming – anders als beim ASP-Vertrag – keine physikalische Zuordnung des Streams zu jedem einzelnen Nutzer. Die encodierten Daten sind jedoch auf Servern hinterlegt, sodass die Voraussetzungen der Körperlichkeit der Sache (i. S. d. BGH-Rechtsprechung) letztlich erfüllt sind.[551]

Für die Einordnung als Mietvertrag spricht schließlich auch der Vergleich mit der Miete eines Datenträgers (Bsp.: Film-DVD). Dies gilt auch mit Blick auf die folgenden, im Wesentlichen technisch bedingten Besonderheiten beim On-Demand-Streaming:

---

[549] Vgl. BGH, Urt. v. 15.11.2006 – XII ZR 120/04, NZM 2007, 379, unter Hinweis auf das Urteil vom 28.10.1992 – XII ZR 92/91, zur Nutzung der Kapazitäten eines Großrechners über „Fernzugang".

[550] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 46.

[551] Borges/*Meents*, Rechtshandbuch Cloud Computing, § 4 Rn. 47.

- Die Wiedergabe des Streams erfordert eine spezielle Decoder-Software beim Clienten;
- Die Daten sind ggf. fragmentiert auf mehrere Server verteilt;
- Der Anbieter hält ggfs. mehrere Streams mit unterschiedlicher Qualität (Encodierung/Übertragungsgeschwindigkeit) und Inhalten (bspw. Sprache) bereit;
- Der Nutzer kann mehrfach (ggfs. sogar zeitgleich) auf den Stream zugreifen;
- Der Nutzer erhält eine sequentielle Kopie der Daten;
- Der Anbieter kann zeitgleich auch anderen Nutzern den Zugriff auf die Daten ermöglichen.

Die Unterschiede zur Miete eines Datenträgers erfordern keine abweichende vertragstypologische Einordnung. Auch im Falle der Verwendung von DVDs erfordert etwa das Abspielen eines Films ggf. eine bestimmte (Decoder-)Software und den Zugriff auf mehrere Fragmente (DVDs). Es kommt zudem nicht selten vor, dass mehrere Versionen eines Werkes auf einem Datenträger gespeichert sind. Dabei dürfte die Frage, welchen Zustand die Mietsache aufweisen muss, um zum vertragsgemäßen Gebrauch geeignet zu sein, (nur) die Frage der konkreten Ausgestaltung des Mietverhältnisses bzw. die Konkretisierung der Hauptleistungspflicht betreffen.

Eine andere Beurteilung ergibt sich auch nicht daraus, dass für den Abspielvorgang beim On-Demand-Streaming die Erstellung einer sequentiellen Kopie der Daten beim Clienten erforderlich ist. Bei einer Gesamtbetrachtung des Abspielvorgangs ergeben sich angesichts der automatischen Löschung der Kopien keine Besonderheiten im Vergleich zum Abspielen eines Datenträgers.

Schließlich handelt es sich bei der vielfachen Verwertungsmöglichkeit des Anbieters beim On-Demand-Streaming zwar um einen erheblichen Unterschied im Vergleich zur Vermietung eines Datenträgers. Dies hat jedoch keine unmittelbaren Auswirkungen auf das konkrete Vertragsverhältnis zwischen Anbieter und Nutzer.

Zumindest im Ergebnis ist es deshalb gerechtfertigt, eine vertragstypologische Einordnung von On-Demand-Streaming eines konkreten Werkes als Mietvertrag i. S. v. § 535 BGB vorzunehmen, zumal sich letztlich auch das überwiegende Schrifttum bei Cloud Computing-Verträgen ganz allgemein für die Anwendung von Mietrecht ausspricht.[552] Im Übrigen ist mit Blick auf die oben genannte ASP-

---

[552] *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, S. 33.

Rechtsprechung des BGH zu vermuten, dass sich die Rechtsprechung bei Fortgeltung der bestehenden Rechtslage ebenfalls zur Anwendung mietrechtlicher Vorschriften entschließen wird. Bisher ist kein Urteil öffentlich geworden, das sich vertieft mit dieser Problematik befasst hat.

(2) Werksammlungen bzw. Abonnements

Die wechselseitigen Vertragspflichten bei umfassenderen Streaming-Verträgen können unterschiedlich ausgestaltet sein. Dies gilt insbesondere auch mit Blick auf die Modalitäten des „Einzelabrufs“. Eine allgemeingültige vertragstypologische Einordnung erscheint daher nicht möglich, sondern hängt von den konkreten Umständen des Einzelfalls ab. Üblicherweise dürften drei Vertragstypen in Betracht kommen:

- Mietvertrag:
- Dienstvertrag;
- Rahmenvertrag, gerichtet auf den wiederkehrenden Abschluss von Miet-, Leih- und/oder Dienstverträgen.

Ist Gegenstand des On-Demand-Streaming-Vertrages eine konkret umschriebene Werksammlung (ein bestimmter Datenbestand), dürften die vorstehenden Ausführungen zu „Einzelwerken im On-Demand-Streaming“ entsprechend gelten. Die gängigen Geschäftsmodelle haben jedoch einen anderen Inhalt, wie ein Blick auf die Geschäftsbedingungen etwa von „Netflix“ oder „Amazon Prime“ verdeutlicht. Angeboten werden von dort sog. „Mitgliedschaften“ oder „Abonnement-Dienste“, bei denen sich der Anbieter (lediglich) verpflichtet, zu Gunsten des Nutzers eine Auswahl von Werken als Stream verfügbar zu halten. Die konkrete Ausgestaltung der Werkauswahl ist dem Anbieter vertraglich ebenso vorbehalten wie ihre stetige Änderung.

Auf Verträge, die auf der Grundlage solcher (flexiblen) Angebote abgeschlossen werden, wird Mietrecht mangels hinreichender Bestimmtheit des Leistungsgegenstandes – der Mietsache – in aller Regel keine Anwendung finden. Zwar besteht auch hier ein wesentliches Merkmal des Streaming-Vertrages in der Verschaffung der Nutzungsmöglichkeit von Daten. Es hängt jedoch von der Werkauswahl des Anbieters ab, welche Daten konkret zur Verfügung gestellt werden. Dieses Wahlrecht dürfte regelmäßig nicht mit der „bloßen“ Einräumung eines Leistungsbestimmungsrechts gemäß § 315 BGB zu erfassen sein.

Die Vereinbarung eines Leistungsbestimmungsrechts nach § 315 BGB setzt die Einigung auf einen Maßstab voraus, nach dem die Leistungsbestimmung erfolgen soll (bspw. ein Doppelzimmer in einem bestimmten Hotel); die Vereinbarung eines „schrankenlosen Wahlrechts“ des Schuldners ist unwirksam, da es dem

Schuldner sonst möglich wäre, seine Verpflichtung als „Essentialie des Vertrages“ vollständig auszuschließen.[553] Soll Gegenstand des Leistungsbestimmungsrechts die Hauptleistungspflicht des Vermieters aus einem Mietvertrag sein, muss folgerichtig die Mietsache – hier die verkörperten Daten (s. o.) – rahmenmäßig bestimmt sein. Dies ist bei kommerziellen Streaming-Angebote in der Regel aber nicht der Fall. Netflix umschreibt die Auswahl der angebotenen Serien und Filme (Daten) etwa wie folgt:

> *„Bei Netflix gibt es Tausende Filme und Serien, die Sie sich sofort auf jedem Gerät ansehen können, das Netflix streamen kann. Sie können beliebig oft pausieren, vor- und zurückspulen oder immer wieder neu ansehen – natürlich alles ohne Werbung. Es ist wirklich so einfach.“*[554]

Selbst wenn in dem Abonnementvertrag der Inhalt der Leistung hinreichend rahmenmäßig beschrieben worden sein sollte, um für einen Mietvertrag als tragfähige Grundlage für eine Leistungsbestimmung nach billigem Ermessen gemäß § 315 Abs. 1 BGB zu dienen, ist zu beachten, dass diese Entscheidung nach § 315 Abs. 3 S. 2 BGB gerichtlich überprüfbar und ggf. durch gerichtliches Urteil zu ersetzen ist. Es dürfte aber von den Vertragsparteien nicht gewollt sein, dass ein Gericht entscheiden soll, welche aktuellen Filme und Serien konkret anzubieten sind. Dies gilt nicht zuletzt aus Sicht des Anbieters, der die fremdbestimmte Leistung ggf. zu erbringen hätte. In diesem Zusammenhang ist zudem von besonderer Bedeutung, dass sich das erforderliche Verhalten des Anbieters nicht in der Auswahl des Filmes oder der Serie aus einem bereitstehenden „Pool“ von Werken erschöpft. In Abgrenzung zu „illegalen“ Streaming-Angeboten hat der Anbieter darüber hinaus die urheberrechtlichen Nutzungsrechte zu erwerben. Eine Leistungsbestimmung durch das Gericht würde daher zumindest mittelbar den Anbieter über die Entscheidung nach § 315 Abs. 3 S. 2 BGB hinaus dazu verpflichten, die entsprechenden Rechte zu erwerben. Diese „Erwerbspflicht“ dürfte sich aber mit der mietvertraglichen Hauptleistungspflicht zur Gebrauchsüberlassung gemäß § 535 Abs. 1 S. 1 BGB nicht mehr erklären lassen.

Es erscheint für Anbieter wie „Netflix“ oder „Amazon Prime“ vielmehr charakteristisch, dass sie - neben der Einräumung der Nutzungsmöglichkeit an den Daten - ihr Angebot fortlaufend aktualisieren, zu diesem Zweck in ständigem Kontakt zu den Urhebern der Werke stehen und von ihnen die Nutzungsrechte erwerben. Teilweise produzieren die Anbieter sogar eigenständig Filme und Serien, wie z. B. die „Netflix Original“-Angebote. Sofern die Nutzungsbedingungen der Anbieter also den Abschluss eines „Abonnement-Pakets“ vorsehen, bei dem der Nutzer gegen monatliche Zahlungen beliebig häufig Inhalte abrufen kann, die ständig verändert und aktualisiert werden, spricht vieles für die Anwendung von Dienstvertragsrecht.

---

[553] Vgl. RG, Urt. v. 11.12.1897 – I 269/97, RGZ 40, 195 (200); Staudinger/*Rieble*, BGB, § 315 Rn. 12, 41 ff., 253 ff.

[554] Siehe https://help.netflix.com/de/node/412 (letzter Abruf: 1.2.2017).

Je nach der Ausgestaltung der Modalitäten des Einzelabrufs kommt allenfalls noch die Konstruktion über einen Rahmenvertrag und den wiederkehrenden Abschluss einzelner Nutzungsverträge in Betracht. Ein Rahmenvertrag ist dadurch gekennzeichnet, dass er für künftig abzuschließende Einzelverträge einen Teil des Inhalts vorwegnimmt, die konkreten rechtlichen Bindungen aber erst durch den Abschluss der Einzelverträge entstehen.[555]

Im Fall von „reinen Abonnement-Paketen" dürften die konkreten Pflichten – Verschaffung der Nutzungsmöglichkeit fortlaufend aktualisierter Inhalte gegen Zahlung eines monatlichen Entgelts – zwar bereits durch den Abschluss eines (einheitlichen) Dienstvertrags begründet werden. Der Aufteilung in Rahmen- und Einzelverträge bedarf es hier nicht. Insbesondere dürfte der Abruf der Daten durch die Nutzung des einzelnen Links rein faktischer Natur sein und keine weiteren Rechtspflichten mehr erzeugen.

Teilweise sehen die Geschäftsmodelle im Bereich des On-Demand-Streaming aber auch (ergänzend) vor, dass man für bestimmte Inhalte zunächst einen Vertrag über die „Mitgliedschaft" bzw. die „Registrierung" abschließen muss und (erst) danach – neben den „abonnierten Inhalten" – auf weitere kostenpflichtige Inhalte zurückgreifen kann (sog. „Pay per View"). Hier dürfte der Vertrag über die „Mitgliedschaft" einen Rahmenvertrag darstellen, der z. B. Zahlungsmodalitäten oder Pflichten im Zusammenhang mit dem Umgang der zur Verfügung gestellten Inhalte regelt. Die konkreten Pflichten zur Bereitstellung des Einzelwerks und zur Zahlung des Entgelts dürften erst mit dem Einzelabruf entstehen, der entsprechend der Ausführungen zu den Einzelwerken im On-Demand-Streaming grundsätzlich als Mietvertrag einzuordnen sein wird.

(3) Typengemischte/Zusammengesetzte Verträge

Sind Gegenstand des Vertrages über Streaming-Dienste weitere Leistungen, ändert dies zunächst nichts an der Grundentscheidung für die vertragstypologische Einordnung des Live-Streaming bzw. On-Demand-Streaming. Zu unterscheiden sind im Wesentlichen drei Konstellationen:

- Stellen die weiteren Leistungspflichten bloße Nebenabreden dar, setzt sich das Recht der Hauptleistung grundsätzlich durch.

- Hat der Anbieter über die oben beschriebenen Leistungen weitere „selbstständige Leistungen" zu erbringen (Bsp.: Hotlineservice), handelt es sich um einen sog. zusammengesetzten Vertrag, bei dem jeder Vertragsteil nach dem Recht des auf ihn zutreffenden Vertragstypus zu beurteilen ist, soweit dies nicht im Widerspruch zum Gesamtvertrag steht.[556]

---

[555] Staudinger/*Feldmann/Löwisch*, BGB, § 311 Rn. 25.

[556] Vgl. auch hier die ASP-Entscheidung des BGH, Urt. v. 15.11.2006 – XII ZR 120/04, NZM 2007, 379.

- Werden die einzelnen Elemente von Streaming-Diensten zu einem eigenen Vertragstyp „verschmolzen“, handelt es sich um einen sog. typengemischten Vertrag, bei dem ggf. jede einzelne Pflicht gesondert zu bewerten ist.

Die Thematik ist im Rahmen dieses Arbeitspapiers nicht weiter zu vertiefen, da es zunächst darum geht, die schuldrechtlichen Besonderheiten/Charakteristika von „reinen“ Streaming-Diensten herauszuarbeiten. Auf etwaige „Mischformen“ ist ggf. zu einem späteren Zeitpunkt einzugehen.

V. Zwischenergebnis

Das deutsche Schuldrecht hält für die Vereinbarung von Streaming-Diensten keine speziellen Regelungen bereit. Einer allgemeingültigen Subsumtion unter bereits vorhandene Vertragstypen steht entgegen, dass ein solcher Vertrag ganz unterschiedliche Rechte und Pflichten der Vertragsparteien beinhalten kann. Besonders deutlich wird dies anhand eines Vergleichs zwischen der unentgeltlichen und einmaligen Nutzung eines Live-Streaming-Angebotes und dem Abschluss eines kostenpflichtigen Abonnementvertrages über Leistungen per On-Demand-Streaming. Wichtige Differenzierungsmerkmale sind folgerichtig:

- Live-Streaming/On-Demand-Streaming;
- Unentgeltlichkeit/Entgeltlichkeit;
- Einmalige Nutzung/Dauerschuldverhältnis.

Abhängig von der konkreten Ausgestaltung dürfte die Rechtsprechung im Grundsatz vermutlich folgende Einordnung vornehmen:

- Live-Streaming = Dienstvertrag oder Auftrag;
- On-Demand-Streaming (Vertrag erfasst bestimmtes Werk) = Miete oder Leihe;
- Abonnement-Verträge über On-Demand-Streaming (abhängig von konkreter Vereinbarung) =
    - Mietvertrag;
    - Dienstvertrag;
    - Rahmenvertrag, auf den wiederkehrenden Abschluss von Miet-, Leih- oder Dienstverträgen gerichtet.

Aus Sicht der Vertragsparteien dürfte diese Differenzierung in der Regel schwer verständlich sein. Zum einen wird eine Vielzahl der Beteiligten schlicht davon ausgehen, dass Leistungen eines Streaminganbieters bzw. die darauf abzielenden Verträge einheitlich dem Recht eines bestimmten Vertragstyps unterliegen. Zudem wird einer nicht juristisch vorgebildeten Vertragspartei zumeist nur schwer

zu vermitteln sein, dass für die vertragsrechtliche Einordnung von zentraler Bedeutung ist, ob und ggf. wie konkret die (verkörperten) Daten vertragsmäßig bestimmt sind. Insbesondere der Nutzer wird vielmehr im Wesentlichen auf den begehrten „Werkgenuss“ beim Streaming abstellen wollen.

Die auf der Anwendbarkeit unterschiedlicher Vertragstypen gründende Unsicherheit bei der konkreten Rechtsanwendung ist ein wichtiger Aspekt bei der Frage, ob gesetzgeberischer Handlungsbedarf besteht. Sie ist jedoch nicht isoliert zu betrachten. In einem nächsten Schritt ist vielmehr zu prüfen, ob die zugeordneten Vertragstypen jeweils angemessene Lösungen für die Vertragsparteien bereithalten. Hiervon hängt ggf. ab, ob mit dem Ziel einer einheitlichen Regelung durch den Gesetzgeber ein eigener Vertragstyp geschaffen oder zumindest – so der Vorschlag von *Faust*[557] – eine Zuordnung zu einem bereits bestehenden Vertragstyp herbeigeführt werden sollte. Soweit geboten, fließen in diese Überlegungen auch die Beschlüsse des 71. Deutschen Juristentages 2016 ein.

VI. Problemfelder/Praktische Fragestellungen aus Sicht der Beteiligten beim On-Demand-Streaming

1. Vorbemerkungen

a. Fokus auf On-Demand-Streaming

Die vorstehenden Ausführungen haben gezeigt, dass die vertragstypologische Einordnung von Vereinbarungen über On-Demand-Streaming-Dienste weitaus größere Probleme bereitet als die Einordnung von Verträgen über Live-Streaming-Dienste. Zugleich ist das Leistungsspektrum durch die für eine gewisse Dauer geschuldete Bereithaltung des Streams üblicherweise deutlich höher, insbesondere wenn Gegenstand der Vertragsbeziehung ein Abonnement (Dauerschuldverhältnis) über On-Demand-Streaming-Dienste ist.

Die weitere Prüfung konzentriert sich daher auf (Abonnement-)Verträge über On-Demand-Streaming-Dienste und die Geeignetheit der vorhandenen schuldrechtlichen Regelungen als (gesetzlicher) Rechtsrahmen für derartige Vertragskonstellationen. Für diese Vorgehensweise spricht auch, dass zwar nicht völlig auszuschließen ist, dass ein etwaiger gesetzgeberischer Handlungsbedarf im Vertragsrecht auch Regelungen zum Live-Streaming erfasst. Dies kommt jedoch vor allem dann in Betracht, wenn (auch) die gegenwärtige Rechtslage keine angemessenen Lösungen für den Bereich des On-Demand-Streaming bereithält.

Zudem liegt der Schwerpunkt dieser Untersuchung auf Streaming-Verträgen, die als gegenseitiger Vertrag ausgestaltet sind, d. h. bei denen der Nutzer im Austausch eine Gegenleistung zu erbringen hat. Wegen der rechtlichen Einordnung von „Daten als Entgelt“ wird auf den nachfolgenden Abschnitt G. Bezug genommen.

---

[557] Vgl. *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, S. 34.

b. AGB-Kontrolle

Bei den klassischen Streaming-Angeboten (s. o.) handelt es sich zumeist um Massengeschäfte, zu deren rechtlicher Ausgestaltung sich die Betreiber Allgemeiner Geschäftsbedingungen bedienen. Der VZBV e.V. hat im Jahr 2014 insgesamt zwanzig Abmahnungen gegen vierzehn Dienste ausgesprochen und dabei – neben überlangen Vertragsbedingungen – 130 Klauseln beanstandet. Betroffen waren hiervon insbesondere Klauseln mit folgenden Inhalten:

- Einseitiges Recht des Anbieters zur Beschränkung und Veränderung des Leistungsgegenstandes;
- Jederzeitiges Kündigungsrecht des Anbieters;
- Einschränkungen von Mängelrechten/Haftungsansprüchen des Nutzers;
- Verwendung rechtswidriger Datenschutzbestimmungen.[558]

Für die Beurteilung gesetzgeberischen Handlungsbedarfs ist daher ungeachtet der vertragstypologischen Einordnung von Streaming-Verträgen darauf zu achten, dass das (allgemeine) AGB-Recht zumindest für Massengeschäfte bereits einen Rechtsrahmen setzt, der selbst bei Fehlen eines gesetzlichen Leitbildes auf einen angemessenen Ausgleich der Interessen der Vertragsparteien abzielt. Von Bedeutung sind insoweit insbesondere die Klauselverbote in §§ 308 und 309 BGB, aber auch etwaige Informationspflichten des Anbieters nach Art. 246 und 246a EGBGB.

c. EU-Richtlinienvorschlag über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte

Die EU-Kommission hat im Dezember 2015 als Teil ihrer Binnenmarktstrategie einen Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte [COM(2015) 634 final] vorgelegt.[559] Die Richtlinie soll von wenigen Ausnahmen abgesehen für alle entgeltlichen Verträge zwischen Verbrauchern und Unternehmern über die Bereitstellung von digitalen Inhalten gelten. Dazu gehören mit Blick auf Art. 2 RL-E auch Vereinbarungen über Streaming-Dienste, wie in Erwägungsgrund 11 ausdrücklich klargestellt wird.

Der Richtlinienvorschlag ist vor allem unter zwei Aspekten von besonderer Bedeutung:

- Die beabsichtigte Vollharmonisierung würde dazu führen, dass der nationale Gesetzgeber bei der Richtlinienumsetzung nur dort über einen eigenen Spielraum verfügt, wo die Richtlinie einen solchen ausdrücklich eröffnet

---

[558] Vgl. Pressemitteilung VZBV vom 14.5.2014, abrufbar (mit Link zur Auflistung der Vorgänge) unter http://www.vzbv.de/pressemitteilung/streaming-dienste-fallen-durch-agb-check (letzter Abruf: 2.5.2017).
[559] Nachfolgend RL-E.

(Bsp.: Art. 14 Abs. 2 RL-E) oder selbst keine konkrete Regelung trifft (Bsp.: B2B-Verträge). Ausgeschlossen wären demzufolge im Anwendungsbereich der Richtlinie nach gegenwärtigem Stand bspw. - mit Ausnahme von Schadensersatzansprüchen - ergänzende/abweichende Regelungen hinsichtlich der konkreten Ausgestaltung von Gewährleistungsansprüchen (Abhilfe bei nicht erfolgter Bereitstellung oder Vertragswidrigkeit, vgl. Art. 11ff. RL-E).

- Fraglich ist, ob die vorgeschlagene Richtlinie (auch) für Streaming-Verträge ein tragfähiges Konzept für einen angemessenen Rechtsrahmen bereitstellt (und damit ggfs. auch außerhalb ihres Anwendungsbereichs ein Vorbild für den nationalen Gesetzgeber sein kann). Dies gilt insbesondere mit Blick darauf, dass die Richtlinie die Verträge über die „Bereitstellung digitaler Inhalte“ keinem (im BGB) bestimmten Vertragstyp zuordnet. Dabei ist kritisch zu hinterfragen, ob damit zugleich ein Verzicht auf gesetzliche Leitbilder (i. S. v. § 307 Abs. 2 BGB) verbunden ist und deshalb – abseits der Klauselverbote in §§ 308, 309 BGB – etwaige Leistungsbeschreibungen der Anbieter grundsätzlich Vertragsinhalt werden, soweit sie nur hinreichend transparent i. S. v. Art. 6 RL-E sind.

2. Einzelne vertragsrechtliche Pflichten / Problemstellungen

Im September 2015 haben die Verbraucherzentralen im Zusammenhang mit dem Marktwächter Digitale Welt einen Bericht vorgestellt, wonach bei einer repräsentativen Umfrage jeder vierte Nutzer (26 Prozent) von Problemen beim Streaming, darunter häufigen Störungen beim Empfang, Problemen mit Preisen und Mitgliedschaft sowie urheberrechtlichen Fragen, etwa die Unterscheidung legaler und illegaler Angebote, berichtet hat.[560] Nachfolgend wird im Einzelnen auf die Vertragspflichten bzw. denkbaren schuldrechtlichen Problemstellungen bei On-Demand-Streaming-Diensten eingegangen und untersucht, ob das geltende Schuldrecht zu interessengerechten Lösungen führt. Ein besonderes Augenmerk wird dabei auf die Abgrenzung von Miet- und Dienstvertragsrecht gelegt.

a. Verfügbarkeit

Für das gesetzliche Leitbild des Mietvertrages ist Anknüpfungspunkt § 535 Abs. 1 S. 2 BGB. Danach gehört es zu den Hauptleistungspflichten des Vermieters, die Mietsache während der gesamten Dauer des Mietvertrages in einem vertragsgemäßen Zustand zu halten. Übertragen auf On-Demand-Streaming-Dienste heißt das, dass der Anbieter für die gesamte Dauer des Vertrages – im Grundsatz – eine 100%ige Verfügbarkeit der in den Vertrag einbezogenen Werke (d. h. eine Zugriffsmöglichkeit auf die hinterlegten Audio-/Videodaten) sicherzustellen

---

[560] Pressemitteilung VZ Rheinland-Pfalz vom 2.9.2015, abrufbar unter http://www.verbraucherzentrale-rlp.de/streaming--jeder-vierte-nutzer-berichtet-von-problemen-2 (letzter Abruf: 2.5.2017).

hat.[561] Im Falle einer Verletzung dieser Vertragspflicht drohen die (gesetzliche) Minderung der geschuldeten Miete oder anderweitige Gewährleistungsansprüche.

Den Parteien steht es zwar im Wesentlichen frei, abweichend von § 535 Abs. 1 S. 2 BGB (zu Gunsten des Anbieters) eine „Verfügbarkeitsquote" individualvertraglich zu vereinbaren, um etwa erforderliche Wartungszeiten zu berücksichtigen. Eine vergleichbare Regelung in Allgemeinen Geschäftsbedingungen wird sich jedoch in der Regel an §§ 307 ff. BGB messen lassen müssen und dürfte deshalb nur in verhältnismäßig engen Grenzen zulässig sein.[562]

Sinnvoll anzuwenden sind diese Grundsätze nur bei solchen Verträgen, die auch schon jetzt als Mietvertrag einzuordnen sind, also ein konkret umschriebenes Werk oder eine bestimmte Werkauswahl betreffen. Hier trägt die ständige Bereithaltung des „Mietobjektes" über den vertraglich vereinbarten Zeitraum den wechselseitigen Interessen der Vertragsparteien angemessen Rechnung.[563] Hingegen passt das Leitbild einer ständigen Verfügbarkeit nicht zu den „dynamischen Diensten" der vorherrschenden Geschäftsmodelle. Wie bereits dargestellt, sind diese Angebote darauf ausgerichtet, zu Gunsten des Nutzers eine Auswahl von Werken als Stream verfügbar zu halten. Die konkrete Ausgestaltung der Werkauswahl (Konkretisierung der abrufbaren Daten) ist dem Anbieter vertraglich ebenso vorbehalten wie ihre stetige Änderung.

Folgerichtig ist für diese Verträge – entsprechend der vorgenommenen vertragstypologischen Einordnung – die Anwendung des (flexibleren) Dienstvertragsrechts zielführend. Danach schuldet der Anbieter zwar auch „die versprochenen Dienste" (§ 611 Abs. 1, 1. Hs. BGB). Anders als beim sachbezogenen Mietrecht erfasst die Hauptleistungspflicht hier jedoch nicht die Bereitstellung eines bestimmten Datenbestandes. Sie ist vielmehr von vorneherein auf ein wechselndes Programmangebot ausgerichtet, was impliziert, dass dem Nutzer zumindest zeitweise bestimmte Werke nicht zur Verfügung stehen.

b. Vertragsgemäßheit der Leistung im Übrigen

Gemäß § 535 Abs. 1 S. 2 BGB hat der Vermieter dem Mieter die Mietsache in einem zum vertragsgemäßen Gebrauch geeigneten Zustand zu überlassen und sie während der Mietzeit in diesem Zustand zu erhalten. Was als vertragsgemäßer Gebrauch angesehen wird, richtet sich dabei in erster Linie nach der konkreten Vereinbarung. Erst wenn eine Bestimmung fehlt und sich der nähere Inhalt auch

---

[561] Vgl. zum Cloud Computing allgemein: *Hilber*, Handbuch Cloud Computing, Teil 2, Rn. 219; *Wicker*, Haftet der Cloud-Anbieter für Schäden beim Cloud-Nutzer? Relevante Haftungsfragen in der Cloud, MMR 2014, 715 (716).

[562] Vgl. *Hilber*, Handbuch Cloud Computing, Teil 2, Rn. 220; Borges/*Meents*, Handbuch Cloud Computing, § 4 Rn. 260 ff. − anders als nach Borges/*Meents* dürfte nach hiesiger Auffassung bei Anwendung von Mietrecht sogar jede Vereinbarung einer Verfügbarkeitsquote der AGB-Kontrolle unterliegen, da das Hauptleistungsversprechen abweichend vom Gesetz ausgestaltet werden soll (vgl. hierzu MüKo/*Wurmnest*, BGB, § 307 Rn. 12).

[563] Vgl. auch die Ausführungen zum Cloud Computing unter vorstehender Ziffer D. IV. 1.

nicht durch Auslegung anhand des Vertragszwecks ermitteln lässt, ist der übliche Gebrauch zu gewähren.[564]

Der anknüpfend an den Sachbezug des Mietrechts in dieser Vorschrift zum Ausdruck kommende Regelungsgehalt ist beim Streaming durchaus kritisch zu sehen. Aus Sicht des Nutzers ist für den vertragsgemäßen Gebrauch in erster Linie maßgeblich, dass die vom Anbieter bereit gehaltenen Audio-/Videodateien auf seinem Empfangsgerät/seinen Empfangsgeräten störungsfrei (und in der gewünschten Qualität) abzuspielen sind. Der Anbieter wird zwar in der Regel zu diesem Zweck mehrere Versionen/Varianten eines Werkes vorhalten. Es liegt jedoch außerhalb seines Verantwortungsbereichs, welches Empfangsgerät der Nutzer (jeweils) verwendet.

Allerdings lässt sich dieses Problem – analog zu den obigen Überlegungen zur vertragstypologischen Einordnung sowie der Miete einer Film-DVD – durch eine entsprechende Konkretisierung der Hauptleistungspflicht lösen. Soweit die Parteien die Verwendung auf einem bestimmten Endgerät vereinbaren, gehört eine entsprechende Abspielmöglichkeit zum vertragsgemäßen Gebrauch des Streams. Liegt hingegen keine besondere Vereinbarung vor, ist die Leistung des Anbieters auch nur am technischen Standard zu messen.[565]

Die Anwendung mietrechtlicher Grundsätze führt daher an dieser Stelle zu denselben Ergebnissen wie die Anwendung von Dienstvertragsrecht. Die Unterscheidung zwischen beiden Vertragstypen wird erst wieder bei der Frage relevant, welche Rechte der Nutzer hat, wenn der Anbieter nicht vertragsgemäß leistet (siehe hierzu nachfolgend unter c.).

Der o.g. Richtlinienentwurf enthält in Art. 6 RL-E eine Regelung zur Vertragsgemäßheit digitaler Inhalte. Auch hiernach soll es zunächst auf den konkreten Vertragsinhalt ankommen (Abs. 1), bevor objektive Maßstäbe herangezogen werden (Abs. 2).

c. Gewährleistung

Findet Mietrecht Anwendung und hat die Mietsache einen Mangel (§ 536 Abs. 1 BGB) bzw. ist dem Nutzer der Gebrauch der Mietsache durch das Recht eines Dritten mindestens teilweise entzogen, gilt Folgendes:

- Der Nutzer kann die Beseitigung des Mangels verlangen;
- Für die Zeit, in der die Tauglichkeit der Mietsache wegen des Mangels aufgehoben ist, schuldet der Nutzer – von Gesetzes wegen – keine Miete;

---

[564] Vgl. MüKo/*Häublein*, BGB, § 535 Rn. 65.

[565] Eine gemietete Film-DVD ist auch nicht allein deshalb mangelhaft, weil ich über kein geeignetes Abspielgerät verfüge.

- Für die Zeit, in der die Tauglichkeit der Mietsache mehr als nur unerheblich gemindert ist, hat der Nutzer – ebenfalls von Gesetzes wegen – nur eine angemessen herabgesetzte Miete zu entrichten;

- Ist dem Nutzer durch den Mangel ein Schaden entstanden und hat der Anbieter den Mangel zu vertreten, hat der Anbieter Schadensersatz zu leisten – bei anfänglichen Mängeln haftet der Anbieter sogar verschuldensunabhängig (§ 536a BGB);

- Liegen die Voraussetzungen der §§ 536b bis 536d BGB vor (Kenntnis des Mangels bei Vertragsschluss, Unterlassen einer erforderlichen Mängelanzeige, vertraglicher Gewährleistungsausschluss), entfallen die vorstehenden Gewährleistungsansprüche des Nutzers.

Demgegenüber kennt das Dienstvertragsrecht keine Gewährleistungsansprüche des Dienstberechtigten. Etwaige Ansprüche wegen Vertragspflichtverletzungen richten sich allein nach §§ 280 ff. BGB. Sie sind demzufolge stets auf Schadensersatz gerichtet und setzen grundsätzlich ein Verschulden des Dienstverpflichteten voraus.

Der 71. Deutsche Juristentag 2016 – Abteilung Zivilrecht – hat unter Ziffer 22 mehrere Beschlüsse gefasst, die mit Blick auf Verträge über „digitale Dienste“ auf eine Änderung des Leistungsstörungsrechts bei Dauerschuldverhältnissen abzielen.[566] Hervorzuheben ist in diesem Zusammenhang die Forderung, abweichend von den bestehenden Regeln des Dienstvertrages ein Minderungsrecht vorzusehen.

Die Forderung des Deutschen Juristentages erscheint nachvollziehbar. Insbesondere aus Nutzersicht dürfte die Beschränkung auf Schadensersatzansprüche nach §§ 280 ff. BGB bei Schlechtleistungen des Anbieters einer Vielzahl von Dienstverträgen (über digitale Inhalte) nicht mehr gerecht werden. Dies gilt im Grundsatz auch für die wechselseitigen Interessen beim On-Demand-Streaming, und zwar insbesondere mit Blick auf die Frage einer verschuldensunabhängigen Minderung der Gegenleistung. Hier sollte nicht danach zu differenzieren sein, ob die Leistung des Anbieters in der (ständigen) Bereithaltung eines bestimmten Werkes oder in einem ständig wechselnden Angebot von Werken besteht. Nicht nur im ersten (nach Mietrecht zu beurteilenden) Fall, sondern in beiden Fällen sollte der Nutzer für die Zeit bzw. in dem Umfang, in dem die Leistung des Anbieters nicht vertragsgemäß ist, nur eine geminderte Gegenleistung schulden. Indes steht einer Begründung gesetzgeberischen Handlungsbedarfs unter Rückgriff auf die Verträge über On-Demand-Streaming-Dienste derzeit entgegen, dass es an belastbaren Erkenntnissen zu Schlechtleistungen bei On-Demand-Streaming-Diensten und deren vertragsrechtlicher Behandlung unter den Vertragsparteien fehlt. Dabei

---

[566] Ziffer 22 der Beschlüsse der Abteilung Zivilrecht, abrufbar unter www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf (letzter Abruf: 1.2.2017).

ist zu berücksichtigen, dass vorübergehende Probleme beim Empfang nicht geeignet sind, um etwa eine Forderung nach einem Minderungsrecht zu rechtfertigen. Dies gilt umso mehr, als auch im Mietrecht nicht jede Minderung der Tauglichkeit der Mietsache zur Mietminderung führt. Zudem verlangen die großen Anbieter von On-Demand-Streaming-Diensten (etwa Netflix oder Amazon Prime) gegenwärtig ein relativ geringes Entgelt. Eine Minderung der Vergütung – ein Minderungsrecht bei solchen Dienstverträgen unterstellt – würde daher wohl regelmäßig allenfalls wenige Euro ausmachen. Schließlich besteht für den Nutzer auch ohne den Vorwurf einer Schlechtleistung in der Regel die Möglichkeit, sich kurzfristig – zumeist binnen Monatsfrist – durch ordentliche Kündigung vom Vertrag zu lösen. Die Anbieter haben demzufolge ein eigenes Interesse daran, den Nutzer durch eine vertragsgerechte Leistung bzw. ein überzeugendes Streaming-Angebot zu binden.

Die vorstehenden Ausführungen gelten – zumindest aus Nutzersicht – gleichermaßen für die Frage, unter welchen Bedingungen sich der Anbieter durch Allgemeine Geschäftsbedingungen von einer Haftung freizeichnen kann.

Sollte der o.g. Richtlinienvorschlag umgesetzt werden, wird hinsichtlich der Haftung eine Unterscheidung zwischen Miet- und Dienstrecht vermutlich gänzlich entbehrlich werden. In Art. 11 und 12 RL-E ist ein einheitliches Haftungsregime für die Fälle vorgesehen, dass der Anbieter die digitalen Inhalte nicht bereitstellt oder nicht vertragsgemäß leistet. Lediglich die Ausgestaltung der Schadensersatzansprüche, die nach nationalem Recht aber ohnehin im Wesentlichen gleichlaufen, soll den nationalen Gesetzgebern überlassen werden.

d. Vergütung/Mietzins

§ 535 Abs. 2 BGB normiert nur die Pflicht des Mieters, die vereinbarte Miete zu zahlen. Die Höhe der Miete können die Parteien bis zur Grenze der Sittenwidrigkeit (§ 138 BGB) frei vereinbaren. Gleiches gilt für die Fälligkeit, auch wenn nach § 579 BGB eine Miete, die nach Zeitabschnitten bemessen ist, grundsätzlich nach Ablauf der einzelnen Zeitabschnitte zu leisten ist. Diese Vorschrift kann von den Parteien abbedungen werden. So ist etwa eine Abrechnung im Nachhinein nach dem exakten Verbrauch oder eine sog. Flatrate möglich. Ebenso können die Parteien frei regeln, wer das Risiko der „Buchungsmenge“ tragen soll.[567]

Die vorstehenden Ausführungen gelten entsprechend für das Dienstvertragsrecht und insbesondere für die dort in §§ 611, 612, 614 BGB getroffenen Regelungen zur Höhe und Fälligkeit der Vergütung. Auch hier sind die Vertragsparteien im Wesentlichen frei, Umfang und Fälligkeit der Vergütung vertraglich festzulegen.

Praktisch relevant dürfte indes die Frage sein, unter welchen Voraussetzungen der Anbieter eine „Preisanpassung“ im laufenden Vertragsverhältnis vornehmen darf. Hierzu finden sich aber weder im Miet- noch im Dienstvertragsrecht konkrete

---

[567] *Wicker*, Vertragstypologische Einordnung von Cloud Computing-Verträgen – Rechtliche Lösungen bei auftretenden Mängeln, MMR 2012, 783 (786).

Vorgaben. Maßgeblich sind insoweit die allgemeinen Regelungen zur Vertragsanpassung/-änderung (siehe insoweit nachfolgend unter e.).

e. Voraussetzungen für Vertragsanpassungen/-änderungen während der Vertragslaufzeit

Eine Abweichung vom Grundsatz der Vertragstreue (pacta sunt servanda) ist gemäß § 313 BGB grundsätzlich nur bei Wegfall der Geschäftsgrundlage vorgesehen. Daneben steht es den Parteien aber im Rahmen ihrer Privatautonomie und in den Grenzen des AGB-Rechts frei, einen Änderungsvorbehalt zu vereinbaren. Treffen die Parteien eine solche Vereinbarung, darf der Anbieter (ggfs.) in dem vertraglich vereinbarten Rahmen eine Änderung des Vertrages herbeiführen. Für die Bestimmung der geänderten Leistung gilt § 315 BGB. Grenzen für die formularmäßige Vereinbarung eines einseitigen Änderungsvorbehalts setzt § 308 Nr. 4 BGB. Danach ist die Vereinbarung eines Rechts des Verwenders, die versprochene Leistung zu ändern oder von ihr abzuweichen, in Allgemeinen Geschäftsbedingungen unwirksam, wenn nicht diese unter Berücksichtigung der Interessen des Verwenders für den anderen Vertragsteil zumutbar ist.

Der o.g. Richtlinienentwurf sieht in Art. 15 RL-E ebenfalls ein Recht zur (einseitigen) Vertragsänderung vor. Danach soll der Anbieter unter bestimmten Voraussetzungen seine vertraglich geschuldete Leistung ändern dürfen, während der Nutzer im Gegenzug ein außerordentliches Kündigungsrecht enthält. Wie das nationale Recht setzt auch Art. 15 RL-E voraus, dass die Parteien die Möglichkeit vereinbart haben, dass der Anbieter den Vertrag einseitig ändern darf.

Ergänzend ist an dieser Stelle allerdings darauf hinzuweisen, dass bei den oben beschriebenen Abonnement- und Rahmenverträge, soweit es sich um Dienstverträge handelt, die Flexibilität des Werkangebots (bereits) Gegenstand der Hauptleistungspflicht des Anbieters ist. Folgerichtig fällt die Konkretisierung bzw. Änderung der Werkzusammenstellung in diesen Fällen – anders als bei der Anwendung von Mietrecht – nicht unter § 315 BGB. Ungeachtet dessen gibt es hinsichtlich der Werkzusammenstellung der Anbieter ohnehin keine Anhaltspunkte dafür, dass die Anbieter ihre vertraglich eingeräumten Rechte (und Pflichten) auf Kosten der Nutzer ausüben (erfüllen). Vielmehr zeigt nicht zuletzt die Gewährung kurzer Kündigungsfristen von üblicherweise einem Monat, dass die Anbieter zumindest derzeit noch darum bemüht sind, im Wettbewerb möglichst viele Kunden zu gewinnen und zu binden.

f. Beendigungsmöglichkeiten

Im Falle der Anwendung mietrechtlicher Regelungen gilt hinsichtlich der Beendigung von Verträgen über On-Demand-Streaming-Dienste grundsätzlich Folgendes:

- Ist der Vertrag befristet, endet er mit Ablauf der vereinbarten Frist (§ 542 Abs. 2 BGB).

- Liegen die Voraussetzungen des § 543 BGB vor, besteht ein Recht zur außerordentlichen Kündigung.

- Weitere Beendigungstatbestände sind der Abschluss eines Aufhebungsvertrages, der Eintritt einer zuvor vereinbarten Bedingung, Rücktritt (§ 346 BGB), Unmöglichkeit, Anfechtung und Wegfall der Geschäftsgrundlage (§ 313 BGB).[568]

Daneben kommt ggf. eine ordentliche Kündigung nach § 580a Abs. 3 BGB in Betracht.[569] Hiernach ist eine ordentliche Kündigung mit einer Frist von höchstens 3 Tagen zulässig.

Bei Anwendung von Dienstvertragsrecht gilt grundsätzlich Folgendes:

- Ist das Dienstverhältnis auf bestimmte Zeit eingegangen, endigt es mit dem Ablauf der Zeit (§ 620 Abs. 1 BGB).

- Ist das Dienstverhältnis nicht befristet, kann es der Nutzer nach Maßgabe der §§ 621 bis 623 BGB kündigen – hiernach ist etwa die Kündigung eines Vertrages, bei dem die Vergütung nach Monaten bemessen ist, spätestens am 15. eines Monats für den Schluss des Kalendermonats zulässig (§ 621 Nr. 3 BGB).

- Liegen die Voraussetzungen des § 626 BGB vor, besteht ein Recht zur außerordentlichen Kündigung.

Aus Sicht des 71. Deutsche Juristentages – Abteilung Zivilrecht – bedarf es einer (einheitlichen) Regelung für ein Kündigungsrecht bei Verträgen über digitale Dienste. Danach soll zumindest im Wege einer Sonderregelung ein Kündigungsrecht von drei Monaten zum Kalendermonatsende vorgesehen werden.[570]

Art. 16 RL-E enthält bereits eine besondere Regelung zur ordentlichen Kündigung von Verträgen über die Bereitstellung digitaler Inhalte. Danach soll der Verbraucher bei unbefristeten oder länger als 12 Monate befristeten Verträgen berechtigt sein, den Vertrag jederzeit nach Ablauf von 12 Monaten zu beenden.

Mit Blick auf das On-Demand-Streaming ist derzeit indessen ein praktisches Bedürfnis für eine gesetzliche Regelung nicht erkennbar. Wie bereits dargestellt, gewähren die Anbieter ihren Kunden bereits freiwillig äußerst kurze Kündigungsfristen.

---

[568] Vgl. Palandt/*Weidenkaff*, BGB, § 542 Rn. 1 ff.

[569] Vgl. *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, S. 36, der die Regelung allerdings „allenfalls" analog anwenden will, da sie nach ihrem Wortlaut nur „bewegliche Sachen" erfasst. Ob diese Einschränkung angesichts der Herleitung der Anwendung des Mietrechts (Verkörperung der Daten auf einer beweglichen Sache) gerechtfertigt ist, kann an dieser Stelle dahinstehen.

[570] Ziffer 23 der Beschlüsse der Abteilung Zivilrecht, abrufbar unter www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf (letzter Abruf: 1.2.2017).

VII. Ergebnisse

Die Vereinbarungen über Streaming-Dienste sind in Abhängigkeit von ihrem konkreten Inhalt unterschiedlichen Vertragstypen im Sinne des BGB zuzuordnen. Dies bereitet bisweilen Schwierigkeiten. Angesichts der praktischen Handhabung besteht ungeachtet der damit verbundenen Rechtsunsicherheit aber kein Anlass, die Anwendung eines bestimmten Rechts gesetzlich anzuordnen.

Auf die „drängenden Fragen“ im Zusammenhang mit der schuldrechtlichen Abwicklung von Verträgen über Streaming-Dienste gibt das BGB aus Sicht aller Beteiligten derzeit zufriedenstellende Antworten. Auch insoweit besteht kein Anlass für gesetzgeberische Maßnahmen.

Sollte der nationale Gesetzgeber im Bereich des (sonstigen) Cloud Computing Maßnahmen treffen, müssten etwaige Auswirkungen auf die Rechtsbeziehungen der Beteiligten bei Verträgen über Streaming-Dienste in die Überlegungen einbezogen werden. Dies gilt insbesondere auch im Falle der – vom 71. Deutschen Juristentag geforderten[571] – Änderungen im Dienstvertragsrecht bzw. Schaffung eigener Regelungen für Verträge über digitale Inhalte, die den Charakter von Dauerschuldverhältnissen haben.

[571] Vgl. nur Ziffern 3, 22-25 der Beschlüsse der Abteilung Zivilrecht, abrufbar unter www.djt.de/fileadmin/downloads/71/Beschluesse_gesamt.pdf (letzter Abruf: 1.2.2017).

F. Soziale Netzwerke

I. Das Phänomen „Soziales Netzwerk“

Das Internet wird in zunehmendem Maße durch soziale Netzwerke geprägt. Sie haben sich in breitem Umfang als Netzwerkplattformen zur Kommunikation unter Nutzern etabliert.

Wesen sozialer Netzwerke ist es, dass breite Kreise der Internetnutzer Inhalte nicht nur überwiegend rezipieren, sondern die Kommunikation aktiv mitgestalten, also zugleich Konsument und Produzent (sog. „Prosumer“) sind.

Ziele können dabei die Teilhabe an der kollektiven Informationsverteilung und Wissensentstehung sowie die Steuerung der eigenen Reputation sein.[572] Am häufigsten werden soziale Netzwerke jedoch dafür genutzt, um sich mit Freunden und in der Familie auszutauschen und in Kontakt zu bleiben.[573] Viele Nutzer greifen über ein soziales Netzwerk auch auf Internetseiten außerhalb des sozialen Netzwerks zu.

1. Begriff und Merkmale sozialer Netzwerke

Begrifflich lassen sich soziale Netzwerke als Dienste im Internet umschreiben, die auf eine gemeinschaftliche Nutzung ausgelegt sind und ihren Nutzern über eine Software den Austausch von Inhalten sowie das Konstituieren sozialer Beziehungen ermöglichen. Die volle Nutzung der Funktionalitäten eines sozialen Netzwerks setzt die Erstellung eines persönlichen Profils voraus. Soziale Netzwerke in diesem Sinne sind (neben Weblogs u.a.) eine Form internetbasierter sozialer Medien. Typische Merkmale sozialer Netzwerke sind Schnittstellen und Verknüpfungen zu anderen Nutzern, Funktionen zur Übermittlung und Rezeption von Inhalten in verschiedenen (multimedialen) Formen und Dateiformaten sowie Möglichkeiten des Empfehlens und Bewertens. Kommunikation kann bilateral zwischen Nutzern, multilateral in Nutzergruppen oder öffentlich erfolgen. Soziale Netzwerke unterscheiden sich sowohl durch ihre Funktionalitäten und Möglichkeiten als auch durch ihre tatsächliche Nutzung von anderen Kommunikationsformen im Internet wie E-Mail und Chat (soweit sie außerhalb sozialer Netzwerke genutzt werden). Gegenüber reinen Kommunikationsdiensten (z. B. Skype und WhatsApp) setzen sie sich vor allem durch die Möglichkeiten, neue Kontakte zu schließen, ab.[574] Soziale Netzwerke bieten im Einzelnen unterschiedliche

---

[572] Vgl. *Hohlfeld/Godulla*, Das Phänomen der Sozialen Medien, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 43 m. w. N.

[573] BITKOM, Soziale Netzwerke 2013, Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet (Dritte, erweiterte Studie), S. 26, abrufbar unter https://www.bitkom.org/noindex/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf (letzter Abruf: 10.3.2017).

[574] So auch Monopolkommission, Sondergutachten gemäß § 44 Abs. 1 S. 4 des Gesetzes gegen Wettbewerbsbeschränkungen – Wettbewerbspolitik: Herausforderung digitale Märkte, BT-Drs. 18/5080, S. 99.

Funktionalitäten, die jeweils in eine andere digitale Umgebung eingebettet sind. Entsprechend dem informationstechnischen Fortschritt sowie sich ändernden Nutzerbedürfnissen und Anbieterstrukturen unterliegen auch soziale Netzwerke etablierter Anbieter einem *Wandel* und sind in ihrer konkreten *Ausgestaltung flüchtig*.[575]

2. Gesellschaftliche Bedeutung

Nach einer Studie aus dem Jahr 2013[576] nutzen 67 Prozent der Internetnutzer in Deutschland aktiv soziale Netzwerke. In der Altersgruppe von 14 bis 19 Jahren sind es 93 Prozent, in der Altersgruppe von 20 bis 29 Jahren sind es 85 Prozent. Obwohl große soziale Netzwerke (Facebook, Google+ u.a.) sich nicht nur an Privatpersonen richten, erfolgt die Nutzung weit überwiegend zu privaten Zwecken, also im Verhältnis zum Anbieter durch Verbraucher. Überwiegend beruflich verwendete soziale Netzwerke (XING, LinkedIn) werden von den Internetnutzern nur zu einem vergleichsweise geringen Anteil aktiv genutzt (XING: ca. 6 Prozent; LinkedIn: unter 5 Prozent). Das in Deutschland mit weitem Abstand über alle Altersgruppen hinweg am häufigsten genutzte soziale Netzwerk ist Facebook, das 56 Prozent der Internetnutzer – in der Altersgruppe unter 30 Jahren sogar 83 Prozent – aktiv verwenden. Alle anderen sozialen Netzwerke – auch Google+ und Twitter – kommen unter Berücksichtigung aller Altersgruppen auf einen Anteil aktiver Nutzer, der jeweils deutlich unter 10 Prozent liegt. Der Abstand von Facebook zu anderen sozialen Netzwerken ist damit in Deutschland noch größer als bei einem weltweiten Vergleich.[577] 69 Prozent der Nutzer in Deutschland – 89 Prozent in der Altersgruppe unter 30 Jahren – besuchen das aktiv genutzte soziale Netzwerk täglich, wobei die Nutzungsintensität bei Facebook deutlich höher als bei anderen sozialen Netzwerken ist.[578] Nutzer schauen auf Facebook aktuell täglich 100 Mio. Stunden Videoinhalte an.[579]

---

[575] Vgl. zum Ganzen: *Hohlfeld/Godulla*, Das Phänomen der Sozialen Medien, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 1, 3 f., 7 f.

[576] BITKOM, Soziale Netzwerke 2013, Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet (Dritte, erweiterte Studie), abrufbar unter https://www.bitkom.org/noindex/Publikationen/2013/Studien/Soziale-Netzwerke-dritte-erweiterte-Studie/SozialeNetzwerke-2013.pdf (letzter Abruf: 10.3.2017).

[577] Vgl. Monopolkommission, Sondergutachten gemäß § 44 Abs. 1 S. 4 des Gesetzes gegen Wettbewerbsbeschränkungen – Wettbewerbspolitik: Herausforderung digitale Märkte, BT-Drs. 18/5080, S. 99, zur Zahl der aktiven Nutzer von sozialen Netzwerken, die auch in Deutschland verwendet werden: Facebook 1,4 Mrd., Google+ 540 Mio., Twitter 284 Mio.

[578] Vgl. zu den statistischen Feststellungen insg. BITKOM, Soziale Netzwerke 2013, Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet (Dritte, erweiterte Studie).

[579] FAZ.NET (ebenso SZ.de) vom 28.1.2016, „Werbung bringt Facebook Milliarden-Gewinn".

3. Geschäftsmodelle

Kommerzielle Betreiber sozialer Netzwerke können auf verschiedenen Wegen Erlöse generieren.

In Betracht kommen Mitgliedsbeiträge von Nutzern, „Freemiummodelle“, bei denen unentgeltliche Basisfunktionen um kostenpflichtige Premiumfunktionen ergänzt werden, sowie die Vermarktung von Werbemöglichkeiten.

Unter den in Deutschland gängigen Modellen mit nennenswerter gesamtgesellschaftlicher und ökonomischer Relevanz finden sich keine sozialen Netzwerke, bei denen die Nutzung generell von der Zahlung eines Entgelts abhängig gemacht wird.

Überwiegend beruflich verwendete soziale Netzwerke (XING und LinkedIn) werden als „Freemiummodell“ betrieben, spielen aber mit Blick auf ihren Anteil an der Gesamtzahl der Nutzer sozialer Netzwerke lediglich eine untergeordnete Rolle.[580]

Das dominierende Geschäftsmodell[581] besteht darin, dass der Anbieter des sozialen Netzwerks persönliche Daten der Nutzer und von ihnen im sozialen Netzwerk eingestellte Inhalte monetarisiert, also wirtschaftlich verwertet.

II. Rechtliche Problemfelder

In der Auseinandersetzung von Rechtsprechung und rechtswissenschaftlicher Literatur mit dem Phänomen sozialer Netzwerke stehen nicht vertragsrechtliche, sondern gesetzliche, insbesondere quasinegatorische, deliktische und urheberrechtliche Ansprüche (z. B. unter dem Gesichtspunkt des Persönlichkeitsrechts) zwischen Nutzern und im Verhältnis zu Dritten, die gesetzliche Haftung von Betreibern (etwa für die Sicherheit der betriebenen Plattformen) sowie straf-, arbeits-, medien- und datenschutzrechtliche[582] Aspekte im Vordergrund.

III. Vertragsrechtliche Fragestellungen und Lösungsansätze

Vertragsrechtliche Fragen stellen sich hinsichtlich des Vertragsschlusses und mit Blick auf die rechtliche Einordnung des Rechtsverhältnisses zwischen dem Betreiber eines sozialen Netzwerks und dessen Nutzer. Die praktisch besonders bedeutsamen und rechtlich am schwierigsten zu qualifizierenden Fragen, die „kostenlose“ soziale Netzwerke aufwerfen, werden im folgenden Unterkapitel „Bezahlen mit Daten am Beispiel der sozialen Netzwerke“ – behandelt.

---

[580] Siehe oben I. 2.
[581] Dieses Geschäftsmodell liegt u. a. Facebook, Google+ und Twitter zugrunde.
[582] Vgl. etwa EuGH, Urt. v. 6.10.2015 − Rs. C-362/14 (Schrems).

1. Vertragsschluss

a. Vertragsparteien

Vertragsrechtliche Fragen stellen sich nur im Verhältnis zwischen Betreiber und Nutzer des sozialen Netzwerks, da nur insoweit eine vertragliche Verbindung angenommen werden kann.

Zwischen Nutzern des sozialen Netzwerks, die nur die gemeinsame Nutzung desselben Kommunikationsmittels verbindet, dürfte eine vertragliche Beziehung demgegenüber ausscheiden.[583]

b. Minderjährigenschutz

Der hohe Anteil (und die hohe absolute Zahl) minderjähriger Nutzer „kostenloser" sozialer Netzwerke wirft Fragen der Wirksamkeit von Vertragsschlüssen beschränkt Geschäftsfähiger nach Maßgabe der §§ 107 ff. BGB auf.

Mit Blick auf die regelmäßig – vor allem hinsichtlich des Datenschutzes – von gesetzlichen Vorgaben abweichenden Nutzungsbedingungen der Betreiber „kostenloser" sozialer Netzwerke wird man ein für Minderjährige lediglich rechtlich vorteilhaftes Geschäft nicht annehmen können. Dass die Einwilligung in eine Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung generell kein zu vernachlässigendes Gefährdungspotential hat, ergibt sich schon aus den speziellen datenschutzrechtlichen Regelungen für die Einwilligung Minderjähriger in Art. 8 EU-DSGVO[584]. Nach Art. 8 Abs. 3 EU-DSGVO wird das allgemeine Vertragsrecht der Mitgliedstaaten, etwa hinsichtlich der Vorschriften zur Gültigkeit, zum Zustandekommen oder zu den Rechtsfolgen eines Vertrags in Bezug auf ein Kind, ausdrücklich unberührt gelassen.

Wenn (beschränkt geschäftsfähige) Minderjährige soziale Netzwerke nutzen, ist deshalb eine Einwilligung des gesetzlichen Vertreters erforderlich. Für eine analoge Anwendung von § 110 BGB wird zutreffend kein Raum gesehen.[585]

Unbefriedigend beim Abschluss von Verträgen über die Nutzung „kostenloser" sozialer Netzwerke ist, dass die Altersgrenzen für die datenschutzrechtliche Einwilligungsfähigkeit einerseits und für die zivilrechtliche Geschäftsfähigkeit andererseits auseinanderfallen. Nach den §§ 2 und 106 BGB sind natürliche Personen vom vollendeten siebenten bis zum vollendeten *18. Lebensjahr* in der Geschäftsfähigkeit beschränkte, durch die §§ 107 ff. BGB geschützte Minderjährige. Nach Art. 8 Abs. 1 Unterabs. 1 S. 1 EU-DSGVO erfordert eine wirksame Einwilligung

---

[583] Vgl. *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 53.

[584] So auch *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag 2016, S. 9.
Bei den datenschutzrechtlichen Bezügen der Thematik wird auch im Folgenden, soweit nicht anders vermerkt, auf die EU-DSGVO Bezug genommen, die ab dem 25. Mai 2018 gilt.

[585] Vgl. dazu näher *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 108 ff.

bei einem Angebot von Diensten der Informationsgesellschaft gemäß Art. 6 Abs. 1 lit. a EU-DSGVO demgegenüber nur, dass der Einwilligende das *16. Lebensjahr* vollendet hat. Art. 8 Abs. 1 Unterabs. 2 EU-DSGVO eröffnet den Mitgliedstaaten sogar die Möglichkeit, diese Altersgrenze auf das vollendete *13. Lebensjahr* abzusenken.

Es stellt sich deshalb die Frage, ob das bürgerliche Recht den Altersgrenzen der Datenschutz-Grundverordnung folgen und dadurch mit Bezug auf Minderjährige einen Gleichlauf von Zivil- und Datenschutzrecht herstellen sollte.

Im Ergebnis besteht für die Herstellung eines solchen Gleichlaufs *kein Anlass*. Art. 8 Abs. 3 EU-DSGVO lässt das allgemeine Vertragsrecht der Mitgliedstaaten hinsichtlich der Rechtsfolgen eines Vertrags unter Beteiligung eines Minderjährigen ausdrücklich unberührt. Es gibt keinen Grund, den zivilrechtlichen Minderjährigenschutz abzusenken.

Eine Anpassung der bürgerlich-rechtlichen Normen des Minderjährigenrechts an die Regelungen, die im Datenschutzrecht hinsichtlich der Einwilligungsfähigkeit gelten, wird auch in der fachlichen Diskussion mit Recht für nicht geboten gehalten.[586]

2. Einordnung der Vertragsbeziehung und wechselseitige Rechte und Pflichten bei Nutzungsverhältnissen mit finanzieller Gegenleistung

Das Phänomen sozialer Netzwerke ist im geltenden Recht nicht konkret geregelt. Angesichts der Besonderheiten dieses digitalen Phänomens im Vergleich zu „analogen“ Kommunikationsmitteln, seiner verschiedenen Erscheinungsformen sowie unterschiedlicher Nutzungsbedingungen lässt sich das Rechtsverhältnis zwischen dem Betreiber eines sozialen Netzwerks und dem Nutzer nicht generalisierend einem im geltenden Recht geregelten Vertragstyp zuordnen. Eine Schwierigkeit bei der rechtlichen Einordnung liegt zudem darin, dass das *konkrete Erscheinungsbild* sozialer Netzwerke einem raschen Wandel unterliegt, sodass es sich bei der Beschreibung und Begriffsbestimmung des Phänomens letztlich um eine *Momentaufnahme*[587] handelt.

Ansatzpunkt für verallgemeinernde Betrachtungen können damit nur gängige Nutzungsbedingungen sein, die den Kern des Geschäftsmodells etablierter Betreiber abbilden und in ihrer Charakteristik eine gewisse Kontinuität aufweisen.

Auf das Nutzungsverhältnis wird in der Regel deutsches Recht Anwendung finden. Die beiden weltweit größten in Deutschland agierenden Betreiber sehen dies ausdrücklich vor.[588] Für Nutzungsverhältnisse mit Verbrauchern – die praktisch

---

[586] So der Beschluss Ziffer 7. der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016.

[587] So plastisch *Hohlfeld/Godulla*, Das Phänomen der Sozialen Medien, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 8.

[588] Facebook regelt dies unter Ziffer 5 der Nutzungsbedingungen für Nutzer mit Wohnsitz in Deutschland; die Nutzungsbedingungen von Google+ für Nutzer in Deutschland sehen dies im letzten Abschnitt vor (Stand jeweils: 28.3.2017).

den Regelfall darstellen (s. o.) – ergibt sich dies bei Fehlen einer anderweitigen Vereinbarung aus Art. 6 Abs. 1 Rom I-VO. Nach Art. 6 Abs. 2 S. 2 Rom I-VO dürfen Verbraucher durch Rechtswahl nicht den zwingenden Schutzvorschriften des Staats, in dem sie ihren gewöhnlichen Aufenthalt haben, in Deutschland also z. B. nicht der Anwendung der §§ 305 ff. BGB auf die Nutzungsbedingungen, entzogen werden.

Entgeltliche Verträge über die Bereitstellung eines sozialen Netzwerks werden im Schrifttum teilweise als Werkvertrag mit Dauerschuldcharakter eingeordnet. Mit der Bereitstellung der Online-Plattform werde ein tatsächlicher Erfolg geschuldet, der darin bestehe, dem Nutzer unter Sicherstellung der Verfügbarkeit und der prägenden Funktionen der Plattform Zugang zum sozialen Netzwerk zu gewähren. Ein Dienstvertrag scheide deshalb aus.[589]

Diese rechtliche Einordnung setzt allerdings voraus, dass der Betreiber nach den vereinbarten Vertragsbedingungen und unter Würdigung aller Umstände tatsächlich eine (ständige) Verfügbarkeit des sozialen Netzwerks und seiner wesentlichen Funktionen schuldet.

In Betracht gezogen wird für besondere Fallgestaltungen unter dem Gesichtspunkt der zeitlich begrenzten Einräumung von Nutzungsrechten an einem „virtuellen Raum“ und unter Berücksichtigung der Rechtsprechung des BGH zu „ASP “-Verträgen[590] auch eine Einordnung als Mietvertrag bzw. als mietvertragsähnliches Rechtsverhältnis.[591]

Im Schrifttum wird des Weiteren eine Rechtsbeziehung mit miet- und dienstvertraglichen Elementen angenommen.[592] In der instanzgerichtlichen Rechtsprechung[593] ist eine Einordnung als „schuldrechtlicher Vertrag mit miet-, werk- und dienstvertraglichen Elementen“ erfolgt.

Letztlich dürfte sich der einschlägige Vertragstypus bei entgeltlichen Verträgen nur nach den im konkreten Rechtsverhältnis vereinbarten Leistungspflichten des Betreibers des sozialen Netzwerks bestimmen lassen. Mit Blick auf die unterschiedlichen Erscheinungsformen und Nutzungsbedingungen sowie den raschen Wandel bei den konkreten Funktionalitäten sozialer Netzwerke dürfte eine *zukunftsfeste Regelung*, die soziale Netzwerke vertragstypologisch einordnet, *kaum möglich* sein.

---

[589] Vgl. zum Ganzen *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 28 m. w. N. auch zur a. A.
[590] BGH, Urt. v. 15.11.2006 – XII ZR 120/04, NJW 2007, 2394 ff.
[591] Vgl. *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 29f. m. w. N. zum Schrifttum.
[592] *Bräutigam*, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635 (640); *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 19.
[593] Vgl. LG Berlin, Urt. v. 17.12.2015 – 20 O 172/15, Tz. 24.

Der Verzicht auf einen gesetzlichen Vertragstypus geht zwar mit dem Fehlen eines gesetzlichen Leitbildes i. S. v. § 307 Abs. 2 Nr. 1 BGB einher. Eine Inhaltskontrolle von Nutzungsbedingungen bleibt jedoch nach dem grundlegenden Wertungsmaßstab in § 307 Abs. 1 BGB möglich. Maßgebliche Bedeutung kommt dabei nach § 307 Abs. 2 Nr. 2 BGB der fallbezogen zu klärenden Natur des Vertrags zu. Sie wird durch den Zweck und Inhalt des Vertrags sowie das durch die Verkehrsauffassung geprägte Leitbild bestimmt. In den Nutzungsbedingungen dürfen damit wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, nicht so eingeschränkt werden, dass das Erreichen des Vertragszwecks gefährdet ist. In der Rechtsprechung[594] haben verschiedene (inzwischen gegenüber Nutzern mit Wohnsitz in Deutschland nicht mehr verwendete) Klauseln – u. a. zur Weiterübertragung und Unterlizenzierung von Nutzungsrechten – in den Nutzungsbedingungen von Facebook aus unterschiedlichen Gründen einer Inhaltskontrolle nach § 307 BGB nicht standgehalten.

Die Kündbarkeit des Vertrags dürfte sich nach den allgemeinen Regelungen und Grundsätzen für die Kündbarkeit von Dauerschuldverhältnissen bestimmen.[595]

IV. Empfehlungen

Eine Anpassung der bürgerlich-rechtlichen Normen des Minderjährigenrechts an die im Datenschutzrecht zur Einwilligungsfähigkeit geltenden Regelungen ist nicht geboten. Für die mit einer Anpassung einhergehende Absenkung des zivilrechtlichen Minderjährigenschutzes gibt es keinen Anlass. Es besteht deshalb kein Regelungsbedarf.

Eine gesetzliche Regelung, die soziale Netzwerke vertragstypologisch einordnet, ist mit Blick auf deren unterschiedliche Erscheinungsformen und den raschen Wandel bei den konkreten Funktionalitäten nicht sinnvoll. Insoweit besteht kein Regelungsbedarf.

---

[594] KG, Urt. v. 24.1.2014 – 5 U 42/14, Tz. 170 ff. (veröffentlicht in juris); die vom BGH am 14.1. 2016 verkündete Revisionsentscheidung – I ZR 65/14 – hatte nur noch die frühere „Freunde finden"-Funktion von Facebook zum Gegenstand.

[595] Dazu näher *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 73 ff.

G. „Bezahlen mit Daten“ am Beispiel der Sozialen Netzwerke

I. Untersuchungsgegenstand: Rechtsverhältnis zwischen dem Anbieter und dem Nutzer eines „kostenlosen“ sozialen Netzwerks

Praktisch und – mit Blick auf den Erfolg des Geschäftsmodells „kostenloser“ Angebote[596] sowie die überwiegende Abneigung von Internetnutzern gegenüber kostenpflichtigen Online-Diensten[597] – wohl auch langfristig den Regelfall stellen „kostenlose“ soziale Netzwerke dar, bei denen der Betreiber Erlöse über die Monetarisierung von persönlichen und sonstigen Daten bzw. Inhalten erzielt, die sich aufgrund Registrierung und Kommunikation über ein Nutzerkonto unmittelbar der Person des Nutzers zuordnen lassen.

Mit Blick auf das dominierende Geschäftsmodell von Anbietern „kostenloser“ sozialer Netzwerke, persönliche Daten der Nutzer und von ihnen im sozialen Netzwerk eingestellte Inhalte zu monetarisieren, sowie den Umstand, dass der Mehrzahl der Internetnutzer durchaus bewusst ist, bei kostenlosen Angeboten im Internet mit ihren Daten zu „bezahlen“[598], wird man auf ein „Bezahlen mit Daten“ gerichtete Klauseln in Nutzungsbedingungen der Betreiber sozialer Netzwerke kaum generell als überraschend i. S. d. § 305c Abs. 1 BGB einstufen können.

Dies schließt – nach Abwägung im Einzelfall auf der Grundlage der konkreten Nutzungsbedingungen – die Unwirksamkeit solcher Klauseln in Geschäftsbedingungen eines Betreibers aufgrund einer Inhaltskontrolle nicht aus.[599] Eine Unwirksamkeit kann etwa im Wege der Verbandsklage nach Maßgabe des Unterlassungsklagengesetzes geltend gemacht werden.

II. Schuldrechtliche Einordnung und Regelungsbedarf

1. Vorliegen einer Hauptleistung des Nutzers

Für die Konstellation des „Bezahlens mit Daten“ stellt sich die Frage, ob das Einräumen einer Befugnis des Betreibers zur Nutzung auf die Person des Nutzers bezogener Daten und Inhalte eine Gegenleistung des Nutzers darstellt.

Von einem Geldbetrag unterscheidet sich die Leistung des Nutzers unter anderem darin, dass persönlichen Daten und Inhalten das für Geld charakteristische Merkmal der Fungibilität – d. h. der (gleichwertigen) Austauschbarkeit durch andere

---

[596] Vgl. z. B. die Registrierungsseite von Facebook: „Facebook ist und bleibt kostenlos“, abrufbar unter https://de-de.facebook.com/ (letzter Abruf: 14.3.2017).

[597] Siehe dazu Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI), Studie „Daten – Ware und Währung“, Eine repräsentative Bevölkerungsbefragung, Hamburg 2014, S. 6, 10, abrufbar unter https://www.divsi.de/wp-content/uploads/2014/11/DIVSI-Studie-Daten-Ware-Waehrung.pdf (letzter Abruf: 14.3.2017).

[598] DIVSI, Studie „Daten – Ware und Währung“, Eine repräsentative Bevölkerungsbefragung, Hamburg 2014, S. 11.

[599] Vgl. *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 52.

Stücke gleicher Gattung und Menge – fehlt. Auch die grundlegenden Funktionen von Geld erfüllen personenbezogene Daten nicht[600].

Gemeinsam hat die Leistung des Nutzers an den Betreiber mit einer Geldzahlung, dass dem Betreiber für die Bereitstellung des sozialen Netzwerks ein wirtschaftlicher Wert – ein *Entgelt* – zugewendet wird.[601] Dass dieser Wert in Relation zum finanziellen Aufwand des Betreibers erheblich ist, ergibt sich aus den hohen Gewinnen, die mit der Monetarisierung von Nutzerdaten aus kommerziellen sozialen Netzwerken erzielt werden.

Der Beurteilung, dass es sich bei Nutzerdaten um einen wirtschaftlichen Wert handelt, lässt sich nicht entgegenhalten, dass der Nutzer selbst (gegenwärtig) kaum eine Möglichkeit hat, seine Daten zu monetarisieren. Dass es einen Markt für Nutzerdaten aus sozialen Netzwerken bzw. für auf Nutzerdaten aus sozialen Netzwerken basierende Leistungen gibt, zeigen schon die beachtlichen Gewinne, die Betreiber sozialer Netzwerke mit der Verwertung solcher Daten erzielen. Dass dieser Markt für private Nutzer nicht zugänglich ist, hat nicht zur Folge, dass die von ihnen eingeräumten Möglichkeiten der Datenverwertung keine Leistung darstellen. Abgesehen davon setzt der schuldrechtliche Leistungsbegriff in § 241 Abs. 1 BGB nicht voraus, dass der Leistungsgegenstand überhaupt einen Geldwert hat[602], sodass es für die Einordnung der Handlung des Schuldners als Leistung auf einen Marktwert letztlich nicht ankommt. Die tatsächlich schwierige Frage nach dem wirtschaftlichen Wert personenbezogener Daten, der auf fundamental komplexen Faktoren beruht und je nach Kontext der beabsichtigten Datenverwendung sehr unterschiedlich sein kann, muss deshalb bei der schuldrechtlichen Einordnung nicht entschieden werden.[603]

---

[600] Geld hat drei Funktionen. Es ist

a) Tauschmittel: Mit Geld können Güter und Dienstleistungen bezahlt werden. Die Möglichkeit, mit Geld zu bezahlen, vermeidet die Schwierigkeit beim Tauschhandel, dass eine beiderseitige Nachfrage der Tauschpartner nach dem Tauschgegenstand des jeweils anderen Teils aufeinandertreffen muss;
b) Wertaufbewahrungsmittel: Geld eröffnet die Möglichkeit, Güter und Dienstleistungen zu einem erst in der Zukunft liegenden Zeitpunkt zu erwerben;
c) Rechnungseinheit: Geld ermöglicht es, den (aktuellen) ökonomischen Wert eines angebotenen Gegenstands zu bemessen.

Die Funktionen von Geld können auch von anderen Gegenständen als Währungseinheiten erfüllt werden (während des Zweiten Weltkriegs erfüllten teilweise Zigaretten diese Funktionen unter Kriegsgefangenen).

[601] Als paradigmatisch dafür mag man die Äußerung des Finanzvorstands der Lufthansa Simone Menne ansehen: „Nach Umsatz sind wir der größte Luftfahrt-Konzern der Welt. Aber die Märkte bewerten Google, WhatsApp nach ganz anderen Maßstäben – nur dank der Daten, die sie generieren. Unsere Kundendaten dagegen werden an der Börse überhaupt nicht bewertet, folglich müssen wir mehr daraus machen." (siehe Magdeburger Volksstimme vom 15.6.2015).

[602] Vgl. dazu ausführlich Staudinger/*Olzen*, BGB, § 241 Rn. 14 ff.

[603] Da kein einheitlicher, für Nutzer in gleicher Weise wie für Anbieter zugänglicher Markt für personenbezogene Daten bzw. für auf solchen Daten basierende Leistungen existiert, dürfte sich auch aus exorbitanten Gewinnspannen von Anbietern keine Sittenwidrigkeit wegen eines

Die in der Literatur vertretene Ansicht, es handele sich bei dem „kostenlosen“ Nutzungsverhältnis um einen den Betreiber einseitig verpflichtenden Vertrag, erscheint aus vorstehenden Erwägungen lebensfremd und – insbesondere unter dem Gesichtspunkt, dass ein einheitlicher Lebensvorgang in Gestalt wechselseitiger zweckgerichteter Leistungen aufgespalten wird – künstlich.[604]

Im Verhältnis zwischen dem Anbieter eines „kostenlosen“ sozialen Netzwerks und dessen Nutzer stehen sich vielmehr wechselseitige (nicht monetäre) Hauptleistungspflichten gegenüber.[605] Anbieter und Nutzer erbringen ihre Leistung jeweils, um die Gegenleistung des anderen zu erhalten.

Mit Blick auf die jeweilige Zweckbindung der wechselseitigen Leistungen liegt beim Vertrag über die „kostenlose“ Nutzung eines sozialen Netzwerks ein *Synallagma* vor.

Der hier vertretene Ansatz ist mit dem Standpunkt des Europäischen Datenschutzbeauftragten (EDSB) in der Stellungnahme 4/2017 vom 14. März 2017 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 9. Dezember 2015 – COM(2015) 634 final –[606] vereinbar.

In seiner Stellungnahme stellt der EDSB die Existenz einer Praxis der Vermarktung personenbezogener Daten fest. Er vertritt zwar den Standpunkt, dass diese Praxis – wie die Praxis des Handels mit Organen lebender Spender – vom Gesetzgeber nicht „abgesegnet“ werden sollte. Andererseits begrüßt er ausdrücklich das Ziel, die Rechtsposition der Verbraucher, von denen Diensteanbieter für eine Bereitstellung digitaler Güter die Preisgabe (für die Leistung des Diensteanbieters nicht notwendiger) personenbezogener Daten verlangen, zu stärken.

Die vom EDSB geäußerten Bedenken gegen das Konzept „Daten als Gegenleistung“ im Richtlinienvorschlag beziehen sich auf den Ansatz der Kommission, dass mit Daten in derselben Weise (“*the same way*“) gezahlt werden kann wie mit

---

wucherähnlichen Rechtsgeschäfts nach § 138 Abs. 1 BGB herleiten lassen (vgl. BGH, Urt. v. 22.12.1999 – VIII ZR 111/99, MDR 2000, 382 f. zur Maßgeblichkeit des marktüblichen Preises und zu sog. gespaltenen Märkten, bei denen für dieselbe Ware in Abhängigkeit davon, in welcher Konstellation sich Marktteilnehmer gegenüberstehen, stark unterschiedliche Preise gezahlt werden; maßgeblich ist dann der für die jeweilige Konstellation marktübliche Preis).

[604] So *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 21, die zugleich darauf hinweisen, dass eine Qualifizierung des Nutzungsverhältnisses als Auftrag gemäß § 662 BGB schon daran scheitern dürfte, dass Betreiber wie Facebook, Google+ u. a. die Nutzung ihres sozialen Netzwerks offenkundig nicht in fremdem Interesse, sondern mit dem Ziel der Gewinnmaximierung anbieten und die Vorschriften des Auftragsrechts zu keinen sach- und interessengerechten Lösungen führen.

[605] In diesem Sinne auch *Benninghoff*, Brauchen wir eine „Button“-Lösung für das Datenschutzrecht, VuR 2013, 361 f.

[606] Abrufbar unter https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf (letzter Abruf: 26.4.2017).

Geld. Personenbezogene Daten seien nicht identisch mit Geld, schon weil sie mehrfach weggegeben werden könnten und ihr Wert nicht messbar sei. Diensteanbieter könnten mit den Daten auch nicht in der gleichen Weise verfahren wie mit Geld. Das Grundrecht auf den Schutz personenbezogener Daten sei mehr als ein einfaches Verbraucherrecht. Es müsse deshalb vermieden werden, personenbezogene Daten als Ware wie jede andere zu behandeln.

Den Erwägungen des EDSB zum Richtlinienvorschlag trägt der im Folgenden dargestellte, auf das nationale Recht bezogene Ansatz in jeder Hinsicht Rechnung. Ein „Bezahlen mit Daten“ wird dem Bezahlen mit Geld schon deshalb nicht gleichgestellt, weil – anders als im Richtlinienvorschlag – nicht die Hingabe von Daten, sondern die Erteilung der datenschutzrechtlichen Einwilligung als Gegenleistung des Verbrauchers eingeordnet wird. Die nachfolgend vorgeschlagenen bürgerlich-rechtlichen Regelungen bauen – anders als die Regelungen im Richtlinienvorschlag – einschränkungslos auf der EU-DSGVO auf. Sie tragen deren Vorgaben – z. B. der freien Widerruflichkeit einer datenschutzrechtlichen Einwilligung – auf der Ebene des bürgerlichen Rechts umfassend Rechnung, u. a. durch die Annahme einer Bedingtheit des Vertrags und die Regelung, dass die Erteilung einer datenschutzrechtlichen Einwilligung nicht einklagbar ist. Das so umrissene Datenschuldrecht vollzieht das Datenschutzrecht auf der Ebene des bürgerlichen Rechts nach. Für die unter die empfohlenen Regelungen fallenden Nutzer werden keine Pflichten eingeführt. Sie erhalten lediglich Rechte, die in einem angemessenen Verhältnis zu ihrer Einwilligung in die ökonomische Verwertung ihrer personenbezogenen Daten stehen. Vertragsmodelle, bei denen Diensteanbieter Gewinne durch die wirtschaftliche Verwertung personenbezogener Daten generieren, sollen dadurch nicht gefördert, ihrer Existenz – die auch der EDSB anerkennt – soll aber angemessen Rechnung getragen werden. Unter diesen Prämissen gibt es keinen Anlass, die datenschutzrechtliche Einwilligung nicht als das zu bezeichnen, was sie ist: die synallagmatisch mit der Leistung des Diensteanbieters verbundene Gegenleistung.

Werden – wie der EDSB mit Bezug auf das Konzept des „Bezahlens mit Daten“ im Richtlinienvorschlag moniert – grundlegende Wertungsentscheidungen des Gesetzgebers durch eine rechtlich zulässige Praxis unterlaufen, kann dem unterschiedlich begegnet werden. Der Gesetzgeber kann zum einen die mit seinen Wertungsentscheidungen unvereinbare Praxis für unzulässig erklären. Zum anderen kann er Regelungen schaffen, welche die Zulässigkeit der Praxis zwar nicht berühren, das Phänomen aber rechtlich ordnen.

Mit Bezug auf den vom EDSB im Kontext mit der Monetarisierung personenbezogener Daten angeführten Handel mit Organen von lebenden Spendern hat sich der Gesetzgeber in Deutschland für ein Verbot entschieden. Nach § 18 des Transplantationsgesetzes ist Organhandel strafbar. Eine Strafbarkeit wird für die einwilligungsbasierte Monetarisierung personenbezogener Daten jedoch nicht – auch nicht vom EDSB – gefordert. Sie widerspräche auch der EU-DSGVO. Vor dem Hintergrund der datenschutzrechtlichen Zulässigkeit eines „Bezahlens mit

Daten“ wäre es inkonsequent, bürgerlich-rechtliche Regelungen für dieses Phänomen, welche für die mit Daten „bezahlenden“ Personen ausschließlich vorteilhaft sind, mit der Begründung abzulehnen, sie würden die Praxis „absegnen“. Faktisch ist dies mit der EU-DSGVO, nach der diese Praxis zulässig ist, ohnehin bereits erfolgt.

Da das Datenschutzrecht als öffentliches Ordnungsrecht nicht dazu dient, Rechtsbeziehungen unter bürgerlich-rechtlichen Aspekten zu regeln, bedarf es eines auf ihm aufbauenden Datenschuldrechts.

2. Art der Hauptleistung des Nutzers

Die Einordnung von Daten bzw. der Einwilligung in die wirtschaftliche Verwertung von Daten als Gegenstand eines Leistungsaustauschs im Rahmen eines Schuldverhältnisses ist gegenwärtig weder auf EU-Ebene noch im deutschen Zivilrecht geregelt. Es gibt bislang – auch in anderen Mitgliedstaaten – kein „Datenschuldrecht“ oder „Datenschuldvertragsrecht“.

a. Personenbezogenheit der Nutzerdaten

Mit Blick darauf, dass der Nutzer eines sozialen Netzwerks Inhalte im Netzwerk nur über ein von ihm mit Daten zu seiner Person eingerichtetes Konto mitteilen kann, lassen sich ihm alle kommunizierten Inhalte als identifizierter bzw. identifizierbarer natürlicher Person zuordnen.

Es handelt sich bei diesen Inhalten somit um *personenbezogene Daten* i. S. d. Begriffsbestimmung in Art. 4 Nr. 1 EU-DSGVO, wonach „personenbezogene Daten“ *alle Informationen* sind, die sich auf eine identifizierbare oder identifizierte natürliche Person beziehen. Nach dem geltenden Verständnis von § 3 Abs. 1 BDSG, dem die Art. 4 Nr. 1 EU-DSGVO vergleichbar weite Begriffsbestimmung in Art. 2 lit. a der EG-Datenschutzrichtlinie[607] zugrunde liegt, sind personenbezogene Daten praktisch sämtliche Daten, die mit einer bestimmten bzw. bestimmbaren Person in Verbindung stehen.[608] Erfasst ist jede Information geistigen Inhalts einschließlich Fotos, Videos und Tonaufnahmen.[609]

Der sachliche Anwendungsbereich nach Art. 2 Abs. 1 EU-DSGVO ist damit bei sozialen Netzwerken regelmäßig eröffnet. Dass es Anbietern sozialer Netzwerke gerade auf einen Personenbezug aller Nutzerdaten ankommt, ergibt sich exemplarisch aus Ziffer 4 der Nutzungsbedingungen von Facebook, wonach Nutzer bei der Registrierung ihren wahren Namen und wahre weitere persönliche Informationen angeben müssen.

---

[607] RL 95/46/EG vom 24. Oktober 1995.
[608] Vgl. Plath/*Plath/Schreiber*, BDSG, § 3 Rn. 12.
[609] Vgl. Plath/*Plath/Schreiber*, BDSG, § 3 Rn. 7.

b. Bedeutung datenschutzrechtlicher Bezüge für die vertragsrechtliche Einordnung

Die schuldrechtliche Einordnung der Hauptleistung des Schuldners lässt sich aus der Datenschutz-Grundverordnung jedoch nicht unmittelbar ableiten. Das dem persönlichkeitsrechtlichen Schutz dienende Datenschutzrecht hat nicht die Funktion, den Leistungsaustausch durch Verträge zu regeln, und stellt keinen Regelungsrahmen für die Äquivalenz in Leistungsaustauschbeziehungen dar. Diese Aufgaben muss und kann allein das Zivilrecht – vor allem das Schuldrecht – erfüllen.

Das schließt indes nicht die Möglichkeit aus, bei der Beurteilung zivilrechtlicher Fragen Regelungen und Wertungen des Datenschutzrechts heranzuziehen.

c. Anknüpfungspunkte für das Vertragsrecht

Die zum deutschen Recht veröffentlichte Rechtsprechung hatte sich mit schuldrechtlichen Fragen der Erscheinungsform des „Bezahlens mit Daten“ bislang nicht zu befassen.

(1) Datenschutzrechtliche Einwilligung als Leistung

In der wenigen rechtswissenschaftlichen Literatur zu diesem Phänomen hat *Schmidt-Kessel*[610] herausgearbeitet, dass die *Leistung des Nutzers* nicht schon in der Übermittlung von Daten gesehen werden könne. Das Interesse des Anbieters „kostenloser“ Dienste im Internet sei vor allem darauf gerichtet, seitens des Nutzers eine *datenschutzrechtliche Einwilligung* in die kommerzielle Verwertung seiner Daten – z. B. zum (Weiter-)Verkauf, zum Schalten personenspezifischer Werbung und zur Profilbildung – zu erhalten. Darin sei die eigentliche, den Anbieter interessierende Hauptleistung des Nutzers zu sehen.[611]

Dieser Ansatz, der mit Bezug auf das abgrenzbare Phänomen „kostenloser“ sozialer Netzwerke auch von *Bräutigam*[612] vertreten wird, ist überzeugend. Nicht mit einer Datenübermittlung, sondern erst mit der datenschutzrechtlichen Einwilligung eröffnet der Nutzer dem Anbieter die Möglichkeit einer Monetarisierung seiner personenbezogenen Daten.

---

[610] Vgl. zum Ganzen *Schmidt-Kessel* et al., Die Richtlinienvorschläge der Kommission zu Digitalen Inhalten und Online-Handel – Teil 2, GPR 2016, S. 54/57-60; *ders.*, Stellungnahme zu den Richtlinienvorschlägen der Kommission zum Online-Handel und zu Digitalen Inhalten für die öffentliche Anhörung im Bundestagsausschuss für Recht und Verbraucherschutz am 11. Mai 2016 (BT-Protokoll-Nr. 18/99), abrufbar unter https://www.bundestag.de/blob/422258/c3ecca9b7286f38bda7e060f7b420c06/schmidt_kessel-data.pdf (letzter Abruf: 14.3.2017).

[611] Siehe auch Beschluss des Bundesrates vom 22.4.2016 zum Dossier COM(2015) 634 final, BR-Drs. 168/16 (B), Ziff. 19.

[612] *Bräutigam*, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635 (640); vgl. auch *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 18 ff.

Dem lässt sich nicht entgegenhalten, die Bereitschaft, sich Werbung auszusetzen, stelle noch keine Gegenleistung dar. Mit einer Einwilligung in die kommerzielle Verwertung seiner personenbezogenen Daten leistet der Nutzer mehr als die Erklärung eines Einverständnisses, personalisierter Werbung ausgesetzt zu werden. Er eröffnet dem Anbieter vielmehr die wirtschaftlich wertvolle Möglichkeit, Werbung zu personalisieren.

Eine Betrachtungsweise, die auf die datenschutzrechtliche Einwilligung als Gegenleistung abstellt, trägt auch der weiten Fassung des Begriffs „personenbezogene Daten" nach Art. 4 Nr. 1 und Erwägungsgrund 26 der EU-DSGVO angemessen Rechnung. Personenbezogene Daten umfassen danach alle Informationen, welche sich auf eine natürliche Person beziehen, die *indirekt* – z. B. über eine Online-Kennung – identifiziert werden *kann*.

(2) Schwächen eines an eine aktive Datenübermittlung anknüpfenden Ansatzes

Ein Ansatz, der wie Art. 3 Nr. 1 des Vorschlags der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 9. Dezember 2015 – COM(2015) 634 final – an der *aktiven Übermittlung* personenbezogener (oder anderer) Daten anknüpft, wäre demgegenüber einerseits zu weitgehend und griffe andererseits zu kurz.[613]

In einer die Internetwirtschaft unnötig beeinträchtigenden Weise *zu weitgehend* wäre ein Abstellen auf die aktive Datenhingabe deshalb, weil ein „Bezahlen mit Daten" dann bereits vorläge, wenn sich das ökonomische Interesse des Anbieters darauf beschränkt, die personenbezogenen Daten des Nutzers nur in anonymisierter Form zu verarbeiten. Nach Erwägungsgrund 26 der EU-DSGVO sollen die datenschutzrechtlichen Regelungen der Datenschutz-Grundverordnung dann nicht gelten, wenn personenbezogene Daten so anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann. Da bereits die im Regelfall[614] mit jedem Aufruf einer Internetseite verbundene Übermittlung der IP-Adresse des Nutzers seinen personenbezogenen Daten zuzurechnen sein kann[615], könnte schon im Aufrufen einer Internetseite der Abschluss eines gegenseitigen

---

[613] Ablehnend zu einem solchen Ansatz auch der Beschluss des Bundesrates vom 22.4.2016 zum Dossier COM(2015) 634 final, BR-Drs. 168/16 (B), Ziff. 20. Zweifelnd: BMWi, „Grünbuch Digitale Plattformen", Mai 2016, abrufbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/gruenbuch-digitale-plattformen.pdf;jsessionid=EB165AD0597141E9B3E45C44923B63AD?__blob=publicationFile&v=12 (letzter Abruf: 14.3.2017), und *Bokor*, Wortprotokoll der 99. Sitzung des Bundestagsausschusses für Recht und Verbraucherschutz vom 11. Mai 2016 (BT-Protokoll-Nr. 18/99), S. 15.

[614] Sieht man einmal von der Nutzung des Internets über ein *Virtual Private Network*, sog. *Onion-Routing* oder sonstige anonymisierende technische Hilfsmittel ab.

[615] Vgl. EuGH, Urt. v. 19.10.2016 − Rs. C-582/14 (Breyer); eine ausführliche Darstellung des Meinungsstandes in der Kontroverse, unter welchen Voraussetzungen IP-Adressen personenbezogene Daten sind, findet sich bei Auer-Reinsdorff/Conrad/*Conrad/Hausen*, IT- und Datenschutzrecht, § 36 Rn. 59 ff.

Vertrags – synallagmatischer Austausch von Informationen des Betreibers der Internetseite gegen Bereitstellung personenbezogener Daten des Nutzers – gesehen werden. Soweit die Europäische Kommission in ihrer Stellungnahme vom 8. September 2016 – C(2016) 5656 final – zu dem Beschluss des Bundesrates vom 22. April 2016 zum Dossier COM(2015) 634 final – BR-Drs. 168/16 (B) – „automatisch generierte Informationen" wie die IP-Adresse den Daten gegenüberstellt, die ein Nutzer „direkt bereitstellt", vermag das nicht zu überzeugen. Denn die IP-Adresse *wird* vom Nutzer durch seinen Zugriff auf eine Internetseite *aktiv* bereitgestellt.

Soweit die Europäische Kommission das „aktive" Bereitstellen wohl i. S. e. „bewussten" Bereitstellens verstanden wissen will[616], führt dies zu kaum überwindbaren Abgrenzungsschwierigkeiten. Zum einen ist das Bewusstsein der Internetnutzer darüber, welche Informationen sie – z. B. über Metadaten (etwa in Fotos) – über sich preisgeben, sehr unterschiedlich ausgeprägt. Die von der Europäischen Kommission befürwortete „klare, aus Sicht des Durchschnittsverbrauchers pragmatische Unterscheidung" würde zudem Abgrenzungen nach einem eigenständigen Rechtsregime erfordern, für die nicht auf die gewachsene Dogmatik zur Datenschutz-Grundverordnung zurückgegriffen werden könnte. Der Internetverkehr würde dann mit Vertragsschlüssen überfrachtet, die nicht den Interessen der Beteiligten entsprechen und den freien Informationsfluss im Internet unnötig behindern. Der Zugriff auf eine Internetseite sollte, wenn er mit der Preisgabe von Daten verbunden ist, an deren Personenbezug der Betreiber der Seite kein Interesse hat, zivilrechtlich als Inanspruchnahme einer unentgeltlichen Leistung beurteilt werden. Für die Inanspruchnahme unentgeltlicher Leistungen im Internet wird mit Recht kein Regelungsbedarf gesehen.[617]

Zu eng ist ein auf die aktive Hingabe personenbezogener Daten abstellender Ansatz deshalb, weil er nicht Fälle erfasst, bei denen der Betreiber einer Internetseite aus Vermarktungsinteresse einen Personenbezug von Daten ohne aktives Zutun des Nutzers herstellt, z. B. über die Auswertung technischer Daten der vom Nutzer verwendeten Hard- oder Software[618] und deren Verknüpfung mit anderweitig erlangten personenbezogenen Daten. Es sollte vertragsrechtlich nicht zu Lasten eines Nutzers gehen, wenn der Anbieter als Teil seines Geschäftsmodells eine technische Umgebung schafft, über die er zu Vermarktungszwecken einen Personenbezug von Daten herstellt, ohne dass Nutzer dies bemerken, und außerhalb eines Vertragsverhältnisses auf eine datenschutzrechtliche Einwilligung hinwirkt.

---

[616] Dafür spricht, dass als Beispiele für „aktiv bereitgestellte Daten" der Name, eine E-Mail-Adresse und Fotos des Nutzers angeführt werden; siehe auch Art. 3 Abs. 1 in der Fassung der Option 1 der von der Ratspräsidentschaft im Laufe der Verhandlungen auf Ratsebene vorgelegten geänderten Textfassung des Richtlinienvorschlags COM(2015) 634 final vom 15.6.2016 (Ratsdok. 10231/16).

[617] Vgl. Beschluss Ziffer 10 der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016.

[618] Vgl. zu den insoweit eröffneten technischen Möglichkeiten Auer-Reinsdorff/Conrad/*Conrad/Hausen*, IT- und Datenschutzrecht, § 36 Rn. 92 ff.

Ein Anknüpfen an die datenschutzrechtliche Einwilligung ist auch deshalb sachgerecht, weil es nach der Interessenlage beider Vertragspartner letztlich keinen Unterschied bedeutet, wie der Anbieter an personenbezogene Daten des Nutzers gelangt, sondern ob er die erlangten personenbezogenen Daten monetarisieren darf.

3. Zivilrechtliche Relevanz des Rechts auf Widerruf der datenschutzrechtlichen Einwilligung

Nach Art. 7 Abs. 3 EU-DSGVO hat der Nutzer das (unentziehbare) Recht, eine Einwilligung in die Verarbeitung seiner personenbezogenen Daten jederzeit zu widerrufen. Durch einen solchen Widerruf wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt, wovon der Nutzer vor Abgabe der Einwilligung in Kenntnis zu setzen ist. Nach Art. 4 Nr. 11 EU-DSGVO erfordert eine wirksame Einwilligung u. a. eine freiwillige, in informierter Weise abgegebene Willensbekundung. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, ist nach Art. 7 Abs. 4 EU-DSGVO zu berücksichtigen, ob die Erfüllung des Vertrags von einer Einwilligung zur Verarbeitung personenbezogener Daten abhängig gemacht wird, die für die Vertragserfüllung nicht erforderlich sind.

a. Datenschutzrechtlicher Widerruf als auflösende Bedingung

In den Fällen eines „Bezahlens mit Daten“ wird, wenn diese Grundsätze Beachtung finden, beiden Vertragsparteien regelmäßig bewusst sein, dass der Nutzer seine datenschutzrechtliche Einwilligung jederzeit widerrufen kann. Die Frage ist, wie dieser Umstand zivilrechtlich einzuordnen ist.

Es dürfte sach- und interessengerecht sein, im jederzeit möglichen und zulässigen datenschutzrechtlichen Widerruf eine *auflösende Bedingung* i. S. v. § 158 Abs. 2 BGB zu sehen. Dies lässt sich auf folgende Erwägungen stützen:

Eine Bedingung gemäß §§ 158 ff. BGB ist die nach dem Willen der Parteien zum Bestandteil eines Rechtsgeschäfts gemachte Bestimmung, welche die Rechtswirkungen des Geschäfts von einem ungewissen zukünftigen Ereignis abhängig macht.[619] Bei der auflösenden Bedingung wird das Fortbestehen der Rechtswirkungen davon abhängig gemacht, dass ein zukünftiges Ereignis nicht eintritt. Wie sich aus § 454 BGB ergibt, kann es sich bei der Bedingung auch um eine sog. Potestativbedingung handeln, bei der das freie Belieben einer Partei zur Bedingung gemacht wird. Der in das freie Belieben des Nutzers gestellte Widerruf der datenschutzrechtlichen Einwilligung kann mithin eine auflösende Bedingung sein.

Nach § 158 Abs. 2 BGB endet die Wirkung des Rechtsgeschäfts mit dem Eintritt der auflösenden Bedingung. Es tritt von Gesetzes wegen wieder der frühere Rechtszustand ein. Der *Bedingungseintritt* hat keine Rückwirkung, *wirkt* also nur *ex nunc*. Nach § 159 BGB kommt es nur dann zu einer Rückwirkung, wenn nach

---

[619] Vgl. dazu und zum Folgenden Palandt/*Ellenberger*, BGB, Einf v § 158 Rn. 1, 10.

dem Inhalt des Rechtsgeschäfts die an den Eintritt der Bedingung geknüpften Folgen auf einen früheren Zeitpunkt zurückbezogen werden sollen. Von der Vereinbarung einer Rückbeziehung wird man bei einer unabdingbar vereinbarten auflösenden Bedingung des Widerrufs der datenschutzrechtlichen Einwilligung indes regelmäßig nicht ausgehen können. Das ergibt sich aus Art. 7 Abs. 3 S. 2 EU-DSGVO, wonach durch den Widerruf der Einwilligung die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung der personenbezogenen Daten ausdrücklich nicht berührt wird. Es ist zugrunde zu legen, dass die Vertragsparteien diese datenschutzrechtliche Situation zivilrechtlich nachvollziehen wollen.

b. Zivilrechtliche Gewährleistung der Freiwilligkeit einer Einwilligung

Mit der vertragsrechtlichen Einordnung des datenschutzrechtlichen Widerrufs als auflösende Bedingung wird der Verzahnung des Zivilrechts mit dem Datenschutzrecht indes nicht vollständig Rechnung getragen.

Aus ihr folgen zwar die vertragsrechtlichen Rechtswirkungen eines datenschutzrechtlichen Widerrufs. Sie löst indes nicht das Problem, dass die schuldrechtliche *Verpflichtung* zur Erteilung einer datenschutzrechtlichen Einwilligung im Ausgangspunkt durch einen datenschutzrechtlichen Widerruf *nicht berührt* wird. Widerruft der Schuldner seine datenschutzrechtliche Einwilligung, ist er bei rein *schuldrechtlicher* Betrachtung verpflichtet, sie sogleich wieder zu erteilen. Ebenso ist er schuldrechtlich zur Erteilung der Einwilligung verpflichtet, wenn er sich nach Vertragsschluss entscheidet, eine Einwilligungserklärung gar nicht erst abzugeben.

Aus zivilrechtlicher Perspektive könnte er in diesen Konstellationen auf Erteilung einer datenschutzrechtlichen Einwilligung in Anspruch genommen und auf der Grundlage einer nach diesem Maßstab schlüssigen Klage zur Abgabe einer Einwilligungserklärung verurteilt werden.

Dies wäre indes mit dem Datenschutzrecht offenkundig nicht vereinbar. Nach der Begriffsbestimmung in Art. 4 Nr. 11 EU-DSGVO ist „Einwilligung“ nur die *freiwillig* abgegebene Willensbekundung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Nach Erwägungsgrund 42 S. 5 EU-DSGVO soll von einer *freiwilligen* Einwilligung nur dann ausgegangen werden, wenn der Einwilligende eine „echte oder freie Wahl“ hat und in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Dem Aspekt der Freiwilligkeit wird u. a. in Art. 7 Abs. 4 EU-DSGVO Rechnung getragen.

Die schuldrechtliche Verpflichtung, eine datenschutzrechtliche Einwilligung zu erteilen, darf den Verpflichteten mithin nicht in einer Weise binden, die mit diesen datenschutzrechtlichen Vorgaben unvereinbar ist.

Ein – im Ausgangspunkt und losgelöst von allen vorangehenden Erwägungen – möglicher Lösungsansatz für dieses Problem könnte darin bestehen, schuldrechtlich wie in § 762 Abs. 1 BGB für Spiel und Wette zu bestimmen, dass durch einen

Vertrag, bei dem das Entgelt in der Erteilung einer datenschutzrechtlichen Einwilligung besteht, einerseits eine Verbindlichkeit nicht begründet wird, andererseits aber das aufgrund des Vertrags Geleistete nicht mangels einer Verbindlichkeit zurückgefordert werden kann.

Die Annahme eines solchen Rechtsverhältnisses mit wechselseitig unvollkommenen Verbindlichkeiten wäre indes weder mit dem Wesen des Vertrags vereinbar noch interessengerecht. Der Vertrag über die „kostenlose" Nutzung eines sozialen Netzwerks hat keinerlei aleatorischen Charakter und mit Blick auf die jeweilige Zweckbindung der wechselseitigen Leistungen stellt er, weil für die vertragstypische Leistung ein Entgelt in Form von Daten geleistet wird, ein *Synallagma* dar.[620]

Dem datenschutzrechtlichen Erfordernis der Freiwilligkeit einer Einwilligung lässt sich auf der Ebene des Vertragsrechts jedoch durch die Regelung einer Unklagbarkeit des Anspruchs auf Erteilung der Einwilligung angemessen und ausgewogen Rechnung tragen. Das Bürgerliche Gesetzbuch kennt eine Unklagbarkeit für das Eheversprechen. Nach § 1297 Abs. 1 BGB kann aus einem Verlöbnis nicht auf Eingehung der Ehe geklagt werden.

Eine Unklagbarkeit allein wäre hier indes nicht hinreichend. So schließt die Unklagbarkeit nach § 1297 BGB nicht aus, dass aus der Nichterfüllung des unklagbaren Anspruchs anderweitige Ansprüche hergeleitet werden. Für den Fall des gebrochenen Eheversprechens können sich solche Ansprüche aus den §§ 1298 bis 1301 BGB ergeben.

Sekundäransprüche wegen Nichterteilung einer vertraglich geschuldeten datenschutzrechtlichen Einwilligung wären indes mit der Datenschutz-Grundverordnung nicht vereinbar, nach deren Erwägungsgrund 42 die Freiwilligkeit der Einwilligung nur gegeben ist, wenn der Einwilligende in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, *ohne Nachteile zu erleiden*.

Es bedarf deshalb ergänzend einer Regelung, die bestimmt, dass aus der Nichterfüllung der nicht klagbaren Verpflichtung, eine datenschutzrechtliche Einwilligung zu erteilen, keine Ansprüche gegen den Verpflichteten hergeleitet werden können.

Eine solche (nicht dispositive) Vorschrift wäre, obwohl sie den zur Einwilligung Verpflichteten gegenüber dem Anbieter einer mit Daten zu „bezahlenden" Leistung vordergründig besser stellt, ausgewogen. Der nicht vorleistungspflichtige Anbieter hat nach § 320 BGB die Möglichkeit, den Beginn bzw. die Fortsetzung seiner Leistungserbringung daran zu knüpfen, dass ihm vom Nutzer die datenschutzrechtliche Einwilligung zur kommerziellen Verwertung personenbezogener Daten erteilt wird bzw. die Einwilligung nicht durch einen Widerruf entfallen ist. Dies entspricht auch gängiger Praxis.

---

[620] Siehe dazu oben unter I. 1.

4. Zivilrechtliches Widerrufsrecht des Nutzers und Rechte der Parteien bei Vertragsbeendigung

Von der Frage, wie das datenschutzrechtliche Widerrufsrecht zivilrechtlich einzuordnen ist, muss die Frage getrennt werden, welche wechselseitigen Rechte und Pflichten die Parteien haben, wenn der Vertrag, der eine „Bezahlung" mit personenbezogenen Daten vorsieht, vom Nutzer *zivilrechtlich widerrufen* oder aus sonstigen Gründen *beendet* wird.

a. Zivilrechtliches Widerrufsrecht des Nutzers

Legt man zugrunde, dass die Vereinbarung der mit Daten „bezahlten" Nutzung eines sozialen Netzwerks einen gegenseitigen Vertrag darstellt, steht dem Nutzer, wenn er Verbraucher ist, gemäß § 312g Abs. 1 BGB ein Widerrufsrecht nach § 355 BGB zu.

Nach § 356 Abs. 5 BGB erlischt dieses Widerrufsrecht bei einem Vertrag über die Lieferung von nicht auf einem körperlichen Datenträger befindlichen Daten, die in digitaler Form hergestellt und bereitgestellt werden, wenn der Unternehmer mit der Ausführung des Vertrags begonnen hat, nachdem der Verbraucher ausdrücklich zugestimmt hat, dass der Unternehmer mit der Ausführung des Vertrags vor Ablauf der Widerrufsfrist beginnt, und der Verbraucher seine Kenntnis davon bestätigt hat, dass er durch die Zustimmung mit Beginn der Ausführung des Vertrags sein Widerrufsrecht verliert.

Ein Widerruf hat nach § 355 Abs. 1 S. 1 BGB zur Folge, dass die Parteien an ihre auf den Abschluss eines Vertrags gerichteten Willenserklärungen nicht mehr gebunden sind. Durch den Widerruf wandelt sich der zunächst wirksame Vertrag *ex nunc* in ein Rückgewährschuldverhältnis um.[621] Die Parteien haben nach § 355 Abs. 3 S. 1 BGB die empfangenen Leistungen unverzüglich zurückzugewähren.

In den Fällen eines „Bezahlens mit Daten" stellt sich das Problem, dass bei einem Widerruf die Rückgewähr der datenschutzrechtlichen Einwilligung nicht möglich ist. Hat der Unternehmer die personenbezogenen Daten des Nutzers bereits kommerzialisiert, kann dies nicht mehr rückgängig gemacht werden. Die geltenden Regelungen zu Rückgewährpflichten des Unternehmers sind darauf zugeschnitten, dass die Leistung des Verbrauchers in einer Geldzahlung besteht.

Für diese Konstellation kommen drei Lösungen in Betracht:

(1.) Für den Fall des Widerrufs könnte ein Wertersatzanspruch des Verbrauchers geregelt werden. Problematisch ist dabei, dass sich der inhalts- und kontextabhängige Wert personenbezogener Nutzerdaten kaum auch nur annähernd bestimmen lassen dürfte.

(2.) Denkbar wäre eine gesetzliche Regelung, die bestimmt, dass der Unternehmer vom Verbraucher als vertragliche Gegenleistung zur Verfügung gestellte Daten nicht nutzen darf, solange der Verbraucher noch zum Widerruf

---

[621] Vgl. Palandt/*Grüneberg*, BGB, § 355 Rn. 4, 12.

berechtigt ist.[622] Eine solche Regelung hätte allerdings praktisch kaum Relevanz, da sie in den Fällen des § 356 Abs. 5 BGB keine Anwendung finden würde.

(3.) Es könnte bestimmt werden, dass den Unternehmer keine Wertersatzpflicht trifft. Dafür ließe sich anführen, dass der Verbraucher nach § 357 Abs. 9 BGB beim Widerruf eines Vertrags über die Lieferung von nicht auf einem körperlichen Datenträger befindlichen digitalen Inhalten seinerseits keinen Wertersatz zu leisten hat.

Vorzugswürdig erscheint letztlich Lösung (3.). Der zivilrechtliche Widerruf hätte damit praktisch die Wirkung einer Vertragsbeendigung für die Zukunft, wie sie der Nutzer auch über den Widerruf der datenschutzrechtlichen Einwilligung erreichen kann.

b. Rechte des Nutzers bei Vertragsbeendigung

(1) Rückgewähr von Daten

Soweit die Schaffung einer gesetzlichen Regelung befürwortet wird, die den Anbieter im Falle eines Widerrufs oder einer sonstigen Beendigung des Vertrags verpflichtet, vom Nutzer zur Verfügung gestellte digitale Inhalte *zurück zu gewähren*[623], erscheint eine solche Regelung mit Bezug auf soziale Netzwerke als nicht erforderlich.

Bei den von einem Nutzer über ein soziales Netzwerk kommunizierten Inhalten handelt es sich – soweit man nicht vom Nutzer in seine Kommunikation eingebundene Kopien von digitalen Inhalten Dritter isoliert betrachtet – regelmäßig um personenbezogene Daten. Hinsichtlich personenbezogener Daten kann der Nutzer indes schon nach Art. 15 Abs. 3 EU-DSGVO mit einem elektronischen Antrag verlangen, dass ihm der Anbieter eine Kopie in einem *gängigen elektronischen Format* zur Verfügung stellt. Ob die so zur Verfügung gestellte Kopie von einem anderen Anbieter akzeptiert wird, gehört zivilrechtlich zur Risikosphäre des Nutzers. Die Forderung, der Dienstleister müsse gesetzlich verpflichtet sein, „dem Auftraggeber bei Vertragsbeendigung alle Daten und Informationen zu überlassen, die dieser oder ein nachfolgender Dienstleister zur Übernahme oder Fortführung des Dienstes benötigt“[624], erscheint für das zivilrechtliche Verhältnis zwischen dem Anbieter und dem Nutzer eines sozialen Netzwerks als zu weitgehend.

Auch hinsichtlich vom Nutzer in seine Kommunikation eingebundener Kopien von digitalen Inhalten Dritter ohne Personenbezug gibt es keinen Anlass für die Regelung eines Rückgewähranspruchs. Dass der Nutzer auf die Quelle der in das

---

[622] So generell für Verbraucherverträge der Beschluss Ziffer 15 der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016.

[623] So der Beschluss Ziffer 6 der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016; siehe auch Art. 13 Abs. 2 lit. c des Richtlinienvorschlags COM(2015) 634 final.

[624] So generell (als Nebenpflicht) für Verträge über digitale Dienste der Beschluss Ziffer 24 lit. a der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016.

soziale Netzwerk eingestellten Kopie später aus tatsächlichen oder rechtlichen Gründen keinen Zugriff mehr hat, sollte nicht zu Lasten des Anbieters eines sozialen Netzwerks gehen.

(2) Recht auf Unterlassung einer weiteren Datennutzung

In Art. 13 Abs. 2 lit. b des Richtlinienvorschlags COM(2015) 634 final ist vorgesehen, dass der Anbieter digitaler Inhalte bei einer Vertragsbeendigung durch den Verbraucher alle Maßnahmen zu ergreifen hat, die erwartet werden können, um die Nutzung einer anderen Gegenleistung als Geld zu unterlassen.

Wenn man die Gegenleistung des Nutzers in der Erteilung seiner datenschutzrechtlichen Einwilligung sieht, erscheint zweifelhaft, ob es der zivilrechtlichen Regelung einer solchen Unterlassungspflicht bedarf.

Nach Art. 7 Abs. 3 S. 1, 2 EU-DSGVO hat der Nutzer das Recht, seine datenschutzrechtliche Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Der Nutzer kann also bereits datenschutzrechtlich erreichen, dass eine weitere Nutzung seiner personenbezogenen Daten nach Vertragsbeendigung nicht mehr stattfindet. Von diesem datenschutzrechtlichen Recht muss der Nutzer nach Art. 7 Abs. 3 S. 3 EU-DSGVO vor Abgabe der Einwilligung in Kenntnis gesetzt werden.

Man wird deshalb kein Bedürfnis für ein darauf bezogenes zivilrechtliches Parallelregime annehmen können.

Angesichts der engen Verzahnung von Datenschutz- und Vertragsrecht ließe sich für die Fälle des „Bezahlens mit Daten“ allerdings argumentieren, dass eine zivilrechtliche Nebenpflicht des Anbieters, den Nutzer bei Vertragsbeendigung auf seine datenschutzrechtlichen Rechte hinzuweisen, interessengerecht sein könnte. Eine Regelung mit dieser Zielrichtung dürfte allerdings mit der Datenschutz-Grundverordnung kaum vereinbar sein. Der Vorrang des Unionsrechts schließt es aus, auf mitgliedstaatlicher Ebene Vorschriften zu erlassen, welche eine vom Unionsrecht betroffene Materie autonom regeln.[625] Man wird deshalb die Regelung einer über Art. 7 Abs. 3 S. 3 EU-DSGVO hinausgehenden Hinweispflicht des Anbieters wohl als unzulässig ansehen müssen.

5. Einordnung der Hauptleistung des Nutzers im System des Schuldrechts

Die vom Nutzer als Voraussetzung einer Nutzung des sozialen Netzwerks zu erteilende datenschutzrechtliche Einwilligung stellt zwar eine Hauptleistungspflicht dar, die zur Eigenart des Vertrags über die „kostenlose“ Nutzung gehört.

Im Schrifttum wird deshalb vertreten, die Gestattung des Nutzers eines sozialen Netzwerks gegenüber dem Betreiber, seine persönlichen Daten und Inhalte kommerziell zu verwerten, könne – wenn man in ihr eine lizenzähnliche Erlaubnis sehe – als eine der Hauptleistung eines Verkäufers oder Vermieters entsprechende

---

[625] Vgl. von der Groeben/Schwarze/Hatje/*Geismann*, Europäisches Unionsrecht, Art. 288 AEUV Rn. 9.

Leistung eingeordnet werden[626]. Eine solche rechtliche Einordnung hätte zur Folge, dass sich beim Vertrag über die „kostenlose" Nutzung eines sozialen Netzwerks zwei jeweils einen anderen Vertragstypus prägende Hauptleistungspflichten gegenüberstünden. Es läge dann nahe, das Vertragsverhältnis als Vertrag *sui generis* nach § 311 BGB einzuordnen.[627] In Betracht zu ziehen wäre zudem ein typengemischter Vertrag in Gestalt eines gekoppelten (doppeltypischen) Vertrags[628], bei dem sich – wie beim Tausch nach § 480 BGB – nicht finanzielle Hauptleistungspflichten gegenüberstehen, die unterschiedlichen Vertragstypen zuzuordnen sind.

Für die Zuordnung zu einem – ggf. neu zu schaffenden – Vertragstyp gibt die datenschutzrechtliche Einwilligung jedoch letztlich nichts her. Einwilligungen natürlicher Personen in die wirtschaftliche Verwertung personenbezogener Daten gemäß Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a EU-DSGVO erfolgen praktisch in den unterschiedlichsten zivilrechtlichen Zusammenhängen, z. B. auch bei der Teilnahme an Bonussystemen, der Installation „kostenloser" Apps und Online-Bestellungen. Die Gemeinsamkeiten zwischen diesen Phänomenen sind gering. Die datenschutzrechtliche Einwilligung als „Entgelt" vermag damit ebenso wenig wie die Hauptleistungspflicht zur Zahlung eines Geldbetrags als Vergütung einen Vertragstypus zu prägen.

Die datenschutzrechtliche Einwilligung des Nutzers stellt mithin die den *Typus* des Vertragsverhältnisses mit dem Anbieter des sozialen Netzwerks *nicht prägende Gegenleistung* dar.

6. Inhalt der vom Nutzer geschuldeten Gegenleistung (Datenqualität)

Personenbezogene Daten unterscheiden sich von Geld u. a. dadurch, dass sie nicht fungibel – d. h. nicht gleichwertig austauschbar gegen andere Stücke gleicher Gattung und Menge – sind. Die subjektive Bedeutung und die objektive Bedeutsamkeit kommunizierter Inhalte sind kontextabhängig und fallen häufig auseinander. Die bei einer Kommunikation über ein soziales Netzwerk generierten personenbezogenen Daten können deshalb unter dem Aspekt der wirtschaftlichen Verwertbarkeit für den Diensteanbieter eine sehr unterschiedliche Qualität haben. Daten, die valide Rückschlüsse auf Präferenzen eines Nutzers zulassen, werden für den Anbieter eines sozialen Netzwerks von größerem Nutzen sein als Daten, die sich für eine zielgenau personalisierte Werbung nicht eignen.

Es stellt sich deshalb die Frage, ob der Nutzer beim „Bezahlen mit Daten" generell oder bei einer dahingehenden vertraglichen Vereinbarung (d. h. praktisch bei ei-

---

[626] Vgl. *Bräutigam*, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635 (640); *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 19 m. w. N.

[627] So *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 22.

[628] Siehe dazu Palandt/*Grüneberg*, BGB, Überbl v § 311 Rn. 19 ff. m. w. N.

ner entsprechenden Klausel in den Nutzungsbedingungen des Anbieters) verpflichtet ist, seine Leistung in einer bestimmten Qualität zu erbringen. Betrachtet man die Pflicht des Nutzers zum „Bezahlen mit Daten“ als eine Gattungsschuld, hätte er nach § 243 Abs. 1 BGB – der über seinen Wortlaut hinaus auch für andere Leistungen als Sachleistungen gilt[629] – Daten von „mittlerer Art und Güte“ zu leisten.

Im Schrifttum wird der Aspekt der *Datenqualität* im Zusammenhang mit „Big Data“ diskutiert[630]. Im Vordergrund steht dabei der Erwerb von Rohdaten und von Resultaten aus Big-Data-Anwendungen.

Von den Fällen des „Bezahlens mit Daten“ unterscheiden sich solche Austauschgeschäfte allerdings dadurch, dass der Leistungsaustausch nicht die Erteilung einer datenschutzrechtlichen Einwilligung zum Gegenstand hat. Datenqualität wird im Zusammenhang mit „Big Data“-Verträgen demgemäß als eine im Kern rein zivilrechtliche Frage ohne datenschutzrechtliche Bezüge angesehen.[631]

Erblickt man beim „Bezahlen mit Daten“ im Rahmen eines gegenseitigen Vertrags die Gegenleistung des Nutzers – wie vorstehend ausgeführt – in der Erteilung einer datenschutzrechtlichen Einwilligung in die kommerzielle Verwertung personenbezogener Daten, scheidet eine Hauptleistungspflicht des Nutzers, Daten in einer bestimmten Qualität bereitzustellen, aus.

7. Zulässigkeit und Grenzen einer formularmäßigen Vereinbarung der Hauptleistung des Nutzers

Sieht man entsprechend den vorstehenden Erwägungen in der Einwilligung des Nutzers in die wirtschaftliche Verwertung seiner personenbezogenen Daten die von ihm zu erbringende Hauptleistung im Synallagma, stellt sich die Frage, ob bzw. inwieweit diese Hauptleistung formularmäßig vereinbart werden kann.

In der Praxis wird die Verwendung personenbezogener Daten des Nutzers regelmäßig in anbieterseitig vorgegebenen „Nutzungsbedingungen“ bzw. „Datenrichtlinien“ geregelt, an deren Akzeptanz der Anbieter die Nutzung des von ihm bereitgestellten sozialen Netzwerks knüpft.[632].

---

[629] Vgl. Palandt/*Grüneberg*, BGB, § 243 Rn. 1.

[630] Vgl. *Hoeren*, Thesen zum Verhältnis von Big Data und Datenqualität – Erstes Raster zum Erstellen juristischer Standards, MMR 2016, 8 f. m. v. w. N.

[631] Vgl. *Hoeren*, Thesen zum Verhältnis von Big Data und Datenqualität – Erstes Raster zum Erstellen juristischer Standards, MMR 2016, 8 (10).

[632] Vgl. z. B. die „Nutzungsbedingungen“ und die „Datenrichtlinie“ von Facebook, abrufbar unter https://de-de.facebook.com/legal/terms bzw. https://de-de.facebook.com/about/privacy, sowie die „Nutzungsbedingungen“ und die „Datenschutzerklärung“ von Google, abrufbar unter https://www.google.de/intl/de/policies/terms/regional.html bzw. https://www.google.de/intl/de/policies/privacy/ (letzte Abrufe jeweils: 14.3.2017).

Stellt man die Einwilligung in die wirtschaftliche Verwertung personenbezogener Daten einer Geldzahlung gleich, begegnet die *zivilrechtliche* Wirksamkeit der Einwilligung in der derzeit üblichen Form Bedenken.

a. Bezugspunkt: „Button"-Lösung für zahlungspflichtige Bestellungen

Nach § 312j Abs. 3 BGB hat der Unternehmer im elektronischen Geschäftsverkehr gegenüber einem Verbraucher, der eine *entgeltliche* Leistung des Unternehmers zum Gegenstand hat, die Bestellsituation so zu gestalten, dass der Verbraucher mit seiner Bestellung *ausdrücklich bestätigt*, dass er sich zu einer *Zahlung* verpflichtet. Erfolgt die Bestellung über eine Schaltfläche, ist diese Pflicht nur erfüllt, wenn diese Schaltfläche gut lesbar mit nichts anderem als den Wörtern „zahlungspflichtig bestellen" oder mit einer entsprechenden eindeutigen Formulierung beschriftet ist (sog. „Button-Lösung").

Es erscheint sach- und interessengerecht, eine solche *Button-Lösung* auch für das „Bezahlen mit Daten" zu wählen und § 312j Abs. 3 BGB entsprechend zu ergänzen.[633] Für den Verbraucher wird dadurch transparent, dass er sich vertraglich zu einer Gegenleistung verpflichtet. Zuwiderhandlungen von Anbietern könnten nach dem Unterlassungsklagengesetz verfolgt werden.

Der Mustertext für die elektronische Schaltfläche (den "Button") könnte in Anlehnung an Art. 6 Abs. 1 lit. a, Art. 7 Abs. 4 EU-DSGVO (sowie – hinsichtlich der Terminologie „für kommerzielle Zwecke" – an Art. 3 Abs. 4 des Richtlinienvorschlags COM[2015] 634 final) lauten:

> *„Bestellen gegen Einwilligung zu einer Verarbeitung personenbezogener Daten für kommerzielle Zwecke des Anbieters."*

Die Datenschutz-Grundverordnung – insbesondere Art. 7 Abs. 2 EU-DSGVO – dürfte einer solchen Regelung nicht entgegenstehen. Der Vorrang des Unionsrechts schließt nur Vorschriften auf mitgliedstaatlicher Ebene aus, welche eine vom Unionsrecht *betroffene Materie* autonom regeln.[634] Die vorgeschlagene Regelung betrifft indes weder die datenschutzrechtliche Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art. 6 EU-DSGVO) noch die datenschutzrechtlichen Bedingungen für eine wirksame Einwilligung (Art. 7 EU-DSGVO),

---

[633] Für die Prüfung einer „Button"-Lösung spricht sich auch der Beschluss des Bundesrats vom 4.11.2016 – Entschließung des Bundesrates zur Verbesserung der Übersichtlichkeit von Allgemeinen Geschäftsbedingungen (AGB), BR-Drs. 577/16 (B) – aus; in der Begründung der Entschließung heißt es: „Für Verbraucherverträge sollte zudem die Einführung der so genannten ‚Button-Lösung' im Hinblick auf die Freigabe von Daten geprüft werden; vor allem für Verträge bei denen ‚mit Daten bezahlt wird'. Dadurch soll den Verbrauchern vor Klicken des Buttons (der zum Eingang des Vertragsverhältnisses führt) noch einmal vor Augen geführt werden, welche Daten sie zu welchen Zwecken mit dem Klick freigeben." Mit einer „Button"-Lösung schon 2013 sympathisierend *Benninghoff*, Brauchen wir eine „Button"-Lösung für das Datenschutzrecht?, VuR 2013, 361 f.

[634] Siehe dazu oben unter I. 4. b. (2).

sondern die *rein zivilrechtliche Frage*, wie eine datenschutzrechtliche Einwilligung (daten*schuld*rechtlich) zum Bestandteil eines synallagmatischen Vertrags gemacht werden kann[635].

Ergänzend sollte § 312a Abs. 3 BGB um eine Regelung ergänzt werden, wonach eine Vereinbarung, die auf ein über das vereinbarte Entgelt für die Hauptleistung hinausgehendes „Bezahlen mit Daten" gerichtet ist, *ausdrücklich* getroffen werden muss.

Nicht interessengerecht für Fälle des „Bezahlens mit Daten" erscheint § 312j Abs. 4 BGB, wonach ein Vertrag nur zustande kommt, wenn der Unternehmer seine Pflicht aus § 312j Abs. 3 BGB erfüllt. Die Regelung belohnt den Anbieter, der gegen die neu geregelte Button-Lösung verstößt, mit einem vertraglosen Zustand, in dem er ggf. datenschutzrechtlich zulässig personenbezogene Daten des Nutzers verwerten kann, ohne seinerseits zu einer vertraglichen Leistung verpflichtet zu sein. Der Nutzer könnte eine von ihm erteilte datenschutzrechtliche Einwilligung zwar ggf. kondizieren. Eine Durchsetzung von Pflichten des Anbieters nach § 818 BGB dürfte jedoch auf praktisch kaum überwindbare Schwierigkeiten stoßen. Es sollte deshalb eine Ergänzung des § 312j Abs. 4 BGB in dem Sinne erwogen werden, dass beim „Bezahlen mit Daten" ein Verstoß gegen den neu gefassten § 312j Abs. 3 BGB nicht das Zustandekommen des Vertrags hindert, sondern lediglich den Verbraucher nicht bindet.[636] Eine entsprechende Ergänzung empfiehlt sich für die Fallgestaltung, dass der Verbraucher eine datenschutzrechtliche Einwilligung als „Zusatzentgelt" leisten soll, in § 312a Abs. 3 BGB.[637]

b. Umgehung durch Leistungsbeschreibung?

Der den vorstehenden Erwägungen zugrundeliegende Ansatz baut darauf auf, dass die kommerzielle Verwertung von personenbezogenen Daten des Nutzers eines sozialen Netzwerks durch den Anbieter nach Art. 6 Abs. 1 lit. a EU-DSGVO einer Einwilligung des Nutzers bedarf. Ist eine solche Einwilligung datenschutzrechtlich nicht erforderlich, scheidet sie auch als Hauptleistungspflicht des Nutzers im Rahmen eines synallagmatischen Vertrags über die „kostenlose" Nutzung eines sozialen Netzwerks aus.

---

[635] Man mag hier parallel folgende Erwägung zu synallagmatischen Verträgen, die eine Geldzahlung als Gegenleistung vorsehen, heranziehen: Das gesetzliche Zahlungsmittel Euro ist währungsrechtlich geregelt. Die zivilrechtliche Frage, wie das gesetzliche Zahlungsmittel zum Bestandteil eines synallagmatischen Vertrags gemacht werden kann, ist jedoch im Bürgerlichen Gesetzbuch bestimmt.

[636] So zum geltenden § 312j Abs. 4 BGB der Beschluss Ziffer 16 lit. a der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016.

[637] Für eine noch weiter gehende Änderung von § 312a Abs. 3 S. 1 BGB Beschluss Ziffer 12 der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016.

Einer datenschutzrechtlichen Einwilligung bedarf es für eine rechtmäßige Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. b EU-DSGVO allerdings nicht, wenn die Verarbeitung *für die Erfüllung des Vertrags erforderlich* ist.

Es stellt sich deshalb die Frage, ob ein Anbieter das *Einwilligungserfordernis* nach Art. 6 Abs. 1 lit. a EU-DSGVO dadurch *umgehen* kann, dass er sein eigenes Interesse an einer kommerziellen Verwertung der personenbezogenen Daten des Nutzers über die Beschreibung seiner Leistung in eine eigene Hauptleistungspflicht – z. B. in die „Pflicht", den Nutzer durchgehend mit personalisierter Werbung zu versorgen bzw. ihm bei Werbung regelmäßig ein „Werbeerlebnis" zu verschaffen – einkleidet.

In der Literatur[638] ist insoweit thematisiert worden, dass ein Anbieter sein eigenes Leistungsversprechen beliebig weit formulieren und dadurch den Anwendungsbereich von Art. 6 Abs. 1 lit. b EU-DSGVO eröffnen könne.[639] Über das Einfallstor des Art. 6 Abs. 1 lit. b EU-DSGVO könnten zivilrechtliche Verträge zentrale Schutzmechanismen der Datenschutz-Grundverordnung, die sich auf die Einwilligung fokussierten, unterlaufen[640]. Das Zusenden personalisierter Informationen lasse sich als Teil eines digitalen Leistungspakets des Anbieters versprechen, dessen Erfüllung die Verarbeitung umfangreicher Informationen über persönliche Präferenzen erforderlich mache.[641]

Im Ergebnis erscheint diese Besorgnis als *nicht* gerechtfertigt.

Schon nach allgemeinen zivilrechtlichen Grundsätzen sind den Möglichkeiten eines Vertragschließenden, das Gefüge an Rechten und Pflichten der Vertragsparteien durch formularmäßig vorgegebene Formulierungen so zu gestalten, dass Rechte als Pflichten und Pflichten als Rechte deklariert werden, Grenzen gesetzt.

---

[638] Vgl. zu diesem Aspekt sehr ausführlich *Graf v. Westphalen/Wendehorst*, Hergabe personenbezogener Daten für digitale Inhalte – Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?, BB 2016, 2179 ff.

[639] Anlass für solche Überlegungen mögen u. a. die Ausführungen des Sachverständigen Staudenmayer in der öffentlichen Anhörung des Bundestagsausschusses für Recht und Verbraucherschutz zu den Richtlinienvorschlägen COM(2015) 634 final und COM(2015) 635 final am 11. Mai 2016 (BT-Protokoll-Nr. 18/99) geben. Der Sachverständige Staudenmayer hat u. a. ausgeführt: „Es gibt nach der Datenschutzgrundverordnung eine ganze Reihe von Gründen, auf deren Grundlage man Daten sammeln und verwerten kann. Einwilligung ist einer. Wir reden hier aber nicht von der Einwilligung, sondern wir reden von Art. 6 Abs. 1b der Datenschutzgrundverordnung, von einem Vertrag als Rechtsgrundlage. Das heißt, im Vertrag selbst wird geregelt, dass Sie Daten einholen. Sie schreiben hinein: Ich möchte für die Hingabe des digitalen Inhalts E-Mail-Adresse, Geburtsdatum, Alter usw. des Verbrauchers. Dann ist die Rechtsgrundlage für die Sammlung dieser Daten der Vertrag selbst." (BT-Protokoll-Nr. 18/99, S. 31).

[640] Vgl. *Graf v. Westphalen/Wendehorst*, Hergabe personenbezogener Daten für digitale Inhalte – Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?, BB 2016, 2179.

[641] *Graf v. Westphalen/Wendehorst*, Hergabe personenbezogener Daten für digitale Inhalte – Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?, BB 2016, 2179 (2183).

Nach § 133 BGB ist bei der Auslegung einer Willenserklärung der wirkliche Wille zu erforschen und nicht an dem buchstäblichen Sinn des Ausdrucks zu haften. Diese Auslegungsregel erstreckt sich auf Leistungsbeschreibungen und ist auch auf Verträge anzuwenden.[642] Das von den Parteien übereinstimmend *Gewollte* hat *Vorrang vor einer absichtlichen Falschbezeichnung*.[643]

Die objektiv und nach einem natürlichen Verständnis von einer Vertragspartei geschuldete Hauptleistung wird nicht dadurch zu einer von der anderen Partei geschuldeten Hauptleistung, weil sie künstlich zu einer solchen stilisiert wird.[644] Das gilt auch dann, wenn eine Vertragspartei nicht nur in der von ihr zu beanspruchenden Gegenleistung, sondern auch in der von ihr zu erbringenden Leistung einen Vorteil für sich sieht und dies im Vertrag einen Ausdruck findet.[645]

Dementsprechend kann der Anbieter eines sozialen Netzwerks das Einwilligungserfordernis nach Art. 6 Abs. 1 lit. a EU-DSGVO nicht dadurch umgehen, dass er sein eigenes Interesse an einer kommerziellen Verwertung der personenbezogenen Daten des Nutzers über die Beschreibung seiner Leistung als eigene Hauptleistungspflicht – z. B. als „Pflicht“, den Nutzer durchgehend mit personalisierter Werbung zu versorgen bzw. ihm bei Werbung regelmäßig ein „Werbeerlebnis“ zu verschaffen – formuliert.

Unerheblich ist dabei, wie Art. 6 Abs. 1 lit. b EU-DSGVO hinsichtlich der Voraussetzung, dass „die Verarbeitung … für die Erfüllung eines Vertrags … erforderlich“ sein muss, europarechtlich autonom auszulegen ist. Die Erfüllung einer vertraglichen Pflicht setzt voraus, dass es eine solche Pflicht gibt. Zur *Erfüllung* eines Vertrags *erforderlich* kann deshalb nur sein, was von einer Vertragspartei überhaupt *vertraglich geschuldet* ist. Was die Parteien eines Vertrags wechselseitig schulden, richtet sich nicht nach Datenschutzrecht, sondern nach dem *zivilrechtlich* auszulegenden Inhalt des Vertrags und den auf ihn anwendbaren Regelungen des *bürgerlichen Rechts*.

Die Verarbeitung personenbezogener Daten des Nutzers eines sozialen Netzwerks für kommerzielle Zwecke des Anbieters mag von einem Nutzer als nicht oder

---

642 Vgl. Palandt/*Ellenberger*, BGB, § 133 Rn. 1, 3.
643 Vgl. Palandt/*Ellenberger*, BGB, § 133 Rn. 7 f.
644 So wird die in einem Austauschvertrag zwischen A und B geregelte Hingabe eines Geldbetrags durch A nicht dadurch zu einer Hauptleistungspflicht von B, weil ein von B vorgegebener formularmäßiger Vertragstext als dessen vertragliche Hauptpflicht bestimmt, A durch die Entgegennahme des Geldbetrags in dem Ziel zu unterstützen, durch die Weggabe materieller Werte inneres Glück und Zufriedenheit zu erlangen.
645 Die vertragliche Pflicht zum Erbringen einer Dienstleistung (z. B. Erteilung von Skiunterricht) gegen Entgelt wird nicht dadurch zu einem „Recht, die Dienstleistung erbringen zu dürfen“, weil das Erbringen der Dienstleistung zugleich einer Neigung des Dienstleistenden (Freude am gemeinsamen Skifahren mit Schülern) entspricht und dies im Text eines schriftlichen Vertrags Ausdruck findet.

jedenfalls nicht nur nachteilig angesehen werden.[646] So kann der Nutzer in personalisierter Werbung eine Informationsquelle oder gar nützliche Hilfestellung für seine Entscheidungen über wirtschaftliche Dispositionen erblicken. Dies ist bei der Verarbeitung seiner personenbezogenen Daten durch den Anbieter zu kommerziellen Zwecken jedoch nicht mehr als ein Nebeneffekt. *Ziel* der kommerziellen Verarbeitung personenbezogener Daten ist es, den Nutzer *im wirtschaftlichen Interesse des Anbieters* bzw. eines Vertragspartners des Anbieters möglichst effektiv in seinen wirtschaftlichen Dispositionen *zu beeinflussen*.

Die Beeinflussung im alleinigen wirtschaftlichen Interesse des Beeinflussenden – d. h. das nicht am Wohl des Beeinflussten ausgerichtete Einwirken auf dessen Entscheidungsprozesse – stellt für den Beeinflussten indes *objektiv nie* einen die Nachteile überwiegenden *Vorteil* dar. Dem lässt sich nicht entgegenhalten, über personalisierte Werbung erhalte der Adressat erst Kenntnisse über für ihn vorteilhafte Produkte und Dienstleistungen, deren Existenz ihm sonst verborgen bliebe. *Ziel der Werbung* ist es nicht, dass der Werbeadressat in den Genuss der angebotenen Leistung kommt, sondern dass er dafür eine *Gegenleistung* – in aller Regel eine *Geldzahlung* – erbringt, deren Höhe (mag sie auch als gering angepriesen werden) nicht seinem Interesse, sondern den Interessen des Anbieters des beworbenen Produkts entspricht.

Aus vorstehenden Erwägungen vermag – entgegen einer im Schrifttum geäußerten Befürchtung[647] – auch Art. 6 Abs. 1 lit. f EU-DSGVO nicht das Einwilligungserfordernis nach Art. 6 Abs. 1 lit. a EU-DSGVO zu verdrängen. Soweit der Anbieter eines sozialen Netzwerks personenbezogene Daten eines Nutzers zu kommerziellen Zwecken verarbeitet, geschieht dies nicht zur „Wahrung" seiner „berechtigten Interessen", sondern in Ausübung seiner durch einen synallagmatischen Vertrag mit dem Nutzer begründeten Rechte.

Die vertragsrechtlichen Fragen, die mit der Nutzung personenbezogener Daten für personalisierte Werbung einhergehen, lassen sich nach Vorstehendem mit den geltenden Regelungen des bürgerlichen Rechts im Ergebnis angemessen bewältigen.

Dass die kommerzielle Verwertung personenbezogener Daten des Nutzers eines sozialen Netzwerks durch dessen Anbieter unabhängig davon, wie sie deklariert wird, keine Leistung des Anbieters gegenüber dem Nutzer darstellt, ist letztlich *so selbstverständlich*, dass es *keiner* darauf bezogenen *Regelung* bedarf.

---

[646] Auch der Skilehrer im vorgenannten Beispiel mag der von ihm gegen Entgelt vertraglich übernommenen Pflicht zur Erteilung von Skiunterricht wegen seiner Freude am gemeinsamen Skifahren positive Aspekte beimessen.

[647] Vgl. *Graf v. Westphalen/Wendehorst*, Hergabe personenbezogener Daten für digitale Inhalte – Gegenleistung, bereitzustellendes Material oder Zwangsbeitrag zum Datenbinnenmarkt?, BB 2016, 2179 (2183).

8. Regelungsbedarf mit Bezug auf Nutzungsverhältnisse ohne finanzielle Gegenleistung

a. Erteilung einer datenschutzrechtlichen Einwilligung als Entgelt

Auf der Grundlage vorstehender Erwägungen stellt sich die Frage, ob gesetzlich klargestellt werden sollte, dass die Erteilung einer datenschutzrechtlichen Einwilligung zur wirtschaftlichen Verwertung personenbezogener Daten wie Geld eine vertragliche Gegenleistung und damit Gegenstand einer vertraglichen Hauptleistungspflicht im Synallagma sein kann.[648]

Dass der Begriff „entgeltlich“ in § 312 Abs. 1 BGB weit ausgelegt werden muss und Verbraucherverträge auch dann als entgeltlich einzuordnen sein können, wenn die vom Verbraucher zu erbringende Gegenleistung nicht in Geld, sondern in Daten besteht, entspricht in der Dogmatik zu § 312 Abs. 1 BGB der wohl (noch) überwiegenden Ansicht.[649]

Für diese Ansicht lassen sich die Materialien aus dem der Vorschrift zugrundeliegenden Gesetzgebungsverfahren anführen, aus welchen sich ergibt, dass der Gesetzgeber den Entgeltbegriff tatsächlich weit verstanden wissen wollte.

Der Regierungsentwurf eines Gesetzes zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung – BT-Drs. 17/12637 vom 6. März 2013 (dort S. 45) – gibt insoweit allerdings wenig Anhaltspunkte. Zum Merkmal der *Entgeltlichkeit* in § 312 Abs. 1 BGB-E enthält er lediglich die Passage: „Entsprechend der Schutzrichtung der Richtlinie ist jedoch nur dann von einem Verbrauchervertrag i. S. d. Richtlinie auszugehen, wenn sich … der Verbraucher (§ 13) zur Zahlung eines Entgelts verpflichtet. Dies ergibt sich bereits aus den Definitionen in Art. 2 Nr. 5 und 6 der Richtlinie.“ Bemerkenswert ist, dass der Gesetzentwurf auf eine „Zahlung“ abstellt und die in Bezug genommenen Regelungen der Verbraucherrechterichtlinie ebenfalls die Wörter „zahlt“ und „Zahlung“ – nicht *Leistung eines Entgelts* – enthalten.

Gewichtigere Anhaltspunkte mit Bezug auf den unverändert aus dem Regierungsentwurf übernommenen und Gesetz gewordenen § 312 Abs. 1 BGB-E enthält die Bundestagsdrucksache 17/13951 – Beschlussempfehlung und Bericht des Rechtsausschusses (6. Ausschuss) zum Regierungsentwurf – vom 12. Juni 2013, in der es auf Seite 71 heißt:

> *„Über diese Änderungen hinaus wurden weitere Änderungen erwogen: … Zum anderen will auch die Verbraucherrechterichtlinie nur Verträge erfassen, bei denen die Waren oder Dienstleistungen gegen*

---

[648] In diesem Sinne – Gegenleistung ist beim „Bezahlen mit Daten“ die Erteilung einer *datenschutzrechtlichen Einwilligung* – der Beschluss Ziffer 5 der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016.

[649] Vgl. insoweit *Brönneke/Schmidt*, Der Anwendungsbereich der Vorschriften über die besonderen Vertriebsformen nach Umsetzung der Verbraucherrechterichtlinie, VuR 2014, 3; dem folgend Palandt/*Grüneberg*, BGB, § 312 Rn. 3; ebenso jurisPK/*Junker*, BGB, § 312 Rn. 20.

> *Entgelt erbracht werden. Auch dies folgt aus den Definitionen der Kauf- und Dienstleistungsverträge in Artikel 2 Nummer 5 und 6 der Richtlinie (‚und der Verbraucher hierfür den Preis zahlt'). Schließlich schränkt das Merkmal ‚entgeltliche Leistung' den Anwendungsbereich der Vorschriften auch nicht zu weitgehend ein. Insbesondere erfordert es nicht, dass das Entgelt in der Zahlung eines Geldbetrags liegt. Vielmehr ist das Merkmal ‚Entgelt' weit auszulegen. Es genügt irgendeine Leistung des Verbrauchers … . Es muss sich also um einen gegenseitigen bzw. einen Austauschvertrag handeln … . Daher können auch Verträge, bei denen der Verbraucher für die Erbringung einer Dienstleistung oder die Lieferung einer Ware dem Unternehmer im Gegenzug personenbezogene Daten mitteilt und in deren Speicherung, Nutzung oder Weitergabe einwilligt, erfasst sein."*

Der Gesetzgeber ist insoweit nicht dem Sachverständigen *Brönneke* gefolgt, der in der öffentlichen Anhörung im Rechtsausschuss des Deutschen Bundestages am 17. April 2013 vorschlug gesetzlich klarzustellen, dass der Geldzahlung ein „Zahlen mit Daten" gleichsteht, und für eine Ergänzung von § 312 Abs. 1 BGB-E folgenden Formulierungsvorschlag gemacht hat: „Als entgeltlich gilt auch eine Leistung, bei der personenbezogene Daten des Verbrauchers erhoben, verarbeitet bzw. genutzt werden."[650]

Der Einschätzung des Gesetzgebers aus dem Jahr 2013 und der ihr folgenden Ansicht im Schrifttum – die veröffentlichte Rechtsprechung hat sich mit dieser Frage bislang nicht konkret auseinandergesetzt – liegt indes ein Verständnis der Verbraucherrechterichtlinie zugrunde, das zunehmend auf Kritik stößt. So vertritt *Faust*[651] mit Nachweisen zum aktuellen Schrifttum[652] den Standpunkt, dass das Erfordernis der Entgeltlichkeit in § 312 Abs. 1 BGB nicht mit der Verbraucherrechterichtlinie in Einklang stehe und deshalb gestrichen werden müsse. Die Verbraucherrechterichtlinie knüpfe in den Art. 6, 8 und 9 an das Vorliegen eines Fernabsatzvertrages an, für den die Begriffsbestimmung in Art. 2 Nr. 7 das Merkmal der Entgeltlichkeit nicht enthalte. Soweit der deutsche Gesetzgeber das Merkmal der Entgeltlichkeit aus den Definitionen von „Kaufvertrag" und „Dienstleistungsvertrag" in Art. 2 Nr. 5, 6 der Richtlinie abgeleitet habe, sei nicht berücksichtigt worden, dass die Regelungen der Verbraucherrechterichtlinie über Informationspflichten und Widerrufsrechte nicht nur für diese Vertragsarten gelten.

Soweit *Faust* daraus folgert, dass eine richtlinienkonforme Auslegung der Vorschrift geboten sei, die auch ein „Bezahlen mit Daten" erfasse, beruht dies letztlich auf der Erwägung, dass die Form eines Entgelts keine Rolle spielen kann,

---

[650] Protokoll der 126. Sitzung des BT-Rechtsausschusses vom 17.4.2013 zur BT-Drs. 17/12637, S. 4 f.

[651] *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag 2016, S. 12 f.

[652] *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag 2016, Fn. 37.

wenn es nach der zugrundeliegenden Richtlinie eines Entgelts überhaupt nicht bedarf. Dann allerdings ist § 312 Abs. 1 BGB zu der Frage, was unter Entgelt zu verstehen ist, auch nicht mehr ergiebig.

Ob die im Vordringen befindliche, von *Faust* vertretene Position Zustimmung verdient, braucht für die hier untersuchte Frage, ob eine gesetzliche Klarstellung sachgerecht ist, aber letztlich nicht entschieden werden.

Zum einen finden die §§ 312 bis 312h BGB in der *Praxis* bei Austauschverhältnissen, in denen die Leistung des Unternehmers als „kostenlos" deklariert wird und der Verbraucher mit Daten „bezahlt", augenscheinlich keine Rolle. So müsste ein Unternehmer nach § 312f Abs. 3 BGB gegenüber dem Verbraucher auch bei der „kostenlosen" Bereitstellung digitaler Inhalte gegen Daten in einer Vertragsbestätigung Angaben zum Widerrufsrecht des Verbrauchers machen. Soweit ersichtlich, wird so in der Praxis aber nicht verfahren.

Zum anderen regelt § 312 BGB – mit dem Ziel eines hohen Verbraucherschutzniveaus – seinem Inhalt nach lediglich den Anwendungsbereich der §§ 312 bis 312h BGB, die sich zu Grundsätzen und *Informationspflichten* sowie zum *Widerrufsrecht* bei *Verbraucherverträgen* verhalten, die unter näher bestimmten Voraussetzungen geschlossen werden. Es handelt sich also um eine auf einen bestimmten Sachbereich bezogene Regelung, die rechtsmethodisch nach dem Grundsatz *lex specialis derogat legi generali* (nur) für diesen Sachbereich den allgemeinen zivilrechtlichen Regelungen vorgeht. Dass Verträge, bei denen der Nutzer mit Daten „bezahlt", ihrem Wesen nach außerhalb des Regelungsbereichs der §§ 312 bis 312h BGB den Regelungen über *synallagmatische Verträge* unterliegen sollen, lässt sich daraus nicht – jedenfalls nicht ohne Weiteres – herleiten.

Eine vertragsrechtliche Gleichstellung von Geld und Daten als Gegenleistung wird auch auf EU-Ebene nicht als geltendes, durch die Verbraucherrechterichtlinie geregeltes Recht angesehen. So heißt es in der Begründung des Richtlinienvorschlags COM(2015) 634 final (S. 2):

> *„In die Vorschläge wurden überdies mehrere Abänderungen des Verordnungsvorschlags für ein Gemeinsames Europäisches Kaufrecht aufgenommen, die das Europäische Parlament in erster Lesung verabschiedet hat: einerseits … andererseits die Ausweitung des Anwendungsbereichs auf bestimmte digitale Inhalte, die gegen eine andere Gegenleistung als Geld bereitgestellt werden."*

In Art. 3 des Richtlinienvorschlags COM(2015) 634 final wird mit Bezug auf den Anwendungsbereich die Geldzahlung dem „Bezahlen mit Daten" ausdrücklich gleichgestellt:

> *„… Verbraucher als Gegenleistung einen Preis zahlt oder aktiv eine andere Gegenleistung als Geld in Form personenbezogener oder anderer Daten erbringt."*

Die Art. 13, 16 und 22 des Richtlinienvorschlags enthalten spezielle Regelungen für „Daten als Entgelt". In einer Information des *European Parliamentary*

Research Service von April 2016[653] wird es als *Neuerung* des Richtlinienvorschlags bezeichnet, dass auch Verträge geregelt werden, bei denen die *Gegenleistung* des Verbrauchers in der *Hingabe von Daten* besteht.

Unter Abwägung aller vorstehenden Gesichtspunkte empfiehlt es sich jedenfalls *zu erwägen*, ob es mit Blick auf die nach geltendem Recht bestehenden dogmatischen Unsicherheiten bei der Einordnung des Phänomens „Bezahlen mit Daten" sachgerecht ist, gesetzlich *klarzustellen*, dass die Erteilung einer datenschutzrechtlichen Einwilligung zur wirtschaftlichen Verwertung personenbezogener Daten wie Geld eine vertragliche Gegenleistung und damit Gegenstand einer vertraglichen Hauptleistungspflicht im Synallagma sein kann.

Wird entsprechend den oben genannten Erwägungen kein Vertragstyp geschaffen, zu dessen prägenden Leistungen die „kostenlose" Bereitstellung eines sozialen Netzwerks gehört, kommt nach der Systematik des Bürgerlichen Gesetzbuchs als *Regelungsort* für die Erteilung der datenschutzrechtlichen Einwilligung als schuldrechtliche Hauptleistungspflicht vorrangig das *allgemeine Schuldrecht* in Betracht. Insoweit verhält es sich nicht anders als bei einer Geldzahlung als Entgelt. Das allgemeine Schuldrecht hält für sie verschiedene Regelungen bereit (§§ 244, 245, 270 BGB). Die Geldzahlung als Entgelt bzw. Gegenleistung prägt jedoch keinen im besonderen Schuldrecht geregelten Vertragstypus.

b. Verarbeitung personenbezogener Daten für eigene Zwecke als Leistung

Zur Gewährleistung von Rechtssicherheit in Fällen missbräuchlicher Vertragsgestaltungen durch Anbieter „kostenloser" sozialer Netzwerke ließe sich eine gesetzliche Klarstellung vertreten, dass die Verarbeitung personenbezogener Daten für kommerzielle Zwecke einer Vertragspartei – vor allem zu Werbezwecken – unabhängig von der vertraglichen Leistungsbeschreibung keine vertragliche Leistung gegenüber der anderen Vertragspartei darstellt. Letztlich erscheint eine solche Klarstellung jedoch als verzichtbar. Im Ergebnis kann es keinem Zweifel unterliegen, dass die Verarbeitung personenbezogener Daten eines Nutzers durch einen Anbieter in dessen – des Anbieters – eigenem kommerziellem Interesse keine Leistung gegenüber dem Nutzer darstellt.

c. Gefahrtragung, Gewährleistung und Haftung

In diametralem Gegensatz zur Verbreitung sowie gesellschaftlichen und ökonomischen Bedeutung von sozialen Netzwerken steht das Fehlen (veröffentlichter) Rechtsprechung sowie einer eingehenderen Diskussion im rechtswissenschaftlichen Schrifttum zu Fragen der Gefahrtragung, Gewährleistung und Haftung im Zusammenhang mit Verträgen über die Nutzung sozialer Netzwerke.

Solchen Fragen kann praktisch durchaus erhebliche Bedeutung zukommen. So mag es für einen Nutzer zu weitreichenden Beeinträchtigungen kommen, wenn

---

[653] Briefing EU Legislation in Progress April 2016, abrufbar unter: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/581980/EPRS_BRI%282016%29581980_EN.pdf (letzter Abruf: 14.3.2017).

eine Mitteilung im sozialen Netzwerk, die nur an einen eng begrenzten Adressatenkreis („Freunde“) gerichtet ist, aufgrund einer Fehlfunktion der Allgemeinheit zugänglich gemacht wird. Sieht man in der ordnungsgemäßen Funktion der Einstellungen zur Privatsphäre eine Kardinalpflicht des Anbieters oder nimmt der Anbieter für die Funktionsfähigkeit der Einstellungen besonderes Vertrauen in Anspruch, dürfte ein Haftungsausschluss auch für fahrlässige Pflichtverletzungen in den Nutzungsbedingungen einer Inhaltskontrolle nach § 307 Abs. 2 Nr. 2 BGB kaum standhalten.[654]

Soweit Fragen der Gefahrtragung, Gewährleistung und Haftung im Schrifttum vereinzelt thematisiert werden, wird eine Anwendbarkeit des allgemeinen Leistungsstörungsrechts (§§ 280 ff. BGB) angenommen.[655]

Ordnet man den Nutzungsvertrag einem oder mehreren im Bürgerlichen Gesetzbuch geregelten Vertragstypen zu, können sich, soweit nicht etwas anderes wirksam vereinbart ist, Primär- und Sekundäransprüche aus den für diese Vertragstypen einschlägigen Regelungen ergeben.

Allerdings schließen die Betreiber sozialer Netzwerke Sekundäransprüche, v. a. Haftungsansprüche, typischerweise in weitem Umfang aus. Die Zulässigkeit solcher Ausschlüsse ist insbesondere an § 307 Abs. 2 Nr. 2 und § 309 Nr. 7, 8 BGB zu messen. Der Frage der Natur des Vertrags kann dann maßgebende Bedeutung zukommen.

Im Kontext der Thematik des „Bezahlens mit Daten“ verdient die Frage besondere Aufmerksamkeit, ob es gerechtfertigt ist, bei Anbietern kostenpflichtiger und Anbietern „kostenloser“ sozialer Netzwerke einen unterschiedlichen Haftungsmaßstab anzulegen. Angesichts des Umstandes, dass es sich beim Vertrag über die „kostenlose“ Nutzung eines sozialen Netzwerks um einen synallagmatischen Vertrag handelt, bei dem der Nutzer eine Gegenleistung erbringt, die im Durchschnitt einen erheblichen wirtschaftlichen Wert hat, erscheint dies nicht gerechtfertigt.

Es könnte deshalb interessengerecht sein, gesetzlich klarzustellen, dass es nicht zu Lasten des Nutzers zu werten ist, wenn die von ihm zu erbringende Gegenleistung nicht in einer Geldzahlung, sondern in seiner Einwilligung in die Nutzung personenbezogener Daten besteht.

---

[654] Zur Bedeutung von Kardinalpflichten und zur Inanspruchnahme besonderen Vertrauens bei § 307 Abs. 2 Nr. 2 BGB vgl. Palandt/*Grüneberg*, BGB, § 307 Rn. 48, 50.

[655] *Bräutigam/Sonnleithner*, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 25, auch zur Frage von Haftungserleichterungen.

IV. Empfehlungen

Die Möglichkeiten des zivilrechtlichen Widerrufs und der Beendigung eines Vertrags, der ein „Bezahlen mit Daten“ vorsieht, erfordern keine grundlegenden Rechtsänderungen.

Mit Blick auf § 357 Abs. 9 BGB, mit welchem Art. 14 Abs. 4 lit. b. der Verbraucherrechterichtlinie umgesetzt worden ist, sollte erwogen werden, für Widerrufsfälle ausdrücklich zu regeln, dass (auch) den Anbieter keine Wertersatzpflicht trifft.

Es könnte sich empfehlen und sollte deshalb erwogen werden, im allgemeinen Schuldrecht allgemein klarzustellen, dass ein Entgelt auch in der Erteilung einer Einwilligung in die Verarbeitung personenbezogener Daten für kommerzielle Zwecke des Vertragspartners bestehen kann.

Mit Blick auf das Erfordernis der Freiwilligkeit einer datenschutzrechtlichen Einwilligung sollte bestimmt werden, dass ein zivilrechtlicher Anspruch auf Erteilung einer solchen Einwilligung nicht klagbar ist und dass aus der Nichterfüllung eines auf Erteilung einer datenschutzrechtlichen Einwilligung gerichteten Anspruchs keine anderweitigen Ansprüche hergeleitet werden können.

Zum Schutz von Verbrauchern empfiehlt sich für das „Bezahlen mit Daten“ eine „Button-Lösung“. Mit einer entsprechenden Ergänzung von § 312j Abs. 3 BGB sollte eine Ergänzung von § 312a Abs. 3 BGB einhergehen. Des Weiteren sollte eine Ergänzung von § 312j Abs. 4 BGB in dem Sinne erwogen werden, dass ein Verstoß gegen den neu gefassten § 312j Abs. 3 BGB, soweit er einen Fall des „Bezahlens mit Daten“ betrifft, nicht das Zustandekommen des Vertrags hindert, sondern lediglich zur Folge hat, dass der Verbraucher an den Vertrag nicht gebunden ist.

Es sollte in Betracht gezogen werden, gesetzlich zu bestimmen, dass es nicht zu Lasten einer Vertragspartei zu werten ist, wenn die von ihr zu erbringende Gegenleistung nicht in einer Geldzahlung, sondern in ihrer Einwilligung in die Nutzung personenbezogener Daten besteht.

H. Erwerb digitaler Inhalte im Wege des Downloads

I. Untersuchungsgegenstand: Erwerb digitaler Inhalte zum rezeptiven Werkgenuss im Wege des Downloads

Im Zuge der fortschreitenden Digitalisierung findet ein Austausch von Inhalten zunehmend in digitaler Form über das Internet statt. Das gilt auch für Inhalte zum rezeptiven Werkgenuss, an denen ein Rechteinhaber einem Erwerber ähnlich wie bei analogen Erwerbssachverhalten gegen Entgelt dauerhaft Rechte einräumt. Hat der Erwerber bei solchen Verträgen eine finanzielle Gegenleistung zu erbringen, besteht die Leistung des Rechteinhabers in der Regel darin, dass er dem Erwerber die Möglichkeit zur dauerhaften berechtigten Nutzung der Inhalte in bestimmten Formen verschafft.

Technisch wird der Erwerb dabei in weitem Umfang im Wege des *Downloads* vollzogen. Dem Erwerber wird kein körperlicher Datenträger (z. B. CD, DVD, Blu-ray Disk) überlassen, sondern er empfängt die vertragsgegenständlichen Inhalte von einem Server über das Internet als digitale Datei. Von dieser Datei wird beim Download auf Rechenressourcen, die dem Erwerber zur Verfügung stehen, eine digitale Kopie hergestellt.

Alternativ kann ein Rechteinhaber ein dauerhaftes Nutzungsrecht an digitalen Inhalten in der Form einräumen, dass er einem Nutzer die Möglichkeit gibt, die Inhalte ohne zeitliche Begrenzung beliebig oft über einen Online-Zugang[656] bzw. im Wege des *Streaming* zu konsumieren. Verträgen über Streaming-Leistungen wird an anderer Stelle näher nachgegangen.[657]

Im vorliegenden Zusammenhang soll unter „Erwerb digitaler Inhalte“ nur ein Erwerb verstanden werden, der technisch in der Form eines *Downloads* erfolgt und bei welchem dem Nutzer die erworbenen Inhalte auf ihm zur Verfügung stehenden Rechenressourcen sowie – anders als bei einem Online-Zugang – ohne fortgesetzten Kontakt zum Anbieter der Inhalte für einen zeitlich und quantitativ unbegrenzten Konsum zur Verfügung stehen.

Der Begriff „digitale Inhalte“ bezieht sich dabei im vorliegenden Kontext nur auf Inhalte zum *rezeptiven Werkgenuss*. Die nachfolgenden Betrachtungen erstrecken sich mithin *nicht* auf sonstige digitale Inhalte, zu denen nach der Legaldefinition in § 312f Abs. 3 S. 1 BGB sämtliche „nicht auf einem körperlichen Datenträger befindlichen Daten, die in digitaler Form hergestellt und bereitgestellt werden“,

---

[656] Vgl. zu einer solchen Konstellation OLG Köln, Urt. v. 26.2.2016 – 6 U 90/15, CR 2016, 458 ff.

[657] Siehe dazu Kapitel 2 Abschnitt E.

und damit auch *Computerprogramme* gehören.[658] Computerprogramme[659] unterscheiden sich von digitalen Inhalten zum rezeptiven Werkgenuss dadurch, dass sie dem Betrieb eines Computers dienen.[660] Für digitale Inhalte zum rezeptiven Werkgenuss ist der Computer demgegenüber nur ein Mittel, die Inhalte wiederzugeben, also sicht- bzw. hörbar zu machen. Computerprogramme unterliegen nicht nur besonderen urheberrechtlichen Regelungen[661], sondern werfen auch zivilrechtlich eigenständig zu beurteilende Fragen auf. So ist z. B. umstritten, ob es eine generelle Pflicht von Softwareanbietern geben sollte, stets die aktuelle Version einer Software zu liefern[662], ob (bzw. inwieweit) Anbieter zur Lieferung von Softwareupdates verpflichtet sind[663] sowie ob und mit welchen Folgen das Vertragsverhältnis aufgrund einer Verpflichtung zur Lieferung von Updates den Charakter eines Dauerschuldverhältnisses annimmt. Des Weiteren ist streitig, ob es für Verträge über Software besonderer Beweislastregelungen bedarf.[664]

Mit Blick darauf, dass der Erwerb digitaler Inhalte in der Praxis vor allem durch Verbraucher erfolgt, sollen sich die nachfolgenden Ausführungen auf Verbraucherverträge beschränken.

II. Gesellschaftliche und ökonomische Relevanz

Exemplarisch für den Handel mit digitalen Inhalten ist der Markt für *E-Books*, d. h. für Bücher in elektronischer Form. Dieser Markt ist – ebenso wie der Markt für E-Reader als speziellen Geräten zum komfortablen Lesen von E-Books – in den zurückliegenden Jahren stark gewachsen. Der mit Büchern (einschließlich Hörbüchern) in Deutschland 2015 erzielte, gegenüber den vorangehenden Jahren leicht gefallene Gesamtumsatz wird in der Branche mit 9,188 Mrd. EUR beziffert.

---

[658] Siehe RegE eines Gesetzes zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung, BT-Drs. 17/12637 vom 6.3.2013, S. 55, zu § 312f Abs. 3 BGB-E: „Absatz 3 enthält in Umsetzung von Artikel 2 Nummer 11 der Richtlinie eine Legaldefinition der digitalen Inhalte. Hierunter fallen Daten, die in digitaler Form hergestellt und bereitgestellt werden, wie etwa Computerprogramme, Anwendungen (Apps), Spiele, Musik, Videos oder Texte."

[659] Dazu zählen auch sog. *native Apps*, die vor allem auf Tablet-Computern und Smartphones, aber auch auf sog. „Wearables" und PCs zum Einsatz kommen. Vgl. dazu – und zur Abgrenzung von im Browser ausgeführten sog. „Web-Apps" – *Baumgartner/Ewald*, Apps und Recht, S. 1.

[660] Vgl. die Definition von *Software* nach ISO/IEC 26514 („program or set of programs used to run a computer"). Siehe zu dieser Begriffsbestimmung und weiteren Definitionen die Nachweise unter www.iso.org (letzter Abruf: 1.3.2017).

[661] Für Computerprogramme enthält die Computerprogramm-Richtlinie (RL 2009/24/EG vom 23. April 2009 über den Rechtsschutz von Computerprogrammen) ein eigenes urheberrechtliches Regime.

[662] Von der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016 abgelehnt mit Beschluss Ziffer 18 lit. a.

[663] Von der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016 abgelehnt mit Beschluss Ziffer 18 lit. b.

[664] Dafür hat sich mit knapper Mehrheit (bei geringer Beteiligung an der Abstimmung) die Abteilung Zivilrecht des 71. Deutschen Juristentags 2016 mit Beschluss Ziffer 20 ausgesprochen.

Nach von der Buchbranche erhobenen Zahlen hat dabei der Umsatz mit E-Books für den privaten Bedarf in Deutschland in den letzten Jahren stetig zugenommen. Im Anschluss an eine Verdreifachung im Jahr 2012 stieg er 2013 um 60,5 %, 2014 um 7,6 % und 2015 um 4,7 %. Im Jahr 2015 trugen E-Books 4,5 % zu dem Umsatz von Büchern (einschließlich Hörbüchern) für den privaten Bedarf bei. Nach Stückzahlen wuchs der Privatkundenmarkt für E-Books – nach einem Wachstum von ca. 15 % im Jahr 2014 – im Jahr 2015 mit 27 Mio. Erwerbsvorgängen um etwa 9 %.[665] Nach einer Untersuchung des Digitalverbandes Bitkom[666] liest in Deutschland etwa jeder Vierte zumindest hin und wieder E-Books. Der Bezug von E-Books erfolgt dabei zu 86 % im Wege des Erwerbs von Einzeltiteln.

Auch der Markt für *Musik* und *Filme bzw. Videos* ist stark durch Vertriebsformen geprägt, bei denen dem Verbraucher der zeitlich und quantitativ unbegrenzte Werkgenuss über einen Download ermöglicht wird.

Nach in der Branche erhobenen Zahlen wurde mit dem Verkauf von *Musik* in Deutschland im Jahr 2015 – über alle Formate hinweg – ein Umsatz von 1,546 Mrd. EUR erzielt. Das Geschäft mit datenträgerlosen digitalen Angeboten machte dabei 31,4 % aus, wobei (neben sonstigen Formen mit einem Anteil von 1,4 %) 15,6 % auf Downloads und 14,4 % auf Streaming entfielen. Während der Umsatz bei Streaming-Diensten um 105,8 % stieg, ging er bei Download-Diensten allerdings um 2,6 % zurück. Nach einer Prognose des Marktforschungsunternehmens GfK soll die Bedeutung des Streamings weiterhin stark wachsen, die von Downloads dagegen weiter abnehmen.[667]

Einer Studie im Auftrag der Filmförderungsanstalt[668] zufolge wurde im Jahr 2014 mit dem Verkauf von *Filmen bzw. Videos* für den individuellen Konsum (Home Video-Markt) ein Gesamtumsatz von 1,370 Mrd. EUR erzielt. Dabei entfielen rund 95 % der Umsätze auf Verkäufe von Datenträgern (DVD und Blu-ray) und etwa 5 % auf den datenträgerlosen Vertrieb digitaler Produkte. Den Markt für Filme bzw. Videos, deren Inhalt über das Internet übermittelt wird, prägen dabei

---

[665] Vgl. zum Ganzen: Frankfurter Buchmesse (Quelle: Börsenverein des Deutschen Buchhandels e. V. 2016), Buch und Buchhandel in Zahlen 2016 (für 2015), abrufbar unter http://www.buchmesse.de/images/fbm/dokumente-ua-pdfs/2016/buchmarkt_deutschland_2016_dt.pdf_58507.pdf, sowie Börsenverein des Deutschen Buchhandels, Der Buchmarkt in Deutschland, 2016, abrufbar unter http://www.boersenverein.de/de/182716 (letzter Abruf jeweils: 1.3.2017).

[666] Bitkom, Die Nutzung von E-Books, Okt. 2016, abrufbar unter https://www.bitkom.org/Presse/Pressegrafik/2016/Oktober/Bitkom-PK-Charts-E-Books-Studie-11-10-2016-final.pdf (letzter Abruf: 1.3.2017).

[667] Vgl. zum Ganzen Bundesverband Musikindustrie, Musikindustrie in Zahlen 2015, S. 9 ff., abrufbar unter http://www.musikindustrie.de/fileadmin/bvmi/upload/06_Publikationen/MiZ_Jahrbuch/bvmi-2015-jahrbuch-musikindustrie-in-zahlen-epaper.pdf (letzter Abruf: 1.3.2017).

[668] GfK im Auftrag der FFA, Der Videomarkt im Jahr 2014, abrufbar unter http://www.bvv-medien.org/fileadmin/user_upload/businessreports/JWB2014.pdf (letzter Abruf: 1.3.2017).

zunehmend Verträge über die zeitlich begrenzte Einräumung von Nutzungsrechten.

Den Rechtsfragen, welche der Erwerb digitaler Inhalte aufwirft, soll im Folgenden – vornehmlich am Beispiel des Erwerbs eines *E-Books* – näher nachgegangen werden.

Ansatzpunkt ist dabei das geltende deutsche Recht. Der Vorschlag der Europäischen Kommission für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte[669] (im Folgenden: RL-Vorschlag COM(2015) 634 final) wird nur behandelt, soweit er spezifisch auf den Erwerb digitaler Inhalte im Wege des Downloads bezogene Rechtsänderungen vorsieht oder konkrete Lösungsansätze zu einem für das deutsche Recht identifizierten Regelungsbedarf enthält.

Soweit das geltende Recht für den Erwerb digitaler Inhalte im Wege des Downloads sach- und interessengerechte Lösungen bereithält, soll hier nicht die grundlegende Frage thematisiert werden, ob Unterschiede in den geltenden Bestimmungen mit Bezug auf den datenträgerlosen und den datenträgergebundenen Erwerb digitaler Inhalte generell gerechtfertigt sind. Betont man den Aspekt der Medienneutralität, wird man diese Frage allerdings verneinen müssen.[670]

III. Bürgerlich-rechtliche Sonderregelungen für Verträge über digitale Inhalte

Das geltende Zivilrecht enthält *keine Regelungen*, die sich *ausschließlich* auf Verträge über den *Erwerb digitaler Inhalte im Wege des Downloads* beziehen.

Auf der Grundlage der Verbraucherrechterichtlinie[671] (VRRL) finden sich im Bürgerlichen Gesetzbuch aber Bestimmungen, die allgemein für *Verträge über digitale Inhalte* und damit auch für den Unterfall des datenträgerlosen Erwerbs digitaler Inhalte über das Internet gelten.

1. Legaldefinition des Begriffs „digitale Inhalte“

a. Geltende Rechtslage

Für den Begriff „digitale Inhalte“ findet sich im Kontext der Regelungen für Verbraucherverträge in § 312f Abs. 3 BGB eine die Begriffsbestimmung in Art. 2 Nr. 11 der VRRL umsetzende Legaldefinition. Digitale Inhalte sind danach *Daten, die in digitaler Form hergestellt und bereitgestellt* werden.

---

[669] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte vom 9. Dezember 2015 – COM(2015) 634 final/2015/0287 (COD).

[670] Vgl. etwa *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 2.; zu den Bestrebungen auf europäischer Ebene, das Recht medienneutral auszugestalten, siehe unten unter III. 1. b.

[671] RL 2011/83/EU vom 25. Oktober 2011

Entsprechend Erwägungsgrund 19 der VRRL, der bei der Auslegung von § 312f Abs. 3 BGB zu berücksichtigen ist, erfordert dies, dass die Bereitstellung der Inhalte *nicht auf einem körperlichen Datenträger* erfolgt.[672] Erwägungsgrund 19 der VRRL enthält dazu im dritten Satz eine eindeutige Aussage: „Werden digitale Inhalte auf einem körperlichen Datenträger wie einer CD oder einer DVD bereitgestellt, sollten diese als *Waren* (*Hervorhebung d. d. Verf.*) im Sinne dieser Richtlinie betrachtet werden". Diese Aussage im zugrundeliegenden europäischen Rechtsakt ist für das die VRRL umsetzende nationale Recht maßgeblich. Dass der deutsche Gesetzgeber mit der Definition in § 312f Abs. 3 BGB dementsprechend nur die datenträgerlose Bereitstellung digitaler Inhalte erfassen wollte, ergibt sich aus den Gesetzgebungsmaterialien. In dem der Regelung in § 312f Abs. 3 BGB zugrundeliegenden Regierungsentwurf[673] werden nur Arten des Bezugs der digitalen Inhalte über das Internet genannt: „Ob die Dateien heruntergeladen, gespeichert und hiernach sichtbar gemacht werden oder während des Herunterladens in Echtzeit sichtbar gemacht werden (Streaming), ist dabei unerheblich."

Erwägungsgrund 19 der VRRL nennt als Beispiele für digitale Inhalte u. a. Texte, Musik und Videos. Der Erwerb eines E-Books stellt damit einen klassischen Fall des Erwerbs digitaler Inhalte dar.

b. Änderungsbestrebungen auf europäischer Ebene

Gegenüber der Definition in Art. 2 Nr. 11 der VRRL baut der RL-Vorschlag COM(2015) 634 final auf einer im Entwurf eines Art. 2 Nr. 1 breiter gefassten Bestimmung des Begriffs „digitale Inhalte" auf. Soweit der vorgeschlagene Art. 2 Nr. 1 lit. a als „digitale Inhalte" Daten bezeichnet, „die in digitaler Form hergestellt und bereitgestellt werden", entspricht dies dem Wortlaut nach zwar Art. 2 Nr. 11 VRRL. Im Richtlinienvorschlag ist aber an anderer Stelle geregelt, dass die Begriffsbestimmung in Art. 2 Nr. 1 lit. a weiter zu verstehen ist. So soll sich nach dem Entwurf eines Art. 20 Nr. 1 die Verbrauchsgüterkaufrichtlinie[674] (VerbrGKRL) nach näheren Maßgaben nicht mehr auf dauerhafte Datenträger mit digitalen Inhalten beziehen. Dementsprechend ist vorgesehen, dass die Richtlinie nach dem Entwurf eines Art. 3 Nr. 1, 3 grundsätzlich auch für entgeltliche Verträge über dauerhafte Datenträger, die ausschließlich der Übermittlung digitaler Inhalte dienen, gilt. Im Entwurf eines Erwägungsgrundes 11 heißt es, dass „diese Richtlinie unabhängig von der Art des für die Datenübermittlung verwendeten Datenträgers für alle digitalen Inhalte gelten" soll.

---

[672] Anders *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 1.

[673] RegE eines Gesetzes zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung, BT-Drs. 17/12637 vom 6.3.2013, S. 55.

[674] RL 1999/44/EG vom 25. Mai 1999.

Die so angestrebte Medienneutralität stellt den datenträgergebundenen Erwerb digitaler Inhalte, der bislang als Sachkauf behandelt wird, dem datenträgerlosen Erwerb gleich. Zur Herstellung der Medienneutralität wird der rechtliche Ansatz für den datenträgergebundenen Erwerb digitaler Inhalte, nicht hingegen für den Erwerb im Wege des Downloads, grundlegend geändert. Für den hier untersuchten Erwerb digitaler Inhalte im Wege des *Downloads* ist der vorstehende Paradigmenwechsel durch den RL-Vorschlag COM(2015) 634 final also nicht von Bedeutung.

2. Sonderregelungen für Verbraucherverträge über digitale Inhalte

Bedeutung hat der Begriff „digitale Inhalte“ im geltenden Bürgerlichen Gesetzbuch zum einen für das *Widerrufsrecht*, zum anderen für *Informationspflichten* des Unternehmers gegenüber einem Verbraucher. Die geltenden bürgerlich-rechtlichen Regelungen zu digitalen Inhalten beschränken sich mithin auf *Verbraucherverträge*.

a. Widerrufsrecht bei Verträgen über digitale Inhalte

(1) Geltende Rechtslage

Nach § 312g Abs. 1 BGB steht dem Verbraucher bei Abschluss eines Fernabsatzvertrags ein Widerrufsrecht gemäß § 355 BGB zu. In der Praxis werden Verbraucherverträge über die datenträgerlose Lieferung digitaler Inhalte ausschließlich über das Internet abgeschlossen und stellen damit Fernabsatzverträge i. S. v. § 312c BGB (sowie Verträge im elektronischen Geschäftsverkehr nach § 312i Abs. 1 BGB) dar.

Für solche Verträge bestimmt § 356 Abs. 2 Nr. 2 BGB, dass die Widerrufsfrist mit Vertragsschluss beginnt. Verträge über digitale Inhalte werden insoweit Verträgen über die Lieferung von (nicht volumenmäßig begrenztem) Wasser, Gas, Strom und Fernwärme gleichgestellt. Mit der Abgrenzung zu den in § 356 Abs. 2 Nr. 1 BGB geregelten Fällen eines Verbrauchsgüterkaufs vollzieht § 356 Abs. 2 Nr. 2 BGB nach, dass es sich bei (nicht volumenmäßig begrenztem) Wasser, Gas und Strom nach Art. 1 Abs. 2 lit. b der VerbrGKRL nicht um „Verbrauchsgüter“ handelt. In Erwägungsgrund 19 der VRRL heißt es vor diesem Hintergrund, dass Verträge über digitale Inhalte wie Verträge über die vorgenannten Gegenstände „für die Zwecke dieser Richtlinie weder als Kaufverträge noch als Dienstleistungsverträge betrachtet werden“ sollen.

Unter den Voraussetzungen des § 356 Abs. 5 BGB erlischt das Widerrufsrecht bei einem Vertrag über die datenträgerlose Lieferung digitaler Inhalte vorzeitig. Ein solches vorzeitiges Erlöschen des Widerrufsrechts erfordert zum einen, dass der Unternehmer mit der *Ausführung* des Vertrags *begonnen* hat, *nachdem* der *Verbraucher* ausdrücklich *zugestimmt* hat, dass dies vor Ablauf der Widerrufsfrist geschieht. Praktisch kann der Unternehmer die Zustimmung des Verbrauchers dadurch einholen, dass er eine Schaltfläche bereitstellt, durch deren Anklicken der Verbraucher seine Zustimmung erklären muss. Zum anderen muss der Verbraucher seine Kenntnis davon bestätigt haben, dass er durch diese Zustimmung sein

Widerrufsrecht mit Beginn der Ausführung des Vertrags verliert. Auch diese Bestätigung kann der Unternehmer über die genannte Schaltfläche einholen.[675]

Den Beginn der Vertragsausführung seitens des Unternehmers wird man beim Erwerb digitaler Inhalte über das Internet im *Beginn des Downloads* zu sehen haben.[676]

Mit § 356 Abs. 5 BGB korrespondiert die Regelung in § 312f Abs. 3 BGB, nach welcher der Unternehmer die entsprechenden Erklärungen des Verbrauchers in einer Vertragsbestätigung nach § 312f Abs. 2 BGB festzuhalten und dem Verbraucher auf einem dauerhaften Datenträger zur Verfügung zu stellen hat.[677] Kommt der Unternehmer dieser Pflicht nicht nach, muss er eine später von ihm behauptete Zustimmung des Verbrauchers zur vorzeitigen Ausführung in Kenntnis des Erlöschens seines Widerrufsrechts beweisen.[678]

Übt der Verbraucher ein ihm trotz Erfüllung durch den Unternehmer noch zustehendes Widerrufsrecht aus, hat er nach § 357 Abs. 9 BGB im Rahmen des Rückgewährschuldverhältnisses auch dann keinen Wertersatz zu leisten, wenn er schon in den Genuss der digitalen Inhalte gekommen ist. Nach § 357 Abs. 1 BGB trifft ihn lediglich die Pflicht, die empfangenen digitalen Inhalte zurückzugewähren. Die Erfüllung einer solchen Rückgabepflicht durchzusetzen, wirft indes erhebliche praktische Schwierigkeiten auf. Weil der Verbraucher über den Download eine elektronische Kopie auf ihm zur Verfügung stehenden Rechenressourcen hergestellt hat, ist seine Rückgewährpflicht nur dann erfüllt, wenn er diese Kopie (und ggf. davon gefertigte weitere Kopien) von seinen Rechenressourcen gelöscht hat. Art. 13 Nr. 2 lit. d des RL-Vorschlags COM(2015) 634 final sieht folgerichtig für den Fall der Vertragsbeendigung vor, dass der Verbraucher die Nutzung heruntergeladener digitaler Inhalte insbesondere durch deren Löschung zu unterlassen hat. Die Löschung wird für den Unternehmer in der Praxis allerdings häufig nicht überprüfbar sein[679]. Er kann diesen Schwierigkeiten indes ohne Weiteres dadurch entgehen, dass er nach Maßgabe von § 356 Abs. 5 BGB die Zustimmung des Verbrauchers dafür einholt, vor Ablauf der Widerrufsfrist mit

---

[675] Vgl. *Graef*, Recht der E-Books und des Electronic Publishing, Rn. 158.
[676] Vgl. *Graef*, Recht der E-Books und des Electronic Publishing, Rn. 158.
[677] Ein „dauerhafter Datenträger" ist nach § 126b S. 2 BGB jedes Medium, das es dessen Empfänger ermöglicht, die auf dem Datenträger enthaltenen Erklärungen so zu speichern, dass sie ihm für einen angemessenen Zeitraum zugänglich sind und unverändert wiedergegeben werden können. Das ist bei einer Datei der Fall, wenn sie – wie beim PDF-Dateiformat – mit einem über das Internet kostenfrei herunterzuladenden Leseprogramm geöffnet werden kann und der Unternehmer auf die Möglichkeit des Downloads hinweist (vgl. *Graef*, Recht der E-Books und des Electronic Publishing, Rn. 152). Die Begriffsbestimmung in Art. 2 Nr. 11 des RL-Vorschlags COM(2015) 634 final enthält insoweit keine Änderungen.
[678] Vgl. RegE eines Gesetzes zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung, BT-Drs. 17/12637 vom 6.3.2013, S. 56.
[679] So auch *Graef*, Recht der E-Books und des Electronic Publishing, Rn. 153; vgl. mit Bezug auf Rücktrittsfälle auch *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 7. b) aa) und 9. d) bb).

der Vertragsausführung zu beginnen, sich die Kenntnis des Verbrauchers von dem damit einhergehenden Verlust des Widerrufsrechts bestätigen lässt und beides gemäß § 312f Abs. 3 BGB dokumentiert.

Für den Widerruf von Verträgen über oder im Zusammenhang mit Finanzierungshilfen für den Erwerb digitaler Inhalte enthalten § 357a Abs. 2 S. 3 BGB und § 358 Abs. 4 BGB mit den Grundsätzen der vorgenannten Bestimmungen korrespondierende Sonderregelungen.

Betrachtet man den datenträgerlosen Erwerb digitaler Inhalte für sich, geben die geltenden Regelungen zum Widerrufsrecht *keinen Anlass für Änderungen*. Sie sind *ausgewogen und praxisgerecht*. Der Frage, ob Unterschiede in der Ausgestaltung und Intensität des verbraucherschützenden Widerrufsrechts mit Bezug auf den datenträgerlosen und den datenträgergebundenen Erwerb digitaler Inhalte grundsätzlich gerechtfertigt sind[680], muss vor diesem Hintergrund hier nicht nachgegangen werden.

(2) Diskutierte Änderungen

Der 71. Deutsche Juristentag 2016 fordert[681], dass die Widerrufsfrist bei digitalen Inhalten, die nicht auf einem körperlichen Datenträger zur Verfügung gestellt werden, erst zu laufen beginnen soll, wenn dem Verbraucher die Möglichkeit gegeben wurde, die digitalen Inhalte online zu *erproben.*[682]

In seinem Gutachten für den 71. Deutschen Juristentag hat *Faust*[683] ausgeführt, dass der Verbraucher in den Fällen des § 356 Abs. 5 BGB die „Katze im Sack" kaufen müsse. Der Sinn des Widerrufsrechts bei Fernabsatzgeschäften bestehe nach § 357 Abs. 7 Nr. 1 BGB aber gerade darin, dem Verbraucher eine Prüfung der erworbenen „Sache" zu ermöglichen. Abweichend von § 356 Abs. 2 Nr. 2 BGB solle die Widerrufsfrist deshalb nicht schon mit Vertragsschluss beginnen, sondern erst dann, wenn der Verbraucher die Möglichkeit gehabt habe, die digitalen Inhalte – z. B. durch Konsum kurzer Abschnitte – online zu erproben. Entsprechend solle § 356 Abs. 2 Nr. 2 BGB dahin geändert werden, dass die Widerrufsfrist beim datenträgerlosen Erwerb digitaler Inhalte erst beginnt, wenn der Verbraucher ausreichend Gelegenheit zur Erprobung der digitalen Inhalte gehabt habe, spätestens jedoch, wenn ihm die Inhalte endgültig zur Verfügung gestellt worden sind.

---

[680] Dazu kritisch *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 7. b).

[681] Beschluss Ziffer 13 der Beschlüsse der Abteilung Zivilrecht. Es sollte allerdings im Blick behalten werden, dass an der Abstimmung nur 34 Personen teilgenommen haben, von denen lediglich 22 für diesen Beschluss gestimmt haben.

[682] Für die Einführung eines Anspruchs auf eine „digitale Inhaltsprobe" spricht sich auch *Lomfeld*, Digitaler Schrott – Widerruf von digitalen Inhalten, ZRP 2016, 174 ff., aus.

[683] *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 7. b).

Im Ergebnis überzeugt dieser Vorschlag nicht. *Faust* spricht sich für eine *Beibehaltung* von § 312g Abs. 2 S. 1 Nr. 6 BGB aus, also für das Nichtbestehen eines Widerrufsrechts bei Verträgen zur Lieferung von Ton- und Videoaufnahmen in einer versiegelten Packung, wenn die Versiegelung nach der Lieferung entfernt wurde. Auch beim Online-Kauf datenträgergebundener digitaler Inhalte kauft der Verbraucher die „Katze im Sack". Selbst bei einem Erwerb im stationären Handel verhält es sich so. Anders als bei einem Kleidungsstück kann der Verbraucher vor dem Kauf eines Videos mit einem Spielfilm im Ladengeschäft im Regelfall nicht durch das Anschauen von Ausschnitten feststellen, ob der Film seinen Vorstellungen entspricht. Auch die Möglichkeit von Hörproben ist im stationären Handel keinesfalls bei jedem Händler üblich. Befürwortet man eine Medienneutralität, dürfte es ein Gebot dieses Grundsatzes sein, den Erwerber datenträgerloser Inhalte in Bezug auf das Widerrufsrecht nicht besser zu stellen als den Käufer eines Datenträgers.[684]

Einem generellen, für alle Vertriebsformen geltenden Recht von Verbrauchern auf Erprobung digitaler Inhalte vor deren Kauf lässt sich entgegenhalten, dass ein solches Recht auch beim Erwerb von Inhalten in analoger Form nicht besteht. Im stationären Buchhandel gibt es zwar eine verbreitete Übung, Kunden vor dem Kauf Gelegenheit zu geben, sie interessierende Bücher anzuschauen. Ein Rechtsanspruch darauf besteht jedoch nicht. Die Möglichkeit für Kunden, Druckwerke vor deren Erwerb durchzusehen, wird zudem – etwa im Verhältnis zwischen Buch- und Zeitschriftenhandel – durchaus unterschiedlich gehandhabt. In welchem Umfang potentielle Käufer Inhalte in analoger Form vor deren Kauf partiell konsumieren können, mag dabei durchaus ein Aspekt sein, dem Verbraucher bei der Wahl ihres Vertragspartners Gewicht beimessen. Es ist damit ein Faktor im Wettbewerb der Händler um Kunden. Auch bei datenträgerlosen digitalen Inhalten entspricht es einer verbreiteten Praxis großer Anbieter (z. B. *Apple/iTunes*, *Google Books*, *Thalia*, *Amazon/Kindle*), kostenlose Leseproben angebotener E-Books bereitzustellen. Dem Bedürfnis von Verbrauchern, digitale Inhalte vor dem Erwerb im Wege des Downloads zu erproben, wird in der Praxis also Rechnung getragen.

---

[684] *Lomfeld*, Digitaler Schrott – Widerruf von digitalen Inhalten, ZRP 2016, 174 ff., sieht einen wesentlichen Unterschied zwischen Büchern, CDs und DVDs einerseits und datenträgerlos vertriebenen digitalen Inhalten andererseits darin, dass nicht verkörperte digitale Inhalte im Anschluss an deren Erwerb vom Verbraucher nicht legal weiterübertragen werden können und der Kunde deshalb „auf dem Schrott endgültig sitzen" bleibe. Diese Sichtweise dürfte den tatsächlichen Marktgegebenheiten kaum Rechnung tragen. Ein Zweitmarkt für den Verkauf von Büchern und Datenträgern ohne Seltenheitswert, auf dem Verbraucher im Schnitt auch nur annähernd den ursprünglichen Kaufpreis erzielen können, ist nicht existent. Vor allem von *Lomfeld* als „Schrott" bezeichnete Inhalte dürften mit Blick auf die durch das Internet hergestellte Transparenz auch bei Verkörperung schwerlich gut weiter zu veräußern sein.

b. Informationspflichten bei Verträgen über digitale Inhalte

Bei einem Fernabsatzvertrag unterliegt der Unternehmer gemäß § 312d Abs. 1 S. 1 BGB Informationspflichten, deren Inhalt sich nach Art. 246a EGBGB bestimmt. Nach der – Art. 6 Abs. 5 der VRRL umsetzenden – Regelung in § 312d Abs. 1 S. 2 BGB werden vom Unternehmer in Erfüllung dieser Informationspflichten gemachte Angaben zum Vertragsinhalt, wenn nicht die Parteien ausdrücklich etwas anderes vereinbart haben.

Gemäß Art. 246a § 1 Abs. 3 Nr. 2 EGBGB hat der Unternehmer den Verbraucher, wenn § 356 Abs. 5 BGB einschlägig ist, über die Umstände zu informieren, unter denen der Verbraucher ein zunächst bestehendes Widerrufsrecht verliert.

Art. 246a § 1 Abs. 1 S. 1 Nr. 1 EGBGB verpflichtet den Unternehmer, dem Verbraucher unabhängig vom konkreten Gegenstand des Fernabsatzvertrags Informationen über die wesentlichen Eigenschaften der Waren oder Dienstleistungen in dem für das Kommunikationsmittel und für die Waren oder Dienstleistungen angemessenen Umfang zur Verfügung zu stellen.

Spezifische Informationspflichten mit Bezug auf Verträge über digitale Inhalte sind in Art. 246a § 1 Abs. 1 S. 1 Nr. 14, 15 EGBGB bestimmt.

Nach Art. 246a § 1 Abs. 1 S. 1 Nr. 14 EGBGB hat der Unternehmer dem Verbraucher Informationen über die *Funktionsweise* digitaler Inhalte einschließlich anwendbarer technischer Schutzmaßnahmen für solche Inhalte zur Verfügung zu stellen. Eine identische Informationspflicht findet sich für den Abschluss von Verbraucherverträgen im stationären Handel in Art. 246 Abs. 1 Nr. 7 EGBGB. Zur Funktionsweise digitaler Inhalte gehört nach Erwägungsgrund 19 der VRRL der Aspekt, wie die digitalen Inhalte verwendet werden können. Als Beispiel nennt der Erwägungsgrund die Möglichkeit, das Verhalten des Verbrauchers nachzuverfolgen. Exemplarisch für anwendbare technische Schutzmaßnahmen führt er das Vorhandensein oder Nichtvorhandensein von technischen Beschränkungen wie den Schutz mittels digitaler Rechteverwaltung (DRM) oder Regionalcodierung auf.

Zu den Informationspflichten des Unternehmers gehört nach Art. 246a § 1 Abs. 1 S. 1 Nr. 15 EGBGB des Weiteren die Verpflichtung, den Verbraucher „gegebenenfalls, soweit wesentlich“ über Beschränkungen der Interoperabilität und der Kompatibilität digitaler Inhalte mit Hard- und Software zu informieren, soweit dem Unternehmer solche Beschränkungen bekannt sind oder bekannt sein müssen. Die Regelung entspricht wörtlich dem für den stationären Handel geltenden Art. 246 Abs. 1 Nr. 8 EGBGB. Nach Erwägungsgrund 19 der VRRL sind mit Informationen über wesentliche Aspekte der Interoperabilität Informationen mit Bezug auf die standardmäßige Hard- und Softwareumgebung, mit der die digitalen Inhalte kompatibel sind, gemeint. Der Erwägungsgrund nennt beispielhaft das

Betriebssystem bzw. dessen Version und erforderliche Eigenschaften der Hardware. Die Einschränkung „gegebenenfalls, soweit wesentlich“ betrifft z. B. veraltete, kaum noch gebräuchliche Betriebssysteme.[685]

Ein schuldhafter Verstoß des Unternehmers kann im Vertragsverhältnis u. a. zur Folge haben, dass der Verbraucher nach § 280 Abs. 1 BGB, ggf. i. V. m. § 241 Abs. 2, § 311 Abs. 2 Nr. 1 BGB, einen Schadensersatzanspruch hat. Steht dem Verbraucher kein Widerrufsrecht mehr zu, kann er ggf. nach § 249 Abs. 1 BGB im Wege der Naturalrestitution eine Vertragsaufhebung verlangen.[686]

Ein Regelungsbedarf wird insoweit nicht thematisiert und ist auch nicht ersichtlich.

IV. Anwendbarkeit der allgemeinen Regelungen des bürgerlichen Rechts auf den Erwerb digitaler Inhalte

Das geltende bürgerliche Recht enthält über die vorgenannten Regelungen hinaus keine konkreten Bestimmungen zum Abschluss und Inhalt von Verträgen über den Erwerb digitaler Inhalte. Das Bürgerliche Gesetzbuch verhält sich weder zu der Frage, wie der Erwerb digitaler Inhalte vertragstypologisch einzuordnen ist, noch zu den wechselseitigen Rechten und Pflichten der Parteien eines entsprechenden Vertrags.

1. Vertragsschluss und Minderjährigenschutz

Der Abschluss eines Kaufvertrags über das Internet bestimmt sich nach den allgemeinen Regelungen (§§ 145 ff. BGB).[687] Für den bürgerlich-rechtlichen Minderjährigenschutz gelten dabei keine besonderen Vorschriften.

a. Vertragsschluss

Allgemein kann bei „online“ erfolgenden Vertragsschlüssen später unklar bzw. schwer feststellbar sein, von wem eine vertragsbegründende Willenserklärung stammt. Lässt sich eine bestimmte Person, die eine zum Vertragsschluss führende Willenserklärung im digitalen Raum abgegeben hat, nachträglich nicht mehr identifizieren, wirft dies die Frage auf, ob der Inhaber des bei einem Diensteanbieter geführten Kontos, über das die Willenserklärung abgegeben worden ist, als Vertragspartner angesehen werden kann. Das Problem tritt immer dann auf, wenn der Erklärende nicht der Inhaber eines Kontos ist, sich aber der Zugangsdaten des Berechtigten bedient hat. Die Rechtsprechung[688] hat in einem solchen Fall ein Handeln unter fremdem Namen angenommen, auf das die Regeln über die Stell-

---

[685] Vgl. RegE eines Gesetzes zur Umsetzung der Verbraucherrechterichtlinie und zur Änderung des Gesetzes zur Regelung der Wohnungsvermittlung, BT-Drs. 17/12637 vom 6.3.2013, S. 74.
[686] Vgl. – auch zu wettbewerbsrechtlichen Unterlassungsansprüchen und einem Unterlassungsklagerecht nach § 2 UKlaG – Erman/*Koch*, BGB, § 312a Rn. 34 und § 312d Rn. 68.
[687] Vgl. BGH, Urt. v. 11.5.2011 – VIII ZR 289/09, Tz. 8, CR 2011, 455, für den Fall des Verkaufs über die Internetplattform *eBay* an den Höchstbietenden.
[688] BGH, Urt. v. 11.5.2011 – VIII ZR 289/09, CR 2011, 455 f.

vertretung sowie die Grundsätze der Anscheins- und Duldungsvollmacht entsprechend anzuwenden seien. Einem Kontoinhaber könnten von einem Dritten unter seinem Namen abgegebene Erklärungen nicht allein deshalb zugerechnet werden, weil er seine Zugangsdaten nicht hinreichend vor einem Zugriff geschützt habe.

Diese Rechtsprechung ist zwar unter dem Aspekt eines möglichen Missbrauchs in der Praxis auf Kritik gestoßen.[689] Sie zeigt jedoch, dass Fragen des Abschlusses eines Vertrags, der über ein bei einem Online-Diensteanbieter geführtes Konto erfolgt, mit der geltenden Rechtsgeschäftslehre durchaus angemessen zu bewältigen sind.

Für Verbraucherverträge über den Erwerb digitaler Inhalte dürfte sich seitens der Anbieter die Frage, wer auf Seiten des Verbrauchers Vertragspartner geworden ist, in der Praxis allerdings kaum einmal stellen. Der Erwerb von E-Books, Videos und Musik erfolgt in weitem Umfang über ein Guthaben auf dem vom Nutzer beim Diensteanbieter geführten Konto. Das Guthaben wird dabei nach verbreiteter Praxis über den nicht an die Person des Kontoinhabers gebundenen Erwerb von Guthabenkarten oder Bons mit Codes realisiert. Der Anbieter der digitalen Inhalte läuft bei einer solchen Verfahrensweise nicht Gefahr, für den Erhalt der Gegenleistung des Nutzers nachträglich herausfinden zu müssen, wer sein Vertragspartner geworden ist. Soweit in der Praxis daneben die Zahlung digitaler Inhalte mit Kreditkarte oder über die Telefonrechnung angeboten wird, birgt dies für Anbieter keine über die allgemeinen Risiken dieser Bezahlformen hinausgehenden Risiken.

b. Minderjährigenschutz

Auch die bürgerlich-rechtlichen Regelungen zum Schutz Minderjähriger (§§ 104 ff. BGB) werfen mit Bezug auf den „online“ erfolgenden Erwerb digitaler Inhalte gegen Bezahlung keine Fragen auf, die nicht auch bei anderen Vertragsschlüssen im Internet unter Beteiligung Minderjähriger auftreten können.

Praktisch dürften sich solche Fragen beim Erwerb digitaler Inhalte mit Blick auf die gängige Praxis der Diensteanbieter, dass digitale Inhalte nur über ein passwortgeschütztes Nutzerkonto mit ausreichendem Guthaben erworben werden können, allerdings eher selten stellen. In aller Regel wird ein Fall des § 110 BGB vorliegen.

---

[689] Vgl. etwa *Härting/Strubel*, Anmerkung zu BGH, Urt. v. 11.5.2011 – VIII ZR 289/09, BB 2011, 2185 (2188 f.), und *Mankowski*, Anmerkung zu BGH, Urt. v. 11.5.2011 – VIII ZR 289/09, CR 2011, 455 (458 f.).

2. Allgemeines Schuldrecht

Mit Bezug auf die geltenden Regelungen des Allgemeinen Schuldrechts gibt es keinen konkreten Bedarf, für den Erwerb digitaler Inhalte besondere Bestimmungen zu schaffen oder geltende Vorschriften zu ändern.[690]

Das gilt insbesondere für die Regelungen zum Inhalt der Schuldverhältnisse (§§ 241 – 304 BGB). Für Fälle, in denen beim Download Probleme auftreten, wird § 269 BGB als interessengerechte Regelung angesehen.[691] Auch hinsichtlich der geltenden Bestimmungen für die Einbeziehung von Allgemeinen Geschäftsbedingungen in Verträge über den Erwerb digitaler Inhalte wird im Schrifttum kein Änderungsbedarf gesehen.[692]

Dass Verträge über den Erwerb digitaler Inhalte durch Allgemeine Geschäftsbedingungen der Anbieter im Sinne eines „*take it or leave it*" dominiert werden, ist kein Spezifikum solcher Verträge, sondern entspricht einer praktisch ausnahmslosen Usance bei über das Internet abgeschlossenen Verbraucherverträgen.

3. Vertragstypologische Einordnung als Kaufvertrag

Von den im Besonderen Schuldrecht geregelten Vertragstypen kommt für den Vertrag über den datenträgerlosen Erwerb digitaler Inhalte allein der Kaufvertrag in Betracht.

Der Erwerb digitaler Inhalte im Wege des Downloads stellt zwar – weil der Vertrag nicht den Erwerb einer Sache i. S. v. § 90 BGB, also eines körperlichen Gegenstands, betrifft – keinen Kaufvertrag gemäß § 433 BGB dar. Fehlt es beim Erwerb digitaler Inhalte an der Verkörperung in einem Datenträger, können die digitalen Inhalte nicht als Sache angesehen werden. Insoweit liegt es anders als beim Kauf eines Datenträgers mit digitalen Inhalten, der als Sachkauf eingeordnet wird.[693]

Die Vorschriften über den Kauf von Sachen finden jedoch, da es sich beim datenträgerlosen Erwerb digitaler Inhalte – wie z. B. beim Erwerb eines E-Books oder einer Audiodatei – um den Kauf eines sonstigen Gegenstands handelt, nach herrschender Meinung gemäß § 453 Abs. 1 BGB entsprechende Anwendung.[694]

---

[690] Zur Umsetzbarkeit verbraucherpolitischer Ziele im bürgerlichen Recht siehe unten V.

[691] Vgl. *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 5.

[692] Vgl. *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 6.

[693] Vgl. BGH, Urt. v. 15.11.2006 – XII ZR 120/04, Tz. 15, CR 2007, 75 f. m. v. w. N.

[694] Vgl. *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 9. a); jurisPK/*Leible/Müller*, BGB, § 453 Rn. 20; *Hauck*, Gebrauchthandel mit digitalen Gütern, NJW 2014, 3616.
Graef, „Recht der E-Books und des Electronic Publishing", 2016, Rn. 158, nimmt zwar einen (im geltenden bürgerlichen Recht als Vertragstyp nicht geregelten) Lizenzvertrag an. Er gelangt dabei aber zu keinen von der h. M. abweichenden Ergebnissen, weil er die §§ 434 ff. BGB auf den Lizenzvertrag für entsprechend anwendbar hält. Der 71. Deutsche Juristentag 2016 hat sich

Der RL-Vorschlag COM(2015) 634 final sieht insoweit keine Änderungen vor. Er enthält sich vielmehr ausdrücklich einer Festlegung dazu, ob ein Vertrag über die Bereitstellung digitaler Inhalte einen Kaufvertrag, Dienstleistungsvertrag, Mietvertrag oder Vertrag *sui generis* darstellt.[695]

Ordnet man den datenträgerlosen Erwerb digitaler Inhalte mit *Faust* und der herrschenden Meinung als Kaufvertrag über einen sonstigen Gegenstand i. S. v. § 453 Abs. 1 BGB ein und stellt man gemäß § 446 S. 1 BGB für die Mangelfreiheit auf den Zeitpunkt ab, in dem der Käufer die digitalen Inhalte erlangt[696], gehört eine nicht konkret vereinbarte spätere Bereitstellung neuerer technischer Versionen i. S. v. „Updates" der digitalen Inhalte nicht zu den Hauptleistungspflichten des Verkäufers.

Das ist bei den hier betrachteten datenträgerlos vertriebenen digitalen Inhalten zum rezeptiven Werkgenuss (zu denen nicht Computerprogramme gehören) sachgerecht. Zur Wiedergabe solcher Inhalte bedarf es einer geeigneten Hard- und Software. Ändert sich diese nicht, gibt es keinen Anlass für ein „Update" von zum Zeitpunkt des Downloads mangelfreien E-Book-, Film- oder Musikdateien. Der Verlust einer anfänglich vorhandenen Kompatibilität wird im Regelfall darauf zurückzuführen sein, dass das zur Anzeige bzw. zum Abspielen der digitalen Inhalte verwendete Wiedergabegerät oder die auf diesem laufende Software – z. B. durch ein *Softwareupdate* – geändert worden ist. Werden Hardware, Software und digitale Inhalte zum rezeptiven Werkgenuss – z. B. E-Book-Reader und E-Books oder Tablet-Computer und Videos – als aufeinander abgestimmt vertrieben, wird man den Anbieter als verpflichtet ansehen können, nicht durch spätere Hard- oder Softwareänderungen einen Werkgenuss nachträglich unmöglich zu machen. Nach der Dogmatik zu § 242 BGB darf eine Vertragspartei die dem anderen Teil aufgrund des Schuldverhältnisses gewährten Vorteile nach beiderseitiger Vertragserfüllung nicht entziehen oder wesentlich schmälern.[697] Fallen Änderungen von Hard- oder Software demgegenüber allein in die Sphäre des Nutzers, erscheint es – wie bei analogen Sachverhaltskonstellationen[698] – nicht interessengerecht, den Anbieter zu verpflichten, datenträgerlos vertriebene digitale Inhalte nachträglich einer anderen technischen Umgebung anzupassen. Der Kaufvertrag über digitale Inhalte

---

in der Diskussion darüber, ob Verträge über digitale Inhalte, die einem urheberrechtlichen Schutz unterliegen, als Lizenzverträge eingeordnet werden sollten, *dagegen* ausgesprochen, bei solchen Verträgen eine *analoge Anwendung des Kaufvertragsrechts auszuschließen* (vgl. Beschluss Ziffer 30 der Abteilung Zivilrecht).

695 Vgl. RL-Vorschlag COM(2015) 634 final, S. 7.

696 Siehe dazu nachstehend unter IV. 5.

697 Vgl. Palandt/*Grüneberg*, BGB, § 242 Rn. 29 m. w. N. Daraus wird u. a. die Pflicht des Verkäufers eines industriell hergestellten technischen Produkts hergeleitet, für die durchschnittliche Nutzungsdauer des Produkts Ersatzteile bereitzuhalten (ebda).

698 Der Verkäufer einer DVD mit einem Spielfilm ist nicht verpflichtet, dem Käufer später eine Blu-ray Disc mit demselben Film zur Verfügung zu stellen, weil sich zwischenzeitlich ein geänderter technischer Standard etabliert hat und der Käufer nun über ein Abspielgerät für Blu-ray Discs verfügt.

zum rezeptiven Werkgenuss würde sonst ohne hinreichenden Anlass den Charakter eines Dauerschuldverhältnisses bekommen.

4. Anwendbare Gewährleistungsregelungen

Mit der Einordnung als Kauf eines sonstigen Gegenstands i. S. v. § 453 BGB finden auf den datenträgerlosen Erwerb digitaler Inhalte die kaufrechtlichen Gewährleistungsregelungen in den §§ 434 ff. BGB entsprechende Anwendung.

Das gilt insbesondere für folgende Regelungsgegenstände:

- Voraussetzungen einer Mangelfreiheit (§ 434 BGB);
- Käuferrechte bei Mängeln (§§ 437, 439 BGB);
- Verjährung von Mängelansprüchen (§ 438 BGB);
- Gefahrübergang (§ 446 BGB).

Bei sachgerechtem Verständnis sind auf den datenträgerlosen Erwerb digitaler Inhalte über § 453 BGB auch die Regelungen über den Verbrauchsgüterkauf (§§ 474 ff. BGB) entsprechend anwendbar. Nach § 474 Abs. 1 S. 1 BGB sind Verbrauchsgüterkäufe zwar nur Verträge, durch die ein Verbraucher von einem Unternehmer eine bewegliche Sache kauft. Nach herrschender Meinung im Schrifttum verweist jedoch § 453 Abs. 1 BGB für den Kauf sonstiger Gegenstände schlechthin auf die Vorschriften über den Sachkauf und damit auch auf die Bestimmungen für den Verbrauchsgüterkauf.[699]

Bedeutung hat dies insbesondere wegen der in § 476 BGB geregelten Beweislastumkehr. Zeigt sich innerhalb von sechs Monaten seit Gefahrübergang ein Mangel des Kaufgegenstands, so wird vermutet, dass dieser bereits bei Gefahrübergang mangelhaft war, es sei denn, diese Vermutung ist mit der Art der Sache oder des Mangels nicht vereinbar.

5. Beurteilung des für den Erwerb digitaler Inhalte geltenden Gewährleistungsrechts

Mit der Frage, ob die kaufrechtlichen Gewährleistungsregelungen beim datenträgerlosen Erwerb digitaler Inhalte zu sachgerechten und ausgewogenen Ergebnissen führen, hat sich *Faust* in seinem Gutachten für den 71. Deutschen Juristentag eingehend auseinandergesetzt.

In seinen überzeugenden Ausführungen gelangt Faust mit Bezug auf die geltenden Regelungen des Bürgerlichen Gesetzbuchs insbesondere zu folgenden Ergebnissen[700]:

---

[699] Vgl. *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 9. c) m. v. w. N. (Fn. 86).

[700] *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 9.; zu Fragen der Verjährung verhält sich das Gutachten nicht.

- Die in § 434 BGB genannten, über § 453 Abs. 1 BGB entsprechend heranzuziehenden Kriterien für eine Sachmangelfreiheit sind mit Bezug auf digitale Inhalte sachgerecht. Die Aufzählung von Kriterien für eine Mangelfreiheit in Art. 6 Abs. 1 lit. a des RL-Vorschlags COM(2015) 634 final bringt insoweit keinen Gewinn an Präzision;
- Der gemäß § 446 S. 1 BGB für die Mangelfreiheit relevante Zeitpunkt führt auch beim Erwerb digitaler Inhalte zu angemessenen Ergebnissen. Nach der über § 453 Abs. 1 BGB entsprechend anwendbaren Regelung zum Gefahrübergang ist auf den Zeitpunkt abzustellen, in dem die digitalen Inhalte die Schnittstelle auf Käuferseite passieren[701];
- Die Rechtsbehelfe des Kaufrechts (Anspruch auf Nacherfüllung, Rücktritt, Minderung, Anspruch auf Schadensersatz statt der Leistung und Aufwendungsersatz) sind auch im Hinblick auf datenträgerlos erworbene digitale Inhalte sach- und interessengerecht;
- Es bedarf für den Erwerb digitaler Inhalte keiner besonderen Beweislastregeln. Die in § 476 BGB geregelte Beweislastumkehr wirft bei der Subsumtion von Fällen des Erwerbs digitaler Inhalte nur Fragen auf, deren Klärung der Rechtsprechung überlassen werden kann.

V. Bürgerlich-rechtliche Einordnung und Umsetzbarkeit verbraucherpolitischer Ziele mit Bezug auf Verträge über den Erwerb digitaler Inhalte

Mit einstimmig gefasstem Beschluss vom 22. April 2016 hat sich die 12. Verbraucherschutzministerkonferenz (VSMK) zu TOP 27 „Daten- und Verbraucherschutz bei digitalen Rechte-Managementsystemen gewährleisten“ dafür ausgesprochen, in verschiedenen Aspekten die Rechtsposition von Verbrauchern beim Erwerb digitaler Inhalte zu stärken.[702]

---

[701] Soweit *Graef*, Recht der E-Books und des Electronic Publishing, Rn. 166, von dem „Beginn des Downloads bzw. dem Zugriff auf die elektronischen Inhalte“ spricht, ist das – anders als im Zusammenhang mit § 356 Abs. 5 BGB (siehe dazu oben II. 2. a.) – nicht überzeugend. Nach allgemeinen Grundsätzen müssen die digitalen Inhalte, um einen Gefahrübergang annehmen zu können, vollständig in die Sphäre des Käufers gelangt sein. Der RL-Vorschlag COM(2015) 634 final verhält sich zu dieser Frage nicht; die auf die Frage des Adressaten der digitalen Inhalte bezogene Regelung in Art. 5 Abs. 2 S. 2 des Richtlinienvorschlags ist zu diesem Punkt unergiebig.

[702] Der Beschluss ist als Teil des Ergebnisprotokolls der 12. Verbraucherschutzministerkonferenz vom 22. April 2016 unter https://www.verbraucherschutzministerkonferenz.de/documents/Endgueltiges_Protokoll_VSMK_2016.pdf veröffentlicht (letzter Abruf: 1.3.2017).

Auf der Grundlage eines mit dem Beschluss zur Kenntnis genommenen Berichts der Projektgruppe „Daten- und Verbraucherschutz bei Digitalen Rechtemanagement-Systemen (DRM) gewährleisten“[703] (im Folgenden: DRM-Projektgruppe) fordert die VSMK zum einen spezifisch auf das Phänomen des „Digitalen Rechtemanagements“ (DRM) – d. h. technischer Mechanismen zur Steuerung der Nutzung digitaler Inhalte – bezogene Rechtsänderungen. Zum anderen spricht sie sich für rechtliche Änderungen aus, deren Bedeutung sich auf den Erwerb nicht durch DRM-Mechanismen geschützter digitaler Inhalte im Wege des Downloads erstreckt.

Spezifisch auf DRM-Systeme zugeschnitten sind die Ziffern 3., 5. und 6. des Beschlusses. Darin werden eine Pflicht der Anbieter digitaler Güter zu einfachen, klaren und verständlichen Informationen über verwendete DRM-Systeme sowie ein umfassendes datenschutzrechtliches Koppelungsverbot beim Einsatz von DRM-Systemen gefordert. Der Bundesminister der Justiz und für Verbraucherschutz wird gebeten, sich für entsprechende Rechtsänderungen auf europäischer Ebene einzusetzen. Diese Forderungen bedürfen keiner ergänzenden vertragsrechtlichen Würdigung. Wie spezifisch auf DRM-Systeme bezogene gesetzliche Informationspflichten von Anbietern gegenüber Verbrauchern in inhaltlicher und formaler Hinsicht angemessen auszugestalten sind, ist eine vorrangig verbraucherpolitisch zu beurteilende Frage, zu deren Beantwortung eine vertragsrechtliche Betrachtung letztlich nichts beitragen kann. Der u. a. auf Fragen eines Koppelungsverbots bezogene Legislativprozess zum Datenschutzrecht auf EU-Ebene ist mit dem Inkrafttreten der Datenschutz-Grundverordnung vom 27. April 2016 inzwischen abgeschlossen.

Eine Würdigung unter schuldrechtlichen Aspekten ist aber mit Bezug auf die verbraucherpolitischen Forderungen veranlasst, die sich allgemein auf Rechte beim Erwerb digitaler Inhalte im Wege des Downloads beziehen.

Unter Ziffer 4 des Beschlusses, der diese Forderungen enthält, heißt es:

> *„Die Nutzung digitaler Güter wird durch die urheberrechtlichen Grenzen der Privatkopie bei digitalen Werken und darauf gestützte Digitale Rechtemanagement-Systeme eingeschränkt. Die Ministerinnen, Minister, Senatorinnen und der Senator der Verbraucherschutzressorts der Länder sind der Auffassung, dass die entgegenstehende Erwartung von Verbraucherinnen und Verbrauchern, digitale Güter möglichst ohne Beschränkungen nutzen zu können, grundsätzlich als berechtigt anzusehen ist. Die Ministerinnen, Minister, die Senatorinnen und der Senator der Verbraucherschutzressorts der Länder halten daher vertragliche und technische Gestaltungen, bei denen den Erwerberinnen und Erwerbern digitaler Güter eine Nutzung auf*

---

[703] Der Bericht ist unter https://www.verbraucherschutzministerkonferenz.de/documents/TOP27_Bericht_der_Projektgruppe.pdf frei abrufbar (letzter Abruf: 1.3.2017).

> *mehreren Endgeräten und ohne Bindungen an bestimmte Systeme ermöglicht wird, für eine interessengerechte Lösung und sprechen sich insoweit für eine gesetzliche Verankerung aus. Beispielsweise könnten die Anbieterinnen/die Anbieter über das bestehende Gewährleistungsrecht hinausgehend verpflichtet werden, ein Mindestmaß an Nutzungsmöglichkeiten zu gewährleisten sowie für den Fall eines Datenverlustes der Erwerberin/dem Erwerber innerhalb einer angemessenen Frist nach dem Download einen Nachlieferungsanspruch einzuräumen."*

Partiell in dieselbe Richtung zielt die Stellungnahme des Bundesrates vom 22. April 2016 zum RL-Vorschlag COM(2015) 634 final – BR-Drs. 168/16 (B) – in der es auf Empfehlung des Ausschusses für Agrarpolitik und Verbraucherschutz unter Ziffer 53 heißt:

> *„Der Bundesrat sieht ein Bedürfnis, die Erwartung der Verbraucher hinsichtlich der Nutzbarkeit und Verfügbarkeit digitaler Inhalte dadurch zu schützen, dass die Anbieter grundsätzlich und unter Berücksichtigung zwingender urheberrechtlicher Schutzbedürfnisse die Möglichkeit einräumen müssen, die digitalen Inhalte auf mehreren, gegebenenfalls registrierten Endgeräten zu nutzen. Es sollte geprüft werden, in der Richtlinie insoweit Mindestanforderungen an die Leistungspflicht der Anbieter zu regeln."*

Dem Bericht der DRM-Projektgruppe folgend klammert der Beschluss der VSMK vom 22. April 2016 zu TOP 27 Forderungen nach einer Änderung des Urheberrechts aus. Die DRM-Projektgruppe hat das genuin urheberrechtliche Thema „Weiterverkauf digitaler Güter", das in einer Studie aus jüngerer Zeit bereits umfänglich aufbereitet worden ist[704], ausdrücklich nicht aufgegriffen und die Klärung anderweitigen Arbeiten vorbehalten.[705]

Es ist eine *rechtspolitische* Entscheidung, ob der *urheberrechtliche Erschöpfungsgrundsatz* auf datenträgerlos vertriebene digitale Inhalte erstreckt und damit deren nicht abdingbare Übertragbarkeit durch Erwerber bestimmt werden soll. Maßgeblich ist insoweit letztlich, ob man darin einen angemessenen Ausgleich der widerstreitenden Interessen von Urhebern bzw. Rechteinhabern einerseits und Erwerbern digitaler Inhalte andererseits sieht. Der Bundesrat hat sich zum Kommissionsvorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über das Urheberrecht im digitalen Binnenmarkt – COM(2016) 593 final – mit Beschluss vom 16. Dezember 2016 – BR-Drs. 565/16 (B) – für die Einführung

---

[704] *T. Kreutzer*, Weiterveräußerungsfähigkeit von digitalen Gütern, Studie im Auftrag des Ministeriums für Ländlichen Raum und Verbraucherschutz Baden-Württemberg, 2015, abrufbar unter https://mlr.baden-wuerttemberg.de/fileadmin/redaktion/m-mlr/intern/dateien/PDFs/Verbraucherschutz/GesamteStudieDigitale_Gueter.pdf (letzter Abruf: 1.3.2017).

[705] Siehe S. 5 des Berichts der DRM-Projektgruppe.

eines Weiterveräußerungsrechts für rechtmäßig erworbene digitale Güter ausgesprochen.[706]

Eine Betrachtung der urheberrechtlichen Aspekte aus einem vertragsrechtlichen Blickwinkel kann zur Beurteilung der Frage, ob es Änderungen des Urheberrechts bedarf und wie diese ausgestaltet sein sollten, im Ergebnis keinen Beitrag leisten. Im Ausgangspunkt können die Parteien aufgrund der Privatautonomie bei Verträgen über den Erwerb digitaler Inhalte zwar Vereinbarungen treffen, welche die urheberrechtliche Rechtslage nicht nachzeichnen. So kann sich der Verkäufer digitaler Inhalte wirksam verpflichten, dem Käufer Rechte einzuräumen, über die er urheberrechtlich nicht verfügen darf. In aller Regel wird es für den Anbieter aber allein interessengerecht sein, seine vorformulierten Vertragsbedingungen am urheberrechtlichen Rahmen auszurichten. Bei der datenträgerlosen Veräußerung digitaler Inhalte stellt es deshalb den praktischen Regelfall dar, dass dem Erwerber lediglich ein nicht übertragbares Recht zum ausschließlich persönlichen Gebrauch übertragen wird, das ihn nicht zur Weiterveräußerung befugt.[707] Eine Änderung dieser Rechtspraxis lässt sich sachgerecht allein über eine die divergierenden Interessen ausgewogen in Ausgleich bringende Änderung erreichen, die auch das *Urheberrecht* berücksichtigt. Erst auf dieser Grundlage wäre es sinnvoll, ein Recht zur Weiterveräußerung datenträgerloser digitaler Inhalte entsprechend einer Forderung des Bundesrates[708] auch im bürgerlichen Recht nachzuvollziehen.

Der Beschluss der VSMK vom 22. April 2016 zu TOP 27 enthält unter Ziffer 4 jedoch auch ausdrücklich *auf das Vertragsrecht bezogene verbraucherpolitische Forderungen*. Der Beschluss spricht sich insoweit für zwei Änderungen aus:

---

[706] In Ziffer 18 des Beschlusses heißt es: „Der Bundesrat setzt sich weiterhin für eine Einführung eines Weiterveräußerungsrechts für rechtmäßig erworbene digitale Güter ein. Die gegenwärtige Rechtslage führt zu einer Ungleichbehandlung körperlicher Werke (z. B. Bücher) gegenüber digitalen Werken (z. B. E-Books), indem Verbraucherinnen und Verbrauchern beim Erwerb von digitalen Gütern häufig durch Allgemeine Geschäftsbedingungen sowie durch technische Schutzmaßnahmen (sog. Digitales Rechtemanagement) untersagt beziehungsweise verwehrt wird, ein erworbenes Produkt etwa weiter zu verkaufen oder zu verschenken. Die rechtliche Absicherung eines allgemeinen Weiterveräußerungsrechtes für ordnungsgemäß erworbene digitale Güter unter der Voraussetzung, dass der Weiterveräußerer keine Kopien des digitalen Werks zurückbehält, ist deshalb geboten."

[707] Vgl. *Hauck*, Gebrauchthandel mit digitalen Gütern, NJW 2014, 3616.

[708] Siehe Stellungnahme des Bundesrates vom 22. April 2016 zum RL-Vorschlag COM(2015) 634 final – BR-Drs. 168/16 (B) – in der es auf Empfehlung des Ausschusses für Agrarpolitik und Verbraucherschutz unter Ziffer 54 heißt: „Er regt außerdem an, im Rahmen von Mindestanforderungen an die Leistungspflicht der Anbieter vorzusehen, dass auf Grund eines Kaufvertrags erworbene digitale Inhalte grundsätzlich auf Dritte übertragen werden können, wenn gewährleistet werden kann, dass die digitalen Inhalte beim ursprünglichen Erwerber nicht mehr vorhanden oder nutzbar sind. Es besteht ein anerkennenswertes wirtschaftliches Interesse des Erwerbers, einzelne digitale Inhalte oder, bspw. im Todesfall, den gesamten Bestand an digitalen Gütern zu übertragen."

- Zum einen sollen Verbraucher einen *schuldrechtlichen* Anspruch darauf haben, erworbene digitale Inhalte *ohne Bindung an ein bestimmtes Gerät und ein bestimmtes technisches System* nutzen zu können. Der dem Beschluss zugrunde liegende Bericht der DRM-Projektgruppe geht dabei nachvollziehbar davon aus, dass nach geltendem Recht eine Beschränkung der Nutzbarkeit digitaler Inhalte auf bestimmte Systeme der vertraglich vorausgesetzten Verwendung entspricht.
- Zum anderen sollen Verbraucher beim Erwerb digitaler Inhalte im Wege des Downloads einen (zeitlich begrenzten) über das geltende Gewährleistungsrecht hinausgehenden vertraglichen Anspruch auf einen *erneuten Download* haben, wenn heruntergeladene Dateien mit digitalen Inhalten bei ihnen in Verlust geraten sind.

Diesen Forderungen soll hier näher nachgegangen werden.

1. Anspruch auf Nutzung digitaler Inhalte ohne Bindung an ein bestimmtes Gerät oder technisches System

Ein Anspruch auf Nutzung digitaler Inhalte ohne Bindung an ein bestimmtes Gerät oder technisches System erfordert beim Erwerb digitaler Inhalte zum rezeptiven Werkgenuss im Wege des Downloads zunächst, dass der Nutzer ein Recht hat, von den digitalen Inhalten *mehrere Kopien* zu fertigen.

a. Urheberrechtliche Aspekte

Lässt man die rechtspolitisch zu entscheidende Frage offen, ob der urheberrechtliche Erschöpfungsgrundsatz auf datenträgerlos vertriebene digitale Inhalte erstreckt werden sollte[709], kommt nur eine Verpflichtung des Anbieters in Betracht, dem Nutzer ein *mehrfaches Herunterladen* erworbener digitaler Inhalte zu ermöglichen. Gesetzliche Vorgaben, ob und unter welchen Voraussetzungen ein Urheber dazu verpflichtet ist, berührt das im Urheberrechtsgesetz geregelte Recht der öffentlichen Wiedergabe. Nach § 15 Abs. 2 S. 1 UrhG hat der Urheber das ausschließliche Recht, sein Werk in unkörperlicher Form öffentlich wiederzugeben. Gemäß § 15 Abs. 2 S. 2 Nr. 2 UrhG umfasst das Recht der öffentlichen Wiedergabe insbesondere das Recht der öffentlichen Zugänglichmachung nach § 19a UrhG. Eine Wiedergabe ist dabei nach § 15 Abs. 3 UrhG öffentlich, wenn sie für eine Mehrzahl von Mitgliedern der Öffentlichkeit bestimmt ist. Unter § 19a UrhG fällt deshalb auch das Recht zur Bereitstellung eines Werkes zum Download über das Internet.[710] Nach § 15 Abs. 1 S. 1, 1. Hs. UrhG hat der Urheber das ausschließliche Recht, sein Werk in körperlicher Form zu verwerten. Als Generalklausel gewährt § 15 UrhG dem Urheber das alleinige Recht, darüber zu entscheiden, wie sein Werk verwertet wird. Das gilt grundsätzlich für jede Nutzung, sofern keine gesetzlichen Erlaubnistatbestände eingreifen. Der Urheber darf deshalb auch al-

---

[709] Siehe dazu oben unter V.
[710] Vgl. Wandtke/Bullinger/*Bullinger*, UrhR, § 19a Rn. 10 f., 23.

lein darüber entscheiden, ob und mit welchen Maßgaben sein Werk durch Downloads verwertet wird. Eine gesetzliche Verpflichtung von Anbietern, beim Erwerb digitaler Inhalte durch einen Verbraucher mehrfache Downloads zuzulassen, müsste daher das *Urheberrecht* berücksichtigen.

b. Interoperabilität und technische Normung als nicht bürgerlich-rechtliche Regelungsmaterien

Klammert man die vorgenannten urheberrechtlichen Aspekte, die ebenfalls vorrangig urheberrechtliche Fragestellung, unter welchen Voraussetzungen und in welchem Umfang ein Verbraucher erworbene digitale Inhalte kopieren darf, sowie die gesondert untersuchte[711] Frage eines vertraglichen Anspruchs auf einen erneuten Download aus, hängt die Möglichkeit der Nutzung heruntergeladener digitaler Inhalte ohne Bindung an ein bestimmtes Gerät oder technisches System vor allem davon ab, dass das *Dateiformat* erworbener digitaler Inhalte mit unterschiedlichen Hard- und Softwareumgebungen *interoperabel* ist.

Die Bedeutung der Interoperabilität von Informationstechnik wird in verschiedensten Zusammenhängen betont.[712]

Eine *Interoperabilität* – d. h. die Fähigkeit zu einem technischen Zusammenwirken – setzt voraus, dass das *Dateiformat* der digitalen Inhalte und die jeweilige *Hard- und Softwareumgebung* miteinander vereinbar, also *kompatibel*, sind. Sicher gewährleistet werden kann eine solche Kompatibilität nur über *verbindliche technische Standards*. Solche Standards setzen eine *technische Normung* voraus.

Das geltende Kaufvertragsrecht ist – wie das Schuldrecht insgesamt – technikoffen ausgestaltet und enthält keine konkreten technischen Vorgaben.

Nach § 434 Abs. 1 S. 1 BGB ist eine Sache frei von Sachmängeln, wenn sie bei Gefahrübergang die *vereinbarte Beschaffenheit* hat. Soweit eine Beschaffenheit nicht vereinbart ist, ist sie gemäß § 434 Abs. 1 S. 2 BGB mangelfrei, wenn sie sich für die *nach dem Vertrag vorausgesetzte Verwendung eignet* oder – nachrangig – wenn sie sich für die *gewöhnliche Verwendung* eignet und eine Beschaffenheit aufweist, die bei Sachen der gleichen Art *üblich* ist und die der Käufer nach der Art der Sache erwarten kann. Diese Regelungen, die die Verbrauchsgüterkaufrichtlinie umsetzen und deren subjektive Prägung Ausfluss der Privatautonomie ist[713], finden über § 453 Abs. 1 BGB auf den Erwerb digitaler Inhalte entsprechende Anwendung.

---

[711] Siehe dazu nachfolgend die Ausführungen unter V. 2.

[712] Vgl. etwa *Mittelstaedt* in Deutsches Ärzteblatt, Heft 25 (24. Juni 2016), S. 4 mit Bezug auf Computer in Krankenhäusern.

[713] Vgl. jurisPK/*Pammler*, BGB, § 434 Rn. 13 f.

Die Beschaffenheit als zentrales Merkmal des Sachmängelrechts ist vom Gesetzgeber nicht definiert worden. Erst recht enthält sich das geltende Sachmängelrecht demgemäß konkreter technischer Vorgaben für eine Mangelfreiheit.

Ein Kraftfahrzeug, das wegen seiner Abmessungen für den öffentlichen Straßenverkehr nicht zulassungsgeeignet ist, eignet sich als Gegenstand eines standardisierten Kaufvertrags zwischen einem Autohändler und einem Verbraucher regelmäßig nicht für die nach dem Vertrag vorausgesetzte Verwendung (Betrieb im öffentlichen Straßenverkehr). Es eignet sich auch nicht für die gewöhnliche Verwendung, also für die Zwecke, zu denen Kraftfahrzeuge von Verbrauchern üblicherweise gebraucht werden. Die fehlende technische Eignung ergibt sich dabei aber nicht aus dem Schuldrecht. Sie folgt vielmehr aus *ordnungsrechtlichen Bestimmungen* für den öffentlichen Straßenverkehr. Nach § 32 Abs. 1 der Straßenverkehrs-Zulassungs-Ordnung (StVZO) darf die höchstzulässige Breite von Kraftfahrzeugen bestimmte Maße nicht überschreiten. Nach § 32 Abs. 1 S. 1 Nr. 5 StVZO beträgt diese Breite bei Personenkraftwagen 2,50 Meter. Zu ermitteln ist die Fahrzeugbreite gemäß § 32 Abs. 1 S. 2 StVZO nach der *ISO-Norm 612-1978*.

Auch in anderen bürgerlich-rechtlichen Zusammenhängen nimmt der Gesetzgeber auf technische Standards lediglich Bezug, ohne sich zum Inhalt der Standards zu verhalten. In § 906 Abs. 1 S. 2 und 3 BGB knüpft er an anderweitig festgelegte technische Werte an. Für die Wirksamkeit einer Vereinbarung von Zahlungsmittelentgelten ist nach § 312a Abs. 4 Nr. 1 BGB u. a. maßgeblich, ob für den Verbraucher eine „gängige“ unentgeltliche Zahlungsmöglichkeit besteht. Was „gängig“, also hinreichend verbreitet, ist und damit in der Praxis herrschenden Standards entspricht, ist bürgerlich-rechtlich – wie mit Bezug auf den Begriff „gewöhnlich“ in § 434 Abs. 1 S. 2 Nr. 2 BGB – nicht bestimmt.

Abgesehen davon, dass die gesetzlichen Regelungen des Schuldrechts keine konkreten technischen Vorgaben enthalten, findet technische Normung in weitem Umfang schon nicht durch öffentliche Stellen, sondern durch private Institute wie z. B. das Deutsche Institut für Normung e. V. (*DIN*) und den Verband der Elektrotechnik Elektronik Informationstechnik e. V. (*VDE*) statt. Auf europäischer Ebene kommt den Normungsorganisationen Europäisches Komitee für Normung (*CEN*), Europäisches Komitee für elektrotechnische Normung (*CENELEC*) und Europäisches Institut für Telekommunikationsnormen (*ETSI*) besondere Bedeutung zu.[714] Nur etwa ein Fünftel aller europäischen Normen geht auf einen Normungsauftrag der Europäischen Kommission zurück.[715] Soweit der Gesetzgeber – wie etwa in § 49 Abs. 2 des Energiewirtschaftsgesetzes (EnWG) – konkret

---

[714] Vgl. zum Ganzen *Germelmann*, Private Regelwerke im Geltungsbereich der Warenverkehrsfreiheit – Konsequenzen der Fra.bo-Entscheidung für die technische Normung in Deutschland, GewerbeArchiv 2014, 335.

[715] Vgl. die Information der EU „Ihr Europa“/„Normung in Europa“ unter http://europa.eu/youreurope/business/product/standardisation-in-europe/index_de.htm (letzter Abruf: 1.3.2017).

auf private technische Regeln verweist, geschieht dies v. a. in *ordnungsrechtlichen* Zusammenhängen.

Auch das Ziel technischer Interoperabilität wird in ordnungsrechtlichen Zusammenhängen verfolgt, wie sich etwa aus § 49 Abs. 4 EnWG ergibt, wonach durch Rechtsverordnung Festlegungen zur Gewährleistung der Interoperabilität von Ladepunkten für Elektromobile erfolgen können.

Für Regelungen, welche Verbrauchern einen Anspruch darauf gewähren, im Wege eines Downloads erworbene digitale Inhalte ohne Bindung an ein bestimmtes Gerät oder technisches System zu nutzen, ist das *bürgerliche Recht* mithin *nicht der richtige Regelungsort*.

Mit Blick darauf, dass das geltende Zivilrecht eine Interoperabilität nicht gewährleistet, legt Art. 246a § 1 Abs. 1 Nr. 15 EGBGB in Umsetzung von Art. 6 Abs. 1 lit. s der VRRL zugrunde, dass „Beschränkungen der Interoperabilität und der Kompatibilität digitaler Inhalte mit Hard- und Software“ gegeben sein können.

2. Vertraglicher Anspruch auf einen erneuten Download

Nach geltendem Recht schuldet der Anbieter dem Nutzer aus einem Vertrag über den Erwerb digitaler Inhalte zum rezeptiven Werkgenuss im Wege des Downloads, in dem nicht die Möglichkeit eines mehrfachen Herunterladens vereinbart ist, nur *einen* Download.

Hat der Anbieter dem Nutzer einen Download ermöglicht und der Nutzer die Inhalte heruntergeladen, ist die vom Anbieter geschuldete Leistung bewirkt. Mit Eintritt des Leistungserfolgs[716] – d. h. dem Abschluss eines vollständigen und mangelfreien Downloads – erlischt das Schuldverhältnis gemäß § 362 Abs. 1 BGB. Nach dem erfolgreichen Herunterladen digitaler Inhalte auf eine vom Nutzer gewählte und vom Anbieter akzeptierte Rechenressource kann der Nutzer nach geltendem Recht, wenn nichts anderes vereinbart ist, keinen Anspruch auf einen erneuten Download geltend machen.

Weder die Vorschriften des Kaufrechts noch die des allgemeinen Schuldrechts enthalten eine Regelung, aus der sich ein Recht auf einen erneuten Download herleiten lässt.

Ein solcher Anspruch lässt sich insbesondere nicht auf § 242 BGB stützen.

Aus § 242 BGB lassen sich im Rahmen eines Vertragsverhältnisses zwar unabdingbare nachwirkende Pflichten herleiten.[717] So bleibt der Schuldner auch nach Vertragserfüllung im Rahmen des Zumutbaren verpflichtet, nichts zu unternehmen, was dem Gläubiger die auf der Grundlage des Vertrags zugeflossenen Vorteile wieder entzieht.[718] Aus solchen (Neben-)Pflichten können sich – auch wenn

---

[716] Vgl. zur Maßgeblichkeit nicht der Leistungshandlung, sondern des Leistungserfolgs BGH, Beschl. v. 29.1.2009 – III ZR 115/08, Tz. 5, NJW 2009, 1085 (1086).
[717] Vgl. dazu Palandt/*Grüneberg*, BGB, § 242 Rn. 5, 20.
[718] Vgl. BGH, Urt. v. 24.10.1989 – XI ZR 8/89, Tz. 15, NJW-RR 1990, 141 (142).

§ 242 BGB selbst grundsätzlich keine Anspruchsgrundlage ist[719] – klagbare Erfüllungsansprüche ergeben.[720]

Daraus kann aber keine Verpflichtung des Anbieters abgeleitet werden, dem Nutzer auch dann einen erneuten Download zu ermöglichen, wenn ihm die Nutzung des ersten Downloads aus Gründen nicht mehr möglich ist, die – wie z. B. bei einer nachträglichen Funktionsunfähigkeit des Speichermediums, auf dem die digitalen Inhalte abgelegt worden sind – seiner Sphäre zuzurechnen sind. Die Leistungspflicht nach Treu und Glauben geht nicht so weit, dass ein Vertragspartner eine vollständig bewirkte Leistung nur deshalb erneut erbringen muss, weil ihm dies ohne messbaren oder nennenswerten Aufwand möglich ist.

So ist für Auskunftsansprüche anerkannt, dass es für deren Herleitung aus § 242 BGB nicht ausreicht, wenn der in Anspruch Genommene die für den Anspruchsteller bedeutsame Auskunft unschwer geben kann. Erforderlich ist des Weiteren eine zwischen den Parteien bestehende Rechtsbeziehung, die es mit sich bringt, dass der Berechtigte in entschuldbarer Weise über Bestehen oder Umfang seines Rechts im Ungewissen ist.[721]

Der Umstand, dass viele Anbieter von Software (z. B. *Microsoft* für „Office"-Programme, *Amazon* u. a.) und von digitalen Inhalten (z. B. *Apple/iTunes*, *Google* [*Google Play Books/Google Play Music* u. a.], *Thalia*, *Amazon/Kindle*) nach deren Erwerb erneute Downloads zum privaten Gebrauch zulassen, spricht dafür, dass der informationstechnische Vorgang eines Downloads als solcher für Anbieter mit einem eher geringen Aufwand einhergeht, also „unschwer" möglich ist. Nach geltendem Recht wird man jedoch nach Vertragserfüllung seitens des Anbieters durch Ermöglichen eines vertraglich vereinbarten einmaligen Downloads keine Rechtsbeziehung mehr annehmen können, aus welcher der Nutzer nach dem in seiner Sphäre eingetretenen Datenverlust Ansprüche auf einen zweiten Download geltend machen kann.

Ein Anspruch des Nutzers auf einen zweiten Download bei Datenverlust in seiner Sphäre setzt somit die Schaffung einer eigenständigen gesetzlichen Anspruchsgrundlage voraus. Zugunsten des Nutzers müsste unter Einschränkung der Vertragsfreiheit und unter Durchbrechung des Grundsatzes, dass der Verkäufer eine vereinbarte Hauptleistung nur einmal zu erbringen hat (Übergabe der Kaufsache und Verschaffung des Eigentums bzw. – beim Rechtskauf – Verschaffung einer dauerhaften Rechtsposition), ein nicht abdingbarer Anspruch auf eine wiederholte Leistung des Anbieters vorgeschrieben werden.

---

[719] Vgl. BGH, Urt. v. 23.4.1981 – VII ZR 196/80, Tz. 12, NJW 1981, 1779.
[720] Vgl. dazu Palandt/*Grüneberg*, BGB, § 242 Rn. 23, 25.
[721] Vgl. zum Ganzen Palandt/*Grüneberg*, BGB, § 260 Rn. 4.

Eine solche auf den Erwerb digitaler Inhalte im Wege des Downloads bezogene Sonderregelung lässt sich im Ergebnis nicht rechtfertigen. Es gibt eine Vielzahl an Sachverhalten, die hinsichtlich der Interessenlage gleichgelagert sind, ohne dass das geltende bürgerliche Recht den Anbieter verpflichtet, seine Hauptleistung unter dem Aspekt erneut zu erbringen, dass dies für ihn mit keinem Aufwand verbunden ist.

Verpasst ein Verbraucher aus Gründen, die nicht in der Sphäre des Unternehmers liegen, einen fest gebuchten Flug oder eine mit Zugbindung gebuchte Bahnfahrt, ist der Unternehmer nicht deshalb verpflichtet, den Verbraucher zu einem anderen Termin zu befördern, weil in anderen Beförderungsmitteln noch Plätze verfügbar sind und durch die Beförderung zu einem anderen Zeitpunkt keine oder nur unerhebliche zusätzliche Kosten verursacht werden. Ebenso verhält es sich mit einer Veranstaltung (Konzert, Filmvorführung o. a.) zu einem bestimmten Termin, für die ein Verbraucher Eintrittskarten erworben hat, die er aber aus in seiner Sphäre liegenden Gründen nicht wahrnimmt. Findet später eine inhaltsgleiche Veranstaltung desselben Anbieters statt, kann der Verbraucher nicht deshalb einen kostenfreien Zutritt verlangen, weil dies für den Veranstalter mit keinen bzw. keinen messbaren Mehrkosten verbunden ist.

Die gesetzliche Verankerung eines schuldrechtlichen Anspruchs auf einen erneuten Download durch Vertrag erworbener digitaler Inhalte zum rezeptiven Werkgenuss würde sich mithin nicht in das geltende Vertragsrecht einfügen.

Abgesehen davon erscheint auch zweifelhaft, ob es für einen solchen Anspruch gegenwärtig ein praktisches Regelungsbedürfnis gibt. Unterstellt man, dass die Möglichkeit eines wiederholten Downloads ein für die Kaufentscheidung von Verbrauchern wesentliches Leistungsmerkmal ist, können sich Anbieter im Wettbewerb um Käufer dadurch hervorheben, dass sie diese Möglichkeit – sei es auch ohne einen Rechtsanspruch darauf – anbieten. Dass eine Mehrzahl großer Anbieter digitaler Inhalte in ihren Nutzungsbedingungen einen mehrfachen Download zulässt und ein solches erneutes Herunterladen auch praktisch keine Schwierigkeiten aufwirft, spricht dafür, dass es sich insoweit um ein Kriterium handelt, das für Verbraucher bei der Wahl des Anbieters eine relevante Rolle spielt und aufgrund des Wettbewerbs der Anbieter um Kunden berücksichtigt wird.

VII. Empfehlungen

Die geltenden *Widerrufsregelungen* sind mit Bezug auf den Erwerb digitaler Inhalte zum rezeptiven Werkgenuss im Wege des Downloads *sachgerecht und ausgewogen*. Für *Änderungen* – insbesondere für die Einführung eines Anspruchs, digitale Inhalte vor dem Kauf online zu erproben – besteht *kein Anlass*.

Die geltenden bürgerlich-rechtlichen Bestimmungen zum *Abschluss von Verträgen* und zum *Minderjährigenschutz* werfen mit Bezug auf den über das Internet erfolgenden Erwerb digitaler Inhalte zum rezeptiven Werkgenuss im Wege des Downloads keine besonderen Schwierigkeiten auf.

Die Regelungen des geltenden Schuldrechts führen mit Bezug auf Verträge über den Erwerb digitaler Inhalte zum rezeptiven Werkgenuss im Wege des Downloads zu sach- und interessengerechten Lösungen. Es bedarf keiner Rechtsänderungen, damit die dem geltenden Schuldrecht zugrundeliegenden gesetzgeberischen Wertungsentscheidungen bei Verträgen über den Erwerb digitaler Inhalte zum Tragen kommen.

Für Regelungen, welche Verbrauchern einen Anspruch darauf gewähren, im Wege eines Downloads erworbene digitale Inhalte ohne Bindung an ein bestimmtes Gerät oder technisches System zu nutzen, ist das *bürgerliche Recht nicht der richtige Regelungsort.*

Die gesetzliche Verankerung eines schuldrechtlichen Anspruchs auf einen erneuten Download vertraglich erworbener digitaler Inhalte zum rezeptiven Werkgenuss würde sich nicht in das geltende Vertragsrecht einfügen.

I. WAP-Billing und Zahlungswege im Internet

I. Allgemeines

Zu differenzieren ist zunächst zwischen mobilen Zahlungssystemen (Bezahlen mit dem Mobiltelefon über NFC [Near Field Communication]), die hier nicht beleuchtet werden sollen, und Zahlungswegen, mit denen Waren oder Dienste online bezahlt werden. Neben die klassischen Varianten der Rechnungstellung, der Zahlung per Kreditkarte, des Lastschrifteneinzuges oder der Nachnahmelieferung sind andere Methoden getreten, die die Abwicklung von Geschäften erleichtern sollen. Dazu zählen Bezahldienste wie Paypal und Paydirekt sowie Zahlungsauslösedienste wie SOFORT Überweisung oder GiroPay, aber auch Ratenzahlungsdiensteanbieter (z. B. RatePAY). Im Bereich des Mobilfunks gibt es zudem die Möglichkeit des sog. WAP-Billing, bei der Diensteanbieter ihre Rechnungsposition über die Telefonrechnung des Anschlussbetreibers gegenüber dem Anschlussinhaber geltend machen.

Davon zu trennen sind Methoden, die es ermöglichen, Verträge online abzuschließen. Hierzu zählen die sog. In-App-Käufe, bei denen im Rahmen einer meist kostenlos angebotenen App (Application Software) Leistungen gegen Entgelt „zugebucht“ werden können. Probleme ergeben sich in diesem Zusammenhang weniger bei den Zahlungswegen, die in der Regel über die oben dargestellten Methoden erfolgen, als vielmehr im Bereich des wirksamen Vertragsschlusses unter Einhaltung der verbraucherschützenden Vorschriften (z. B. der Buttonlösung) und insbesondere in wettbewerbsrechtlicher Hinsicht.

Von diesen Themenkomplexen wiederum zu trennen sind die virtuellen Währungen, die im nächsten Abschnitt beleuchtet werden.

II. Bezahldienste

Hinter diesen Modellen stehen klassische Zahlungsmethoden, wie die Zahlung im Lastschriftverfahren, über Kreditkarte oder per (Online-)Überweisung. Tatsächlich weisen diese Zahlungsmethoden in der Praxis kaum Probleme auf. Beim Lastschriftverfahren ist die Problemlosigkeit ohne Weiteres dadurch zu erklären, dass in der Regel das SEPA-Basislastschriftverfahren verwendet wird, in dessen Rahmen der Zahlungspflichtige die Möglichkeit hat, innerhalb einer Frist von acht Wochen ab dem Tag der Belastungsbuchung ohne Angabe von Gründen die Erstattung des Zahlungsbetrags zu verlangen. Macht er von diesem bedingungslosen Erstattungsrecht Gebrauch, wird die Zahlung zurückgebucht. Derjenige, der sich auf einen Zahlungsanspruch beruft, muss diesen auf konventionellem Weg durchsetzen.

Bei sog. Zahlungsauslösediensten wird dem Zahlungsauslösedienstleister lediglich der Zugang zum Zahlungskonto des Zahlungspflichtigen eröffnet. Durch diesen Zugang kann der Zahlungsauslösedienstleister die Zahlung elektronisch einleiten und dem Zahlungsempfänger die Sicherheit geben, dass das Geld auf dem

Weg zu ihm ist. Dafür soll künftig in Umsetzung der Zweiten Zahlungsdiensterichtlinie auch eine gesetzliche Grundlage geschaffen werden.[722]

III. WAP-Billing

Beim WAP-Billing handelt es sich um ein Verfahren, dass es Nutzern von Mobilfunkgeräten mit mobiler Datenverbindung erlaubt, Online-Dienstleistungen (z. B. den Zugang zu einem digitalen Zeitungsprodukt oder einen Video-Download) bequem über die Rechnung des Mobilfunkanbieters zu bezahlen, ohne dem Dienstleister (sog. Drittanbieter) Zahlungsdaten übermitteln zu müssen.[723]

1. Technischer Hintergrund[724]

Das WAP-Billing beruht auf einer Besonderheit des sog. „Wireless Application Protocols“ (WAP). Dieser (mittlerweile überholte) Technologie-Standard dient dazu, Internetseiten für das Surfen über eine mobile Datenverbindung am Mobiltelefon oder am Tablet zu optimieren. Ruft ein Nutzer eine WAP-Seite, die in der Regel von Internetseiten, die andere Aufzeichnungs- und Protokollstandards (z. B. Hypertext Markup Language - HTML) verwenden, optisch nicht zu unterscheiden ist, über eine mobile Datenverbindung auf, hat der Webseiten-Betreiber die Möglichkeit, die sog. „Mobile Subscriber Integrated Services Digital Network Number“ (MSISDN) des Besuchers auszulesen. Diese Nummer ist der SIM-Karte des verwendeten Mobiltelefons fest zugeordnet und ermöglicht es somit, den Mobilfunkteilnehmer zu identifizieren. Sie gibt ferner Aufschluss darüber, bei welchem Mobilfunkanbieter der Nummerninhaber als Kunde registriert ist. Der WAP-Standard kann allerdings nur dann eingesetzt werden, wenn das Telefon den Internet-Datentransfer über eine Mobilfunkverbindung abwickelt. Wird hingegen eine WLAN-Verbindung genutzt, kann dieser Protokollstandard nicht genutzt und die MSISDN durch den Drittanbieter nicht über das Internet ausgelesen werden.

2. Rechtlicher Hintergrund

Das eigentliche Abrechnungsverfahren wird über einen sog. WAP-Billing-Prozess abgewickelt, in dessen Ergebnis die Rechnungsposition des Drittanbieters in die Telefonrechnung des Anschlussinhabers einfließt:

Hat der Drittanbieter die Telefonnummer des Anschlussinhabers – wie dargestellt – erlangt, dann kann er, wenn er mit dem (Mobil-) Telekommunikationsanbieter (genauer: dem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten) einen entsprechenden Inkasso- oder Factoringvertrag geschlossen hat,

---

[722] Entwurf eines Gesetzes zur Umsetzung der Zweiten Zahlungsdiensterichtlinie, BR-Drs. 158/17.

[723] *Wegner*, Betrugsstrafbarkeit bei Missbrauch des „WAP-Billing“-Verfahrens, NStZ 2016, 455.

[724] Vgl. zu diesem Absatz *Wegner*, Betrugsstrafbarkeit bei Missbrauch des „WAP-Billing“-Verfahrens, NStZ 2016, 455.

diese Nummer dem Telekommunikationsanbieter mit der jeweiligen Rechnungsposition und der Behauptung eines entsprechenden vertraglichen Anspruches übermitteln. Der Telekommunikationsanbieter zieht dann die Forderung über die Telefonrechnung beim Anschlussinhaber ein. Diese Möglichkeit ist im Gesetz – mit Ausnahme der allgemeinen Regelungen zur Forderungsabtretung in §§ 398 ff. BGB – zwar nicht ausdrücklich geregelt, weshalb die Anbieter häufig ein solches Recht in den Allgemeinen Geschäftsbedingungen mit dem Anschlussinhaber vereinbaren. Allerdings setzen die §§ 45d Abs. 3, 45h, 45k Abs. 2 S. 3 und 45p Telekommunikationsgesetz (TKG) voraus, dass der Anbieter grundsätzlich berechtigt ist, Entgelte für Leistungen Dritter in die Rechnung aufzunehmen. Das rechnungstellende Unternehmen muss in diesen Fällen neben den Informationen nach § 45h Abs. 1 TKG den Rechnungsempfänger gemäß § 45h Abs. 3 TKG auch darauf hinweisen, dass dieser berechtigt ist, begründete Einwendungen gegen einzelne Forderungen zu erheben.

Bezahlt der Anschlussinhaber die Rechnung nicht, hat der Telekommunikationsanbieter nach § 45k Abs. 2 S. 1 TKG grundsätzlich das Recht, den Anschluss zu sperren, wenn sich der Teilnehmer mit Zahlungsverpflichtungen von mindestens 75 EUR in Verzug befindet und der Telekommunikationsanbieter die Sperre zwei Wochen zuvor schriftlich angedroht hat. Gemäß § 45k Abs. 2 S. 2 TKG dürfen allerdings Forderungen im Rahmen von § 45k Abs. 2 S. 1 TKG dann nicht berücksichtigt werden, wenn der Teilnehmer gegen diese schlüssige Einwendungen form- und fristgerecht vorgetragen hat. Dies gilt nach § 45k Abs. 2 S. 3 TKG ebenso für nicht titulierte Forderungen Dritter. Nach der Intention des Gesetzgebers ist es insoweit ausreichend, dass der Anschlussinhaber schlicht widerspricht; *schlüssige* Einwände muss er gegen die Forderungen von Drittanbietern – auch wenn diese zwischenzeitlich an den Telekommunikationsanbieter abgetreten wurden – nicht geltend machen. In der Begründung zum Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen vom 4. Mai 2011 (BT-Drs. 17/5707, 67) heißt es:

> *„Durch die Änderungen in Absatz 2 Satz 2 und Satz 3 werden die Anforderungen an die Einbeziehung von – auch abgetretenen – Forderungen Dritter in die Berechnung der Zahlungsverpflichtungen, auf Grund derer eine Sperre zulässig ist, erhöht. Diese Forderungen müssen, soweit sie bestritten sind, tituliert sein, um bei der Berechnung berücksichtigt zu werden. Dies ist deswegen sachgerecht, weil dem Teilnehmer ansonsten zur Abwendung einer Sperre zugemutet würde, gegenüber dem Rechnung stellenden Unternehmen Ausführungen zu behaupteten Forderungen zu machen, die ihre Grundlage gar nicht in einem vertraglichen Verhältnis zu dem Rechnung stellenden Unternehmen, sondern zu dritten Unternehmen haben. Regelmäßig können Gläubiger gegen Schuldner erst nach Erlangung eines Titels vollstrecken. Es erscheint unverhältnismäßig, dass ihnen abweichend davon das scharfe Instrument einer Sperre im Sinne des*

§ 45k gewährt wird, wenn sie ihre Forderung auf die Telefonrechnung des Schuldners setzen lassen."

3. Problemaufriss

Bei dem international auch als „Cramming" oder „Mobile Cramming" bekannten Phänomen beklagen Verbraucher, dass in ihren Mobilfunkrechnungen „Entgelte für Leistungen Dritter" abgerechnet werden, die sie nicht in Anspruch genommen haben. Nach einer vom BMJV in Auftrag gegebenen Studie ist jeder achte Mobilfunknutzer bereits einmal von unzulässigem WAP-Billing betroffen gewesen.[725] Die in Rechnung gestellten Beträge betragen auffallend häufig 4,99 EUR pro Woche oder auch schon 2,99 EUR pro Tag. Die Verbraucher berichten übereinstimmend, dass sie sich nicht erklären könnten, wie sie ein solches Abo abgeschlossen haben könnten. Tatsächlich ist für die Verbraucherzentralen nur in Einzelfällen ein wirksamer Vertragsschluss nachvollziehbar. Hinweise auf die vorgeschriebene Widerrufsbelehrung finden sich regelmäßig nicht. Oftmals versichern die Betroffenen, auch keinen Preis oder Allgemeine Geschäftsbedingungen gesehen zu haben. Vielmehr haben der jeweilige Anschlussinhaber oder dessen minderjährige Kinder (bewusst oder unbewusst) nur auf einen – etwa in einer SMS, einem Werbebanner oder einer Softwareapplikation (App) enthaltenen – Link geklickt. Der dahinter stehende Anbieter unterstellt damit den Abschluss eines Abonnement-Vertrages über (nicht selten fragliche) Leistungen.[726] Auch dann, wenn die Betroffenen der Rechnungsposition widersprechen und die Rechnung anteilig kürzen, setzen die Telekommunikationsanbieter nach Erfahrungen der Verbraucherzentralen den Anspruch durch und sperren oftmals den Mobilfunkanschluss oder drohen eine solche Sperrung zumindest an, was bei den meisten Anschlussinhabern ausreicht, um sie zur Zahlung zu bewegen. Nach dem Ergebnis der vom BMJV in Auftrag gegebenen Studie hat der Mobilfunkanbieter den Anschluss in immerhin 18 Prozent der Fälle gesperrt, in denen der Verbraucher mit einem Widerruf der Lastschrift wegen einer bestrittenen Drittanbieterforderung auf die Weigerung des Mobilfunkanbieters, den strittigen Betrag zu erstatten, reagierte.[727] Ferner verweisen die Mobilfunkanbieter bei Einwendungen häufig[728] auf den Drittanbieter oder darauf, dass sie den Drittanbieter auf die Anforderungen für einen wirksamen Vertrag hingewiesen hätten und deshalb ein Einwand des Anschlussinhabers, er habe auf der Internetseite des Drittanbieters keinen Hinweis darauf wahrgenommen, dass er sich zu einer Zahlung verpflichte, nicht zutreffen könne. Dem Anschlussinhaber bleibt dann nur die Möglichkeit, gegen

---

[725] YouGov 2016 – Verbraucherbefragung WAP-Billing/Ergebnisbericht für das BMJV, S. 4.
[726] Vgl. Pressemitteilung der Verbraucherzentrale Sachsen, http://www.verbraucherzentrale-sachsen.de/whatsapp-whatsabo; *Bleich*, WAPzocke – Mit Smartphone-Abofallen wird weiter Kasse gemacht, C't 24/11, http://www.heise.de/ct/inhalt/2011/24/.
[727] YouGov 2016 – Verbraucherbefragung WAP-Billing/Ergebnisbericht für das BMJV, S. 34.
[728] In 36 Prozent der Beschwerdefälle hat der Mobilfunkanbieter den Kunden an den Drittanbieter verwiesen (YouGov 2016 – Verbraucherbefragung WAP-Billing/Ergebnisbericht für das BMJV, S. 33).

eine (angedrohte) Sperre eine einstweilige Anordnung bei Gericht zu beantragen. Hiervon wird er regelmäßig wegen der letztlich verhältnismäßig geringen Beträge absehen und stattdessen die Forderung begleichen. Diese Vermutung wird durch die äußerst geringe Anzahl an gerichtlichen Verfahren in diesem Bereich bestätigt. Dass sich Verbraucher gegen eine Sperre des Telefonanschlusses mit einer einstweiligen Anordnung gewährt hätten, wurde von den Gerichten nicht berichtet. Auch die Zahl der Verfahren, in denen es um Forderungen von Drittanbietern geht, ist überschaubar. Von den Gerichten wurde dazu berichtet, dass die Forderungen nahezu ausschließlich von den Telefonanschlussanbietern geltend gemacht wurden.

Die vorhandenen gesetzlichen Schutzmechanismen erscheinen vor diesem Hintergrund nicht ausreichend, um Anschlussinhaber hinreichend gegen unberechtigte Forderungen zu schützen. Als problematisch erweist sich nicht nur das Agieren unseriöser Drittanbieter, denen mit einem WAP-Billing-Prozess eine einfache Möglichkeit eröffnet wird, unbegründete Forderungen erfüllt zu erhalten. Auch die Formulierung in § 45k Abs. 2 S. 2 und 3 TKG, wonach nicht titulierte Forderungen nur dann außer Betracht bleiben, wenn der Anschlussinhaber seine Einwände gegen die Forderung *schlüssig* begründet und dies „ebenso“ für Forderungen Dritter gilt, eröffnet den Telekommunikationsanbietern einen vermeintlichen Bewertungsspielraum, den diese für sich nutzen und der zu nicht unerheblichen Rechtsunsicherheiten führt. Dass auch einige Gerichte die Auffassung vertreten, der Kunde müsste Einwendungen gegen die Forderungen des Drittanbieters gemäß § 45k Abs. 2 S. 2 und 3 TKG *schlüssig* begründen, obwohl dies nach dem Willen des Gesetzgebers gerade nicht gewollt war (vgl. die Ausführungen oben), spricht für ein Klarstellungsbedürfnis.

Derzeit verspricht allein die Einrichtung einer Drittanbietersperre einen wirksamen Schutz vor der unberechtigten und unerwünschten Inanspruchnahme durch Drittanbieter. Der Verbraucher hat gemäß § 45d Abs. 3 TKG einen Anspruch auf Einrichtung einer Drittanbietersperre; über diesen Anspruch muss er nach § 43a Abs. 1 Nr. 14 TKG im Vertrag in klarer, umfassender und leicht zugänglicher Form informiert werden. Gleichwohl haben umfangreiche Aufklärungsmaßnahmen in einschlägigen Publikationen nicht zu einer spürbaren Verbesserung der Situation geführt. Problematisch erscheint insofern auch, dass der Verbraucher selbst aktiv werden muss, um sich effektiv zu schützen. Hierzu hat er regelmäßig erst dann Veranlassung, wenn er bereits unberechtigt in Anspruch genommen wurde. Häufig verlangen die Anbieter zur Einrichtung der Drittanbietersperre eine schriftliche Erklärung oder einen entsprechenden Anruf bei ihrer Servicehotline. Hierdurch wird aber der Anschlussinhaber auf einen anderen Weg verwiesen, als den, über den der Anbieter selbst kommuniziert (das Internet). Der Nachteil einer Drittanbietersperre liegt allerdings darin, dass der Anschlussinhaber in der Regel von dem Zahlungsmodell WAP-Billing insgesamt, d. h. auch gegenüber seriösen Anbietern, ausgeschlossen ist.

4. Lösungsmöglichkeiten

Dieser Hintergrund spricht für die Notwendigkeit, den dargestellten Zahlungsprozess für die Anschlussinhaber daraufhin zu überprüfen, diesen rechtssicherer und transparenter zu gestalten. Die 12. Verbraucherschutzministerkonferenz teilt diesen Befund und hat am 22. April 2016 unter den Topoi „Telekommunikation: Schutz vor unseriösen Drittanbieterabrechnungen verbessern“ und „Schutz vor Drittanbieterabrechnungen auf Mobilfunkabrechnungen“ einen entsprechenden Beschluss gefasst.[729]

Folgende Lösungsmöglichkeiten können in Betracht gezogen werden:

a. Voreinstellung einer Drittanbietersperre

Ein möglicher Ansatzpunkt zur Entschärfung der Problematik könnte darin gesehen werden, dass das Inkasso durch Drittanbieter generell nur auf *ausdrücklichen* Kundenwunsch und *im Einzelfall* aktiviert würde. Dies könnte durch ein grundsätzliches Verbot, Forderungen von Drittanbietern über die Telefon- oder Mobilfunkrechnung einzuziehen, soweit nicht der Verbraucher in jedem Einzelfall zugestimmt hat, gewährleistet werden. Die Telekommunikationsanbieter wären dann gehalten, dieses Verbot durch geeignete technische Vorkehrungen umzusetzen.

Diese Möglichkeit wird auch von der Verbraucherschutzministerkonferenz favorisiert, indem sie die Bundesregierung um Prüfung einer gesetzlichen Regelung bittet, nach der künftig beim Abschluss von Telekommunikationsverträgen eine Drittanbietersperre voreingestellt wird und eine nachträgliche Änderung während der gesamten Vertragsdauer jederzeit kostenlos möglich sein soll (vgl. Beschluss der VSMK unter Ziffer 2). Ferner wird die Bundesregierung aufgefordert, darauf hinzuwirken, dass neben der gesetzlichen pauschalen Drittanbietersperre künftig auch selektive Sperren kostenfrei möglich sind und die Transparenz bei der automatischen Abbuchung von Dienstleistungen Dritter verbessert wird (vgl. Beschluss der VSMK unter Ziffer 3).

Der Bundesrat hat dieses Anliegen – allerdings ohne Beteiligung der Justizressorts – ebenfalls aufgegriffen und anlässlich der Stellungnahme zum Entwurf eines Dritten Gesetzes zur Änderung des Telekommunikationsgesetzes[730] für Neuverträge eine Opt-in-Lösung durch Einfügung eines § 45d Abs. 4 TKG-E vorgeschlagen.[731] Demnach soll der Telefonanbieter verpflichtet sein, die Identifizierung des Mobilfunkanschlusses des Verbrauchers zur Inanspruchnahme und Abrechnung einer neben der Verbindung erbrachten Leistung unentgeltlich netzseitig zu sperren. Ferner soll der Anbieter verpflichtet sein, diese Sperre unverzüg-

---

[729] https://www.verbraucherschutzministerkonferenz.de/documents/Endgueltiges_Protokoll_VSMK_2016.pdf, TOP 35 und 36, S. 61 f.
[730] BR-Drs. 436/16.
[731] Vgl. Ziffer 3 der BR-Drs. 436/16 (B).

lich und unentgeltlich auf Verlangen des Verbrauchers insgesamt oder für bestimmte Anbieter oder Leistungen aufzuheben. Für bereits bestehende Verträge soll die bislang vorgesehene Opt-out-Lösung um einen Anspruch auf unverzügliche und unentgeltliche Ausnahme bestimmter Anbieter oder Leistungen von der Sperrung ergänzt werden.

Der Bundestag ist dem Vorschlag des Bundesrates indes nicht gefolgt. Vielmehr ist mit einem neuen § 45d Abs. 4 TKG gesetzlich (nur) verankert worden, dass die Bundesnetzagentur Verfahren festlegt, *die die Anbieter öffentlich zugänglicher Mobilfunkdienste und die Anbieter des Anschlusses an das öffentliche Mobilfunknetz anwenden müssen, um die Identifizierung eines Mobilfunkanschlusses zur Inanspruchnahme und Abrechnung einer neben der Verbindung erbrachten Leistung zu nutzen. Diese Verfahren sollen den Teilnehmer wirksam davor schützen, dass eine neben der Verbindung erbrachte Leistung gegen seinen Willen in Anspruch genommen und abgerechnet wird.*[732] Dieses sog. Redirect-Verfahren, bei dem der Kunde zum Vertragsabschluss über eine Drittanbieterleistung auf eine Internetseite des Mobilfunkanbieters umgeleitet wird, wird bereits vereinzelt praktiziert. Es bietet allerdings keinen hinreichenden Schutz gegen unseriöse Drittanbieter bzw. unberechtigte Abrechnungen. Zu Rechtsunsicherheiten könnte es im Verhältnis von § 45d Abs. 4 TKG-E zu § 45k Abs. 2 S. 2 und 3 TKG kommen. Denn wie oben dargelegt, gehen bereits bisher manche Telekommunikationsanbieter davon aus, dass einfaches Bestreiten der Drittanbieterforderung nicht ausreichend sei. Bei verpflichtender Einführung des Redirect-Verfahrens könnte diese Argumentation Vorschub erhalten. Das Problem der faktischen Beweislastumkehr (siehe dazu sogleich im nächsten Absatz) dürfte damit jedenfalls nicht gelöst werden.

b. Widerspruchsmöglichkeit

Nach dem Wortlaut von § 45h Abs. 3 TKG kann der Rechnungsempfänger *begründete Einwendungen* gegen einzelne Forderungen erheben. Nach § 45k Abs. 2 S. 3 TKG bleiben nicht titulierte, *bestrittene Forderungen* Dritter bei der Berechnung des Betrages, mit dessen Zahlung sich der Teilnehmer im Verzug befindet, außer Betracht. Die in diesen Vorschriften bereits angelegte Widerspruchsmöglichkeit könnte konsequenter ausgestaltet werden. Denn die in § 312j Abs. 4 BGB vorgesehene Beweislastverteilung wird durch die benannten Vorschriften des TKG zumindest in ihrer praktischen Anwendung überlagert. Der Verbraucher muss nämlich nach der Lesart mancher Telekommunikationsanbieter schlüssige oder sogar begründete Einwände gegen die Drittanbieterforderung geltend machen, ohne dass dieser seinerseits die Einhaltung der Vorgaben aus § 312j Abs. 3 BGB (sog. Buttonlösung) belegen muss.

Insofern könnte sich eine klarstellende Regelung dergestalt anbieten, dass eine Forderung des Drittanbieters, welcher der Anschlussinhaber binnen einer bestimmten Frist widerspricht, nicht über die Telefonrechnung eingezogen werden

---

[732] BT-Drs. 18/11811.

darf. Anders als nach derzeit gültiger Rechtslage müsste das Telekommunikationsunternehmen eine dergestalt bestrittene Forderung nicht nur bei der Frage unberücksichtigt lassen, ob der Anschluss wegen eines Zahlungsrückstands gesperrt werden kann, sondern dürfte die Forderung gegenüber dem Anschlussinhaber überhaupt nicht mehr im Rahmen des regulären Abrechnungsmodus einziehen. Die Telefonrechnung wäre um diese Position zu korrigieren und eventuelle Zahlungen zurück zu überweisen. Dem Drittanbieter oder – im Fall der Forderungsabtretung – dem Telekommunikationsunternehmen bliebe dann die Möglichkeit, eine berechtigte Forderung gegenüber dem Anschlussinhaber auf dem üblichen gerichtlichen Weg durchzusetzen. Insoweit könnten auch die bereits jetzt gesetzlich vorgesehenen Schutzmechanismen Wirkung entfalten, weil der Dritt- oder Telekommunikationsanbieter dann verpflichtet wäre, den wirksamen Vertragsschluss zu beweisen (z. B. die Einhaltung der Vorgaben des § 312j Abs. 3 BGB).

Im Ergebnis wäre dieses Verfahren für den Anschlussinhaber mit dem bedingungslosen Erstattungsrecht bei Lastschriften vergleichbar. In diesem Verfahren erteilt der Zahlungspflichtige dem Zahlungsempfänger (dies wäre vorliegend der Drittanbieter) ein Lastschriftmandat. Der Zahlungsdienstleister des Zahlungsempfängers zieht dann über den Zahlungsdienstleister des Zahlungspflichtigen den Betrag ein. Der Zahlungsdienstleister des Zahlungspflichtigen belastet zwar nunmehr dessen Konto (und reicht den Betrag an den Zahlungsdienstleister des Zahlungsempfängers weiter, der diesem den Betrag gutschreibt). Der Zahlungspflichtige kann den Zahlungsbetrag aber innerhalb einer Frist von acht Wochen erstattet verlangen (§ 675x Abs. 2 BGB i. V. m. Nummer 2.5 der Musterbedingungen des Bankenverbandes über die Bedingungen für Zahlungen mittels Lastschrift im SEPA-Basislastschriftverfahren [jeweils Stand: 1. Februar 2016]). Der Zahlungsdienstleister des Zahlenden erhält daraufhin den Betrag vom Zahlungsdienstleister des Zahlungsempfängers erstattet, der seinerseits den dem Empfänger gutgeschriebenen Betrag wieder zurückbucht. Allerdings soll mit der Widerspruchsmöglichkeit nicht die Bank zur Rückbuchung verpflichtet werden, sondern der Telekommunikationsanbieter soll bei einem entsprechenden Widerspruch die Rechnung insoweit korrigieren, den entsprechenden Betrag nicht einfordern bzw. bereits gezahlte Beträge an den Verbraucher zurückerstatten.

Auch die Verbraucherschutzministerkonferenz sieht in der Einführung eines Widerspruchsrechts eine Möglichkeit, den Mechanismus der Abbuchung von unberechtigten Drittforderungen über die Telefonrechnung außer Kraft zu setzen (vgl. Beschluss der VSMK unter Ziffer 6).

IV. In-App-Käufe

Mit In-App-Käufen können, wie es der Name bereits vermuten lässt, bestimmte Dinge innerhalb der App selbst gekauft und bezahlt werden. Auf diese Weise kann man bspw. Premium-Funktionen oder Verbesserungen in Spielen freischalten oder sogar Abos abschließen. Die Kaufabwicklung erfolgt über den jeweiligen App-Store und die dort hinterlegte Zahlungsmethode.

Probleme ergeben sich hinsichtlich der Wirksamkeit des Vertrages und insbesondere in wettbewerbsrechtlicher Hinsicht[733], wenn die zunächst kostenlos angebotene App nur durch Hinzubuchen kostenpflichtiger Parameter überhaupt genutzt werden kann. Die auftretenden Schwierigkeiten im Zusammenhang mit der Wirksamkeit der geschlossenen In-App-Käufe dürften mit den geltenden Regelungen, insbesondere § 312j BGB, sachgerecht gelöst werden können.

V. Empfehlungen

Zahlungswege im Internet, mit denen Waren oder Dienste online bezahlt werden (Bezahldienste, Direktüberweisungsverfahren und Ratenzahlungsdiensteanbieter), begründen derzeit – abgesehen von der Umsetzung der Zweiten Zahlungsdienstrichtlinie in deutsches Recht – keinen gesetzgeberischen Handlungsbedarf. Zahlungsauslösedienste sollen künftig in Umsetzung der Zweiten Zahlungsdiensterichtlinie gesetzlich geregelt werden.

Die Abrechnung über Leistungen von Drittanbietern im Rahmen der Telefon- oder Mobilfunkrechnung weist ein Defizit im Verbraucherschutz auf. Die geltenden gesetzlichen Regelungen reichen nicht aus, um dem Missbrauch der Abrechnungsmethode durch unseriöse Drittanbieter zu begegnen.

Gesetzliche Regelungen sollen den Verbraucher wirksam vor ungewollten und rechtsgrundlosen Zahlungen im Rahmen der Abrechnung von Drittanbieterleistungen über die Telefon- oder Mobilfunkrechnung schützen. Dabei sollte insbesondere ein grundsätzliches Verbot, Forderungen von Drittanbietern über die Telefonrechnung einzuziehen, soweit nicht der Verbraucher in jedem Einzelfall ausdrücklich zugestimmt hat, ebenso in Betracht gezogen werden wie ein fristgebundenes Widerspruchsrecht gegenüber dem Telekommunikationsanbieter gegen die Einziehung der konkreten Forderung.

Probleme hinsichtlich der Wirksamkeit des Vertrages im Bereich von In-App-Käufen können mit den bestehenden Regelungen, insbesondere § 312j BGB, gelöst werden.

[733] Nicht Gegenstand der Prüfungen der Arbeitsgruppe.

J. Virtuelle Währungen

I. Allgemeines

Mit dem Begriff der virtuellen Währungen werden in Abgrenzung zum elektronischen Geld (digitales Bargeld, das auf einem elektronischen Gerät oder räumlich entfernt auf einem Server gespeichert ist) insbesondere die Kryptowährungen definiert. Sie werden als Tauschmittel verwendet und dürften als alternative Zahlungsmittel zunehmend Bedeutung erlangen. Durch kryptographisch abgesicherte Protokolle und dezentrale Datenhaltung ermöglichen Kryptowährungen bargeldlosen digitalen Zahlungsverkehr ohne Zentralinstanzen wie etwa Banken. An die Stelle eines bedruckten Stücks Papier (Geldschein) oder eines geprägten Stücks Metall (Münze) zur Repräsentation des Tauschwerts tritt der Besitz eines kryptographischen Schlüssels zu einem ebenfalls kryptographisch signierten Guthaben in einer gemeinschaftlichen Buchführung (Blockchain). In der Regel wird dabei eine vorher festgelegte Anzahl an Währungseinheiten durch das gesamte System gemeinschaftlich erzeugt, wobei die Rate vorher festgelegt und veröffentlicht bzw. durch den kryptographischen Modus der Erzeugung limitiert ist.

Die Europäische Kommission definiert in dem Vorschlag für eine Richtlinie zur Änderung der Geldwäscherichtlinie[734] virtuelle Währungen als eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde und nicht zwangsläufig an eine echte Währung angebunden ist, aber von natürlichen oder juristischen Personen als Zahlungsmittel akzeptiert wird und auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann (vgl. Art. 1 Abs. 2 Unterabs. c des Richtlinienvorschlags).

Derzeit existieren ca. 600 virtuelle Währungen, von denen Bitcoin die bekannteste und am weitesten verbreitete ist.[735] In Deutschland wurden bislang lediglich Bitcoin anerkannt. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ordnet Bitcoin als *mit Devisen vergleichbare Rechnungseinheiten im Sinne des § 1 Abs. 11 S. 1 Nr. 7 Kreditwesengesetz (KWG)* ein.[736] Sie sind damit weder gesetzliches Zahlungsmittel noch E-Geld i. S. d. § 1a Abs. 3 Zahlungsdiensteaufsichtsgesetzes (ZAG), Devisen oder Sorten.

Die folgenden Ausführungen beziehen sich deshalb auf Bitcoin.

---

[734] Vorschlag für eine Richtlinie zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinie 2009/101/EG (COM(2016) 450 final).

[735] Entschließung des Europäischen Parlaments vom 26.5.2016 zu virtuellen Währungen (2016/2007(INI)), Erwägungsgrund A.

[736] https://www.bafin.de/DE/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node.html (letzter Abruf 30.3.2017).

II. Technischer Hintergrund

Bitcoin ist eine virtuelle Währung, die in einem dezentralen Netzwerk elektronisch geschaffen und verwahrt wird. Es sind Datenmengen, die dem jeweiligen Nutzer in verschlüsselter Form bereitstehen.[737] Jeder, der am Bitcoin-System teilnehmen möchte, benötigt eine spezielle, frei verfügbare Software (den sog. Bitcoin-Core oder Bitcoin-Client) und einen leistungsfähigen Rechner.[738] Das Gesamtvolumen der Bitcoins ist durch das Protokoll auf 21 Millionen Einheiten begrenzt. Bitcoins können geteilt werden.

Bitcoin-Transaktionen ähneln am ehesten dem Banküberweisungsverfahren.[739] Wie Einlagen auf einem Bankkonto existieren Bitcoins nur in Form von digitalen Datensätzen. Die für den Übertragungsvorgang vom Client in einer so genannten „Wallet-Datei" angelegten Bitcoin-Adressen beinhalten ein aus einem öffentlichen und einem privaten Teil bestehendes kryptografisches Schlüsselpaar. Während der öffentliche Schlüssel zum Empfangen von Beträgen weitergegeben werden kann und als eine Art Kontonummer fungiert, dient der private Schlüssel zur Autorisierung von Transaktionen.[740] Bei einer Transaktion werden aus dem elektronischen Portemonnaie des Absenders (der Wallet) Bitcoins in die elektronische Geldbörse des Empfängers transferiert.[741] Die Übertragung von Bitcoins geschieht über einen Zusammenschluss von Rechnern über das Internet und wird mit einer speziellen Peer-to-Peer-Anwendung abgewickelt.[742] Im Unterschied zu einer Banküberweisung erfolgt die Transaktion also ohne den Umweg über eine zentrale Instanz. Die Zuordnung eines Bitcoins zu einer bestimmten Person erfolgt dezentral auf Basis einer öffentlich dokumentierten Transaktionshistorie (der sog. Blockchain).[743]

Die Nachverfolgbarkeit und Autorisierung des Zahlungsvorgangs werden durch den Einsatz zweier kryptographischer Schlüssel sichergestellt. Einerseits kommt ein privater Schlüssel zum Einsatz, den nur der Inhaber der jeweiligen Bitcoins kennt. Damit werden Transaktionen dieser Bitcoins autorisiert. Vergleichbar ist dieser private Schlüssel mit einer eigenhändigen Unterschrift.[744] Andererseits wird ein öffentlicher Schlüssel benutzt, aus dem die Bitcoin-Adresse abgeleitet

---

[737] *Engelhardt/Klein*, Bitcoins – Geschäfte mit Geld, das keines ist − Technische Grundlagen und zivilrechtliche Betrachtung, MMR 2014, 355.
[738] *Goger*, Bitcoins im Strafverfahren – Virtuelle Währung und reale Strafverfolgung, MMR 2016, 431.
[739] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.
[740] *Beck*, Bitcoins als Geld im Rechtssinne, NJW 2015, 580.
[741] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.
[742] *Heine*, Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining, NStZ 2016, 441.
[743] *Beck*, Bitcoins als Geld im Rechtssinne, NJW 2015, 580.
[744] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.

wird.[745] Dieser ist vergleichbar mit dem Bankkonto eines Empfängers einer Geldtransaktion. Wer also Bitcoins überweisen möchte, muss zunächst die aus dem öffentlichen Schlüssel generierte Empfängeradresse mitgeteilt bekommen, um dann eine bestimmte Zahl von eigenen Bitcoins mit der Empfängeradresse zu einer Transaktion zu verbinden, die er sodann mit seinem privaten Schlüssel signiert.[746]

Mit dem privaten Schlüssel können beliebig viele Transaktionen signiert werden. Dass Bitcoins nur einmal ausgegeben bzw. übertragen werden können, wird durch die Blockchain-Technologie sichergestellt. Neue Transaktionen werden in Blöcken gesammelt und an die Blockchain angehängt. Diese müssen von der Nutzergemeinschaft bestätigt werden.[747] Dies geschieht derart, dass die Nutzer mit dafür vorgesehenen Programmen kryptografische Aufgaben lösen. Wenn das Ergebnis der Aufgabe innerhalb gewisser Parameter liegt, werden der Blockchain neue Transaktionen in Form eines Blocks hinzugefügt und dem Lösenden eine bestimmte Anzahl von Bitcoins als „proof of work" gutgeschrieben. Diese (originäre) Erwerbsform von Bitcoins wird als „Mining" (Schürfen) bezeichnet.[748]

Eine Transaktion kann ohne Angabe persönlicher Daten durchgeführt werden. Gleichzeitig kann jeder Nutzer beliebig viele Schlüsselpaare und damit Pseudonyme haben. Auch für das Einrichten der Konten ist keine Angabe persönlicher Daten, sondern lediglich die Installation einer frei verfügbaren Software nötig. Selbst der Eintausch der Bitcoins in echtes Geld erfordert nicht zwingend die Angabe persönlicher Daten. So kann man die Angabe von Kontodaten zum Empfang des Geldes umgehen, indem man über spezielle Dienste, z. B. Localbitcoins, andere Bitcoin-Nutzer in seiner Umgebung ausfindig macht und sich von ihnen nach Ausführung der Bitcoin-Transaktion bar bezahlen lässt. Die zur Anmeldung erforderliche E-Mail-Adresse kann man vorher als „Wegwerfadresse" bei einem Dienst generieren, der die Identität des Inhabers verschleiert. Die Geheimhaltung der eigenen Identität ist bei Nutzung des Bitcoin-Systems daher weitestgehend möglich.[749]

Die Blockchain-Technologie (auch als Technologie der dezentralen Transaktionsnetzwerke oder Distributed Ledger Technology – DLT – bezeichnet) ermöglicht einerseits die Nachverfolgbarkeit und Verifikation sämtlicher Transaktionen. Sie wird auf den Rechnern aller Nutzer und damit öffentlich, aber dezentral gespeichert und kann online eingesehen werden. Aus ihr ist ersichtlich, dass eine (mit

---

[745] *Kütük/Sorge*, Bitcoin im deutschen Vollstreckungsrecht – Von der „Tulpenmanie" zur „Bitcoinmanie", MMR 2014, 643.

[746] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.

[747] *Kütük/Sorge*, Bitcoin im deutschen Vollstreckungsrecht – Von der „Tulpenmanie" zur „Bitcoinmanie", MMR 2014, 643.

[748] *Beck*, Bitcoins als Geld im Rechtssinne, NJW 2015, 580.

[749] Vgl. zum gesamten Absatz *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.

dem privaten Schlüssel) signierte Transaktion einer bestimmten Menge von Bitcoins auf ein bestimmtes Konto (öffentlicher Schlüssel) überwiesen wurde. Die Blockchain kann man sich als Kontobuch vorstellen, das jede jemals mit Bitcoins getätigte Transaktion enthält und daher einen vollständigen Überblick über die gesamte Historie des Bitcoin-Systems gibt.[750] Sie ist aufgrund ihrer Technologie resistent gegen äußere (manipulative) Einflüsse.

Andererseits ist die Blockchain auch Quelle neuer Bitcoins. Denn wie oben bereits erläutert, werden durch die Fortführung der Blockchain neue Bitcoins generiert. Die dahinter stehenden Algorithmen sind so beschaffen, dass mit steigender Anzahl von erzeugten Einheiten der zur Lösung der Aufgabe erforderliche Rechenaufwand steigt. Gleichzeitig wird auch die Anzahl der ausgegebenen Bitcoin-Einheiten pro Block in bestimmten Zeitabständen reduziert. So wird sichergestellt, dass ein maximales Gesamtvolumen von 21 Millionen Einheiten erzeugt werden kann.[751]

III. Problemfelder

Auf Grund ihrer virtuellen Eigenschaft sind Bitcoins zivilrechtlich schwer einzuordnen. Es handelt sich weder um eine Sache i. S. d. § 90 BGB, da es an der Körperlichkeit fehlt, noch um eine Forderung i. S. d. § 241 Abs. 1 BGB. Denn letztere setzt eine schuldrechtliche Verbindung von Schuldner und Gläubiger voraus, aus der der Gläubiger vom Schuldner etwas verlangen kann.[752]

Kryptowährungen sind aber auch keine sonstigen Rechte. Diese setzen voraus, dass ihr Inhaber von einem oder mehreren Schuldnern ein bestimmtes Verhalten oder Unterlassen verlangen kann (relative Rechte) oder dass der Inhaber von allen ein bestimmtes Verhalten verlangen kann (absolute Rechte).[753] Dies ist bei virtuellen Währungen jedoch nicht der Fall.

Vielmehr manifestiert sich die Inhaberschaft allein in der *faktischen Möglichkeit*, Transaktionen mit seinem privaten Schlüssel zu initiieren und zu signieren. Dennoch spielen Bitcoins im Online-Handel eine Rolle und werden von einer wachsenden Zahl von Online-Shops als Zahlungsmittel akzeptiert. Ihren Wert erhalten Bitcoins ausschließlich durch den Handel. Das bedeutet, dass der Wert nur entsteht und erhalten bleibt, solange es Nutzer gibt, die bereit sind, Bitcoins als Gegenleistung für (reale) Waren oder Dienstleistungen bzw. Geld zu akzeptieren. Einen innewohnenden Wert besitzen Bitcoins nicht.

---

[750] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.
[751] *Beck*, Bitcoins als Geld im Rechtssinne, NJW 2015, 580.
[752] Vgl. *Rückert*, Vermögensabschöpfung und Sicherstellung bei Bitcoins – Neue juristische Herausforderungen durch die ungeklärte Rechtsnatur von virtuellen Währungen, MMR 2016, 295.
[753] Palandt/*Grüneberg*, BGB, Einl. v. § 241 Rn. 5.

1. Online-Handel

Zivilrechtlich relevant ist vor allem der legale Zahlungsverkehr mit Bitcoins im Bereich des E-Commerce. Verträge über Bitcoins sind aufgrund der Vertragsfreiheit prinzipiell wirksam. Fraglich ist allerdings, welche Rechtsbeziehungen bei Bitcoin-Transaktionen ganz allgemein, und wenn neben Händler und Kunden Intermediäre eingeschaltet werden, bestehen sowie welche Normen anwendbar sind. Ferner ist zweifelhaft, auf welche Ansprüche sich die „Rückgabe" von Bitcoins stützen lässt, ob es evtl. einen Rückbuchungsanspruch gibt, und wie Kunden von Online-Händlern bei der Bezahlung mit Bitcoins am besten geschützt werden können.

Die Beantwortung dieser Fragen hängt von der Rechtsnatur der Bitcoins sowie der zugrundeliegenden schuldrechtlichen Verträge ab.

a. Kaufvertrag

Beim Erwerb von Bitcoins gegen Geld scheidet die Annahme eines Kaufvertrages i. S. v. § 433 BGB bereits deshalb aus, weil es sich bei Bitcoins mangels einer Verkörperung nicht um Sachen i. S. v. § 90 BGB handelt. Bei der Bezahlung von Waren mit Bitcoins scheitert die Qualifikation als Kaufvertrag daran, dass es sich bei Bitcoins nicht um Geld handelt (siehe oben).

b. Entsprechende Anwendung von Kaufrecht

Allerdings erklärt § 453 BGB die Vorschriften über den Sachkauf für den Kauf von Rechten und sonstigen Gegenständen für entsprechend anwendbar.

Bitcoins sind aber weder als relative noch als absolute Rechte zu qualifizieren (siehe oben). Mangels Verkörperung kann kein Eigentum an Bitcoins bestehen, § 903 BGB. Ob es sich um Immaterialgüterrechte i. S. d. Urhebergesetzes (UrhG) handeln kann, ist zweifelhaft. Denn einzelne Bitcoins sind weder als persönliche geistige Schöpfung i. S. v. § 2 Abs. 2 UrhG noch als Software i. S. v. § 69a Abs. 1 UrhG einzuordnen. Bitcoins wohnt auch kein Anspruch inne, weil es dafür am Anspruchsgegner (etwa einer ausgebenden Stelle) fehlt. Die Frage nach Rechten an virtuellen Gütern (letztlich digitale Daten) ist bislang ungeklärt und vom Gesetzgeber nicht geregelt.

Allerdings gilt § 453 BGB auch für sonstige Gegenstände. Teilweise wird vertreten, dass virtuelle Gegenstände als Immaterialgüter im Sinne dieser Vorschrift verkauft werden können, soweit sie übertragbar sind.[754]

c. Tausch

Teilweise wird angenommen, der Eintausch von Waren gegen Bitcoins sei als Tausch i. S. d. § 480 BGB zu qualifizieren. Allerdings sind mögliche Objekte eines Tauschvertrags grundsätzlich nur Sachen und Rechte. Lediglich bei einem sehr weiten Verständnis des Tauschobjekts auch als vermögenswertes Gut, das in

---

[754] *Diegmann/Kunz,* Praxisfragen bei Onlinespielen, NJW 2010, 561.

einer von der Rechtsordnung gebilligten Weise übertragen werden kann, ließen sich Verträge, die den Austausch von Waren gegen Bitcoins zum Gegenstand haben, so einordnen.[755]

d. Atypischer Werkvertrag

Vertreten wird, dass es sich bei der Anschaffung von Bitcoins gegen eine Vergütung um einen „atypischen Werkvertrag" handele, was wohl auf der Erwägung beruht, dass bei solchen Vereinbarungen nicht die bloße Bemühung um einen Transfer der Bitcoins, sondern der Erfolg der Bitcoin-Transaktion geschuldet sein muss. Diese Erwägung hilft allerdings nicht weiter, wenn es um Verträge geht, bei denen Waren mit Bitcoins bezahlt werden.[756]

e. Analogien zum Wertpapierrecht

Was den Transaktionsvorgang angeht, ist an die für den konventionellen elektronischen Zahlungsverkehr diskutierten Ansätze wie Abtretungskonstruktionen oder Analogien zum Wertpapierrecht zu denken. Diese sind allerdings sämtlich auf Drei-Personen-Verhältnisse zugeschnitten. Da Bitcoin-Transaktionen Peer-to-Peer ablaufen und es an einem Emittenten fehlt, sind diese Lösungen nicht einfach auf Bitcoins übertragbar.[757]

f. Zwischenergebnis

Die rechtlichen Rahmenbedingungen des Einsatzes von Bitcoins im E-Commerce sind schwer einzuordnen. Eine solche rechtliche Einordnung ist derzeit eher ein rechtstheoretisches Problem, denn Erkenntnisse zu praktischen Schwierigkeiten in diesem Bereich gibt es bislang nicht. Zu beachten ist, dass virtuelle Währungen auch nicht von Jedermann genutzt werden (können), weil dies gewisse Kenntnisse und technische Voraussetzungen (z. B. Anlegen einer Wallet) erfordert und darüber hinaus das Geschäft mit Bitcoins hochspekulativ ist.

Der Wert einer rechtlichen Qualifizierung erscheint auch durch die technischen Gegebenheiten begrenzt. Denn eine einmal getätigte Transaktion kann – ungeachtet etwaiger Ansprüche – tatsächlich nicht rückgängig gemacht werden. Der Verlust des privaten Schlüssels bedeutet den Verlust der Bitcoins. Das System der virtuellen Währung unter Nutzung der Blockchain-Technologie basiert gerade auf der Freiheit von äußeren (auch staatlich regulierenden) Eingriffen, sodass bereits deshalb in zivilrechtlicher Hinsicht kein gesetzgeberischer Handlungsbedarf besteht.

---

[755] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.
[756] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.
[757] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.

2. Haftungsrechtliche Probleme

Bei der Abwicklung von Bitcoin-Transaktionen sind die Haftung und die Risikoverteilung zwischen dem Online-Händler und dem Kunden nicht geklärt. Was geschieht etwa bei einem Datenverlust oder -missbrauch? Zur Beantwortung dieser Frage kommt es auf die Einordnung der Rechtsbeziehungen im Bitcoin-System an. Denn die allgemeinen schuldrechtlichen Regelungen des BGB, insbesondere §§ 280 ff., 320 ff. BGB sind nur so weit anwendbar, wie sie nicht von Spezialregelungen verdrängt werden. Wie oben gezeigt, gelingt bereits die vertragsrechtliche Einordnung nicht ohne Weiteres, weshalb auch Haftungsfragen im Bitcoin-System noch erheblichen Rechtsunsicherheiten unterliegen.[758] Allerdings sind, wie oben bereits erwähnt, bislang keine Erkenntnisse zu derartigen Schwierigkeiten vorhanden. Dies liegt sicherlich auch an der Blockchain-Technologie, die einen Missbrauch oder Verlust nahezu ausschließt. Rechtlicher Regelungsbedarf dürfte deshalb im Zivilrecht nicht bestehen.

3. Zwangsvollstreckung

Angesichts ihres Werts und ihrer zunehmenden Verkehrsfähigkeit stellt sich die Frage, ob und inwieweit auf Bitcoins im Rahmen der Zwangsvollstreckung zugegriffen werden kann. Die Zwangsvollstreckung richtet sich nach den Regelungen der Zivilprozessordnung (ZPO).

a. Anwendbarkeit §§ 808 ff. und 829 ff. ZPO

Mangels Verkörperung können Bitcoins nicht der Vollstreckung in körperliche Sachen nach §§ 808 ff. ZPO unterliegen. Die klassische Forderungsvollstreckung nach §§ 829 ff. ZPO erscheint in Ermangelung einer zentralen ausgebenden Stelle, die als Drittschuldner in Betracht kommt, ebenfalls keine geeignete Grundlage zu sein.

b. Vollstreckung in Bitcoins als andere Vermögensrechte

In Betracht kommt die Vollstreckung in andere Vermögensrechte nach § 857 ZPO. Demnach sind Rechte aller Art als Vermögensrechte pfändbar, die einen Vermögenswert dergestalt verkörpern, dass die Pfandverwertung zur Befriedigung des Gläubigers führen kann.[759] § 857 ZPO beinhaltet eine Auffangnorm, um das Vermögen des Schuldners umfassend als Haftungsgrundlage zu erschließen.[760] Nicht von § 857 ZPO erfasst und unpfändbar sind bloße Befugnisse

---

[758] *Boehm/Pesch*, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung − Eine erste juristische Einordung, MMR 2014, 75.

[759] BGH, Beschl. v. 5.7.2005 – VII ZB 5/05 (juris); BGH, Beschl. v. 20.12.2006 – VII ZB 92/05 (juris).

[760] Prütting/Gehrlein/*Ahrens*, ZPO, § 857 Rn. 1.

oder Handlungsmöglichkeiten[761] und tatsächliche Verhältnisse sowie Vermögensinbegriffe.[762] Geht man davon aus, dass sich die Inhaberschaft, wie oben dargestellt, allein in der faktischen Möglichkeit, Transaktionen mit seinem privaten Schlüssel zu initiieren und zu signieren, manifestiert, mithin eine rein tatsächliche Möglichkeit darstellt, wären virtuelle Währungen nicht pfändbar. Dies erscheint insofern unbefriedigend, als damit eine Möglichkeit eröffnet würde, um zunächst vorhandenes (reales) Vermögen durch Eintausch in eine virtuelle Währung dem Gläubigerzugriff zu entziehen.

c. Tatsächliche Grenzen der Zwangsvollstreckung

Ungeachtet der Frage nach der rechtlichen Einordnung sind der Zwangsvollstreckung aber auch in tatsächlicher Hinsicht Grenzen gesetzt. Denn selbst wenn man durch entsprechende Anwendung von § 857 Abs. 1 ZPO i. V. m. § 836 Abs. 3 ZPO eine Pfändbarkeit und eine daraus resultierende Verpflichtung des Schuldners zur Auskunftserteilung annähme, erscheint eine Vollstreckung gegen den Willen des Schuldners oder ohne dessen Mitwirkung ausgeschlossen. Bislang sind auch keine Entscheidungen zur Erzwingung der Preisgabe der Zugangsinformationen bekannt geworden. Auf Bitcoins gegen den Willen des Inhabers zuzugreifen, begegnet praktischen Schwierigkeiten. Denn zum einen erlaubt der Besitz des kryptographischen Schlüssels es dem Inhaber ungeachtet einer rechtlichen Befugnis, von jedem beliebigen Ort aus über die Bitcoins zu verfügen. Bspw. ist es dem Inhaber trotz Sicherstellung seines Rechners, trotz Arrest- oder Pfändungsanordnung rein tatsächlich zu jeder Zeit möglich, über einen beliebigen Internetzugang über die Bitcoins zu verfügen. Eine solche Verfügung ist ungeachtet ihrer rechtlichen Qualifizierung oder Wirksamkeit rein tatsächlich nicht umkehrbar. Die Vollstreckung wäre gescheitert. Zum anderen setzt jegliche Verfügung über die Bitcoins die Inhaberschaft über den kryptographischen Schlüssel voraus, der in der Wallet hinterlegt ist, die wiederum in der Regel passwortgesichert sein dürfte. Man könnte zwar versuchen, den Schuldner gemäß § 836 Abs. 3 ZPO analog zur Preisgabe des Passwortes zu zwingen, jedoch haben auch diese Zwangsmittel ihre Grenzen. Darüber hinaus hat der Schuldner jederzeit die Möglichkeit, das Passwort nachträglich zu ändern.

d. Praktische Erfahrungen

Praktische Erfahrungen liegen lediglich im Bereich der strafrechtlichen Vermögensabschöpfung vor. Im Ergebnis einer Länderumfrage wurde festgestellt, dass die Verwertung der Bitcoins bislang nur unter Mitwirkung des Inhabers erfolgt ist. Dies dürfte an der oben bereits angedeuteten Schwierigkeit aufgrund der technischen Gegebenheiten liegen.

---

[761] Musielak/*Voit*/*Becker*, ZPO, § 857 Rn. 2a.
[762] Prütting/Gehrlein/*Ahrens*, ZPO, § 857 Rn. 11.

e. Zwischenergebnis

Als Befund kann deshalb festgehalten werden, dass die Verwertung von Bitcoins derzeit *bei Mitwirkung* des Schuldners möglich ist und mit den geltenden Regelungen vereinbar sein dürfte. Bei fehlender Mitwirkung sind der Verwertung aber durch die Technologie Grenzen gesetzt.

IV. Ergebnisse

Die zivilrechtliche Qualifizierung von virtuellen Währungen und die Identifizierung der rechtlichen Rahmenbedingungen ihres Einsatzes im E-Commerce sind im Hinblick auf die angewendete Technologie schwierig. Erkenntnisse zu praktischen Schwierigkeiten in diesem Bereich gibt es bislang nicht, sodass insofern derzeit kein gesetzgeberischer Handlungsbedarf besteht.

Der Zugriff auf und die Verwertung von Bitcoins im Rahmen der Zwangsvollstreckung ist bei Mitwirkung des Schuldners möglich und dürfte mit den geltenden Regelungen vereinbar sein. Anlass für gesetzgeberische Maßnahmen besteht derzeit nicht.

Kapitel 3: Digitales Persönlichkeitsrecht

A. Vorbemerkung

Die Arbeitsgruppe hat Phänomene der „digitalen Welt“, die einen Bezug zum allgemeinen Persönlichkeitsrecht haben, gesammelt, den in der „analogen Welt“ entwickelten Fallgruppen zum allgemeinen Persönlichkeitsrecht zugeordnet und die in Rechtsprechung und Literatur vorgeschlagenen Lösungswege zur Kenntnis genommen und diskutiert.

Dabei hat der Arbeitsgruppe die Frage vor Augen gestanden, ob die Rechtsordnung eine digitale Persönlichkeit anerkennen und schützen muss. Die Arbeitsgruppe verneint diese Frage vorerst, weil das Persönlichkeitsrecht in der Menschenwürde gründet und die bislang diskutierten Falllösungen auf Grundlage des geltenden Rechts auch das Handeln im digitalen Raum und die damit im Zusammenhang stehenden Ausprägungen der Persönlichkeit der handelnden Person sachgerecht erfassen.

Die Arbeitsgruppe hat sich bei ihrer weiteren Arbeit auf die nachfolgend als prüfungswürdig gekennzeichneten Phänomene konzentriert. Als zentrales Anliegen wurde, in Übereinstimmung mit der Stellungnahme des Bundesrates vom 6. November 2015, BR-Drs. 440/15, die gesetzliche Verankerung eines Auskunftsrechts bei Verletzungen des allgemeinen Persönlichkeitsrechtes herausgearbeitet. Im Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG – BR-Drs. 315/17) wurde diese Forderung nunmehr seitens der Bundesregierung aufgegriffen. Allerdings sieht die Arbeitsgruppe auch insoweit weiteren gesetzgeberischen Handlungsbedarf.

Gesetzgeberischer Handlungsbedarf wird zudem im Hinblick auf die Einführung eines transparenten, unkomplizierten und effizienten Löschungsverfahrens bei Diensteanbietern gesehen. Die Arbeitsgruppe hat entsprechende Kriterien eines sachgerechten Löschungsverfahrens sowie einer effektiven Rechtsdurchsetzung herausgearbeitet. Die Regelungsmöglichkeiten sind jedoch durch europäische Einflüsse begrenzt. Zum einen haben sich telemedienrechtliche Regelungen an den Vorgaben der Richtlinie über den elektronischen Geschäftsverkehr (E-Commerce-Richtlinie)[763] zu orientieren, zum anderen bringen die am 25. Mai 2016 in Kraft getretene und ab dem 25. Mai 2018 anwendbare EU-DSGVO[764] wie auch der Entwurf der Verordnung über Privatsphäre und elektronische Kommunikation (E-Privacy-Verordnung)[765] Unsicherheiten in datenschutzrechtlicher

[763] Richtlinie 2000/31/EG (“Richtlinie über den elektronischen Geschäftsverkehr”).
[764] Verordnung 2016/679/EU (“EU-Datenschutzgrundverordnung”).
[765] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation), COM(2017) 10 final, 10. Januar 2017.

Hinsicht mit sich, deren Auswirkungen auf die Lösung von Fällen mit Persönlichkeitsrechtsbezug in Rechtsprechung und Literatur noch nicht hinreichend geklärt worden sind.

Abgesehen von dem Löschungsverfahren bei Diensteanbietern sind gewichtige Fehlentwicklungen derzeit nicht ersichtlich. Da zudem das auf richterlicher Rechtsfortbildung beruhende allgemeine Persönlichkeitsrecht nicht gesetzlich geregelt ist, sieht die Arbeitsgruppe auch für die Zukunft allenfalls in Detailfragen Gesetzgebungsbedarf und hält es im Allgemeinen für vorzugswürdig, die Rechtsentwicklung im Wesentlichen weiterhin der Rechtsprechung zu überlassen.

B. Verbreitung von Tatsachen und Meinungen über Neue Medien

I. Schutz des allgemeinen Persönlichkeitsrechts in der „digitalen Welt“

1. Verbreitung herabsetzender Tatsachenbehauptungen oder Werturteile

Die Verbreitung herabsetzender Tatsachenbehauptungen oder Werturteile erfährt in der „digitalen Welt“ besondere Ausprägungen. Auf sie wendet die Praxis die Maßstäbe der „analogen Welt“ zum Schutz der Ehre und vor Verfremdung der Persönlichkeit an. Die Arbeitsgruppe hält dies grundsätzlich für angemessen.

Herabsetzungen durch Tatsachenbehauptungen oder Werturteile bzw. Beleidigungen in der digitalen Welt sind in vielerlei Hinsicht denkbar, etwa

- zweiseitig über E-Mail, SMS, Tweet, Messenger-Text usw.,
- gegenüber einem beschränkten Nutzerkreis über Chat-Foren, WhatsApp-Gruppen usw.,
- auf (potentiell) jedermann zugängliche Weise, z. B. in folgenden Konstellationen:
    - Jemand wird in einem Artikel negativ dargestellt, der in einem Blog oder in einer online erscheinenden Zeitung (z. B. Spiegel-Online) „veröffentlicht“ wird, und möchte die Löschung des Beitrags erreichen.
    - Jemand wird in einem (möglicherweise anonymen) Kommentar zu einem Artikel negativ dargestellt, der in einem Blog oder in einer online erscheinenden Zeitung „veröffentlicht“ wird, und möchte die Löschung der Kommentare erreichen.
    - Jemand wird auf einer Internetseite (ohne Pressebezug) negativ dargestellt und möchte die Löschung der Darstellung erreichen.

Besondere internetspezifische Ausprägungen einer Herabsetzung sind dabei:

- Verfälschung des Abbildes durch Fotomontagen.

- Autocomplete-Funktion bei Suchmaschinen: Gibt man im Suchfenster gängiger Suchmaschinen einen Begriff ein, werden Wortkombinationen angeboten, um die Suche zu beschleunigen. Grundlage ist ein Algorithmus, der z. B. entsprechend der Häufigkeit vorangegangener Nutzeranfragen besonders häufige Suchanfragen ausgibt. Gab man etwa im Jahr 2013 das Wort „Bettina Wulff" in das Google-Suchfenster ein, schlug die Suchmaschine „Bettina Wulff Escort" und „Bettina Wulff Prostituierte" als Wortkombinationen vor.

Der Schutz des allgemeinen Persönlichkeitsrechts umfasst den Schutz vor Beeinträchtigungen der sozialen Anerkennung durch abträgliche öffentliche Bemerkungen, die in der digitalen Welt in besonderer Weise ausgeprägt sein können. Nach den Recherchen der Arbeitsgruppe bestimmen die Gerichte die Reichweite des Ehrschutzes in der digitalen Welt (und mit Blick auf den Schutz der digitalen Persönlichkeit vor Verfremdung) ebenso wie in der analogen Welt.[766]

Im Grundsatz ist dieser Ansatz angemessen. Fraglich könnte sein, ob Nutzer der digitalen Medien schutzbedürftiger sind, wenn sie spontan und unüberlegt Äußerungen treffen, ohne sich über deren Wirkkreis Gedanken zu machen. Die Kommunikation über soziale Medien ersetzt in vielen Situationen persönliche Gespräche, deren Inhalt, auch bei Persönlichkeitsrechtsverletzungen, in der Vergangenheit nur zu einem geringen Prozentsatz Gegenstand von Gerichtsverfahren geworden ist. Mit der Kommunikation über soziale Medien geht allerdings die Perpetuierung der Kommunikation und damit auch etwaiger Persönlichkeitsrechtsverletzungen einher. Das Opfer kann anders als beim gesprochenen Wort die Persönlichkeitsrechtsverletzung dauerhaft und aus erster Hand wahrnehmen. Dadurch und wegen des oftmals potentiell unbeschränkten Adressatenkreises derartiger Perpetuierung (auf Foren, in sozialen Netzwerken usw.) besteht abstrakt ein Risiko vermehrter gerichtlicher Auseinandersetzungen. So soll es „Shitstorm-Provokateure" geben, und im angloamerikanischen Raum sei Twitter bereits „ein Markt für Beleidigungskläger".[767] Der Arbeitsgruppe fehlen jedoch ausreichende empirische Grundlagen, um das Bedürfnis für einen gesetzgeberischen Eingriff beurteilen zu können. Denn es erscheint nicht ausgeschlossen, dass nach wie vor

---

[766] BGH, Urt. v. 23.9.2014 –VI ZR 358/13, juris Rn. 25 ff. (Ärztebewertung II); BGH, Urt. v. 28.7.2015 – VI ZR 340/14, juris Rn. 27 ff.; BGH, Urt. v. 14.5.2013 – VI ZR 269/12, juris Rn. 21 f. („Google-Autocomplete-Funktion"); BGH, Urt. v. 23.6.2009 – VI ZR 196/08, juris Rn. 30 („spickmich"); LG Berlin, Urt. v. 19.1.2010 – 27 O 1147/09, juris Rn. 24 f.; *Härting*, Internetrecht, Rn. 15 ff.; *Glaser*, Grundrechtlicher Schutz der Ehre im Internetzeitalter, NVwZ 2012, 1432; *Ladeur/Gostomzyk*, Der Schutz von Persönlichkeitsrechten gegen Meinungsäußerungen in Blogs, NJW 2012, 710.

[767] *Heckmann*, Juristische Betrachtung des Shitstorms, abrufbar unter http://www.theeuropean.de/dirk-heckmann/11145-juristische-betrachtung-des-shitstorms (letzter Abruf 19.1.2017).

die Lebenswirklichkeit einen Großteil solcher Fälle von den Gerichten fernhält[768], sodass es – alle denkbaren Maßnahmen sind mit Rechtsschutzhindernissen verbunden – im Ergebnis sinnvoller sein könnte, von einer Regelung abzusehen. Es handelt sich zudem um ein Feld, in dem die Rechtsprechung eine Balance zwischen den Interessen des sich unbedacht Äußernden und denen des Geschädigten schaffen kann. Die Anwendung der in der „analogen Welt" erstellten Grundsätze auch für diese Konstellationen erscheint sachgerecht. Die Erörterung gesetzgeberischer Eingriffe wird daher zurückgestellt. Sie soll erst dann wieder aufgegriffen werden, wenn hinreichende empirische Grundlagen auf eine Fehlentwicklung in der Praxis hindeuten (denkbar sind: vorangehende formlose Mahnung als Voraussetzung für Abmahnkostenersatz, höhenmäßige Beschränkung des Abmahnkostenersatzes, Ergänzung von § 15a EGZPO, Güterichterzuständigkeit).

2. Veröffentlichungen ohne herabsetzenden Charakter

Auch nicht herabsetzende Veröffentlichungen können persönlichkeitsrechtsrelevant sein. Das allgemeine Persönlichkeitsrecht schützt in seiner Ausprägung als Recht auf informationelle Selbstbestimmung und Recht am eigenen Wort und Bild die Entscheidungshoheit darüber, wem man persönliche Informationen, Bilder oder Zitate zur Verfügung stellt. Seit digitale Werkzeuge und Speichertechnologien das Erinnern einfach und billig machen, ist zudem die Erkenntnis gewachsen, dass das allgemeine Persönlichkeitsrecht auch dort tangiert sein kann, wo ursprünglich rechtmäßige Veröffentlichungen dauerhaft abrufbar sind.

Bei Veröffentlichungen ohne herabsetzenden Charakter ist unter anderem an folgende Konstellationen zu denken:

- Verbreitung von Bildern oder Zitaten
- Zwangsoutings
- Rechtmäßige Verdachtsberichterstattung (Berichterstattung über Ermittlungsverfahren), wenn sich ein Verdacht nicht bestätigt.[769]
- Eine besondere internetspezifische Ausprägung sind dabei die ständig verfügbare Archivierung und dauerhafte Verlinkung persönlicher Informationen in Suchmaschinen. Bei dieser Fallgruppe erscheinen folgende Sachverhalte erwähnenswert:

---

[768] So z. B. bei den sogen. „Schulhoffällen", bei denen Recherchen der Arbeitsgruppe ergeben haben, dass derartige Bagatellfälle bislang offenbar im Wesentlichen außergerichtlich geregelt werden.

[769] Vgl. zu den Anforderungen an die zulässige Verdachtsberichterstattung und zum Anspruch auf Löschung einer entsprechenden Altmeldung im Online-Archiv einer Tageszeitung BGH, Urt. v. 16.2.2016 – VI ZR 367/15: Ist unklar, ob die Verdachtsberichterstattung bzw. die Berichterstattung über die Einleitung eines Ermittlungsverfahrens zulässig war, ist der Beitrag zu löschen.

- Dritte veröffentlichen Informationen, an denen zu diesem Zeitpunkt die Allgemeinheit ein Interesse hat, sodass sie zunächst frei von Persönlichkeitsrechtsverletzungen verbreitet werden. Jahre später besteht das Interesse der Allgemeinheit jedoch nicht mehr und der Betroffene möchte die Informationen löschen.
- Der Rechteinhaber selbst veröffentlicht Informationen über sich, die er zu einem späteren Zeitpunkt aus dem Internet entfernen möchte. Ein Jugendlicher stellt bspw. Partyfotos in ein soziales Netzwerk ein, die er vor einer Bewerbung löschen möchte, sei es von seinem eigenen Account oder von Accounts Dritter, auf die die Fotos gelangt sind.

Mit der dauerhaften Auffindbarkeit durch Suchmaschinen hat sich der EuGH in seinem Urteil vom 13. Mai 2014 – Rs. C-131/12 („Google Spain“) auseinandergesetzt. In diesem Zusammenhang wurde immer wieder von einem „Recht auf Vergessen“ bzw. „Recht auf Vergessenwerden“ gesprochen - Begrifflichkeiten, die der Kläger vor dem spanischen Gericht sowie die spanische und die italienische Regierung im Verfahren verwendeten. In der Sache erhob der Kläger gegen die Herausgeberin einer weit verbreiteten Tageszeitung sowie gegen Google Spain und Google Inc. Beschwerde, da bei Eingabe seines Namens in die Suchmaschine des Google Konzerns den Internetnutzern Links zu zwei Seiten einer Tageszeitung aus dem Jahr 1998 angezeigt wurden, die eine Anzeige enthielten, in der unter Nennung des Namens des Klägers auf die Versteigerung eines Grundstücks im Zusammenhang mit einer wegen Forderungen der Sozialversicherung erfolgten Pfändung hingewiesen wurde. Die Veröffentlichung dieser Informationen war damals zunächst rechtmäßig erfolgt. Der Kläger begehrte nunmehr von Google Inc. und Google Spain zwei Jahre später, die ihn betreffenden personenbezogenen Daten zu löschen oder zu verbergen, sodass diese weder in den Suchergebnissen noch in den Links zu der Tageszeitung erschienen.

Der EuGH stellte fest, dass der Suchmaschinenbetreiber personenbezogene Daten verarbeitet und Verantwortlicher i. S. d. Richtlinie 95/46 ist. Er urteilte ferner, dass die Verarbeitung personenbezogener Daten auch dann nicht den Bestimmungen der Richtlinie entsprechen kann, wenn die Daten zwar nicht sachlich unrichtig sind, jedoch nicht den Zwecken der Verarbeitung entsprechen, nicht erheblich sind oder darüber hinausgehen, nicht auf den neuesten Stand gebracht sind oder länger als erforderlich aufbewahrt werden.

Der Löschung entgegenstehen können grundsätzlich Grundrechte Dritter, wie bspw. die Meinungsfreiheit, Medienfreiheit, Kunst- und Wissenschaftsfreiheit oder die unternehmerische Freiheit. Bemerkenswerterweise hat der EuGH in seiner Entscheidung angenommen, dass der Eingriff des Suchmaschinenbetreibers in das Persönlichkeitsrecht der betroffenen Person besonders schwerwiegend ist und das „Recht auf Vergessenwerden“ im Allgemeinen gegenüber den Interessen

Dritter überwiegt.[770] Es bleibt abzuwarten, wie die Interessenabwägung durch die Rechtsprechung in Zukunft vorgenommen wird.

Das nunmehr in Art. 17 Abs. 2 EU-DSGVO normierte Recht („Recht auf Vergessenwerden“) verfolgt eine ähnliche Zielsetzung wie das EuGH-Urteil.

Art. 17 Abs. 1 EU-DSGVO normiert zunächst die Voraussetzungen, unter denen die betroffene Person einen Anspruch auf Löschung der ihre Person betreffenden Daten hat. Liegen die Voraussetzungen vor, ist der Verantwortliche zur unverzüglichen Löschung der personenbezogenen Daten verpflichtet. Art. 17 Abs. 1 EU-DSGVO sieht folgende Löschungsgründe vor: Die fehlende Notwendigkeit der Datenspeicherung zur Zweckerfüllung, den Widerruf der Einwilligung, den Widerspruch gegen die Verarbeitung, die Unrechtmäßigkeit der Verarbeitung, die anderweitige Rechtspflicht zur Löschung und die Erhebung personenbezogener Daten eines Kindes in Bezug auf diesem angebotene Dienste der Informationsgesellschaft. In Art. 17 Abs. 3 EU-DSGVO sind Ausnahmen zu Abs. 1 normiert: Die Ausübung des Rechts auf freie Meinungsäußerung und Information, die Erfüllung einer Rechtspflicht oder die Erfüllung öffentlicher Aufgaben, das Vorliegen eines öffentlichen Interesses im Bereich der öffentlichen Gesundheit, die im öffentlichen Interesse liegende Verarbeitung zu Archivzwecken, Forschungszwecken und statistischen Zwecken und die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Von besonderem Interesse erscheinen Konstellationen, in denen Minderjährige in die Verarbeitung ihrer Daten zunächst freiwillig einwilligen, diese Daten jedoch Jahre später gelöscht haben wollen. In der Literatur gibt es Stimmen, die ein Recht auf einen digitalen Neustart mit Eintritt der Volljährigkeit fordern. Die von einer Gruppe von Bürgerinnen und Bürgern am 5. Dezember 2016 dem EU-Parlament und der Öffentlichkeit vorgestellte Vorschlag für eine Charta der Digitalen Grundrechte der Europäischen Union sieht ebenfalls unter Art. 18 das Recht auf Digitalen Neuanfang vor.[771]

Art. 17 Abs. 1 Buchst. f EU-DSGVO normiert die Möglichkeit, personenbezogene Daten, die aufgrund einer nach Art. 8 Abs. 1 EU-DSGVO wirksamen Einwilligung erhoben wurden, zu löschen. Art. 8 Abs. 1 EU-DSGVO regelt die Anforderungen an die Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft, das dem Kind direkt gemacht wird. Art. 17 Abs. 1 Buchst. f EU-DSGVO trägt nach Erwägungsgrund 65 dem Umstand Rechnung, dass ein Kind die mit der Verarbeitung verbundenen Gefahren und damit auch die Tragweite seiner Einwilligung nicht immer vollumfassend überblicken kann.

Dabei ist die Norm bedauerlicherweise unpräzise formuliert. Es stellt sich zunächst die Frage, welche Altersgrenze maßgeblich ist. Hier wird vertreten, es sei auf die nach Art. 8 EU-DSGVO für die Einwilligung bestehende Altersgrenze

---

[770] *Boehme-Neßler*, Das Recht auf Vergessenwerden, NVwZ 2014, 825 (829).

[771] Charta der Digitalen Grundrechte der Europäischen Union, abrufbar unter http://www.digitalcharta.eu (letzter Abruf: 19.1.2017).

beziehungsweise auf das auf der Öffnungsklausel des Art. 8 Abs. 1 S. 3 EU-DSGVO beruhende nationale Recht abzustellen.[772] Weitere Schwierigkeiten bereitet die Frage, ob der Löschungsanspruch nur bei solchen Verarbeitungen greift, die auf einer Einwilligung des Kindes beruhen, oder auch bei Verarbeitungen personenbezogener Daten von Kindern auf anderer Rechtsgrundlage. Aufgrund des Erwägungsgrundes 65 wird vertreten, Art. 17 Abs. 1 Buchst. f EU-DSGVO beschränke sich auf Einwilligungsfälle.[773] Damit wäre der Anwendungsbereich der Norm neben Art. 17 Abs. 1 Buchst. b EU-DSGVO allerdings gering. Problematisch ist schließlich ebenfalls, dass eine wortgetreue Auslegung zu dem widersinnigen Ergebnis führt, dass eine Löschpflicht ohne Antrag besteht und Daten immer dann zu löschen wären, wenn die Voraussetzungen des Art. 8 Abs. 1 i. V. m. Art. 6 Abs. 1 Buchst. a EU-DSGVO vorliegen, d. h. unmittelbar nach ihrer Erhebung. Aus diesem Grund wird in der Literatur angenommen, dass Art. 17 Abs. 1 Buchst. f EU-DSGVO keine Löschpflicht des Verantwortlichen begründet, da dies ansonsten den Maßgaben der wirksamen Einwilligung zuwiderlaufen würde, sondern lediglich einen Löschanspruch auf Antrag beinhaltet.[774]

Wie exemplarisch gezeigt bringt die Vorschrift des § 17 EU-DSGVO zahlreiche Detailfragen mit sich, auch zu Regelungsspielräumen der nationalen Gesetzgeber, die bislang nicht gelöst sind. Im Gesetzesentwurf der Bundesregierung zur Umsetzung der EU-DSGVO[775] wird in § 35 BDSG-E das „Recht auf Löschung“ über die Fälle des Art. 17 Abs. 3 EU-DSGVO hinaus weiter eingeschränkt. Auch ist noch nicht absehbar, ob der nun vorliegende Entwurf der EU-Kommission einer E-Privacy-Verordnung zu weiteren datenschutzrechtlichen Regeln für die digitale Kommunikation führen wird. Die Arbeitsgruppe muss die Frage nach den Regelungsspielräumen auf nationaler Ebene daher gegenwärtig zurückstellen.

II. Auskunft über die Identität von Tätern und Teilnehmern

Regelmäßig weiß das Opfer einer Persönlichkeitsrechtsverletzung nicht, wer hinter einer bestimmten Veröffentlichung steht. Beiträge in Internetforen oder über soziale Netzwerke sind vielfach anonym oder pseudonym. Das Opfer einer Persönlichkeitsrechtsverletzung kennt oft nur die Identität des Diensteanbieters, der das jeweilige Forum, das soziale Netzwerk oder die Webseite betreibt, auf der der beanstandete Beitrag festgehalten ist. Praktisch bedeutsam ist diese Problematik insbesondere bei Bewertungsportalen.

Grundsätzlich besteht allerdings de lege lata kein zivilrechtlicher Anspruch des Opfers einer Persönlichkeitsrechtsverletzung gegen den Diensteanbieter auf Auskunft über die Identität des Täters oder Teilnehmers. Ein zivilrechtlicher Auskunftsanspruch lässt sich zwar aus Treu und Glauben gem. § 242 BGB ableiten.

---

[772] Kühling/Buchner/*Herbst*, DS-GVO, Art. 17 Rn. 34.
[773] Kühling/Buchner/*Herbst*, DS-GVO, Art. 17 Rn. 35.
[774] Gola/*Nolte/Werkmeister*, DS-GVO, Art. 17 Rn. 27.
[775] Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (BR-Drs. 110/17).

Die Rechtsprechung hält aber die Erfüllung eines solchen Auskunftsanspruchs wegen § 12 Abs. 2 TMG für unmöglich und weist Auskunftsklagen demgemäß ab.[776] Nach § 12 Abs. 2 TMG darf nämlich ein Diensteanbieter für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwenden, soweit das TMG oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat. Als einzige solche in Betracht kommende Erlaubnisnorm lässt § 14 Abs. 2 TMG im Einzelfall die Auskunft über Bestandsdaten zu, aber nur, soweit dies für Zwecke der Strafverfolgung, der Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus sowie zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist. Die Rechtsprechung hat auch eine analoge Anwendung dieser Bestimmung aufgrund ihrer restriktiven Fassung auf Persönlichkeitsrechtsverletzungen abgelehnt, nicht ohne jedoch die Beschränkung der Ermächtigung zur Auskunftserteilung auf Inhaber von Rechten am geistigen Eigentum als wenig nachvollziehbar und eine Ausweitung auf Persönlichkeitsrechtsverletzungen durch den Gesetzgeber als wünschenswert darzustellen.[777]

Der Betroffene hat daher nach derzeit geltendem Recht nur die Möglichkeit, Strafantrag zu stellen, um nach Einleitung des Ermittlungsverfahrens über sein strafprozessuales Akteneinsichtsrecht die von der Staatsanwaltschaft ermittelte Identität des Beschuldigten zu erfahren (§ 406e StPO). Dieses Verfahren kommt jedoch lediglich bei Beleidigungsdelikten in Betracht; steht das Recht auf informationelle Selbstbestimmung in Rede, scheidet ein Delikt, das Anlass für einen Strafantrag geben könnte, oftmals aus.

Anlässlich einer Stellungnahme zur Änderung des Telemediengesetzes (TMG) hat der Bundesrat am 6. November 2015 beantragt, § 14 Abs. 2 TMG um Fälle der Persönlichkeitsrechtsverletzung zu erweitern. Dies entspricht der Forderung der Arbeitsgruppe. Die Bundesregierung hat in ihrer Gegenäußerung erklärt, dass hiergegen keine Einwände bestehen und dass, vorbehaltlich einer weiteren Prüfung, eine Ausdehnung auf alle absoluten Rechte erwogen werden sollte.[778] Im Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) vom 5. April 2017 hat die Bundesregierung die Forderung des Bundesrats nunmehr aufgegriffen.[779] Entgegen der Auffassung der Bundesregierung in der Begründung zu Artikel 2 des NetzDG-E begründet allerdings künf-

---

[776] BGH, Urt. v. 1.7.2014 – VI ZR 345/13, NJW 2014, 2651-2653 („Ärztebewertung I“).
[777] BGH, Urt. v. 1.7.2014 – VI ZR 345/13, NJW 2014, 2651-2653 („Ärztebewertung I“).
[778] BT-Drs. 18/6745, S. 17.
[779] http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_NetzDG.pdf?__blob=publicationFile&v=2 (letzter Abruf: 2.5.2017).

tig auch § 24 BDSG-E, der eine Übermittlung personenbezogener Daten zu anderen Zwecken als denen, zu denen sie erhoben wurden (hier: zur Rechtsverfolgung Dritter), vorsieht, eine Verpflichtung von Diensteanbietern zur Datenübermittlung an private Dritte wegen Persönlichkeitsrechtsverletzungen nicht. Da sich § 24 BDSG-E nicht ausdrücklich auf Telemedien bezieht, wird bereits die Sperrwirkung des § 12 Abs. 2 TMG nicht aufgehoben.

Eine darüber hinausgehende Frage ist, ob für den Auskunftsanspruch lediglich § 242 BGB herangezogen wird oder ob ein eigener Auskunftsanspruch mit Richtervorbehalt kodifiziert werden sollte.

Zu konstatieren ist zunächst, dass Art. 15 Abs. 2 E-Commerce-Richtlinie einem zivilrechtlichen Auskunftsanspruch ohne behördliche bzw. richterliche Anordnung nicht entgegensteht, obwohl der Wortlaut zunächst darauf hindeutet. Die Entscheidung des EuGH in Sachen „Promusicae/Telefonica“[780] legt nämlich das Verständnis nahe, dass Art. 15 Abs. 2 E-Commerce-Richtlinie die darin geregelten behördlichen Maßnahmen ungeachtet des in Art. 15 vorgesehenen Grundsatzes, dass keine allgemeine Überwachungspflicht besteht, zulässt, jedoch keine Aussage über die Voraussetzungen zivilrechtlicher Auskunftspflichten trifft.

Ungeachtet dessen könnte es sich anbieten, den Auskunftsanspruch selbst – ebenso wie im gewerblichen Rechtsschutz geschehen – gesetzlich zu kodifizieren. Dies könnte etwa im Telemediengesetz oder aber – indes nicht nur bezogen auf strafbare Inhalte – im NetzDG geschehen.

Hierfür spricht, dass die Inanspruchnahme auf Auskunft im Hinblick auf Bestands- und Nutzungsdaten dem Verhältnismäßigkeitsgrundsatz genügen muss.[781] Zudem erfordert auch die Prüfung, ob eine Persönlichkeitsrechtsverletzung vorliegt, oftmals eine Abwägung grundrechtlich geschützter Positionen. Es erscheint daher sinnvoll, die Auskunft über Bestands- oder Nutzungsdaten von der vorherigen richterlichen Anordnung abhängig zu machen, vergleichbar dem – indes auf Verkehrsdaten zugeschnittenen – § 101 Abs. 9 UrhG. Hiernach wäre auch die einer Änderung des § 14 Abs. 2 TMG entgegengehaltene Befürchtung, damit werde der § 13 Abs. 6 TMG zugrundeliegende Gedanke der anonymen Dienstenutzung im Internet ausgehöhlt und die Bereitschaft zur Meinungsäußerung im Internet beeinträchtigt, entkräftet.

III. Unterlassung, Beseitigung (Löschung) und Widerruf

1. Ansprüche gegen Täter, Teilnehmer und Dritte, insbesondere Intermediäre

Sind Täter oder Teilnehmer der Persönlichkeitsrechtsverletzung bekannt, können sie auf Unterlassung und Beseitigung, d. h. Löschung der Inhalte, nach §§ 823

---

[780] EuGH, Urt. v. 29.1.2008 − Rs. C-275/06 (Promusicae/Telefónica), GRUR 2008, 241.

[781] Vgl. § 101 Abs. 4 UrhG und EuGH, Urt. v. 29.1.2008 − Rs. C-275/06 (Promusicae/Telefónica), GRUR 2008, 241.

Abs. 1, 2 BGB, §§ 185 ff. StGB, 1004 analog BGB in Anspruch genommen werden. Ein Widerruf kommt bei einer gegenwärtigen rechtswidrigen Störung durch unwahre Tatsachen in Betracht, soweit ein solcher verhältnismäßig ist.

Bei rufschädigenden Meinungsäußerungen kann dem Verletzten auf negatorischer und deliktischer Grundlage zudem ein Anspruch auf Veröffentlichung einer strafbewehrten Unterlassungsverpflichtung des Verletzers zustehen, wenn die unzulässige Meinungsäußerung öffentlich erfolgt ist und die Publikation der Unterwerfungserklärung zur Beseitigung der noch andauernden Folgen der Äußerung für das Ansehen des Verletzten erforderlich ist.[782]

Bleibt der Verursacher, sei er Täter oder Teilnehmer, des verletzenden Beitrags unbekannt, sind Ansprüche wegen eines Auslandsbezugs nicht oder nicht effektiv durchsetzbar oder hat der Betroffene die Daten selber hochgeladen, wird sich der Betroffene an den Intermediär wenden wollen, bei dem der Beitrag gespeichert ist, also insbesondere an den jeweiligen Diensteanbieter. Hierauf soll im Folgenden näher eingegangen werden.

Auch Diensteanbieter können als Intermediäre grundsätzlich auf Löschung persönlichkeitsrechtsverletzender Beiträge in Anspruch genommen werden.[783] Die Ansprüche sind nicht subsidiär gegenüber den Ansprüchen gegen Täter oder Teilnehmer.[784] Auch die EU-DSGVO, die einen datenschutzrechtlichen Ansatz verfolgt, unterscheidet nicht zwischen Tätern, Teilnehmern und Dritten.

Dieser Löschungsanspruch gegenüber Intermediären kann grundsätzlich gerichtlich durchgesetzt werden. Dazu stehen dem Betroffenen die gleichen Mittel zu Gebote wie gegenüber dem Verursacher. Der Betroffene kann daher gerichtlich die Löschung verlangen, auch im Wege einstweiligen Rechtsschutzes. Der Intermediär ist in diesem Falle als Störer zur Beseitigung des die Persönlichkeitsrechtsverletzung verursachenden Beitrages verpflichtet.

Löschungsansprüche gegenüber Intermediären können nach geltendem Recht auf unterschiedlicher Grundlage bestehen.

---

[782] BGH, Urt. v. 25.11.1986 – VI ZR 57/86, NJW 1987, 1400.

[783] LG Hamburg, Urt. v. 7.11.2014 – 324 O 660/12 (Google); LG Heidelberg, Urt. v. 9.12.2014 – 2 O 162/13 (Google); zu anderen Ausprägungen des allgemeinen Persönlichkeitsrechts EuGH, Urt. v. 13.5.2014 – Rs. C 131/12 (Google); dazu *Deutsches Institut für Vertrauen und Sicherheit im Internet*, Digitaler Kodex, abrufbar unter http://irights.info/artikel/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/23838 (letzter Abruf: 19.1.2017); https://www.divsi.de/projekte/digitaler-kodex/recht-auf-vergessenwerden/ (letzter Abruf: 19.1.2017); OLG Hamburg, Urt. v. 7.7.2015 – 7 U 29/12 (Online-Pressearchiv der Süddeutschen Zeitung); LG Hamburg, Urt. v. 24.1.2014 – 324 O 264/11 (Google) ; a.A. LG Berlin, Urt. v. 21.8.2014 – 27 O 293/14, juris Rn. 16 (Google Deutschland); LG Hamburg, Urt. v. 10.7.2015 – 324 O 17/15 (Yahoo!); zum anwendbaren Recht OVG Schleswig-Holstein, Urt. v. 4.9.2014 – 4 LB 20/13 (Facebook-Fanpage).

[784] BGH, Urt. v. 27.3.2007 – VI ZR 101/06, juris Rn. 13.

Sollen Daten gelöscht werden, die der Anspruchsteller selbst auf einer Plattform eingestellt hat, dürfte ein vertraglicher Löschungsanspruch gegen den Plattformbetreiber bestehen (soweit er nicht – insbesondere durch AGB – ausgeschlossen wurde). Als Beispiel sind Fotos zu nennen, die ein Nutzer auf seinen Account bei Facebook oder Instagram hochgeladen hat und die er zu einem späteren Zeitpunkt entfernen möchte; maßgeblich sind insbesondere die Allgemeinen Geschäftsbedingungen der jeweiligen Plattformen.

Handelt es sich um Daten, die nicht der Anspruchsteller, sondern ein Dritter hochgeladen hat, besteht zwischen dem Anspruchsteller und dem Plattformbetreiber keine Vertragsbeziehung. In solchen Fällen könnte aber ein vertraglicher Löschungsanspruch des Dritten (um dessen Account es geht) gegen den Plattformbetreiber bestehen, dessen Geltendmachung der Anspruchsteller nach Lage des Einzelfalls auf vertraglicher oder deliktischer Grundlage verlangen kann.

Diensteanbieter müssen, ausgehend von der telemedienrechtlichen Privilegierung in § 10 TMG, Beiträge und Verlinkungen zwar nicht generell vorab, aber auf einen Hinweis hin in angemessener Zeit prüfen und ggf. beseitigen sowie zumutbare Vorkehrungen zur Verhinderung zukünftiger Rechtsverletzungen treffen. Dies betrifft bspw. Betreiber von Suchmaschinen, Foren, Social-Media-Plattformen, Online-Marktplätzen, Online-Archiven und Online-Enzyklopädien.

Daneben kommen datenschutzrechtliche Ansprüche in Betracht. Zu unterscheiden ist zwischen Löschungsansprüchen auf datenschutzrechtlicher Grundlage nach

- nationalem Recht (Bundesdatenschutzgesetz und Landesdatenschutzgesetze) und
- europäischem Recht. Insoweit ist wiederum zu unterscheiden zwischen der geltenden Datenschutzrichtlinie, auf deren Grundlage das Google-Urteil des EuGH ergangen ist,[785] und der EU-DSGVO. Letztere umfasst in Art. 17 eine Bestimmung zum Recht auf Löschung (und damit auch auf Vergessenwerden).

Bei der Geltendmachung von Ansprüchen gegenüber Dritten ist im Einzelnen zwischen den jeweiligen Intermediären zu unterscheiden.

a. Suchmaschinenbetreiber

Bereits bevor die Literatur und der EuGH das allgemeine „Recht auf Vergessen(werden)“ thematisierten, war anerkannt, dass den Betreiber einer Internet-Suchmaschine grundsätzlich dann eine Prüfungspflicht trifft, wenn er Kenntnis

---

[785] EuGH, Urt. v. 13.5.2014 − Rs. C-131/12, vgl. dazu *Boehme-Neßler*, Das Recht auf Vergessenwerden – ein neues Internet-Grundrecht im Europäischen Recht, NVwZ 2014, 825; *Luch/Schulz/Kuhlmann*, Ein Recht auf Vergessenwerden als Ausprägung einer selbstbestimmten digitalen Persönlichkeit, EuR 2014, 698.

von der Rechtsverletzung erlangt. Weise ein Betroffener den Betreiber einer Internet-Suchmaschine auf eine rechtswidrige Verletzung seines Persönlichkeitsrechts hin, sei der Betreiber der Suchmaschine daher verpflichtet, zukünftig derartige Verletzungen zu verhindern[786.] Die Störerhaftung eines Suchmaschinenbetreibers setze daher eine Verletzung von Prüfpflichten voraus.[787]

Der Betreiber einer Suchmaschine ist nach der Rechtsprechung grundsätzlich auch nicht verpflichtet, die durch eine Software generierten Suchergänzungsvorschläge generell vorab auf etwaige Rechtsverletzungen zu überprüfen. Dies würde, wurde argumentiert, den Betrieb einer Suchmaschine mit einer der schnellen Recherche der Nutzer dienenden Suchergänzungsfunktion unzumutbar erschweren, wenn nicht gar unmöglich machen. Eine entsprechende präventive Filterfunktion komme allenfalls für bestimmte Bereiche, wie etwa Kinderpornographie, in Betracht, sie vermöge jedoch nicht allen denkbaren Fällen einer Persönlichkeitsrechtsverletzung vorzubeugen.

Soweit Suchmaschinen, insbesondere auch die des Marktführers Google, zudem häufig über eine Bildersuchfunktion verfügen, bei der ein im Zuge der Indexierung aufgefundenes Bild in seinem Datenvolumen reduziert und als Vorschaubild im sog. Thumbnail-Cache auf Servern des Suchmaschinenbetreibers vorübergehend abgespeichert wird, besteht auch ein Löschungsanspruch im Hinblick auf diese Bilder, wenn hierdurch eine Persönlichkeitsrechtsverletzung verursacht wird.

Gleiches gilt im Zusammenhang mit der Veröffentlichung von sog. „Snippets“. Diese beinhalten bei einer durch eine Suchmaschine verlinkten Internetseite regelmäßig den Titel dieser Seiten, die jeweilige URL bzw. einen Teil davon und einen kurzen Textauszug, der das räumliche Umfeld der eingegebenen Suchbegriffe auf der Quellseite anzeigt. Hierdurch kann die beanstandete, persönlichkeitsrechtsverletzende Darstellung nicht nur im Wege der Verlinkung, sondern auch unmittelbar durch den Suchmaschinenbetreiber bewirkt werden. In diesem Fall haftet der Betreiber einer Internet-Suchmaschine als Störer für ein rechtswidriges Snippet, wenn er nach den erforderlichen und ausreichenden Hinweisen nicht die ihm möglichen und zumutbaren Schritte unternimmt, um weitere Rechtsverletzungen zu verhindern, und somit ihm obliegende Prüfpflichten verletzt.[788]

b. Internet-Foren

Ähnliches gilt auch gegenüber den Betreibern von Onlineforen. Auch diese sind zwar nach der Rechtsprechung nicht verpflichtet, die Beiträge vorab darauf zu überprüfen, ob Vorkehrungen zu treffen sind, um in ihnen vorkommende Namen von einer Auffindbarkeit durch Suchmaschinen auszunehmen. Eine solche Verpflichtung entsteht jedoch, wenn der Betreiber des Internetforums durch einen

---

[786] BGH, Urt. v. 14.5.2013 – VI ZR 269/12.
[787] OLG Hamburg, Urt. v. 16.8.2011 – 7 U 51/10.
[788] LG Hamburg, Urt. v. 7.11.2014 – 324 O 660/12 (zu Google).

qualifizierten Hinweis des Betroffenen darauf aufmerksam gemacht wird, dass die fortdauernde Auffindbarkeit des Beitrags durch Namenssuche nunmehr sein allgemeines Persönlichkeitsrecht verletzt und Vorkehrungen gegen diese Verletzung zu treffen sind.[789]

Nach der neueren Rechtsprechung des EuGH soll im Übrigen auch bereits das Setzen eines Links im Internet für eine (urheberrechtliche) Haftung z. B. des Betreibers einer Nachrichtenseite ausreichen können, sofern dieser böswillig handelt.[790]

c. Social-Media-Plattformen

Diese Rechtsprechung dürfte auch auf Social-Media-Plattformen und Seiten mit Kommentierungsfunktion entsprechend anwendbar sein.

d. Online Marktplatz

Ähnlich wie bei Internetforen kann eine Verletzung des allgemeinen Persönlichkeitsrechts auch auf Internetmarktplätzen erfolgen (etwa: Angebot unter dem Namen eines Dritten, Angebote mit persönlichkeitsrechtsverletzenden Inhalten etc.).

Der BGH hat – wenn auch in markenrechtlichem Kontext – unter Fortentwicklung (auch) seiner das Persönlichkeitsrecht betreffenden Rechtsprechung entschieden, dass einen Betreiber eines Online-Marktplatzes als Störer die mit einem Unterlassungsanspruch durchsetzbare Verpflichtung trifft, zukünftig derartige Verletzungen zu verhindern, wenn er auf eine Verletzung des Persönlichkeitsrechts eines Betroffenen durch ein auf dem Marktplatz eingestelltes Verkaufsangebot hingewiesen wird. Dies setzt voraus, dass der Hinweis so konkret gefasst ist, dass der Adressat des Hinweises den Rechtsverstoß unschwer – das heißt ohne eingehende rechtliche und tatsächliche Überprüfung – feststellen kann. Dabei hängt das Ausmaß des insoweit vom Betreiber zu verlangenden Prüfungsaufwandes von den Umständen des Einzelfalls ab, insbesondere vom Gewicht der angezeigten Rechtsverletzungen auf der einen und den Erkenntnismöglichkeiten des Betreibers auf der anderen Seite.[791]

e. Online-Archive

Wenn das allgemeine Persönlichkeitsrecht eines Betroffenen durch persönlichkeitsrechtsverletzende Einträge in einem Online-Archiv beeinträchtigt wird, kann dem Betroffenen gegen dessen Betreiber ein Anspruch darauf zustehen, es zu unterlassen, diese Beiträge in der Weise zum Abruf bereitzuhalten, dass sie durch Eingabe des Namens des Betroffenen in Internet-Suchmaschinen von diesen aufgefunden werden. Für das Entstehen der Verantwortlichkeit des Betreibers des Internetforums für derartige Beiträge gelten die für die Verantwortlichkeit der Betreiber von Internetforen entwickelten Grundsätze.

---

[789] BGH, Urt. v. 27.3.2007 – VI ZR 101/06.
[790] EuGH, Urt. v. 8.9.2016 − Rs. C-160/15.
[791] BGH, Urt. v. 17.8.2011 – I ZR 57/09, BGHZ 191, 19-35 („Stiftparfüm“).

Daneben wird nach der Rechtsprechung auch die Verpflichtung zur Löschung im Rahmen des „Rechts auf Vergessen(werden)“ auf die Betreiber von Online-Archiven erstreckt. Wenn das allgemeine Persönlichkeitsrecht eines Betroffenen in der Weise beeinträchtigt wird, dass ältere, ursprünglich einmal rechtmäßig in das Internet eingestellte Beiträge in einem Internetarchiv nach Erlöschen eines allgemeinen öffentlichen Interesses an den berichteten Vorgängen weiterhin zum Abruf bereitgehalten werden, kann dem Betroffenen ebenfalls der soeben dargestellte Anspruch zustehen.[792]

f. Online-Enzyklopädien

Die Rechtsprechung hat ferner bestimmte Online-Enzyklopädien – namentlich Wikipedia – wie Online-Foren behandelt. Auch hierbei stellt der Betreiber Dritten die Plattform und der Speicherplatz zur Verfügung, damit diese selbstverfasste Beiträge hinterlegen können, sodass jedermann daran mitarbeiten, Artikel erstellen und bearbeiten kann, wobei weder eine Vorabkontrolle noch eine nachträgliche Steuerung durch eine zentrale Redaktion stattfindet.[793]

g. Host-Provider

Gegenüber sog. „Host-Providern“, also etwa den Betreibern von Blogangeboten und Hostern von Webseiten, hat die Rechtsprechung ebenfalls darauf abgestellt, dass ein Anspruch auf Unterlassung der Verbreitung einer in einem Blog enthaltenen Äußerung eines Dritten nur in Betracht kommt, wenn zumutbare Prüfpflichten verletzt wurden. Der Host-Provider ist erst verantwortlich, wenn er Kenntnis von der Verletzung des Persönlichkeitsrechts erlangt. Dies setzt voraus, dass die Beanstandung des Betroffenen so konkret gefasst ist, dass der Rechtsverstoß auf der Grundlage der Behauptungen des Betroffenen unschwer bejaht werden kann. Eine Verpflichtung zur Löschung des beanstandeten Eintrags besteht, wenn auf der Grundlage der Stellungnahme des für den Blog Verantwortlichen und einer etwaigen Replik des Betroffenen unter Berücksichtigung etwa zu verlangender Nachweise von einer rechtswidrigen Verletzung des Persönlichkeitsrechts auszugehen ist.[794]

Cloud-Provider werden in der Literatur teilweise Host-Providern gleichgestellt.[795]

h. Access-Provider

Der BGH hat im Zusammenhang mit einer Urheberrechtsverletzung entschieden, dass ein Telekommunikationsunternehmen, das Dritten den Zugang zum Internet bereitstellt, von einem Rechteinhaber als Störer nach entsprechender Abwägung der widerstreitenden Interessen auch darauf in Anspruch genommen werden kann,

---

[792] OLG Hamburg, Urt. v. 7.7.2015 – 7 U 29/12.
[793] LG Hamburg, Urt. v. 16.5.2008 – 324 O 847/07, juris Rn. 26 (zu Wikipedia).
[794] BGH, Urt. v. 25.10.2011 – VI ZR 93/10, BGHZ 191, 219-228 („Blog-Eintrag“).
[795] *Neidinger*, Anmerkung zur Entscheidung des BGH, Urt. v. 26.11.2015 – I ZR 174/14, CR 2016, 408 (410).

den Zugang zu Internetseiten zu unterbinden, auf denen urheberrechtlich geschützte Werke rechtswidrig öffentlich zugänglich gemacht werden. Access-Providern seien Netzsperren zuzumuten, wenn das Opfer zuvor erfolglos zumutbare Anstrengungen unternommen hat, die Verantwortlichen in Anspruch zu nehmen, die – wie der Betreiber der Internetseite (Content-Betreiber) – die Rechtsverletzung selbst begangen haben oder – wie der Host-Provider – zur Rechtsverletzung durch die Erbringung von Dienstleistungen beigetragen haben. Eine Sperrung sei aber nicht erst in den Konstellationen zumutbar, in denen ausschließlich rechtsverletzende Inhalte auf der Internetseite bereitgehalten werden, sondern bereits dann, wenn nach dem Gesamtverhältnis rechtmäßige gegenüber rechtswidrigen Inhalten nicht ins Gewicht fallen.[796]

Auch wenn eine Inanspruchnahme von Access-Providern als Störer damit grundsätzlich möglich ist, sind die Voraussetzungen für die Inanspruchnahme von Access-Providern hoch. Der BGH hat als Beispiele für zumutbare Maßnahmen zur Aufdeckung der Identität von Content- und Host-Providern die Einschaltung staatlicher Ermittlungsbehörden im Wege der Strafanzeige und private Ermittlungen durch Beauftragung eines Detektives oder anderer Unternehmen genannt. Ein Vorgehen gegen den Access-Provider wird daher in aller Regel scheitern.

Es ist derzeit offen, ob diese Grundsätze auch auf schwerwiegende Persönlichkeitsrechtsverletzungen Anwendung finden. Der Vorsitzende des I. BGH-Senats soll dies in einem Interview jedoch bejaht haben.[797]

i. Network-Provider

Die Störerhaftung von Network-Providern (Betreiber einer Telekommunikationsinfrastruktur, durch die Informationen geleitet werden) dürfte regelmäßig an den technischen Schwierigkeiten für den Network-Provider scheitern, die Verletzung zu verhindern oder zu erschweren – es sei denn, sie sind gleichzeitig Access-Provider.

Mit dem Zweiten Gesetz zur Änderung des Telemediengesetzes vom 21. Juli 2016[798] hatte der Gesetzgeber den Versuch unternommen, die Störerhaftung von Betreibern öffentlicher WLAN-Netze zu beseitigen, um so den weiteren Ausbau

---

[796] BGH, Urt. v. 26.11.2015 – I ZR 174/14; BGH, Urt. v. 26.11.2015 – I ZR 3/14.

[797] Interview mit dem Vorsitzenden des I. BGH-Senats: „*Mit dem Urteil sei grundsätzlich der Weg geebnet, Telekommunikationsunternehmen zu solchen Sperrmaßnahmen zu verpflichten, sagte der BGH-Senatsvorsitzende Wolfgang Büscher. Dies gilt im Prinzip auch für andere Webseiten, die ganz überwiegend illegale Inhalte bereithalten, bspw. Portale, die Volksverhetzung betreiben. Einzelne Hetzparolen auf einem ansonsten legalen Portal rechtfertigen aber keinesfalls eine Internetsperre*." http://www.sueddeutsche.de/wirtschaft/bundesgerichtshof-gema-gegen-telekom-dieses-urteil-ermoeglicht-das-sperren-von-webseiten-1.2755438 (letzter Abruf: 1.2.2017).

[798] BGBl. I 2016, 1766.

öffentlicher WLAN-Hotspots voranzutreiben. Die Begründung des zugrundliegenden Gesetzentwurfs der Bundesregierung[799] sah vor, im Jahr 2018 zu evaluieren, ob das Ziel des Gesetzes, eine breitere Verfügbarkeit öffentlicher Hotspots in Deutschland zu schaffen, erreicht wurde. Von Experten war bezweifelt worden, dass mit der erfolgten Erstreckung des § 8 TMG auf WLAN-Betreiber auch bloße Unterlassungsansprüche von dem Haftungsausschluss erfasst werden.[800] Im Übrigen ist zwischenzeitlich durch den EuGH festgestellt worden, dass (auch gewerbliche) WLAN-Betreiber verpflichtet werden können, ihr WLAN durch ein Passwort zu sichern, wenn über dieses Netz zuvor Urheberrechtsverletzungen, wie etwa durch Filesharing, begangen worden sind; eine Verpflichtung zur Leistung von Schadenersatz bestehe demgegenüber nicht.[801] Die Bundesregierung hat daraufhin den inzwischen dem Bundesrat zugeleiteten Entwurf eines Dritten Gesetzes zur Änderung des Telemediengesetzes[802] (3. TMGÄndG-E) vorgelegt, mit dem die durch das EuGH-Urteil erneut verstärkte Rechtsunsicherheit im Hinblick auf die Haftung von WLAN-Betreibern für Rechtsverstöße Dritter beseitigt werden soll. Mit den vorgesehenen Änderungen in §§ 7 und 8 TMG soll der Umfang der Haftungsbeschränkung eindeutig geregelt, insbesondere die reine Unterlassungshaftung u.a. mit der Folge ausgeschlossen werden, dass nicht-verantwortliche Anbieter nicht auf Abmahnkosten in Anspruch genommen werden können. Wird das Recht am geistigen Eigentum durch einen WLAN-Nutzer verletzt, soll der Rechteinhaber im Einzelfall die Möglichkeit haben, eine Nutzungssperre gegen den WLAN-Betreiber zu erwirken, um eine Wiederholung der Rechtsverletzung zu verhindern, wobei die Sperrung zur Abhilfe erforderlich und angemessen und dem Diensteanbieter zumutbar sein muss. Eine behördliche Anordnung, vor Gewährung des Zugangs eine Registrierung oder die Eingabe eines Passworts zu verlangen oder das Anbieten des Dienstes dauerhaft einzustellen, soll ausdrücklich ausgeschlossen werden.

j. Domain-Registrar

Streit besteht zur Haftung von Domain-Registraren. Die Rechtsprechung hat Ansprüche gegen Domain-Registrare auf Unterlassung des Bereithaltens, Verlinkens, Verbreitens oder Zugänglichmachens der angegriffenen Äußerungen in den unter der von diesen registrierten und verwalteten Domain erreichbaren Beiträgen bislang tendenziell eher verneint.[803]

---

[799] Vgl. BR-Drs. 440/15 (S. 5 der Begründung des Entwurfs).

[800] Vgl. die Nachweise bei n-tv.de vom 27.7.2016, abrufbar unter http://www.n-tv.de/technik/Stoererhaftung-ist-noch-nicht-vom-Tisch-article18278471.html (letzter Abruf: 19.1.2017).

[801] EuGH, Urt. v. 15. 9.2016 − Rs. C-484/14 (Mc Fadden).

[802] BR-Drs. 276/17.

[803] OLG Frankfurt, Beschl. v. 16.9.2015 – 16 W 47/15, NJW-RR 2016, 618 f.: Ein Domain-Registrar sei eher mit einem Access Provider vergleichbar als mit einem Host Provider. Die Regeln der Störerhaftung seien daher nicht ohne Weiteres übertragbar. Eine Handlungspflicht werde nur ausgelöst, wenn die Persönlichkeitsrechtsverletzung offenkundig ist (ebenso, bei einer Urheberrechtsverletzung, OLG Saarbrücken, Urt. v. 22.10.2014 – 1 U 25/14).

2. Reichweite des Löschungs-/Beseitigungsanspruchs

Unproblematisch richtet sich der Löschungsanspruch gegen den Täter auf die Beseitigung der Erstveröffentlichung. Gerade Internetveröffentlichungen verbreiten sich jedoch oft unkontrollierbar weiter, sodass die Beseitigung der Erstveröffentlichung die Persönlichkeitsrechtsverletzung nicht immer beendet. Dem trägt die Rechtsprechung Rechnung, indem sie den Beseitigungsanspruch des Opfers gegen den Ersttäter auf alle rechtswidrigen, im Internet abrufbaren Tatsachenbehauptungen erstreckt, wenn und soweit sie nachweislich falsch sind und die Beseitigung unter Abwägung der beiderseitigen Rechtspositionen zur Beseitigung des Störungszustands geeignet, erforderlich und zumutbar ist.[804] Dabei bejaht die Rechtsprechung sowohl die äquivalente als auch die adäquate Kausalität, da Meldungen im Internet typischerweise von Dritten verlinkt und kopiert würden. Der Zurechnungszusammenhang wird auch nicht deshalb verneint, weil die Persönlichkeitsrechtsverletzung insoweit erst durch das selbständige Dazwischentreten Dritter verursacht wird. Denn durch die Vervielfältigung der Abrufbarkeit des Beitrags durch Dritte verwirklicht sich eine durch die Veröffentlichung des Ursprungsbeitrags geschaffene internettypische Gefahr.[805] Für die Falschheit einer Tatsachenbehauptung streitet die dem § 186 StGB zu entnehmende Beweislastumkehr.[806]

Der Klageantrag ist darauf zu richten, den Ersttäter zu verurteilen, auf die Löschung im Internet abrufbarer Einträge hinzuwirken.[807] Nicht abschließend geklärt ist hierbei, welche Anforderungen an das „Hinwirken“ zu stellen sind. Es bleibt abzuwarten, inwiefern die Rechtsprechung die Anforderungen präzisiert.

Deliktische Löschungsansprüche können natürlichen und – unter dem Gesichtspunkt des sozialen Geltungsanspruchs von Wirtschaftsunternehmen – juristischen Personen zustehen.[808] Insoweit kann davon ausgegangen werden, dass die vorstehend dargestellten Voraussetzungen im Wesentlichen auch auf juristische Personen übertragen werden können.[809]

Eingriffe des Gesetzgebers sind zurzeit nicht geboten.

---

[804] Näher BGH, Urt. v. 28.7.2015 – VI ZR 340/14, NJW 2016, 56, Rn. 13 m. w. N.; *Peifer*, Beseitigungsansprüche im digitalen Äußerungsrecht, NJW 2016, 23; OLG Hamburg, Beschl. v. 18.2.2015 – 7 W 24/15, juris Rn. 3 ff.; OLG Celle, Urt. v. 29.1.2015 – 13 U 58/14, juris Rn. 20; LG Kaiserslautern, Urt. v. 8.7.2014 – HK O 33/13, juris Rn. 21; BGH, Urt. v. 26.11.2015 – I ZR 3/14.

[805] BGH, Urt. v. 28.7.2015 – VI ZR 340/14.

[806] BVerfG, Beschl. v. 28.6.2016 – 1 BvR 3388/14.

[807] BGH, Urt. v. 28.7.2015 – VI ZR 340/14.

[808] Vgl. z. B. BGH, Urt. v. 28.7.2015 – VI ZR 340/14, NJW 2016, 56, Rn. 27 m. w. N.

[809] Vgl. BGH, Urt. v. 14.5.2013 – VI ZR 269/12; die Entscheidung erging gegen die Suchmaschine von „Google“, mit der eine Nähe der klagenden Aktiengesellschaft zu „Scientology“ hergestellt werden konnte.

3. Reichweite des Widerrufsanspruchs

Bei der Veröffentlichung unrichtiger Tatsachen, nicht aber bei Meinungsäußerungen, kann das Opfer einer Persönlichkeitsrechtsverletzung einen öffentlichen Widerruf verlangen.

Mit Blick auf den Widerrufsanspruch stellt sich wegen der unkontrollierbaren Verbreitung von Internetbeiträgen die Frage, an welchem Ort ein Widerruf platziert werden muss. Denn der Widerruf muss an sich geeignet sein, denselben Grad an Aufmerksamkeit zu erzeugen, den die bekämpfte Behauptung beansprucht hat, sodass er grundsätzlich am gleichen Ort zu veröffentlichen ist.[810] Verbreitet sich jedoch die Erstveröffentlichung, sollte der Täter möglicherweise auch auf die Verbreitung des Widerrufs und die Beseitigung der Äußerungen Dritter auf Basis der Ursprungsäußerung hinwirken müssen. Die Entwicklung der Rechtsprechung bleibt abzuwarten.

In datenschutzrechtlicher Hinsicht könnten unter dem Aspekt des Beseitigungsanspruchs Art. 17 Abs. 2, 19 EU-DSGVO den Defiziten künftig teilweise Rechnung tragen.[811] Mit Blick auf Widerrufsansprüche bestehen jedoch gewisse Zweifel, ob Art. 19 EU-DSGVO Anwendung findet („Berichtigung"). Es soll daher beobachtet werden, ob die Defizite durch das künftige EU-Recht, einhergehend mit einer entsprechenden Bewertung in Literatur und Rechtsprechung, hinreichend ausgeräumt werden können. Die Arbeitsgruppe stellt die Thematik daher einstweilen zurück.

4. Sog. „Streisand-Effekt"

Verfahren zur Abwehr und Beseitigung von Persönlichkeitsrechtsverletzungen führen oftmals dazu, dass gerade dadurch öffentliche Aufmerksamkeit entsteht, dass weitere Personen Kenntnis erlangen oder erlangen können und sich die Persönlichkeitsrechtsverletzung vertieft. Dieser sog. „Streisand-Effekt" ist aus der „analogen Welt" bekannt und in der „digitalen Welt" nicht grundsätzlich anders, wenn er auch hinsichtlich der potentiellen Verbreitungsrisiken ein anderes Ausmaß hat. Wirksame Lösungsansätze sind bislang nicht ersichtlich.

Soweit unrichtige Tatsachenbehauptungen Gegenstand des Verfahrens sind, kann der Effekt dadurch relativiert werden, dass auch die gerichtlich festgestellte Unrichtigkeit der Tatsachenbehauptungen öffentlich wird.

Allerdings enthält die EU-DSGVO Regelungen, die dazu führen könnten, dass sich Persönlichkeitsrechtsverletzungen im Verfahren zu ihrer Abwehr und Beseitigung oft noch vertiefen:

Art. 17 Abs. 2 EU-DSGVO, der die Bekanntgabe von Löschanträgen an Dritte anordnet, kann bei Verletzungen des Rechts auf informationelle Selbstbestimmung kontraproduktiv sein (ebenso beim Recht am eigenen Wort/Bild). Es ist

---

[810] BGH, Urt. v. 15.11.1994 – VI ZR 56/94, juris Rn. 62 f.
[811] Vgl. dazu Erwägungsgrund 66 der EU-DSGVO.

zweifelhaft, ob die Vorschrift in diesen Fällen anwendbar ist. Ihre Anwendung widerspricht möglicherweise dem Zweck der EU-DSGVO.[812]

- Verbleiben Zweifel, ob Art. 17 Abs. 2 EU-DSGVO flächendeckend Anwendung findet, könnte an eine Nachjustierung auf europäischer Ebene oder eine Beschränkung im nationalen Recht gedacht werden.[813]
- Verbleiben keine Zweifel, sollte auf die Ausarbeitung einer nationalen Vorschrift hingewirkt werden, die dem Schutz der informationellen Selbstbestimmung Rechnung trägt. Wünschenswert ist es, die in Art. 17 Abs. 2 EU-DSGVO vorgesehene Bekanntgabe vom Willen des Opfers abhängig zu machen, indem z. B. im Löschantragsformular eine entsprechende Option aufgenommen wird.

Es soll daher auch hier zunächst beobachtet werden, ob und ggf. in welcher Weise Literatur und Praxis die Problematik aufgreifen.

5. Löschungsverfahren der Diensteanbieter

Mehrere Betreiber von Suchmaschinen und Social-Media-Plattformen haben mittlerweile Verfahren eingerichtet, mit denen Nutzer auf Persönlichkeitsrechtsverletzungen hinweisen können.

a. Bestandsaufnahme

Der erste Zugang wird regelmäßig über ein Formular gewährt, in dem der Betroffene seine Rechte geltend machen kann.

Die rechtlichen Vorgaben sind verhältnismäßig allgemein. Wie dargelegt, verlangt die Rechtsprechung jedoch für den Erfolg eines gerichtlich durchzusetzenden Löschungsbegehrens grundsätzlich, dass der Intermediär auf die Persönlichkeitsrechtsverletzung hingewiesen wird, damit er dem (materiell-rechtlichen) Löschungsanspruch genügen kann. Ihm bleibt eine angemessene Prüffrist, deren Dauer sich nach den Umständen des jeweiligen Einzelfalles richtet. Geht der Intermediär den Hinweisen nicht nach, kann der Rechtsweg beschritten werden.[814]

Inhaltlich geht die Rechtsprechung davon aus, dass bei unwahren Tatsachenbehauptungen die Abwägung grundsätzlich zu Gunsten des Betroffenen zu erfolgen habe.[815] Auch der EuGH hat ausgeführt, dass die geschützten Rechte der betroffenen Person im Allgemeinen die Interessen der Internetnutzer überwiegen würden. Der Ausgleich könne aber in besonders gelagerten Fällen von der Art der betroffenen Person und vom Interesse der Öffentlichkeit am Zugang zu der Information abhängen. In der Literatur ist dieses Abwägungsprogramm als „unterkomplex“

---

[812] Z. B. Erwägungsgrund 78 der EU-DSGVO einerseits, Erwägungsgrund 66 der EU-DSGVO andererseits.
[813] Vgl. Art. 23 Abs. 1 Buchst. j. EU-DSGVO, Erwägungsgrund 73 der EU-DSGVO.
[814] LG Heidelberg, Urt. v. 9.12.2004 – 2 O 162/13 (zu Google).
[815] LG Hamburg, Urt. v. 7.11.2014 – 324 O 660/12 (Google).

kritisiert worden; es wird vorgeschlagen, weitere Aspekte in die Abwägung einzubeziehen:

- Grenzen der Schmähkritik und Verleumdung,
- Recht auf Resozialisierung,
- Aggregation von Informationen aus verschiedenen Quellen und Lebensbereichen zu einem „Abbild der Onlinepersönlichkeit“,
- drohender materieller oder immaterieller Schaden.[816]

Die Europäische Kommission hat am 31. Mai 2016 zusammen mit Facebook, Twitter, YouTube und Microsoft einen Verhaltenskodex vorgestellt, mit dem die Verbreitung schwerer Persönlichkeitsrechtsverletzungen im Internet bekämpft werden soll. Darin haben sich die IT-Unternehmen dazu verpflichtet, klare und wirksame Verfahren für die Prüfung von Meldungen über „Hate Speech“ in ihren Diensten einzuführen. So sollen die Anträge mehrheitlich in weniger als 24 Stunden geprüft und die beanstandeten Beiträge bzw. Seiten erforderlichenfalls gelöscht beziehungsweise gesperrt werden.

Das Bundesministerium der Justiz und für Verbraucherschutz hat zusammen mit Facebook, Google und Twitter sowie zivilgesellschaftlichen Organisationen eine Task Force zum Umgang mit Hassbotschaften im Internet eingesetzt. Deren im Dezember 2015 veröffentlichtes Ergebnispapier sah vor, dass Nutzern einfache Möglichkeiten zum Melden von Hassbotschaften zur Verfügung gestellt werden, dass deutsches Recht bei der Prüfung dieser Meldungen zu Grunde gelegt werden solle, und dass die Mehrzahl der rechtswidrigen Inhalte binnen 24 Stunden gelöscht werden solle. Erhebungen haben indes ergeben, dass nach wie vor zu wenige strafbare Hasskommentare gelöscht werden, die von den Nutzern gemeldet werden. Ein von jugendschutz.net durchgeführtes Monitoring der Löschpraxis sozialer Netzwerke von Januar/Februar 2017 hat ergeben, dass die Beschwerden normaler Nutzer gegen Hasskriminalität und andere strafbare Inhalte nach wie vor nicht unverzüglich und ausreichend bearbeitet werden.

Auch wenn über Art und Umfang von Löschungsansprüchen gegen Diensteanbieter im Allgemeinen wenig bekannt ist, erlauben allein die von Google veröffentlichten Angaben über die gegen Google gerichteten Löschungsverfahren den Schluss auf eine immense Praxisbedeutung:

Weltweit wurden danach zwischen dem 29. Mai 2014 und dem 19. Januar 2017 675.624 Ersuchen zur Löschung von 1.865.610 URLs aus Anlass des Google-Urteils des EuGH gegenüber Google gestellt, die zu 43,2 % erfolgreich waren

---

[816] *Luch/Schulz/Kuhlmann*, Ein Recht auf Vergessenwerden als Ausprägung einer selbstbestimmten digitalen Persönlichkeit, EuR 2014, 698.

(aus Deutschland waren 328.231 URLs durch 90.488 Ersuchen betroffen; 48,1 % der betroffenen URLs wurden gelöscht).[817]

Die übrigen 56,8 % sind potentielle Gerichtsverfahren.

Am häufigsten betroffen sind folgende zehn Websites (8 % aller URLs):

- www.facebook.com (15.815 URLs entfernt)
- profileengine.com (10.409 URLs entfernt)
- groups.google.com (7.716 URLs entfernt)
- www.youtube.com (8.016 URLs entfernt)
- annuaire.118712.fr (8.856 URLs entfernt)
- twitter.com (6.875 URLs entfernt)
- plus.google.com (6.621 URLs entfernt)
- badoo.com (5.237 URLs entfernt)
- www.wherevent.com (4.906 URLs entfernt)
- www.192.com (4.092 URLs entfernt).

Die Verfahren sind je nach Diensteanbieter uneinheitlich ausgestaltet, erscheinen aufwändig, nicht immer übersichtlich, die bereitgestellten Formulare sind teilweise schwer aufzufinden, die Entscheidungsprozesse nicht transparent. Der hohe Grad an Praxisrelevanz der Löschungsverfahren dokumentiert zudem, dass deren ungeeignete Ausgestaltung das Potential in sich birgt, die gerichtliche Praxis erheblich zu belasten:

- Google – dessen sich etwa auch das deutsche Portal „T-Online“ zur Websuche bedient – ermöglicht die Löschung über ein Online-Formular, das jedoch erst aufgefunden werden kann, wenn man über die Rubriken „Datenschutz“ – „Häufig gestellte Fragen“ zu der Frage „Wie setzt Google die Entscheidung des EuGH um“ gelangt. Daraufhin erhält der Anfragende eine automatisch erstellte Antwort mit einer Bestätigung, dass der Antrag eingegangen ist. Anschließend wird der Fall geprüft. Aufgrund der hohen Anzahl der bereits gestellten Anträge könne dies allerdings einige Zeit dauern. Bei der Bearbeitung des Antrags werde geprüft, ob die Ergebnisse veraltete Informationen über das Privatleben enthalten. Zudem werde untersucht, ob ein öffentliches Interesse an den verbleibenden Informationen besteht, z. B., wenn es um Betrugsmaschen, berufliches Fehlverhalten, strafrechtliche Verurteilungen oder das öffentliche Verhalten als (gewählter oder nicht gewählter) Amtsträger geht. Das Formular selbst verlangt Anga-

---

[817] Tagesaktuelle Daten, auch zur Erfolgsquote, abrufbar unter https://www.google.com/transparencyreport/removals/europeprivacy/?hl=de (letzter Abruf 19.1.2017).

ben zur Identität des Anspruchsstellers, eine genaue Bezeichnung der verlinkten Internetseiten sowie eine Erläuterung der Beeinträchtigung. Zudem wird die eingescannte Übersendung eines Identitätspapiers verlangt.[818]

- Die von Microsoft betriebene Suchmaschine „Bing“ (einschließlich AOL, die mit Bing kooperiert, und Yahoo, die ebenfalls die Websuche über Bing ermöglicht) bietet über den Link „Datenschutz in Europa“ (der indes über Yahoo nicht aufgerufen werden kann) einen formularmäßigen Antrag zur Sperrung von Bing-Suchergebnissen in Europa.
- Die Suchmaschine de.ask.com ermöglicht – obgleich auch in Deutschland auf Deutsch betrieben – ein Löschungsbegehren nur in englischer Sprache per E-Mail an einen Kontakt in Irland.

Zum konkreten Abwägungsprozess bei den Suchmaschinenbetreibern selbst ist bislang wenig bekannt. Google bezeichnet sie als „schwierige Abwägungen“, die man als privates Unternehmen nicht in jedem Fall zweifelsfrei vornehmen könne und empfiehlt als Rechtsbehelf, sich an „die lokalen Datenschutzbehörden“ zu wenden.

Google gibt an, es sei ein Team aus speziell zu diesem Zweck ausgebildeten Prüfern in Dublin (Irland) gebildet worden. Seit dem 1. November 2015 würde bei etwa 30 % der Ersuchen eine Zweiteinschätzung bei erfahrenen Prüfern oder Unternehmensjuristen eingeholt.

Auch Facebook steht wegen seiner Löschpolitik in der Kritik: Erst jüngst haben ca. 70 US-Menschenrechtsgruppen an Facebook appelliert, die Praktiken des Unternehmens bei der Löschung von Inhalten offen zu legen. Die Organisationen verlangen von dem sozialen Netzwerk u. a., dass es seine Richtlinien für das Löschen von Inhalten für die Öffentlichkeit zugänglich macht.[819]

Eine Anhörung der Verantwortlichen ist nur selten vorgesehen.

- Wikipedia sieht eine siebentägige Löschdiskussion vor, an der sich auch die Verantwortlichen beteiligen können (anders bei sog. Schnelllöschungsverfahren, etwa im Fall offensichtlicher Persönlichkeitsrechtsverletzungen). Der beanstandete Artikel erhält einen rot umrahmten Hinweis auf den Eingang eines Löschantrags mit einem Link zur Löschdiskussion. Nach der Löschung können die Verantwortlichen gegenüber dem für die Löschung verantwortlichen Administrator remonstrieren und eine „Löschprüfung“ durch einen anderen Administrator einleiten.

---

[818] In der Vergangenheit wurde ausdrücklich der Scan des Personalausweises verlangt, was jedoch teilweise als Verstoß gegen § 20 Abs. 2 PersAuswG angesehen wurde. Danach darf ein Personalausweis weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden.

[819] http://www.spiegel.de/netzwelt/web/facebook-us-menschenrechtsgruppen-fordern-offenlegung-von-loeschprozessen-a-1119093.html (letzter Abruf: 1.2.2017).

- Google gibt Löschungen über ein sog. „Webmaster-Tool“ bekannt. Wenn die Verantwortlichen dieses Tool nutzen, werden sie informiert und können die Überprüfung der Löschungsentscheidung beantragen.

b. Vorschläge zum Löschungsverfahren

Die bisherigen Bemühungen von Plattformanbietern, effektiv gegen Persönlichkeitsrechtsverletzungen vorzugehen, reichen vielerorts nicht aus. Es ist daher erforderlich, eine schnelle und effektive Bearbeitung von Hinweisen auf rechtswidrige Inhalte durch Plattformanbieter sowie erforderlichenfalls eine zügige Löschung sicherzustellen.

Die Arbeitsgruppe hat wünschenswerte Bestandteile eines sachgerechten Löschungsverfahrens herausgearbeitet, deren Übereinstimmung mit bestehenden und künftigen europäischen Vorgaben überprüft werden muss, wenn sich ein belastbares Meinungsbild zur Auslegung der EU-DSGVO herausgebildet und sich die e-Privacy Verordnung konkretisiert hat.

(1) Vereinheitlichung und Transparenz

Die Löschungsersuchen sollten einheitlich und verbraucherfreundlich sein.

- Erforderlich erscheint eine gewisse Vereinheitlichung der Antragsbearbeitung bei den verschiedenen Diensteanbietern, insbesondere bei der Initiierung der Löschungsverfahren durch die Betroffenen – etwa im Sinne eines „Notice-and-Takedown-Verfahrens, vgl. Artikel 14 Abs. 3 der Richtlinie über den elektronischen Geschäftsverkehr. Zu vereinheitlichen wären die Vorgaben im Hinblick auf die Antragstellung, d.h. die Auffindbarkeit des Antrags, die Antragssprache sowie die Antragsübermittlung.
- Auffindbarkeit des Löschantrags: Zu fordern ist eine „Button-Lösung“, die es ermöglicht, mit Hilfe eines klar gekennzeichneten Buttons in der Nähe eines Beitrags mit einem Klick ein Löschantragsformular aufzurufen (z. B. „Verstoß melden“, „Feedback mitteilen“).
- Antragssprache: Das Löschantragsformular sollte in der Sprache abgefasst sein, in der die jeweilige Veröffentlichung (z. B. die Webseite) abgefasst ist. Zudem sollte es ergänzend in Englisch verfügbar sein, wenn die Veröffentlichung nicht in deutscher Sprache erfolgte.
- Die Datenschutzbehörden sollten auf eine im Übrigen „effektive, durchschaubare, barrierefreie Verfahrensgestaltung“ hinwirken.

(2) Verfahren

Das zu fordernde unkomplizierte Löschungsverfahren darf andererseits nicht zu einer voraussetzungslosen Löschung führen. Im Hinblick auf das einzuhaltende Löschverfahren ist vielmehr auf die oben dargestellten Voraussetzungen des zugrundeliegenden materiell-rechtlichen Löschungsanspruches abzustellen. Die Löschung des Beitrags oder die Sperrung des Zugangs hierzu ist nur zulässig, wenn dies unter Abwägung der Beeinträchtigung des Betroffenen mit dem Grundrecht auf Meinungsfreiheit des Äußernden und unter Wahrung der Grundsätze des Meinungspluralismus geboten ist.

Diese Abwägung und die Prüfung der Voraussetzungen ist daher durch den Intermediär im Verfahren durch den ausreichenden Einsatz geeigneten und geschulten Personals sicherzustellen. Erforderlich hierfür dürfte zudem sein, dass die Intermediäre ihre Kriterien zur Löschung und das Verfahren offenlegen.

Wo dies möglich ist, sollten beanstandete Beiträge zudem zunächst entsprechend markiert werden, um – etwa bei einem als „Fake-News“ beanstandeten Beitrag – bereits in der Prüfungsphase zu verdeutlichen, dass der Inhalt dieses Beitrags umstritten ist. In geeigneten Fällen kann auch eine Löschungsdiskussion sinnvoll sein; Wikipedia sieht etwa – mit Ausnahme von sog. „Schnelllöschungsverfahren“ – eine siebentägige Diskussion vor, an der sich auch die Verantwortlichen beteiligen können.

(3) Anhörung

Grundsätzlich geboten ist eine Pflicht zur Anhörung der für den Beitrag Verantwortlichen.

Weder die Interessen der Verantwortlichen noch das Informationsinteresse der Allgemeinheit scheinen im Löschungsverfahren nach der EU-DSGVO berücksichtigt zu sein. Ausnahmen bestehen, soweit der jeweilige Diensteanbieter sie bei der Ausgestaltung des Verfahrens berücksichtigt. Auch im Hinblick auf telemedienrechtliche Möglichkeiten eines „Notice-and-Takedown-Verfahrens“ bestehen bislang keine Vorgaben zu der Frage der Anhörung des Verantwortlichen.

Eine Anhörung der Verantwortlichen ist auch grundsätzlich technisch möglich und zumutbar:

- Foren- und Portalbetreiber sowie Betreiber von Online-Enzyklopädien können den Löschantrag auf dem Forum/Portal bekanntgeben.
- Suchmaschinenbetreiber können über das in der EU in vielen Fällen vorgeschriebene Impressum den jeweiligen Seitenbetreiber kontaktieren.
- Für Online-Archive und Access-Provider dürfte eine Anhörungspflicht demgegenüber grundsätzlich nicht in Frage kommen.

Die vom BGH entwickelten Grundsätze über die Anhörung der Verantwortlichen sollen beibehalten werden.

- Der BGH hatte zunächst den Diensteanbietern eine Art Schiedsrichterfunktion[820] zuerkannt:[821]

  Ein Tätigwerden des Hostproviders ist nur veranlasst, wenn der Hinweis so konkret gefasst ist, dass der Rechtsverstoß auf der Grundlage der Behauptungen des Betroffenen unschwer - das heißt ohne eingehende rechtliche und tatsächliche Überprüfung - bejaht werden kann. Dabei hängt das Ausmaß des insoweit vom Provider zu verlangenden Prüfungsaufwandes von den Umständen des Einzelfalls ab, insbesondere vom Gewicht der angezeigten Rechtsverletzungen auf der einen und den Erkenntnismöglichkeiten des Providers auf der anderen Seite. Regelmäßig ist zunächst die Beanstandung des Betroffenen an den Verantwortlichen zur Stellungnahme weiterzuleiten. Bleibt eine Stellungnahme innerhalb einer nach den Umständen angemessenen Frist aus, ist von der Berechtigung der Beanstandung auszugehen und der beanstandete Eintrag zu löschen. Stellt der Verantwortliche die Berechtigung der Beanstandung substantiiert in Abrede und ergeben sich deshalb berechtigte Zweifel, ist der Provider grundsätzlich gehalten, dem Betroffenen dies mitzuteilen und ggf. Nachweise zu verlangen, aus denen sich die behauptete Rechtsverletzung ergibt. Bleibt eine Stellungnahme des Betroffenen aus oder legt er ggf. erforderliche Nachweise nicht vor, ist eine weitere Prüfung nicht veranlasst. Ergibt sich aus der Stellungnahme des Betroffenen oder den vorgelegten Belegen auch unter Berücksichtigung einer etwaigen Äußerung des für den Blog Verantwortlichen eine rechtswidrige Verletzung des Persönlichkeitsrechts, ist der beanstandete Eintrag zu löschen.

- Mit Blick auf Bewertungsportale hat er den Portalbetreibern „reaktive Prüfungspflichten“ zugewiesen. Ihr Umfang orientiert sich am Zumutbaren im Einzelfall. Erhält der Portalbetreiber einen Hinweis, der so konkret gefasst ist, dass der Rechtsverstoß auf Grundlage der Behauptung des Betroffenen unschwer bejaht werden kann, ist ein erkennbar ernsthafter Versuch der Ermittlung und Bewertung des gesamten Sachverhalts unter Berücksichtigung einer etwaigen Stellungnahme des für den beanstandeten Beitrag Verantwortlichen erforderlich.[822] Im konkreten Fall hatte der bewertete Arzt eingewendet, es habe kein Kontakt im Sinne einer Heilbehandlung zu dem Bewertenden stattgefunden, und damit den Schutz der Meinungsäußerung durch einen Angriff auf den zugrundeliegenden Sachverhalt relativiert.

---

[820] *Höch*, Bewegung bei Bewertungsportalen – wie Unternehmen ihren Ruf im Netz besser schützen können, BB 2016, 1475 (1478).
[821] BGH, Urt. v. 25.10.2011 – VI ZR 93/10, juris Rn. 26 f. („blogspot.com“).
[822] BGH, Urt. v. 1.3.2016 – VI ZR 34/15, juris Rn. 24, 38-43 (“jameda.de II”).

Bei der Entscheidung, ob die Verantwortlichen vor der Löschung angehört werden, sollte auch das öffentliche Interesse an einem Beitrag berücksichtigt werden. Hierfür kann z. B. die Anzahl der Aufrufe ein Indiz darstellen.

Die Anhörung soll grundsätzlich vor der Löschung stattfinden, in Eil- und Evidenzfällen nachträglich.

(4) „Rechtsbehelfsbelehrung“

Angezeigt erscheint eine Unterrichtung des Antragstellers und der jeweils unterlegenen Seite über den Ausgang der Löschverfahren. Eine Begründungspflicht wäre zwar aus Verbrauchersicht vorteilhaft, sollte aber nicht verbindlich vorgeschrieben werden, weil die damit verbundenen Personalkosten kleinere Diensteanbieter zu sehr belasten würden, und das Verfahren zur Bearbeitung von Löschungsansprüchen damit zu einer Markteintrittsbarriere für Diensteanbieter werden kann. Um den Nutzern zu verdeutlichen, dass die Möglichkeit eines rechtlichen Vorgehens im Hinblick auf den beanstandeten Beitrag von dieser Entscheidung unberührt bleibt, sollte die Mitteilung einen entsprechenden Hinweis enthalten. Wird ein Ombudsmann (hierzu Punkt 5 (c) eingeführt, kann es sich anbieten, auf diesen hinzuweisen.

(5) Rechtsdurchsetzung

Es bestehen zahlreiche Defizite bei der Rechtsdurchsetzung, insbesondere im – häufigen – Fall eines Auslandsbezugs.

(a) Durchsetzung im Ausland

Wünschenswert ist die Benennung eines Zustellungsbevollmächtigten innerhalb der EU für Forderungsschreiben, Schriftsätze und Klagen.

Die Justizministerinnen und Justizminister richteten im Zusammenhang mit der Thematik der so genannten „Hate Speech“ auf ihrer Herbstkonferenz am 17. November 2016 in Berlin an den Bundesjustizminister u.a. die Bitte, geeignete Lösungsvorschläge zu entwickeln, die eine effektive Löschung von „Hate Speech“ ermöglichen und dabei sicherstellen, dass Schriftsätze und Klagen an Internetunternehmen mit Sitz im Ausland zeitnah zugestellt werden können. Als denkbare Möglichkeit wurde aufgezeigt, die Internetunternehmen im medialen Bereich, die ihre Geschäftstätigkeit gerade auch auf den deutschen Markt ausrichten, zu verpflichten, in Anlehnung und Ausweitung der Regelung des § 184 ZPO generell und unabhängig von einem bereits bestehenden Prozessrechtsverhältnis einen Zustellungsbevollmächtigten im Inland zu benennen, an den Schriftstücke zugestellt und E-Mails gesendet werden können.

Angesichts des grenzüberschreitenden Charakters dieser Problematik und zur Verhinderung europarechtswidriger Zustände sollte auf eine entsprechende Regelung auf EU-Ebene hingearbeitet werden. Nationale Regeln sehen sich immer der Gefahr der Europarechtswidrigkeit ausgesetzt, zum einen wegen Verstoßes gegen die Grundfreiheiten, zum anderen wegen Verstoßes gegen europäisches Sekundärrecht.

Im Anwendungsbereich der EU-Zustellverordnung Nr. 1393/2007 sind fiktive Inlandszustellungen, wie etwa nach § 184 Abs. 1 S. 2 ZPO, bei Nichtbenennung eines Zustellungsbevollmächtigten wegen Verstoßes gegen Sekundärrecht europarechtswidrig. Der EuGH geht davon aus, dass die Zustellverordnung für Zustellungen an „im Ausland Ansässige" abschließende Regelungen enthält.[823]

Nicht in den Konflikt mit der EU-Zustellverordnung käme eine nationale Regelung, nach der die Mitgliedstaaten einem Unternehmen lediglich aufgeben würden, einen Zustellungsbevollmächtigten zu benennen, ohne dass sich eine Zustellfiktion anschließt. Insofern sieht Erwägungsgrund (8) der Verordnung Nr. 1393/2007 vor, dass diese nicht für die Zustellung eines Schriftstücks an den Bevollmächtigten einer Partei in dem Mitgliedstaat gilt, in dem das Verfahren anhängig ist, unabhängig davon, wo die Partei ihren Wohnsitz hat.[824]

Eine solche Verpflichtung zur Benennung eines Zustellungsbevollmächtigten, insbesondere wenn sie bußgeldbewehrt ist, würde allerdings eine Beschränkung des freien Dienstleistungsverkehrs i. S. v. Art. 56 AEUV (ex Art. 49 EGV) darstellen und bedürfte der Rechtfertigung nach gemeinschaftsrechtlichen Maßstäben, d.h. der Mitgliedstaat müsste nachweisen, dass im Hinblick auf die betreffende Tätigkeit zwingende Gründe des Allgemeininteresses bestehen, die Beschränkungen des freien Dienstleistungsverkehrs rechtfertigen, dass dieses Interesse nicht bereits durch die Vorschriften des Niederlassungsstaats gewahrt ist und dass das gleiche Ergebnis nicht durch weniger einschränkende Bestimmungen erreicht werden kann. Der EuGH hat in einer Entscheidung vom 11. Juni 2009 die Verhältnismäßigkeit einer österreichischen Regelung verneint, die in einem anderen Mitgliedstaat regulär niedergelassene Patentanwälte, die vorübergehend in Österreich Dienstleistungen erbringen wollten, verpflichtete, einen in Österreich wohnhaften Zustellungsbevollmächtigten zu bestellen.[825] Hierzu hat er ausgeführt: „Die Notwendigkeit, einen ordnungsgemäßen Verfahrensablauf zu gewährleisten, lässt sich zwar als zwingenden Grund des Allgemeininteresses anführen, der eine Beschränkung des freien Dienstleistungsverkehrs rechtfertigen kann. Wie die Kommission jedoch dargetan hat, geht die Verpflichtung, einen in Österreich wohnhaften Zustellungsbevollmächtigten zu bestellen, über das hinaus, was zur Erreichung dieses Ziels erforderlich ist. Zum einen bieten die modernen elektronischen Kommunikationsmittel den Patentanwälten die Möglichkeit, die notwendige Kommunikation mit Gerichten und Verwaltungsbehörden auf angemessene Weise zu gewährleisten. Es ist nämlich unstreitig, dass es verschiedene technische Mittel, wie Telefax und E-Mail gibt, die eine Zustellung von gerichtlichen und behördlichen Mitteilungen ermöglichen. Zum anderen setzt die postalische Zustellung nicht voraus, dass im Aufnahmestaat ein Zustellungsbevollmächtigter bestellt wird. Sie kann unmittelbar zwischen den Mitgliedstaaten ohne diesen Vermittler durchgeführt werden, wie dies in den Artikeln 14 und 16

---

[823] EuGH, Urt. v. 19.12.2012 – Rs. C-325/11.
[824] Vgl. EuGH, Urt. v. 19.12.2012 − Rs. C-325/11, NJW 2013, 443 ff., juris, Rn. 24.
[825] EuGH, Urt. v. 11.6.2009 – Rs. C-564/07.

der Verordnung Nr. 1348/2000 anerkannt wurde, die bei Ablauf dem vorliegenden Fall in der mit Gründen versehenen Stellungnahme gesetzten Frist in Kraft waren, und wie dies fortan mit den Artikeln 14 und 16 der Verordnung Nr. 1393/2007 anerkannt wird.“[826]

In Straf- und Bußgeldverfahren stehen die Art. 2, 3 Abs. 1 Buchst. c und 6 Abs. 1 und Abs. 3 der Richtlinie 2012/13/EU über das Recht auf Belehrung und Unterrichtung in Strafverfahren Rechtsvorschriften eines Mitgliedstaats zwar nicht grundsätzlich entgegen, nach welcher der in einem Strafverfahren Beschuldigte, der in diesem Mitgliedstaat keinen Wohnsitz hat, für die Zustellung eines an ihn gerichteten Strafbefehls einen Zustellungsbevollmächtigten benennen muss; allerdings ist zu gewährleisten, dass der Beschuldigte tatsächlich über die volle Frist für die Einlegung des Rechtsmittels verfügt.[827] Auch insofern sind nationale Regelungen nur beschränkt sinnvoll.

Übersetzungspflichten sollten sich nach den allgemeinen Vorschriften richten. Der Aufwand für die Vorlage einer Übersetzung erscheint angesichts des verfassungsrechtlichen Gebots eines fairen Verfahrens hinnehmbar.

Im Beschlussweg ergangene Unterlassungsverfügungen eines deutschen Gerichts haben im Ausland nur beschränkte Wirkung. Mögliche Maßnahmen zur Steigerung der Effizienz einstweiliger Verfügungen gegen ausländische Diensteanbieter sind derzeit jedoch nicht ersichtlich. In EU-Mitgliedsstaaten sind einstweilige Verfügungen nach Art. 42 Abs. 2 Brüssel-Ia-VO (EU) 1215/2012 ohne Exequaturverfahren vollstreckbar.

(b) Einführung eines Verbandsklagerechts

Mit dem Ende Februar 2016 in Kraft getretenen Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts wurde eine Verbandsklagebefugnis für Datenschutzverstöße in § 2 Abs. 2 Nr. 11 UKlaG eingeführt. Die Regelung dürfte auch im Hinblick auf § 80 EU-DSGVO als Teilumsetzung der Öffnungsklausel nach Art. 80 Abs. 2 EU-DSGVO zulässig sein.[828]

Da das Datenschutzrecht seine Wurzeln im Recht auf informationelle Selbstbestimmung hat, welches als Teil des Persönlichkeitsrechts definiert wurde, dürfte für einige Konstellationen, die das allgemeine Persönlichkeitsrecht betreffen, der Weg der Verbandsklage eröffnet sein. Für Persönlichkeitsrechtsverletzungen außerhalb verbraucherschützender Vorschriften des Datenschutzrechts wäre es sinnvoll, ein Verbandsklagerecht für die Fälle einzurichten, in denen der Diensteanbieter nicht das geforderte Löschverfahren vorhält. Dies erscheint im Hinblick auf

---

[826] EuGH, Urt. v. 11.6.2009 − Rs. C-564/07.
[827] EuGH, Urt. v. 15.10.2015 – Rs. C-216/14.
[828] Kühling/Buchner/*Bergt*, DS-GVO, Art. 80 Rn. 13, 18; *Halfmeier*, Die neue Datenschutzverbandsklage, NJW 2016, 1126; *Schantz*, Die Datenschutz-Grundverordnung, NJW 2016, 1841; a.A. Gola/*Werkmeister*, DS-GVO, Art. 80 Rn. 18.

das ausgeprägt ungleiche Machtverhältnis zwischen den großen Anbietern, wie z. B. Google oder Facebook einerseits, sowie dem im Einzelfall Betroffenen andererseits jedenfalls für den Bereich der „digitalen Welt“ geboten.

(c) Einführung eines sog. „Ombudsmanns“

Ausgehend von den oben dargestellten Selbstverpflichtungen der Diensteanbieter gegenüber der Europäischen Kommission und dem Bundesministerium der Justiz und für Verbraucherschutz könnte überdies die Einführung eines sog. Ombudsmanns für Streitigkeiten im Zusammenhang mit Persönlichkeitsrechtsverletzungen im Internet angedacht werden. Dieser könnte - wie etwa der sog. Ombudsmann für Versicherungen in § 214 VVG - privatrechtlich als eingetragener Verein organisiert werden und als Schlichtungsstelle nach dem Verbraucherstreitbeilegungsgesetz für derartige Streitigkeiten zwischen Betroffenen und den Intermediären dienen und mit deren Zustimmung auch gegenüber Diensteanbietern vermitteln, die ihre Niederlassung nicht in Deutschland haben.

Entsprechende Beschwerdestellen bestehen teilweise bereits, etwa die Beschwerdestelle des Verbands der Deutschen Internetwirtschaft e.V.[829] Finanziert werden könnte die Einrichtung durch die Diensteanbieter selbst - in Erfüllung ihrer Selbstverpflichtung zur Bekämpfung von Persönlichkeitsrechtsverletzungen und zur Vermeidung unnötiger Rechtsstreitigkeiten. Nutzern stünde auf diese Weise eine unbürokratische Stelle zur Verfügung, an die sie sich nach erfolglosem Herantreten an den Intermediär auf elektronischem Wege wenden könnten, ohne - insbesondere bei grenzüberschreitenden Sachverhalten - den Rechtsweg beschreiten zu müssen. Da dies auf einer Selbstverpflichtung der Internetanbieter beruht, stünden auch europarechtliche Vorgaben einer solchen Lösung nicht entgegen.

(d) Ergänzende öffentlich-rechtliche Rechtsdurchsetzung

Allgemein ist bei der Frage der Lösung von Durchsetzungsproblemen allerdings auch zu beachten, dass die bestehenden Defizite bei einer zivilrechtlichen Geltendmachung von Ansprüchen teilweise dadurch relativiert werden, dass dem Betroffenen auf dem Sektor des Datenschutzes auch öffentlich-rechtliche Eingriffsnormen und -befugnisse zur Seite gestellt sind. Zu nennen sind hier nach geltendem Recht etwa §§ 38, 43 BDSG, §§ 43a ff TKG sowie rundfunkstaatsvertragliche und landesrechtliche gefahrenabwehrrechtliche Ermächtigungsgrundlagen. Darüber hinaus sieht auch die EU-DSGVO derartige Möglichkeiten vor, vgl. dort z. B. Art. 55 ff., 77, 78.

---

[829] https://www.eco.de/services/internet-beschwerdestelle.html.

(6) Rechtliche Rahmenbedingungen für eine gesetzliche Lösung

(a) EU-DSGVO

In datenschutzrechtlicher Hinsicht enthält Art. 17 Abs. 2 EU-DSGVO Regelungen zum Löschungsverfahren. Ein belastbares Meinungsbild zur Frage, inwieweit der nationale Gesetzgeber das entsprechende Löschungsverfahren gesetzlich weiter ausgestalten kann, hat sich jedoch noch nicht herausgebildet. Die weiteren Entwicklungen sind insoweit abzuwarten. Auch das jüngst erschienene Gutachten von Martini u.a.[830] verhält sich hierzu nicht abschließend.

(b) Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr

Auch außerhalb des Anwendungsbereichs der EU-DSGVO erfahren mögliche telemedienrechtliche Regelungen im Hinblick auf Löschungsverfahren auf zivilrechtlicher Rechtsgrundlage im Zusammenhang mit Telemediendiensten Einschränkungen durch die Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr - die nach Art. 2 Abs. 4 (vgl. Erwägungsgrund 21) der EU-DSGVO durch letztere nicht berührt wird.

Die Richtlinie über den elektronischen Geschäftsverkehr (2000/31/EG) sieht in Art. 3 Abs. 2 vor, dass die Mitgliedsstaaten den freien Verkehr von Diensten der Informationsgesellschaft aus einem anderen Mitgliedsstaat nicht aus Gründen einschränken dürfen, die in den durch die Richtlinie koordinierten Bereich fallen. Jedenfalls im Hinblick auf Diensteanbieter, die innerhalb des Geltungsbereichs der Richtlinien 2000/31/EG und 89/552/EWG niedergelassen sind, können Regelungen folglich mit der Richtlinie in Konflikt stehen. Nicht anwendbar ist die Richtlinie allerdings auf Dienste von Anbietern, die in einem Drittstaat niedergelassen sind (vgl. Erwägungsgrund 58).

Zwar können Maßnahmen, die aus Gründen des Schutzes der öffentlichen Ordnung - einschließlich der Hetze u.a. aus Gründen der Nationalität sowie der Verletzung der Menschenwürde -, des Schutzes der öffentlichen Gesundheit, der öffentlichen Sicherheit sowie des Schutzes der Verbraucher bei jeweils ernsthafter und schwerwiegender Gefahr für diese Rechtsgüter erforderlich sind, getroffen werden. Voraussetzung hierfür ist allerdings, dass der betreffende Mitgliedstaat vor Ergreifen der betreffenden Maßnahmen den Mitgliedstaat, in dem der betreffende Dienstleister seinen Sitz hat, vergeblich zu entsprechenden Maßnahmen aufgefordert und die Kommission über die Absicht entsprechender Maßnahmen unterrichtet hat.

Speziell im Hinblick auf die identifizierten wünschenswerten Bestandteile eines sachgerechten Löschungsverfahrens sieht Art. 14 der Richtlinie 2000/31/EG - wie es in § 10 TMG umgesetzt wurde - vor, dass ein Diensteanbieter nicht für die

---

[830] *Kühling/Heberlein/Kühl/Nink/Weinzierl/Wenzel,* Die Datenschutzgrundverordnung und das nationale Recht – Erste Überlegungen zum nationalen Regelungsbedarf, abrufbar unter http://www.foev-speyer.de/files/de/downloads/Kuehling_Martini_et_al_Die_DSGVO_und_das_nationale_Recht_2016.pdf (letzter Abruf: 19.1.2017).

gespeicherte fremde Information (Hosting) verantwortlich ist, wenn der Anbieter keine tatsächliche Kenntnis von der rechtswidrigen Tätigkeit oder Information hat und er sich in Bezug auf Schadensersatzansprüche auch keiner Umstände bewusst ist, aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wird, und der Anbieter, sobald er diese Kenntnis erlangt, unverzüglich tätig wird, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

Nach Abs. 3 lässt diese Vorschrift allerdings die Möglichkeit unberührt, dass die Mitgliedstaaten Verfahren für das Entfernen einer Information oder die Sperrung des Zugangs zu ihr festlegen. Erwägungsgrund 40 führt aus, dass Diensteanbieter unter bestimmten Voraussetzungen verpflichtet sind, tätig zu werden, um rechtswidrige Tätigkeiten zu verhindern oder abzustellen. Die Bestimmungen der Richtlinie sollten eine geeignete Grundlage für die Entwicklung rasch und zuverlässig wirkender Verfahren zur Entfernung unerlaubter Informationen und zur Sperrung des Zugangs zu ihnen bilden. Auch Erwägungsgrund 46 geht davon aus, dass die Richtlinie die Möglichkeiten der Mitgliedsstaaten unberührt lässt, spezifische Anforderungen vorzuschreiben, die vor der Entfernung von Informationen oder der Sperrung des Zugangs unverzüglich zu erfüllen sind.

Unter diesem Gesichtspunkt könnte sich eine telemedienrechtliche Regelung, die ein sog. „Notice-and-Takedown-Verfahren“ (zu diesem Begriff vgl. Art. 21 Abs. 2 der Richtlinie) im Sinne der oben dargestellten wünschenswerten Bestandteile eines sachgerechten Löschungsverfahrens vorschreibt, als richtlinienkonform erweisen.

Allerdings ist zudem zu beachten, dass für Diensteanbieter mit Sitz in einem anderen europäischen Mitgliedstaat (etwa Irland im Hinblick auf Google oder Facebook) nach dem sog. Herkunftslandsprinzip (§ 3 Abs. 2 TMG) das dortige Telemedienrecht anwendbar sein kann. Die in verschiedenen Staaten jeweils unterschiedliche Rechtslage kann dazu führen, dass Löschungen von Inhalten durch die Diensteanbieter nur auf Grundlage ihrer jeweiligen Allgemeinen Nutzungsbedingungen bzw. der Gemeinschaftsstandards der sozialen Netzwerke möglich sind.

Eine mögliche gesetzliche Ausgestaltung eines „Notice and Takedown-Verfahrens“, wie es Art. 14 der Richtlinie 2000/31 EG voraussetzt, könnte daher am effektivsten auf europäischer Ebene erfolgen. Art. 21 Abs. 2 der Richtlinie sieht in diesem Zusammenhang vor, dass bei – alle zwei Jahre stattfindenden – Evaluierungen der Richtlinie im Hinblick auf das etwaige Erfordernis einer Anpassung dieser Richtlinie insbesondere zu untersuchen ist, ob Vorschläge in Bezug auf die Haftung der Anbieter von Hyperlinks und von Instrumenten zur Lokalisierung von Informationen, Verfahren zur Meldung und Entfernung rechtswidriger Inhalte („Notice-and-Takedown-Verfahren“) und eine Haftbarmachung im Anschluss an die Entfernung von Inhalten erforderlich sind.

Die EU-Kommission hat im Jahr 2012 unter den Titel “Notice and Action: A clean and open Internet” eine Konsultation hierzu durchgeführt. Diese ergab unter-

schiedliche Ergebnisse, wobei sich zahlreiche Teilnehmer für ein solches Verfahren aussprachen. Die Kommission hat dieses Thema auch in ihrer Digital-Single-Market Strategie aufgegriffen.

Schließlich gilt es auch im Hinblick auf die übrigen identifizierten Problemstellungen, die Vorgaben der Richtlinie 2000/31/EG zu beachten.

In Bezug auf die Antragssprache enthält die Richtlinie keine Vorgaben. Es wird indes als richtlinienkonform angesehen, dass die Informationen nach § 5 TMG, der gewisse Informationspflichten für Diensteanbieter vorsieht, in der Sprache vorgehalten werden müssen, in der auch die übrigen Inhalte der Seite verfasst sind.[831] Es könnte sich daher anbieten, dies für die deutsche Sprache entsprechend gesetzlich zu konkretisieren, wenn man das Löschungsverfahren telemedienrechtlich regeln will.

Im Hinblick auf die Frage eines Zustellungsbevollmächtigten bieten sich angesichts der dargestellten europarechtlichen Rahmenbedingungen allerdings nach Auffassung der Arbeitsgruppe für rein nationale Lösungsansätze kaum Möglichkeiten. Zwar ließe sich die Pflicht, einen Zustellungsbevollmächtigten im Inland zu benennen, im Telemediengesetz normieren - etwa im Rahmen der Informationspflichten nach § 5 TMG. Dies wäre auf Diensteanbieter in Drittstaaten anwendbar. Es wäre jedoch fraglich, ob dies im Hinblick auf Diensteanbieter mit Sitz in der EU mit den Vorgaben der Richtlinie 2000/31/EG vereinbar wäre.

(c) E-Privacy-Verordnung[832]

Der Verordnungsvorschlag der Kommission über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (E-Privacy-VO) ist als Lex specialis zur EU-DSGVO ausgestaltet und soll wie diese am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft treten und ab dem 25. Mai 2018 gelten. Der Verordnungsvorschlag legt Vorschriften zum Schutz von Grundrechten und Grundfreiheiten natürlicher und juristischer Personen bei der Bereitstellung und Nutzung elektronischer Kommunikationsdienste fest und regelt insbesondere das Recht auf Achtung des Privatlebens und der Kommunikation sowie den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Vom sachlichen Anwendungsbereich sind nicht nur Internetzugangsdienste und Dienste, die ganz oder teilweise in der Übertragung von Signalen bestehen, sondern auch interpersonelle Kommunikationsdienste umfasst, wie auch vernetzte Geräte und Maschinen. Der Verordnungsentwurf enthält

---

[831] *Brunst*, Umsetzungsprobleme der Impressumspflicht bei Webangeboten, MMR 2004, 8 (12 f); *Müller-Broich*, TMG, § 5 Rn. 17 ff.

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

unter anderem Regelungen zum Schutz von Metadaten. Diese sollen grundsätzlich nur nach Einwilligung des Nutzers oder nach Anonymisierung für Werbung und andere Zwecke, die über die Gewährleistung der Funktionalität hinausgehen, genutzt werden. Für individuell zugeschnittene Werbeangebote müssen die Betreiber vorab die Datenschutz-Aufsichtsbehörden konsultieren, bevor sie die ausdrückliche Einwilligung der Nutzer einholen. Die Konsultation ist keineswegs unverbindlich: Die Anbieter müssen sich nach dem Verordnungsentwurf an die Empfehlungen der Behörden halten. Nutzer dürfen außerdem jederzeit ihre Einwilligung zurücknehmen, wobei der Anbieter sie daran jedes halbe Jahr erinnern muss. Auch die Informationspflicht über Cookies wird neu ausgestaltet. Über Cookies zu Konfigurationszwecken muss nicht mehr aufgeklärt werden. Dafür müssen Browser so konfigurierbar sein, dass Cookies der direkt besuchten Webseite akzeptiert, solche von Drittanbietern verweigert werden. Der ursprünglich weitreichende Privacy by Design-Gedanke findet im Verordnungsentwurf nur in abgeschwächter Form Berücksichtigung. Nicht mehr vorgesehen ist, dass vom Start weg nutzerfreundliche Einstellungen voreingestellt sein müssen. Die Software muss den Nutzer bei der Installation lediglich noch über Privatsphäre-Einstellungen informieren und seine Einwilligung für Einstellungen einholen. Ferner wird es keine technisch organisatorischen Schutzpflichten der Dienstanbieter zur Gewährleistung einer Ende-zu-Ende Verschlüsselung geben. Die Verwendung von E-Mail Daten bei Kundenbeziehung soll erlaubt sein. Der Verordnungsentwurf ist schließlich flankiert von umfassenden Sanktionsmaßnahmen.

(d) Mögliche Regelungsorte

Wollte man – soweit europarechtlich zulässig, oder nach Änderung der europarechtlichen Vorgaben – die identifizierten Bestandteile eines sachgerechten Löschungsverfahrens gesetzlich normieren, bietet sich eine Regelung im Telemediengesetz an, die sich an alle Diensteanbieter geschäftsmäßiger, in der Regel gegen Entgelt angebotener Telemedien richtet, die fremde Informationen für einen Nutzer speichern. Eine solche Regelung könnte etwa im Umfeld des § 10 TMG – bspw. durch Einfügung eines § 10a TMG – geschaffen werden. Auch die gesetzliche Anerkennung des Ombudsmanns als Schlichtungsstelle könnte im TMG erfolgen. Sollte der Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken[833] (RegE-NetzDG) verabschiedet werden, könnte eine Regelung – allerdings nicht beschränkt auf strafbare Inhalte – auch darin erfolgen.

Wie durch den Deutschen Bundestag in seiner Entschließung vom 2. Juni 2016, basierend auf der Grundlage der Beschlussempfehlung des Ausschusses für Wirtschaft und Energie zu BT-Drs. 18/8645, festgestellt, ist es allerdings vorrangig

---

[833]http://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_NetzDG.pdf?__blob=publicationFile&v=2 (letzter Abruf: 7.4.2017).

eine europäische Aufgabe, ein einheitliches Haftungsregime für Rechtsverletzungen im Internet zu kodifizieren. Dies ist auch seitens der Europäischen Kommission in ihrer am 9. Dezember 2015 veröffentlichten Mitteilung „Schritte zu einem modernen europäischeren Urheberrecht“[834] erkannt worden. Soweit darin gleichzeitig angekündigt worden war, zu prüfen, inwieweit Änderungen insbesondere bei der Rechtsdurchsetzung erforderlich sind, hat die Kommission in ihrer Mitteilung „Für eine faire, effiziente und wettbewerbsfähige auf dem Urheberrechtsschutz beruhende europäische Wirtschaft im digitalen Binnenmarkt“ vom 19. September 2016 in Aussicht gestellt, dass sie im Anschluss an die öffentliche Konsultation zur Frage der Evaluierung und Modernisierung des Rechtsrahmens für die Durchsetzung der Rechte des geistigen Eigentums sowie nach Abschluss der Evaluierung ggf. Vorschläge für erforderliche Änderungen des Rechtsrahmens zur Verbesserung der Vorschriften für die Ahndung von Schutzrechtsverletzungen auf diesem Sektor unterbreiten werde. Diese Vorschläge gilt es nach Auffassung der Arbeitsgruppe zunächst abzuwarten. Davon abgesehen, erscheint es in jedem Fall wünschenswert, dass von Seiten der Bundesregierung anlässlich einer Überarbeitung der sich gegenwärtig in der Evaluierung befindenden E-Commerce-Richtlinie darauf hingewirkt wird, dass dem nationalen Gesetzgeber bei der Anpassung des einschlägigen EU-Sekundärrechts noch ausreichende Spielräume für die normative Ausgestaltung der Thematik des Löschungs- bzw. „Notice-und-Takedown“-Verfahrens verbleiben.

Der am 5. April 2017 im Bundeskabinett beschlossene Entwurf des NetzDG beseitigt das von der Arbeitsgruppe festgestellte Bedürfnis nach Implementierung eines einheitlichen Löschverfahrens für Verletzungen des allgemeinen Persönlichkeitsrechts nicht. Der Entwurf enthält zwar Vorgaben für das Beschwerdemanagement und das Löschungsverfahren in Bezug auf rechtswidrige Veröffentlichungen im Internet, beschränkt sich dabei allerdings bewusst auf die Bekämpfung sogenannter Hasskriminalität in größeren sozialen Netzwerken und macht vor allem Vorgaben zum Ablauf des Prüfungs- bzw. Löschungsverfahrens innerhalb der Organisation des Anbieters nach Eingang einer Beschwerde über strafbare Inhalte. Nach dem Entwurf sollen Anbieter sozialer Netzwerke mit mindestens zwei Millionen Nutzern in Deutschland u.a. bußgeldbewährt verpflichtet werden, ein Verfahren vorzusehen, dass die Entfernung oder Sperrung rechtswidriger Inhalte binnen sieben Tagen, im Fall offensichtlicher Rechtswidrigkeit binnen 24 Stunden nach Eingang der Beschwerde gewährleistet. Als rechtswidrige Inhalte i. S. d. RegE-NetzDG gelten dabei ausdrücklich nur solche, die den Tatbestand einzeln aufgezählter Vorschriften des Strafgesetzesbuches erfüllen.

---

[834] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Für eine faire, effiziente und wettbewerbsfähige auf dem Urheberrechtsschutz beruhende europäische Wirtschaft im digitalen Binnenmarkt, COM(2016) 592 final.

Das dargestellte Bedürfnis für gesetzgeberische Maßnahmen zur generellen Einführung eines einheitlichen, transparenten und verbraucherfreundlichen Löschungsverfahrens bei allen Diensteanbietern und bei jedweder Persönlichkeitsrechtsverletzung sowie zur Verbesserung der Rechtsdurchsetzungsmöglichkeiten im Hinblick auf zivilrechtliche Ansprüche besteht daher auch dann fort, wenn das geplante Gesetz zur Rechtsdurchsetzung in sozialen Netzwerken verabschiedet wird.

IV. Schadensersatz und Schmerzensgeld

1. Ansprüche gegen Täter und Teilnehmer

Schadensersatzansprüche wegen Persönlichkeitsrechtsverletzungen können zum Ersatz immaterieller Schäden berechtigen. Die Rechtsprechung gewährt eine Geldentschädigung bei Verletzungen des allgemeinen Persönlichkeitsrechts gestützt auf § 823 Abs. 1 BGB i. V. m. Art. 1 Abs. 1, 2 Abs. 1 GG bei einem schwerwiegenden Eingriff, der nicht in anderer Weise befriedigend ausgeglichen werden kann.[835]

In der digitalen Welt sind Verletzungen des allgemeinen Persönlichkeitsrechts etwa auf Internetforen an eine potentiell unbeschränkte Öffentlichkeit gerichtet, bergen das Risiko unkontrollierter Verbreitung und sind potentiell immerwährend abrufbar. Die Praxis ermittelt daher Schmerzensgelder bei digitalen Persönlichkeitsrechtsverletzungen, jedenfalls im Internet, nach presserechtlichen Maßstäben. In einer Entscheidung vom 17. Dezember 2013 hat der BGH dabei ausgeführt, dass eine Geldentschädigung wegen Verletzung des allgemeinen Persönlichkeitsrechts durch eine Internetveröffentlichung nicht generell höher oder niedriger zu bemessen ist als eine Entschädigung wegen eines Artikels in den Printmedien.[836] Dieser Maßstab wird in der Literatur angegriffen. Für ein generell höheres Schmerzensgeld wird angeführt, dass der Kreis der potentiellen Wahrnehmungsadressaten ungleich größer sei als bei einer Printveröffentlichung oder jedenfalls nicht abschätzbar sei, welche Reichweite die Veröffentlichung hat.[837]

---

[835] BGH, Urt. v. 15.11.1994 – VI ZR 56/94, GRUR 1995, 224.

[836] BGH, Urt. v. 17.12.2013 – VI ZR 211/12, MMR 2015, 137; OLG Oldenburg, Urt. v. 11.8.2015 – 13 U 25/15, MMR 2016, 67 (15.000,00 € bei pornografischer Fotomontage).

[837] Vgl. insoweit auch BGH, Urt. v. 17.11.2015 – VI ZR 493/14, juris Rn. 24: „*Es begegnet auch keinen Bedenken, dass das Berufungsgericht für die zwei Gegendarstellungen Print und Online jeweils einen Betrag von 15.000 € angesetzt hat. Insoweit hat es mit Recht darauf abgestellt, dass im Onlinebereich - anders als im Printbereich - die archivierungsfähige Berichterstattung für unbegrenzte Zeit zum Abruf bereit stehen und über Suchmaschinen aufgefunden werden kann. Die dadurch gegebene Perpetuierungswirkung erhöht die Verletzungsgefahr und rechtfertigt eine gebührenrechtliche Gleichbehandlung zur Printberichterstattung, auch wenn die entsprechenden Aufrufe im Internet zunächst relativ gering sind. Dem steht nicht entgegen, dass einzelne Online-Beiträge eine Recherche des Internetnutzers voraussetzen bzw. erst über gezieltes "Anklicken" aufrufbar sind. Angesichts der Möglichkeiten von Suchmaschinen, die bei bloßer Eingabe eines bestimmten Suchbegriffs, wie bspw. des Namens einer Person, die im Netz*

Für eine niedrigere Bemessung wird angeführt, dass das im Internet veröffentlichte spontane Wort der Kommunikationsform der digitalen Welt entspreche und der Veröffentlichungsaufwand nicht wesentlich höher sei als beim Sprechen; auch sei der Kreis derjenigen, die den Beitrag wahrnehmen, oftmals sehr überschaubar.

Diese Ansätze verkennen die grundlegende von der Rechtsprechung entwickelte Konzeption des Ersatzes immaterieller Schäden. Nach der Rechtsprechung handelt es sich bei der Ermittlung der Geldentschädigung immer um eine Einzelfallprüfung, in der dann unter anderem auch die genannten Kriterien (z. B. der Kreis der tatsächlichen oder potentiellen Wahrnehmungsadressaten sowie das Maß des Verschuldens des Verletzers) Berücksichtigung finden. Pauschale Annahmen verbieten sich dabei. Eine Kodifizierung der bewährten Rechtsprechung, etwa im Rahmen des § 253 ZPO, hält die Arbeitsgruppe nicht für angezeigt.

2. Ansprüche gegen Dritte, insbesondere Intermediäre

Grundsätzlich bestehen keine Schadensersatz- und Schmerzensgeldansprüche gegenüber Diensteanbietern als Intermediäre.

Ein Schadensersatzanspruch gegenüber einem Diensteanbieter kann jedoch bestehen,

- wenn Diensteanbieter eigene Inhalte über ihr Medium verbreiten;
- wenn Diensteanbieter sich Beiträge der Nutzer zu Eigen machen, indem nach außen für einen verständigen Durchschnittsnutzer auf der Grundlage einer Gesamtbetrachtung aller relevanten Umstände erkennbar die Übernahme der inhaltlichen Verantwortung oder die zurechenbare Identifizierung mit den Aussagen erfolgt. Streit besteht darüber, ob ein zu Eigen machen bei jeder Veränderung durch den Diensteanbieter gegeben ist. Jedenfalls bei einer inhaltlich-redaktionellen Überarbeitung wird man in der Regel wohl davon ausgehen müssen;
- wenn ein Diensteanbieter eine Verweisung auf Internetseiten mit einem unschwer zu bejahenden persönlichkeitsrechtsverletzendem Inhalt nicht dauerhaft entfernt, nachdem er hierauf hinreichend konkret hingewiesen und zur Löschung aufgefordert wurde oder nur unzureichende Maßnahmen ergriffen hat, um einer Wiederholungsgefahr zu begegnen (Störerhaftung). Auf § 10 S. 1 TMG, wonach Diensteanbieter für fremde Informationen grundsätzlich nicht verantwortlich sind, und § 7 Abs. 2 S. 1 TMG, wonach Diensteanbieter nicht für die Überwachung der von ihnen übermittelten Informationen verantwortlich sind, soll sich insoweit der Diensteanbieter

---

einschlägigen Inhalte ohne Weiteres anbieten und aufrufbar präsentieren, ist das Verletzungspotential jedenfalls dem eines Printmediums vergleichbar (vgl. auch OLG Köln, Beschl. v. 19.1.2012 – 15 W 63/11, AfP 2012, 268 Rn. 8).“

nicht berufen können, da die Verantwortlichkeit nur im Falle fehlender Kenntnis ausscheidet;[838]

- aus lauterkeitsrechtlichen Gründen (§ 4 Nr. 2 UWG). Voraussetzung ist allerdings, dass der Anspruchssteller ein Mitbewerber ist (§§ 2 Abs. 1 Nr. 3, 8 Abs. 3 Nr. 1 UWG) oder die Klagebefugnis nach Maßgabe von § 8 Abs. 3 Nrn. 2-4 UWG in Anspruch genommen werden kann. Weiter muss der Diensteanbieter seine neutrale Vermittlerposition verlassen und eine aktive Rolle spielen, die ihm eine Kenntnis von bestimmten Daten oder eine Kontrolle über sie verschaffen konnte.[839]

Nach der Rechtsprechung des EGMR kann eine von einem nationalen Gericht verhängte Entschädigungszahlung für die nicht automatische Löschung persönlichkeitsrechtsverletzender Inhalte konventionsgemäß sein, wenn (so jedenfalls im konkreten Fall)

- es sich um eine offensichtliche Persönlichkeitsrechtsverletzung handelt,
- die Inhalte zwar noch am Tag der Beanstandung, aber erst sechs Wochen nach ihrer Veröffentlichung entfernt werden,
- die Persönlichkeitsrechtsverletzung vorhersehbar war,
- die Rechtsverfolgung wegen der für die Nutzer eröffneten Anonymität erschwert ist und
- der Portalbetreiber kommerzielle Interessen verfolgt.[840]

Es besteht jedoch keine konventionsrechtliche Verpflichtung für die nationalen Gesetzgeber, Regelungen zu schaffen, wonach rufschädigende Kommentare auf wirtschaftlich betriebenen Internetplattformen automatisch zu löschen sind.

In jüngster Zeit müssen sich allerdings insbesondere soziale Medien wachsender Kritik, vor allem wegen Falschmeldungen, stellen. Hier ist z. B. von Facebook und Google angekündigt worden, Seiten mit falschen Inhalten von firmeneigenen Werbeplattformen entfernen zu wollen.[841]

Insgesamt sieht die Arbeitsgruppe derzeit keinen über die geltende Rechtslage hinausgehenden Regelungsbedarf.

---

[838] BGH, Urt. v. 1.3.2016 – VI ZR 34/15, juris Rn. 19 („jameda.de II“); LG Heidelberg, Urt. v. 9.12.2014 – 2 O 162/13 (zu Google).
[839] BGH, Urt. v. 19.3.2015 – I ZR 94/13, juris Ls. 3 (“Hotelbewertungsportal”).
[840] EGMR, Urt. v. 16.6.2015 – 64569/09 (Delfi AS ./. Estland); vgl. auch EGMR, Urt. v. 2.2.2016 – 22947/13 (Magyar Tartalomszolgáltatók Egyesülete und Index.hu Zrt ./. Ungarn).
[841] Handelsblatt v. 16.11.2016 („Bestellte Wahrheiten“) unter Verweis auf US-Medien, wie die „New York Times“.

V. Internationale Zuständigkeit und anwendbares Recht

Innerhalb der EU können Klagen wegen Persönlichkeitsrechtsverletzungen nach Art. 5 Nr. 3 EuGVVO bei den Gerichten des Mitgliedstaats, in dem sich die Niederlassung des Inhalteanbieters befindet, oder bei den Gerichten des Mitgliedstaats, in dem sich der Mittelpunkt der Interessen des Betroffenen befindet, erhoben werden.[842]

Im Übrigen hat der BGH festgestellt, dass zur Entscheidung über Klagen wegen Persönlichkeitsbeeinträchtigungen durch im Internet abrufbare Veröffentlichungen die deutschen Gerichte nach § 32 ZPO international zuständig sind, wenn die als rechtsverletzend beanstandeten Inhalte objektiv einen deutlichen Bezug zum Inland in dem Sinne aufweisen, dass eine Kollision der widerstreitenden Interessen nach den Umständen des konkreten Falls im Inland tatsächlich eingetreten sein kann oder eintreten kann. Dies sei dann anzunehmen, wenn eine Kenntnisnahme der beanstandeten Meldung nach den Umständen des konkreten Falls im Inland erheblich näher liegt als es aufgrund der bloßen Abrufbarkeit des Angebots der Fall wäre und die vom Kläger behauptete Beeinträchtigung seines Persönlichkeitsrechts durch eine Kenntnisnahme von der Meldung (auch) im Inland eintreten würde.[843]

Dabei wurde deutsches materielles Recht in der Vergangenheit regelmäßig als anwendbar angesehen, weil die Anspruchsteller ihr Bestimmungsrecht bei persönlichkeitsrechtlichen Sachverhalten – die aufgrund des Ausnahmetatbestands in Art. 1 Abs. 2 lit. g Rom II-VO dem allgemeinen Deliktsstatut unterliegen, das auch nicht durch das Herkunftslandprinzip nach § 3 Abs. 2 TMG verdrängt wird – gemäß Art. 40 Abs. 1 S. 2 EGBGB zugunsten des deutschen Rechts ausgeübt haben.[844] Nach Art. 40 Abs. 1 S. 2 EGBGB kann der Verletzte verlangen, dass anstelle des Rechts des Staates, in dem der Ersatzpflichtige gehandelt hat, das Recht des Staates angewandt wird, in dem der Erfolg eingetreten ist. Der danach maßgebliche Erfolgsort liegt aufgrund der grundsätzlich weltweiten Abrufbarkeit von Internetseiten jedenfalls auch in Deutschland.

Allerdings kann die Rechtsdurchsetzung gegenüber Klagegegnern mit Sitz im Ausland angesichts der Zustellungsdauer und der erforderlichen Übersetzungen mit erheblichen praktischen Erschwernissen verbunden sein. Insofern wird auf die obigen Ausführungen unter B. III. 5. b. (5) (a) verwiesen.

---

[842] EuGH, Urt. v. 25.10.2011 − Rs. C-509/09 und Rs. C-161/10; BGH, Urt. v. 8.5.2012 − VI ZR 217/08, NJW 2012, 2197.
[843] BGH, Urt. v. 25.10.2011 – VI ZR 93/10, BGHZ 191, 219.
[844] BGH, Urt. v. 8.5.2012 − VI ZR 217/08, NJW 2012, 2197.

C. Profilbildung und Verhaltensprognose durch „Big Data“-Analysen

Die Digitalisierung ermöglicht das Sammeln und Verarbeiten von Daten in einem Ausmaß, das sich von der analogen Welt nicht nur quantitativ unterscheidet. Durch die zunehmende Datenerhebung in allen Bereichen des Lebens entstehen immer mehr Daten, die von verschiedenen Stellen ausgewertet und genutzt werden. Wenn private Anbieter Daten sammeln und sie verarbeiten, erwerben sie Kenntnisse über einzelne Nutzer. Sie können daraus Rückschlüsse auf die Person ziehen, die auf ein detailliertes Persönlichkeitsprofil hinauslaufen können. Dabei ist oft nicht klar, wer mit den Daten was macht, ob sie weitergegeben, ob und wie sie mit anderen Daten in Beziehung gesetzt werden und wer welche Erkenntnisse aus ihnen ableitet. Unklar bleibt meist auch, welche Daten zu welchen Zwecken gesammelt werden, was mit ihnen geschieht und welche Chancen und Risiken damit verbunden sind. Stimmen Nutzer in einer Datenschutzerklärung der Verarbeitung bestimmter Daten zu, treffen sie oft keine informierte Entscheidung, sondern akzeptieren die vorgegebenen Bedingungen – teilweise, ohne sie wirklich zur Kenntnis genommen zu haben, sei es wegen ihres Umfangs, der Sprache oder auch nur, um eine Anwendung nutzen zu können.

Auch bei einer Profilbildung (Profiling) auf der Grundlage rechtmäßig erlangter Daten, insbesondere mit Hilfe von Big-Data-Analysen, ist das Recht auf informationelle Selbstbestimmung betroffen. Als praktisches Beispiel für eine – missbrauchsanfällige – Big-Data-Analyse kann etwa auf den kürzlich in Russland entwickelten Gesichtserkennungsalgorithmus der App „FindFace“ verwiesen werden, der es ermöglicht, ein beliebiges Gesicht in sozialen Netzwerken zu suchen, zu identifizieren sowie ein Profil von ihm abzubilden.[845] Auch die Browser-Erweiterung der Firma „Web of Trust“ (WOT) scheint sich in einer rechtlichen Grauzone zu bewegen, indem sie u. a. Daten zum Surf-Verhalten eines Nutzers an einen Server im Ausland übermittelt, wo ein Profil erstellt und zur gewerblichen Nutzung weitergegeben wird.[846]

---

[845] https://www.welt.de/politik/ausland/article156076669/Russische-Software-erkennt-jeden-Menschen-auf-der-Strasse.html (letzter Abruf: 2.2.2017); http://www.spiegel.de/netzwelt/web/findface-app-mit-gesichtserkennung-loest-hype-in-russland-aus-a-1092951.html (letzter Abruf: 1.2.2017); http://www.bild.de/digital/smartphone-und-tablet/dating-apps/wie-legal-ist-find-face-46199040.bild.html (letzter Abruf: 1.2.2017).

[846] http://www.computerbild.de/artikel/cb-News-Internet-Web-of-Trust-Add-on-Nutzerdaten-16641917.html (letzter Abruf: 1.2.2017); http://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html (letzter Abruf: 1.2.2017); http://www.tagesspiegel.de/politik/nackt-im-netz-die-daten-entbloessen-alles/14785192.html (letzter Abruf: 1.2.2017); http://www.handelsblatt.com/technik/sicherheit-im-netz/web-of-trust-browser-erweiterung-spaeht-offenbar-nutzer-aus/14779688.html (letzter Abruf: 1.2.2017).

Datenerhebungen zur Profilbildung sowie Profilbildungen selbst sind grundsätzlich nicht zulässig:

- Nach § 4 Abs. 1 BDSG ist eine Verarbeitung personenbezogener Daten rechtswidrig, soweit sie nicht durch einen gesetzlich normierten Erlaubnistatbestand gerechtfertigt ist oder der Betroffene eingewilligt hat. Ohne seine Mitwirkung dürfen personenbezogene Daten nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder dies in anderer Weise gerechtfertigt ist, z. B. aufgrund der Erforderlichkeit für die Erfüllung der Verwaltungsaufgabe oder des Geschäftszwecks, im Hinblick auf die Wahrung berechtigter Interessen, und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden, vgl. § 4 Abs. 2 BDSG.
- Nach § 28b BDSG (Scoring) darf zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen mit Hilfe bereits zulässigerweise gespeicherter Daten ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben werden, u.a. wenn die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verhaltens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind (§ 28b Nr. 1 BDSG - Scoring). Streitig ist dabei, ob sich dies nur auf das Kredit- bzw. Finanz-Scoring bezieht.[847]
- Nach Art. 22 EU-DSGVO darf eine Person dem Profiling, das Maßnahmen zur Folge hat, durch die sich rechtliche Konsequenzen für die betroffene Person ergeben, oder die ähnliche erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Personen hat, nur im Ausnahmefall unterworfen werden (Erforderlichkeit für die Vertragserfüllung, Gestattung durch Rechtsvorschrift, Einwilligung). Das Profiling darf sich nicht ausschließlich auf eine automatisierte Verarbeitung stützen (vgl. auch Erwägungsgrund 71).

Dagegen lässt das Datenschutzrecht wohl die vorgelagerte Erhebung und Übermittlung (scheinbar) irreversibel anonymisierter Daten zu. Im Detail ist aber vieles ungeklärt:

- Streit besteht, ob Daten personenbezogen sind, wenn sie mit Hilfe anderer Daten ausgewertet und einer bestimmten Bezugsgröße und damit letztlich einer bestimmten Person zugeordnet werden können, über die ein Profil erstellt werden könnte.[848] Nach Erwägungsgrund 26 der EU-DSGVO sollen

---

[847] *Hoeren*, Thesen zum Verhältnis von Big Data und Datenqualität, MMR 2016, 8 (10); *Erbs/Kohlhaas/Ambs*, Strafrechtliche Nebengesetze, § 28b BDSG, Rn. 205.

[848] *Werkmeister/Brandt*, Datenschutzrechtliche Herausforderungen für Big Data, CR 2016, 233 (234 ff.) m. w. N.; *Brisch/Pieper*, Das Kriterium der „Bestimmbarkeit" bei Big Data Analyseverfahren, CR 2015, 724; *Spindler*, Datenschutz und Persönlichkeitsrechte im Internet – Der

Daten auch dann personenbezogen sein, wenn sie zwar einer Pseudonymisierung unterzogen worden sind, jedoch durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten. Dies spricht für einen eher weiter gefassten Personenbezugs-Begriff. Die Frage ist dem EuGH vorgelegt worden, allerdings auf der Grundlage des vor der EU-DSGVO geltenden Datenschutzrechts, d.h. der Datenschutzrichtlinie 95/46/EG.[849] Dieser hat zwischenzeitlich entschieden, dass z. B. eine dynamische IP-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff auf seine allgemein zugängliche Website gespeichert wird, für den Betreiber zu den personenbezogenen Daten zählt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, den Nutzer anhand der Zusatzinformationen, über die dessen Internetzugangsanbieter verfügt, identifizieren zu lassen. Mit dieser Möglichkeit soll jedoch dann nicht zu rechnen sein, wenn eine Identifizierung gesetzlich verboten sei oder es hierzu eines unverhältnismäßigen Aufwands bedürfe.[850]

- Die datenschutzrechtliche Verantwortlichkeit ist ungeklärt, wenn – wie bei Big-Data-Anwendungen üblich – Kooperationen zwischen den Anwendern bestehen. Dabei kann der Grundsatz aufgestellt werden, dass in der Regel derjenige datenschutzrechtlich verantwortlich ist, der den Einfluss auf die Zwecke und Mittel der Datenverarbeitung – und zwar hinsichtlich des „ob“ und des „wie“ – hat.
- Unklar ist weiter die Reichweite des Zweckbindungsgrundsatzes: Nach künftigem europäischen Recht dürfen Daten zu einem abweichenden Zweck grundsätzlich nur dann weiterverarbeitet werden, wenn dies mit dem ursprünglichen Zweck vereinbar ist, wobei dies anhand verschiedener, allerdings nicht abschließender Kriterien zu prüfen ist (Art. 6 Abs. 4 EU-DSGVO).

Auch die Anspruchssituation von Betroffenen mit Blick auf Big-Data-Analysen erscheint, abgesehen von besonders greifbaren Fällen, weitgehend ungeklärt. In den Fällen rechtswidriger Profilbildung wird man von dem Bestehen eines Unter-

---

Rahmen für Forschungsaufgaben und Reformbedarf, GRUR-Beil. 2014, 101; *Kinast/Kühnl*, Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten, NJW 2014, 3057 (aus datenschutzrechtlicher Perspektive); *Christl*, Kommerzielle digitale Überwachung im Alltag, abrufbar unter http://crackedlabs.org/dl/Studie_Digitale_Ueberwachung_Kurzfassung.pdf (letzter Abruf 17.1.2017); ; BVerfG, Urt. v. 15.12.1983 − 1 BvR 209/83, juris Rn. 147 („Volkszählung“); BVerfG, Urt. v. 12.4.2005 − 2 BvR 1027/02, juris Rn. 79-84 („Beschlagnahme von Datenträgern“); BVerfG, Beschl. v. 4.4.2006 − 1 BvR 518/02, juris Rn. 69 f. („Rasterfahndung“); BVerfG, Beschl. v. 13.6.2007 − 1 BvR 1550/03, 2357/04, 603/05, juris Rn. 85-88 („Kontenabfrage“); *Ohrtmann/Schwiering*, Big Data und Datenschutz – Rechtliche Herausforderungen und Lösungsansätze, NJW 2014, 2984.

[849] BGH, Beschl. v. 28.10.2014 − VI ZR 135/13.

[850] EuGH, Urt. v. 19.10.2016 − Rs. C-582/14.

lassungsanspruchs ausgehen können. Demgegenüber ist zweifelhaft, ob bzw. unter welchen Voraussetzungen Auskunftsansprüche über Art und Umfang der Datenerhebung, -übermittlung und -verarbeitung, an denen vielfach ein Interesse bestehen dürfte, gegeben sind. Die datenschutzrechtlichen (Vorab-)Informations- und Benachrichtigungspflichten (§§ 4 Abs. 3, 4a Abs. 1 S. 2, 33 Abs. 1 BDSG, § 13 Abs. 1 TMG, Art. 14, 15 EU-DSGVO) stoßen an praktische Grenzen, z. B. weil der Verwendungszweck, über den vorab informiert werden muss, im Vorhinein oft nicht feststeht oder die verantwortliche Stelle nur mit unverhältnismäßigem Aufwand solche Informationen an die Betroffenen bekanntgeben kann. Nach den Recherchen der Arbeitsgruppe besteht nach geltendem Recht kein Anspruch auf Auskunft über den Algorithmus, dessen Operation den Einzelnen in seinem Persönlichkeitsrecht einschränken kann.[851] Die in Art. 14 EU-DSGVO insoweit vorgesehene Informationspflicht entfällt nach Art. 14 Abs. 5 Buchst. b EU-DSGVO, soweit die Erteilung sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde, wobei dies insbesondere für wissenschaftliche, historische oder statistische Zwecke gelten soll.

Insgesamt gesehen sollte die Thematik von „Big Data“ im Blick behalten werden. Hierzu zählt auch eine Initiative von Bürgern zu einer „Charta der Digitalen Grundrechte der Europäischen Union“, die am 5. Dezember 2016 dem Europäischen Parlament und der Öffentlichkeit vorlegt wurde. Darin wird eine Gefährdung der Menschenwürde durch Big Data gesehen und unter anderem die Offenlegung von Algorithmen gefordert.[852] Der Sachverständigenrat für Verbraucherfragen hat in seinem im Dezember 2016 erschienenen Gutachten „Verbraucherrecht 2.0“ ebenfalls gefordert, die den Algorithmen zugrunde liegenden Parameter bei Algorithmen mit direktem Verbraucherkontakt transparent zu machen sowie diese durch standardisierte Offenlegungspflichten gegenüber einer neu zu gründenden Digitalagentur gleichsam auf ihre rechtliche Unbedenklichkeit zu prüfen.[853] Es ist festzustellen, dass die Debatte zum Thema „Big Data“ in tatsächlicher und rechtlicher Hinsicht ausgesprochen vielschichtig und weder rein national noch auf den Bereich der Europäischen Union beschränkt sinnvoll regelbar ist. Die Arbeitsgruppe sieht daher keine Möglichkeit, innerhalb der zur Verfügung stehenden Zeit insoweit abschließende Ergebnisse zu erzielen.

---

[851] BGH, Urt. v. 28.1.2014 − VI ZR 156/13 (Schufa-Scoring); BVerfG, 1 BvR 756/14 (anhängig).

[852] Charta der Digitalen Grundrechte der Europäischen Union, abrufbar unter http://www.digitalcharta.eu (letzter Abruf: 17.1.2017).

[853] Gutachten des Sachverständigenrats für Verbraucherfragen, Verbraucherrecht 2.0, abrufbar unter http://www.svr-verbraucherfragen.de/2016/12/01/sachverstaendigenrat-fuer-verbraucherfragen-legt-gutachten-zu-verbraucherrecht-2-0-vor/ (letzter Abruf: 17.1.2017).

D. Klarnamenpflicht im Internet

Einige Diensteanbieter, wie Facebook, verlangen von ihren Nutzern, unter ihrem Klarnamen aufzutreten. Ergibt sich der Verdacht, dass ein Name nicht zutreffend verwendet wird, verlangt Facebook von dem jeweiligen Nutzer eine Ausweiskopie und sperrt ggf. das Nutzerkonto. Dies beeinträchtigt das Recht auf informationelle Selbstbestimmung und widerspricht § 13 Abs. 6 TMG, wonach ein Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist.

In der (juristischen und politischen) Debatte um den Schutz der Anonymität im Internet können verschiedene Ebenen beobachtet werden, wobei die grundrechtliche Dimension stets eine wichtige Rolle spielt. Das Recht auf Anonymität ist dabei im unmittelbaren Umfeld des allgemeinen Persönlichkeitsrechts angesiedelt.[854] Das allgemeine Persönlichkeitsrecht beinhaltet nämlich auch das Recht, in gewählter Anonymität zu bleiben und die eigene Person nicht in der Öffentlichkeit dargestellt zu sehen.[855] Das BVerfG hat sich mehrfach mit der Anonymisierung von Daten befasst.[856]

Zurzeit wird um die Frage des Klarnamenzwangs in sozialen Netzwerken gestritten. Der Hamburgische Datenschutzbeauftragte, der aufgrund des Sitzes der deutschen Facebook-Niederlassung in Hamburg zuständig ist, hat gegen das soziale Netzwerk Facebook ein Verfahren vor den Verwaltungsgerichten um die Frage geführt, ob er Facebook verbieten konnte, deutsche Nutzer zur Angabe ihres Klarnamen zu zwingen. Das OVG Schleswig hat in einem Eilverfahren entschieden, dass deutsches Recht keine Anwendung findet, das OVG Hamburg hat die Frage offengelassen. Die Hauptsacheentscheidungen hierzu stehen noch aus.[857]

Des Weiteren wird die Frage diskutiert, ob vor dem Hintergrund des Grundrechtsschutzes, der Regelungen zur Datensparsamkeit (insbesondere in § 3a BDSG) und dem für Telemediendiensteanbieter vorgesehenen Gebot der Gewährleistung anonymer Nutzung inklusive anonymer Bezahlung nach § 13 Abs. 6 TMG Internet-

---

[854] *Bäumler/v. Mutius*, Anonymität im Internet, 1 (6).

[855] KG Berlin, Urt. v. 16.3.2007 − 9 U 88/06, GRUR-RR 2007, 247.

[856] BVerfG, Beschl. v. 16.7.1969 − 1 BvL 19/63, BVerfGE 27, 1, 7 („Mikrozensus“); BVerfG, Urt. v. 15.12.1983 − 1 BvR 209/83, BVerfGE 65, 1 (49 f.) („Volkszählung“).

[857] OVG Schleswig, Beschl. v. 22.4.2013 − 4 MB 11/13, NJW 2013, 977: Keine Anwendbarkeit deutschen Rechts gegenüber der Facebook Ireland Limited. In einem Parallelverfahren hat das BVerwG die Frage, ob ein deutscher Datenschutzbeauftragter gegenüber der Facebook Ireland Limited vorgehen dürfe, jedoch dem EuGH vorgelegt; OVG Hamburg, Beschl. v. 30.6.2016 − 5 Bs 40/16. Zu weiteren Rechtsstreitigkeiten: Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit, abrufbar unter https://www.datenschutz-hamburg.de/news/detail/article/der-hamburgische-datenschutzbe auftragte-profilnamen-bei-facebook-frei-waehlbar.html?tx_ttnews[backPid]=1&cHash=c2a6 cea29f0fd07dae7ca92f86c724cc (letzter Abruf: 19.1.2017).

nutzer generell identifizierbar sein sollten. Nach § 13 Abs. 6 TMG hat ein Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist.[858] Grundlage der Diskussion ist die politische Forderung, dass Rechtsverletzungen im Internet besser verfolgbar sein sollten.[859] Insbesondere zur Aufklärung schwerer Straftaten ist kürzlich der Zwang von Telekommunikationsanbietern zur Vorratsdatenspeicherung erneut eingeführt worden.[860] Hiergegen ist jedoch von verschiedener Seite Verfassungsbeschwerde erhoben worden; eine Entscheidung darüber steht noch aus.[861]

Der Schutz der Anonymität im Internet ist auch grundsätzlicher Kritik ausgesetzt, weil Anonymität ihrerseits rechtswidriges Verhalten im Internet begünstigen kann. Es wird daher diskutiert, ob ein genereller Klarnamenzwang für Äußerungen im Internet vor dem Hintergrund zunehmender, teils justiziabler Äußerungen gegen einzelne Gruppen geboten sein kann, wobei es u.a. – ebenfalls im Zusammenhang mit Facebook – um die Frage der Sperre von volksverhetzenden Inhalten und die Rolle von sozialen Netzwerken geht.[862]

Bei der Frage der Behandlung der Anonymität im Internet ist ferner zu beobachten, dass u.a. bei den Webseiten klassischer Medienangebote (z. B. Spiegel Online) die Kommentarfunktion vollständig oder bei einzelnen Artikeln zu sensitiven Themen generell deaktiviert wird. Andererseits wird immer wieder darauf

---

[858] Vgl. auch *Härting*, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065 (2068); *Heckmann*, Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderung für Ehrschutz und Profilschutz, NJW 2012, 2631 (2632) jew. m. w. N.; zur Zumutbarkeit bei Hosting-Diensten, die regelmäßig für rechtsverletzende Handlungen durch Nutzer missbraucht werden, OLG Hamburg, Urt. v. 30.9.2009 − 5 U 111/08, juris Rn. 88, MMR 2010, 51 (54) („Rapidshare II").

[859] Vgl. LG München I, Urt. v. 12.1.2012 − 7 HK O 1398/11, CR 2012, 605; *Heckmann* nennt dies das „Dilemma der Anonymität" in „Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderung für Ehrschutz und Profilschutz", NJW 2012, 2631 (2632); zum ursprünglichen Entwurf des Gesetzes zur Änderung des TMG: *Mantz/Sassenberg*, Die Neuregelung der Störerhaftung für öffentliche WLANS – eine Analyse des TMG-RefE vom 11.3.2015, CR 2015, 298 (300).

[860] BT-Drs. 18/5088, dazu *Nachbaur*, Vorratsdatenspeicherung „light" rechtswidrig und allenfalls bedingt von Nutzen, ZRP 2015, 215.

[861] Spiegel Online v. 27.1.2016, Wer alles gegen die Vorratsdatenspeicherung klagt, abrufbar unter: http://www.spiegel.de/netzwelt/netzpolitik/vorratsdatenspeicherung-wer-klagt-vor-dem-bundesverfassungsgericht-a-1074152.html (letzter Abruf: 19.1.2017).

[862] Vgl. Süddeutsche Zeitung v. 31.7.2015, abrufbar unter http://www.sueddeutsche.de/digital/klarnamen-bei-facebook-menschen-hetzen-auch-unter-echten-namen-1.2589458 (letzter Abruf: 19.1.2017); *Schurig*, Anonyme und offene Hetze gegen Ausländer im Netz nimmt zu, 30.7.2015, becklink 2000728 (letzter Abruf: 19.1.2017).

hingewiesen, dass strafbare Inhalte bereits heute vielfach unter Klarnamen veröffentlicht werden.[863]

In der Diskussion tritt Facebook für einen Klarnamenzwang ein. Auf der anderen Seite vertreten insbesondere bürgerschaftliche Gruppen eine Position der anonymen Nutzung des Internets. Auch einige große Telemediendiensteanbieter wie z. B. Google oder Apple, wenden sich u.a. gegen umfassende Pflichten zur Auskunft über ihre Nutzer.[864] Generell wird in diesem Zusammenhang zu differenzieren sein zwischen der Offenlegung der Daten gegenüber dem Diensteanbieter zur Nutzung und Abrechnung und der Pflicht, die Identität bei Nutzung der Dienste auch gegenüber Dritten – etwa durch die Klarnamenpflicht bei Facebook – offenzulegen. Nach Stimmen in der Literatur kann der Anbieter nämlich von dem Nutzer eine Registrierung unter richtigem Namen verlangen, da sich das Recht auf Anonymität nur auf die Nutzung von Telemedien, nicht aber auf die Nutzeranmeldung bezieht.[865]

Die EU-DSGVO enthält keine § 13 Abs. 6 TMG entsprechende Regelung. Sie sieht allerdings in Art. 5 Abs. 1 Buchst. c), 25 EU-DSGVO den aus § 3a BDSG bekannten Grundsatz der Datenminimierung vor, aus dem sich auch ein Gebot zur anonymen Nutzung von Diensten ableiten lassen könnte.[866]

Da die Frage der Verwendung von Klarnamen in § 13 Abs. 6 TMG gesetzlich geregelt und im Übrigen die gesellschaftliche Diskussion noch nicht abgeschlossen ist, besteht aus Sicht der Arbeitsgruppe insoweit gegenwärtig kein Handlungsbedarf.

E. Profildiebstahl

Ein „Identitätsdiebstahl“ ist aus der analogen Welt bekannt. In der digitalen Welt hat der Identitätsdiebstahl eine besondere Bedeutung, weil bei der Nutzung zahlreicher digitaler Dienste Profile angelegt werden und die Nutzer unter ihren Profilen, mit Klarnamen oder Pseudonym, im Rechtsverkehr auftreten oder identifizierbar sind. Bei Diensten wie Facebook, Xing oder LinkedIn findet private oder berufliche Kommunikation sogar unter lebenslaufähnlichen Steckbriefen statt, bei einigen Online-Spielen zwischen Avataren.

---

[863] FAZ v. 1.12.2015, Hetze im Internet gegen Flüchtlinge häufig unter Klarnamen, abrufbar unter http://www.faz.net/aktuell/politik/fluechtlingskrise/hetze-gegen-fluechtlinge-im-internet-haeufig-unter-klarnamen-13942395.html (letzter Abruf: 19.1.2017); Süddeutsche Zeitung v. 31.7.2015, Menschen hetzen auch unter echtem Namen, abrufbar unter http://www.sueddeutsche.de/digital/klarnamen-bei-facebook-menschen-hetzen-auch-unter-echten-namen-1.2589458 (letzter Abruf: 19.1.2017).

[864] https://www.heise.de/mac-and-i/meldung/Apple-CEO-Tim-Cook-Datenschutz-ein-fundamentales-Menschenrecht-2836809.html (letzter Abruf: 1.2.2017).

[865] *Kersten*, Anonymität in der liberalen Demokratie, JuS 2017, 193.

[866] Vgl. auch *Härting*, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065 (2068).

Besondere Phänomene eines Identitätsdiebstahls in der digitalen Welt sind etwa folgende Fallkonstellationen:

Jemand legt unbefugt ein Profil mit den Daten eines anderen an und

- kommentiert unter dem Twitter-Profil eines anderen politische Ereignisse,
- kritisiert, beleidigt oder verbreitet über ein Xing-Profil Informationen über den Arbeitgeber des anderen oder kontaktiert für alle sichtbar, einschließlich des Arbeitgebers des Betroffenen, einen Headhunter,
- provoziert über MyHammer oder das eBay-Verkäuferkonto eines anderen durch mangelhafte Vertragsabwicklungen negative Bewertungen.

Ebenso in Rede stehen Fallkonstellationen, in denen jemand das Online-Profil eines anderen unbefugt übernimmt. Das Online-Rollenspiel Second Life kam 2007 in die Diskussion, als Hacker kindlich aussehende Avatare anderer Nutzer kaperten und sexuelle Dienste anboten.

Das Phänomen des Identitätsdiebstahls wird, jedenfalls in dem hier angesprochenen Sinn, bislang kaum diskutiert.

Dies dürfte damit zusammenhängen, dass regelmäßig das (Alias-)Namensrecht nach § 12 S. 2 BGB oder sogar strafrechtliche Vorschriften verletzt sind und das Verhalten in diesen Fällen ohne Weiteres rechtswidrig ist. Wird das Bild eines Anderen im Rahmen eines Identitätsdiebstahls unbefugt verwendet, kann zudem ein Verstoß gegen § 22 KunstUrhG in Betracht kommen.[867]

Anders kann es sich verhalten, wenn Äußerungen über ein nur ähnliches Profil als Satire verstanden werden müssen und der Kunst- und Meinungsfreiheit unterliegen (wie z. B. Scherzanrufe von Stimmenimitatoren in der analogen Welt).

Die wesentlichen Problemfelder (Unterlassungs- und Beseitigungsanspruch, Schadensersatz- und Schmerzensgeldanspruch) dürften im Übrigen weitgehend denjenigen entsprechen, die bei den Ansprüchen gegen Täter und Teilnehmer von Ehrverletzungen diskutiert werden (vgl. die obigen Ausführungen).

Auch die weiteren Problembereiche (Auskunftsanspruch, Löschungsanspruch) dürften im Wesentlichen denjenigen entsprechen, die bei den Ansprüchen gegen Dritte gegenüber Ehrverletzungen diskutiert werden. Insbesondere dürften die Grundsätze, nach denen Intermediäre nach einem konkreten Hinweis verpflichtet sind, festgestellte Persönlichkeitsrechtsverletzungen zu beseitigen, auch auf unter falschem Namen angelegte Profile anwendbar sein. Hat also ein Diensteanbieter Kenntnis davon erlangt, dass ein Dritter unter dem Namen des tatsächlichen Na-

---

[867] Zur Übertragung „analoger Maßstäbe“ des Namens- und Aliasnamensschutzes in die digitale Welt BVerfG, Beschl. v. 21.8.2006 − 1 BvR 2047/03. Zum grundsätzlich strafbaren sog. „Phishing“ zwecks Verwendung fremder Online-Kontozugangsdaten s.u. im Abschnitt „Integrität und Vertraulichkeit informationstechnischer Systeme“.

mensträgers ein Profil angelegt hat, muss er wirksame Vorsorgemaßnahmen gegenüber weiteren Verletzungen, etwa die Überwachung des Anmeldeverfahrens der Mitglieder, soweit sie technisch möglich und zumutbar sind, treffen.[868]

Nach den Recherchen der Arbeitsgruppe bieten viele Diensteanbieter Verfahren an, um Identitätsdiebstähle abzustellen. So bietet Facebook den Button „Profil melden" an, woraufhin Facebook, heißt es, vom Inhaber des Profils eine Ausweiskopie verlangt und, wenn diese nicht innerhalb einer bestimmten Frist vorliegt, das Nutzerkonto löscht.

Die faktischen Rechtsdurchsetzungsprobleme dürften daher insgesamt gesehen mit denjenigen bei Löschungsansprüchen vergleichbar sein. Speziell gegen Profildiebstahl ist allerdings eine „Button-Lösung" bereits weit verbreitet, sodass viele Rechtsdurchsetzungsprobleme erst entstehen, wenn der Diensteanbieter dem Verlangen des wahren Profilinhabers nicht oder nicht zeitnah nachkommt. Insoweit besteht allerdings auch ein gewisser Schutz durch die Berücksichtigung des Zeitmoments bei der im Nachhinein festzusetzenden Höhe des Schmerzensgelds.

Vor diesem Hintergrund sieht die Arbeitsgruppe derzeit in diesem Themenbereich keinen Regelungsbedarf.

F. Ausspähen von Daten

Das allgemeine Persönlichkeitsrecht kann auch betroffen sein, wenn jemand persönliche Daten durch Trojaner oder durch List ausspäht (Phishing) oder die Steuerung der Webcam am Computer eines anderen übernimmt und so unbemerkt Einblick in den persönlichen Lebensbereich eines anderen erhält.[869] Dies kann sowohl punktuell geschehen als auch großflächig in Zusammenhang mit Botnetzen. Als Botnetz lässt sich der illegale Zusammenschluss einer Vielzahl von Systemen bezeichnen, die ferngesteuert und für kriminelle Zwecke missbraucht werden können. Zu diesen Systemen zählen nicht nur Computersysteme oder mobile Anwendungen. Mittlerweile visieren die Täter sämtliche internetfähigen Geräte an, also auch Router, Multimediacenter mit Internetanschluss, Fernsehgeräte und sogar internetfähige Haushaltsgeräte wie Kühlschränke. Damit ein System zum Teil eines Botnetzes wird, muss es sich zuvor mit Malware infiziert haben.

Botnetze werden auch für Distributed Denial of Service Attacken (DDoS-Attacken) missbraucht, bei denen gekaperte Systeme dazu genutzt werden, bestimmte Server mit wiederkehrenden Anfragen gezielt zu überlasten, bis sie schließlich zusammenbrechen und nicht mehr erreichbar sind. Weitere Möglichkeiten, die der Einsatz des Botnetzes bietet, sind Spam-Kampagnen und die Tarnung anderer Angriffe. Das Programmieren der Malware ist strafrechtlich vom

---

[868] BGH, Urt. v. 10.4.2008 − I ZR 227/05, juris Rn. 16 (zu einem eBay-Profil; vorangehend OLG Brandenburg, Urt. v. 16.11.2005 − 4 U 5/05).

[869] Vgl. *Borges*, Rechtsfragen beim Phishing – Ein Überblick, NJW 2005, 3313; *Schulte am Hülse/Klabunde*, Abgreifen von Bankzugangsdaten im Onlinebanking, MMR 2010, 84 zum Phishing.

objektiven Tatbestand des § 202c Abs. 1 Nr. 2 StGB erfasst. Der Einsatz von Malware zur Ausspähung von Daten unter Überwindung von Sicherheitsvorkehrungen fällt unter § 202a Abs.1 StGB. Sollen Daten abgefangen werden, die sich im Übermittlungsvorgang befinden, greift § 202b StGB. Werden vorhandene Daten zerstört oder verändert, ist § 303a Abs. 1 StGB, ggf. § 303b StGB einschlägig. Bei der Verbreitung von Malware ist darüber hinaus die Verwirklichung von §§ 44 Abs. 1, 43 Abs. 2 Nr. 3 und Nr. 4 BDSG nicht fernliegend. DDoS-Attacken unterfallen dem Straftatbestand des § 303b Abs. 1 Nr. 2 StGB. Die Internet Service Provider sind nach § 109 Abs. 2 TKG gehalten, im bestimmten Umfang präventive Schutzvorkehrungen gegenüber Botnetzen zu treffen.[870]

Eine Initiative des Bundesrates sieht nunmehr vor, einen eigenen Straftatbestand bei unbefugtem Verschaffen, in Gebrauch nehmen, Beeinflussen oder in Gang setzen von informationstechnischen Systemen zu schaffen, sofern die Tat geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen.[871]

Zu der generellen Problematik, ob Daten oder ein Recht am eigenen Datenbestand als sonstiges Recht i. S. d. § 823 Abs. 1 BGB anzuerkennen sind und ob Daten nach geltendem Recht hinreichend gegen unberechtigten Zugriff geschützt sind, wird auf die diesbezüglichen Ausführungen in Kapitel 1 (Dateneigentum) verwiesen.

Rechtlich nicht hinreichend erfasst sind zur Zeit Konstellationen, in denen digitale Anwendungen ohne hinreichende Information der Nutzer auf Handy-, Computer- und sonstige elektronische Daten zugreifen und diese weiterleiten, ohne dass damit eine Zugangssicherung überwunden wird. Denkbar ist es auch, Fallkonstellationen hierunter zu fassen, in denen Handy-Apps unangemessene Berechtigungen einholen (etwa die Auslesung des Adressbuchs, womit nicht nur in Rechte des App-Erwerbers, sondern auch in die Rechte derjenigen eingegriffen wird, die im Adressbuch vermerkt sind). Die Rechtslage ist insoweit jedoch unklar. In der Literatur werden AGB-rechtsähnliche Inhaltskontrollen von Datenschutzerklärungen vorgeschlagen. Gefordert wird etwa, die Wirksamkeit einer datenschutzrechtlichen Einwilligung von einem inhaltlichen Zusammenhang zwischen den von einer App übermittelten Daten und dem Gegenstand der App abhängig zu machen. Das heißt, eine Nutzereinwilligung zur Übermittlung von Standortdaten wäre zulässig, wenn die App Verkehrsstaus meldet oder Navigationsfunktionen aufweist; sie wäre unzulässig, wenn die App nur den Dauerbetrieb des Kamerablitzes am Mobiltelefon zulässt (Taschenlampen-App).

Die Anspruchslage, auch mit Blick auf Ansprüche gegenüber Diensteanbietern, wenn dort hinterlegte Daten durch Dritte ausgespäht werden, erscheint nach den bisherigen Recherchen der Arbeitsgruppe ungeklärt. Das BVerfG hat als Ausprä-

---

[870] Umfangreiche Darstellung: *Roos/Schumacher*, Botnetzes als Herausforderung für Recht und Gesellschaft – Zombies außer Kontrolle?, MMR 2014, 377.
[871] BR-Drs. 338/16.

gung des allgemeinen Persönlichkeitsrechts ein Grundrecht auf Schutz der Integrität und Vertraulichkeit informationstechnischer Systeme geschaffen. Das Grundrecht ist drittschützend und damit im Verhältnis von Privaten zueinander von Belang.[872]

Mit Blick auf Diensteanbieter dürfte allerdings dann regelmäßig ein vertraglicher Anspruch in Betracht kommen, wenn eine vertragliche Pflicht zur Verwahrung der entsprechenden Daten und als Nebenpflicht die Beachtung von Sicherheitsvorkehrungen bestand.

In der Fallgruppe „gierige Taschenlampen-App“ können Einzelpersonen ihrem Persönlichkeitsrecht in der Regel kaum effektiv Geltung verschaffen. Das bereits bestehende Verbandsklagerecht nach § 2 Abs. 2 Nr. 11 UKlaG effektiviert jedoch die Stellung der Verbraucher. Danach können Verbände Unterlassungs- und Beseitigungsansprüche erheben, wenn gegen Vorschriften verstoßen wird, welche die Zulässigkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eines Verbrauchers durch einen Unternehmer regeln, wenn die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden. Art. 80 EU-DSGVO lässt dies auch zukünftig zu.[873]

Hierzu ist darauf hinzuweisen, dass bspw. der Verbraucherzentrale Bundesverband (vzbv) zwischenzeitlich zum dritten Mal ein Klageverfahren gegen Facebook angestrengt hat (u. a. wegen irreführender Werbung für einen angeblich kostenlosen Dienst, kritischer Voreinstellungen sowie diverser Klauseln in den Nutzungsbedingungen).[874] Dass darüber hinaus auch die Einschaltung der Datenschutzbeauftragten dazu beitragen kann, den Interessen der Nutzer Gehör zu verschaffen, scheint das jüngste Verhalten von Facebook zu belegen, wonach das Unternehmen vor dem Hintergrund entsprechender Beanstandungen des Hamburgischen, aber auch der britischen Datenschutzbeauftragten die Weitergabe von Daten europäischer Whats-App-Nutzer vorerst gestoppt haben soll.[875]

Da insbesondere die bereits bestehenden Verbandsklagerechte den Rechtsschutz der Nutzer in vielen Fällen verbessern und die Botnetzinitiative des Bundesrates noch keinen Abschluss gefunden hat, ist zunächst die nationale und europäische Rechtsentwicklung weiter zu beobachten, ohne dass akuter Handlungsbedarf besteht.

---

[872] BVerfG, Urt. v. 27.2.2008 − 1 BvR 370, 595/07, BVerfGE 120, 274 (302-315) („Online-Durchsuchung“).
[873] Vgl. dazu Erwägungsgrund 142 der EU-DSGVO.
[874] http://www.vzbv.de/pressemitteilung/vzbv-klagt-gegen-facebook (letzter Abruf: 1.2.2017).
[875] https://www.welt.de/wirtschaft/article159391467/Datenweitergabe-von-WhatsApp-an-Facebook-gestoppt.html (letzter Abruf am 1.2.2017).

G. Ungewollte Einflüsse Dritter

Das allgemeine Persönlichkeitsrecht kann auch betroffen sein, wenn

- jemand mit unerwünschten Inhalten beim Surfen konfrontiert wird (z. B. pornografische Bildinhalte auf einer Nachrichten-Webseite) oder
- jemand unerwünschte Spam-E-Mails oder Werbe-SMS erhält.

Das allgemeine Persönlichkeitsrecht schützt vor ungewollten Einflüssen Dritter, insbesondere in die Privatsphäre. Der private Lebensbereich soll als Ausfluss des personalen Selbstbestimmungsrechts von jedem Zwang zur Auseinandersetzung mit unerwünschten Inhalten freigehalten werden. Ein privates E-Mail-Postfach gehört zur Privatsphäre in diesem Sinn.

Ob damit auch ein Schutz vor der Konfrontation mit unerwünschten Inhalten erfasst ist, scheint weitgehend offen zu sein und wird, soweit ersichtlich, kaum diskutiert. Es ist insbesondere unklar, wie weit der Schutz vor ungewollten Einflüssen Dritter beim „Aufenthalt im Internet“ geht, beim Surfen auf fremden Webseiten, die am eigenen Bildschirm in der eigenen Wohnung dargestellt werden.[876] Das praktische Bedürfnis an einer dahingehenden Regelung erscheint aber zweifelhaft.

Die Rechtslage zum unerwünschten Empfang von Spam und sonstiger Werbung ist dagegen weitgehend geklärt. Das Persönlichkeitsrecht schützt vor unzumutbaren Belästigungen und damit auch, wegen des andernfalls drohenden Nachahmungseffekts, vor unerbetener Werbung.[877] Gegen Verursacher von Spam und ungewünschter Werbung besteht grundsätzlich ein Unterlassungs- und Schadenersatzanspruch. Die Frage der Folgenbeseitigung dürfte sich regelmäßig nicht stellen.

---

[876] BGH, Urt. v. 15.4.1975 − VI ZR 93/73, juris Rn. 13 f.: Die Auslage pornografischer Hefte in einer Buchhandlung ist keine Persönlichkeitsrechtsverletzung, wenn der Einzelne in quantitativer wie in qualitativer Hinsicht nur in der Anonymität des Publikums betroffen ist und die Schriften gegen seinen Willen nicht mehr als oberflächlich zur Kenntnis nehmen muss.

[877] BGH, Urt. v. 15.12.2015 − VI ZR 134/15 (Persönlichkeitsrechtsverletzung durch automatische elektronische Eingangsbestätigung, die auch Werbung enthält); KG, Urt. v. 8.1.2002 − 5 U 6727/00, juris Rn. 23 ff. (E-Mail-Werbung); OLG Bamberg, Urt. v. 12.5.2005 − 1 U 143/04, juris Rn. 12 (E-Mail-Werbung); LG Lübeck, Beschl. v. 10.7.2009 − 14 T 62/09 (E-Mail-Werbung); LG Berlin, Urt. v. 14.1.2003 − 15 O 420/02 (SMS-Werbung); BGH, Urt. v. 14.1.2016 − I ZR 65/14 (Facebook-Freunde-finden-Funktion als Werbung, allerdings mit wettbewerbsrechtlicher Lösung; zuvor KG, Urt. v. 24.1.2014 − 5 U 42/12); AG Wedding, Urt. v. 10.5.2010 − 22b C 243/09 (Vorkehrungen gegen die Bestellung eines Versandhandel-Newsletters durch unbekannten Dritten); die im Rahmen des Double-Opt-In-Verfahrens eingehende Bestätigungsmail für das Abonnement eines Newsletters ist dagegen hinzunehmen (LG Essen, Urt. v. 20.4.2009 − 4 O 368/08, juris Rn. 25).

Dass es Möglichkeiten der Rechtsdurchsetzung beim Erhalt ungewollter Werbung auch gegenüber Intermediären gibt, erscheint ebenfalls gesichert.[878]

Ein differenziertes Bild ergibt sich im Hinblick auf Online-Werbeblocker. Online-Werbeblocker sind Computerprogramme, die die Darstellung von Online-Werbung auf Webseiten unterdrücken. Dabei ist das allgemeine Persönlichkeitsrecht des Nutzers in Abwägung mit dem Interesse des Unternehmers, seine Leistungen nur gegen Konsum der Werbung zu erbringen, zu bringen.

Bislang hatte sich die Rechtsprechung hierzu unter lauterkeitsrechtlichen Aspekten zu befassen. Ob Anbieten, Vertrieb und Bewerbung derartiger Werbeblocker lauterkeitsrechtlich zulässig ist, ist bislang in Rechtsprechung und Literatur umstritten.[879] Bei einigen Werbeblockern besteht für Werbende die Möglichkeit, von den Blockierfiltern ausgenommen zu werden, wenn sie an den Betreiber des Werbeblockers eine Vergütung zahlen.[880] Insoweit scheint auf programmiertechnischer Ebene derzeit einiges im Fluss zu sein: z. B. will Facebook die Blockade von Online-Werbung durch sogen. Adblocker (künftig) auf technischem Weg verhindern; im Gegenzug hierfür sollen jedoch die Nutzer mit einem Software-Update selbst festlegen können, welche Werbung sie sehen wollen und welche nicht.[881]

Nach Auffassung der Arbeitsgruppe sollte insoweit die weitere Entwicklung auf diesem Gebiet beobachtet werden. Anhaltspunkte für ein zwingend gebotenes Tätigwerden zum jetzigen Zeitpunkt werden nicht gesehen.

---

[878] Z. B. AG Wedding, Urt. v. 10.5.2010 − 22b C 243/09 (Vorkehrungen gegen die Bestellung eines Versandhandel-Newsletters durch unbekannten Dritten); vgl. auch BGH, Urt. v. 14.1.2016 − I ZR 65/14 (Facebook-Freunde-finden-Funktion, die durch Dritte ausgelöst wird, als Facebook-Werbung).

[879] Zulässig: LG München, Urt. v. 27.5.2015 − 37 O 11673/14 (nicht rechtskräftig); a.A. OLG Köln, Urt. v. 24.6.2016 − I-6 U 149/15: Kein Verstoß gegen das Verbot gezielter Behinderung gem. § 4 Nr. 4 UWG. Verbot aggressiver Praktik i. S. v. § 4a Abs. 2 Nr. 3 UWG, wenn die Blockade erst durch ein „Lösegeld“ des Werbewilligen gelöst werden kann.

[880] Die Standard-Konfiguration des Werbeblockers kann etwa vorsehen, dass „nicht aufdringliche Werbung“ – eben die Werbung solcher Werbender, die ein „Lösegeld“ entrichtet haben – zugelassen wird.

[881] http://www.tagesschau.de/wirtschaft/facebook-241.html (letzter Abruf: am 1.2.2017).

H. Ergebnisse

Es bedarf nicht der ausdrücklichen Anerkennung eines digitalen Persönlichkeitsrechtes, weil das von der Rechtsprechung entwickelte allgemeine Persönlichkeitsrecht in der Menschenwürde gründet und die bislang diskutierten Falllösungen auf Grundlage des geltenden Rechts auch das Handeln im digitalen Raum und die damit im Zusammenhang stehenden Ausprägungen der Persönlichkeit der handelnden Person sachgerecht erfassen.

Die Verbreitung herabsetzender Tatsachenbehauptungen oder Werturteile erfährt in der „digitalen Welt“ besondere Ausprägungen. Dem begegnet die Rechtsprechung unter Hinzuziehung der in der „analogen Welt“ entwickelten Kriterien. Da eine Fehlentwicklung in der Praxis gegenwärtig nicht erkennbar ist, werden gesetzgeberische Eingriffe an dieser Stelle nicht empfohlen.

Auch nicht herabsetzende Veröffentlichungen oder Verbreitungen können unter dem Gesichtspunkt des Rechts auf informationelle Selbstbestimmung persönlichkeitsrelevant sein. Besondere Betrachtung findet die zunächst rechtmäßige Verbreitung sachlich richtiger Daten, die nachträglich unzulässig wird. Das vom EuGH entwickelte Recht auf Vergessen(werden) ist dieser Fallgruppe zuzuordnen. Aufgrund bestehender Unklarheiten über die Reichweite dieses Rechts im Einzelnen und vor dem Hintergrund der künftig geltenden EU-Datenschutzgrundverordnung (EU-DSGVO) bleibt abzuwarten, inwiefern dem nationalen Gesetzgeber noch Raum für eine eigene gesetzliche Gestaltung dieses Themas verbleibt.

Um die Täter einer Persönlichkeitsrechtsverletzung im Internet zu ermitteln, hat der Betroffene nach derzeit geltendem Recht, wenn überhaupt, lediglich die Möglichkeit, Strafantrag zu stellen, um nach Einleitung des Ermittlungsverfahrens über sein strafprozessuales Akteneinsichtsrecht die von der Staatsanwaltschaft ermittelte Identität des Beschuldigten zu erfahren. Einem Auskunftsanspruch steht nach der Rechtsprechung § 14 Abs. 2 TMG entgegen. Eine gesetzgeberische Lösung kann vernünftig jedoch nur im Zusammenhang mit der Implementierung der EU-DSGVO in das nationale Recht getroffen werden. Eine solche Lösung dürfte § 24 Abs. 1 BDSG-E nicht darstellen, da auch dieser durch § 12 Abs. 2 TMG gesperrt sein dürfte. Die Forderung der Arbeitsgruppe nach einer rechtlichen Lösung in § 14 Abs. 2 TMG wurde nunmehr von der Bundesregierung im Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG) aufgegriffen. Es erscheint jedoch darüber hinaus sinnvoll, die Auskunft von einer vorherigen richterlichen Anordnung abhängig zu machen.

Sind Täter oder Teilnehmer einer Persönlichkeitsrechtsverletzung bekannt, können sie auf Unterlassung, Beseitigung und Widerruf in Anspruch genommen werden. Sind diese unbekannt, verbleibt dem Einzelnen die Möglichkeit, gegen den Intermediär vorzugehen. Hier ist zwischen den einzelnen Intermediären und deren Möglichkeit, eine Verletzung des allgemeinen Persönlichkeitsrechts zu verhindern oder abzustellen, zu differenzieren. In der Regel bestehen Ansprüche gegenüber Intermediären (Bsp. Betreibern von Suchmaschinen, Internetforen, Online Archiven, Host-Providern, Access Providern) lediglich bei der Verletzung zumutbarer Prüfpflichten. Die Prüfpflicht setzt einen vorherigen qualifizierten Hinweis des Betroffenen voraus.

Die Möglichkeit des Betroffenen, diesen qualifizierten Hinweis gegenüber dem Intermediär abzugeben und das sich anschließende Löschungsverfahren sind in der Praxis uneinheitlich ausgestaltet und erschweren die Rechtsverfolgung unzumutbar. Wünschenswert ist eine Vereinheitlichung der Antragsbearbeitung der verschiedenen Diensteanbieter. Zu favorisieren ist dabei eine einfache „Button-Lösung“, also ein einfach erreichbarer Button in der Nähe des beanstandeten Beitrags, mit dem Betroffene Persönlichkeitsrechtsverletzungen melden können. Das Antragsformular sollte in der Sprache der Veröffentlichung und in englischer Sprache abgefasst sein. Eine Anhörung der für den Beitrag Verantwortlichen wäre seitens der Portalbetreiber und Suchmaschinenbetreiber technisch möglich und geboten. Es wäre sinnvoll, ein solches Verfahren mit einem Verbandsklagerecht zu flankieren. Eine gesetzliche Ausgestaltung eines solchen „Notice-und-Take-down-Verfahrens“ könnte am effektivsten auf europäischer Ebene erfolgen. Das Bedürfnis für ein solches Verfahren besteht für Persönlichkeitsrechtsverletzungen auch für den Fall fort, dass das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken verabschiedet wird.

Schadensersatzansprüche sind gegenüber Tätern und Teilnehmern, i. d. R. aber nicht gegenüber Intermediären denkbar, es sei denn der Intermediär verbreitet eigenen Inhalt über sein Medium, macht sich die Beiträge der Nutzer zu Eigen oder wird auf qualifizierten Hinweis nicht tätig.

Zur Entscheidung über Klagen gegen Persönlichkeitsbeeinträchtigungen durch im Internet abrufbare Veröffentlichungen sind die deutschen Gerichte im Geltungsbereich der EuGVVO nach Art. 5 Nr. 3 EUGVVO zuständig, wenn sich der Mittelpunkt der Interessen in Deutschland befindet, im Übrigen können sie nach § 32 ZPO international zuständig sein, wenn die als rechtsverletzend beanstandeten Inhalte objektiv einen deutlichen Bezug zum Inland aufweisen.

Zur Vereinfachung der Rechtsdurchsetzung bietet es sich an, einen sog. Ombudsmann für Streitigkeiten im Zusammenhang mit Persönlichkeitsrechtsverletzungen im Internet einzuführen.

Praktische Schwierigkeiten begegnen der Rechtsverfolgung gegen ausländische Unternehmen bereits bei der Zustellung der Klageschrift aber auch bei der anschließenden Vollstreckung der erlangten Titel im Ausland. Auf europäischer Ebene könnte diesen Schwierigkeiten durch die Verpflichtung zur Benennung eines inländischen Zustellungsbevollmächtigten begegnet werden.

Big Data, verstanden als die Bearbeitung großer Datenvolumen zur Gewinnung von Erkenntnissen über Marktteilnehmer, ist ein vielschichtiges Phänomen, das es zu beobachten gilt. Zum einen ist der Fokus auf die Nutzer zu richten, die oft keine informierten Entscheidungen zur Preisgabe ihrer Daten treffen. Zum anderen ist die Bearbeitung der Daten mit Algorithmen im Blick zu halten. Hierbei wird teilweise gefordert, diese gegenüber der Öffentlichkeit oder gegenüber einer hierfür einzurichtenden Behörde offen zu legen.

Nach § 13 Abs. 6 TMG muss der Diensteanbieter die Nutzung der Telemedien anonym oder pseudonym ermöglichen. Dadurch wird die Verfolgung von Rechtsverletzungen im Internet beeinträchtigt. Dieses Spannungsverhältnis sollte Gegenstand der gesellschaftlichen Diskussion sein. Gesetzgeberischer Handlungsbedarf wird zurzeit nicht gesehen.

Der Profildiebstahl im Internet kann strafrechtlich sanktioniert werden. Die wesentlichen Problemfelder (Unterlassungs- und Beseitigungsanspruch, Schadensersatz- und Schmerzensgeldanspruch) dürften im Übrigen weitgehend denjenigen entsprechen, die bei den Ansprüchen gegen Täter und Teilnehmer von Ehrverletzungen diskutiert werden.

Das Ausspähen von Daten sowohl punktuell als auch großflächig unter Rückgriff auf das Instrument des Botnetzes ist Gegenstand gesellschaftlicher und politischer Diskussion. Die Arbeitsgruppe sieht es in Bezug auf die Problematik der Botnetze als zweckmäßig an, zunächst das angestoßene Gesetzgebungsverfahren abzuwarten.

Unter dem Stichwort der „Ungewollten Einflüsse Dritter“ ist insbesondere an unerwünschte Werbe-E-Mail aber auch an Phänomene wie Online-Werbeblocker zu denken. Die Rechtslage bei unerwünschter E-Mail-Werbung ist geklärt. Es sollte zunächst der Rechtsprechung vorbehalten bleiben, auch auf andere Phänomene der ungewollten Einflussnahme Dritter zu reagieren. Zurzeit ist keine Fehlentwicklung ersichtlich.

Kapitel 4: Digitaler Nachlass

A. Übersicht über die bearbeiteten Fragestellungen

Die Arbeitsgruppe ist folgenden Themenkreisen nachgegangen:

(1.) Vererbbarkeit eines Accounts

(2.) Testamentarische Regelung

(3.) Vorsorge bzgl. des „digitalen Nachlasses“

(4.) Annahme und Ausschlagung des Erbes

(5.) Postmortales Persönlichkeitsrecht

(6.) Vererbbarkeit einer Website des Verstorbenen

(7.) Vererbbarkeit von Nutzungsrechten bei E-Books, Musik- und Video-Downloads

(8.) Vererbbarkeit bei Online-Banking, PayPal etc. (Online-Zahlungsverkehr)

(9.) Vererbbarkeit bei „virtuellen Gegenständen“ (Avatare, etc.)

(10.) Probleme des anwendbaren Rechts bei internationalem Bezug (etwa ausländische Provider)

(11.) Regelungsbedarf im Hinblick auf den Übergang von Telekommunikationsverträgen auf die Erben

Im Folgenden werden diese elf Themenkreise jeweils einzeln dargestellt. Dabei wird zunächst der Diskussionsstand dargestellt. Dem schließen sich die Stellungnahme der Arbeitsgruppe sowie etwaige Regelungsvorschläge an.

B. Die Themenkreise im Einzelnen

I. Vererbbarkeit eines Accounts

1. Fragestellungen:

Zum Themenkreis Vererbbarkeit wurden folgende Fragen als wesentlich erkannt:

- Können Anbieter in AGB beliebigen Umgang mit einem Account im Todesfall vorsehen (z. B. dass ein Account bei Tod erlischt/nicht vererblich ist) oder sollte sich das an objektiven Kriterien festmachen müssen? Gibt es bei Beendigung der Vertragsbeziehung nicht wenigstens einen Anspruch auf Herausgabe der Daten?
- Können z. B. positive Bewertungen eines Verkäufers auf Erben übertragen werden (Übertragbarkeit des „guten Namens“ analog § 25 HGB)? Wären ansonsten juristische Personen im Vorteil gegenüber natürlichen Personen?
- Muss zwischen Daten mit Vermögenscharakter und höchstpersönlichen Daten unterschieden werden?

2. Diskussionsstand zur Vererbbarkeit des „digitalen Nachlasses“

a. Definition des „digitalen Nachlasses“

In der Literatur ist bereits die Definition des „digitalen Nachlasses“ selbst umstritten. Der *Deutsche Anwaltsverein* (DAV), der sich in einer Stellungnahme zu Fragen des digitalen Nachlasses bereits im Jahr 2013 sehr ausführlich mit der Thematik auseinandersetzt hat, definiert den digitalen Nachlass im Glossar seiner Stellungnahme folgendermaßen:

> *„Beschreibt die Gesamtheit des digitalen Vermögens, also Urheberrechte, Rechte an Websites, Domains sowie sämtliche Vertragsbeziehungen zwischen Providern (siehe Provider) und dem Erblasser (siehe Erblasser) hinsichtlich der Nutzung des Internets selbst, aber auch hinsichtlich diverser Internetangebote (beispielhaft aufgezählt: Verträge über Zugang zu und Dienste auf sozialen Netzwerken, E-Mail Dienste, Internetportale, etc.) und erfasst damit auch die Gesamtheit aller Accounts (siehe Account) und Daten des Erblassers im Internet.“*[882]

In der Literatur wird z. T. vorgeschlagen, den „digitalen Nachlass“ als „die Gesamtheit der Rechtsverhältnisse des Erblassers betreffend informationstechnische Systeme einschließlich des gesamten elektronischen Datenbestands des Erblassers“ zu definieren.[883] Teilweise wird auf die Definition in „Wikipedia“ („Als digitaler Nachlass werden Accounts und Daten im Internet bezeichnet, die nach dem Tode des Benutzers weiter bestehen bleiben“) verwiesen.[884] Inzwischen wird auch die Ansicht vertreten, dass eine einheitliche Definition des „digitalen Nachlasses“ kaum möglich sei.[885]

b. Ausgangspunkt der Diskussionen zum „digitalen Nachlass“ in der Literatur

Allgemein wird in der juristischen Fachliteratur zwar vielfach Rechtsunsicherheit im Hinblick auf die Fragen des digitalen Nachlasses beklagt.[886] Bemerkenswert

---

[882] Stellungnahme des Deutschen Anwaltsvereins durch die Ausschüsse Erbrecht, Informationsrecht und Verfassungsrecht zum Digitalen Nachlass – Stellungnahme Nr. 34/2013, S. 93 (im Folgenden zitiert als *DAV*); ebenso *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (Herzog ist eine der Autorinnen der DAV-Stellungnahme).

[883] *Deusch*, Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2 (2/3). Dieser Definition folgen auch *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (262).

[884] *Pruns*, Keine Angst vor dem digitalen Nachlass! Erbrechtliche Grundlagen – Alte Probleme in einem neuen Gewand?, NWB 2013, 3161 ff.; eine Kombination aus den beiden vorgenannten Definitionen findet sich bei *Klas/Möhrke-Sobolewski*, Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3473).

[885] *Ludyga*, Der digitale Nachlass – zivilrechtliche Aspekte, juris Die Monatszeitschrift 2016, 442 (443).

[886] *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (266); *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? –

ist in diesem Zusammenhang hingegen, dass nur ganz vereinzelt konkrete Regelungslücken bzw. Harmonisierungsbedarf zwischen verschiedenen Rechtsgebieten aufgezeigt werden.[887] Ein grundlegender Regelungsbedarf (quasi für eine umfassende Neuordnung der Probleme um den digitalen Nachlass) wird in der Literatur allgemein nicht gesehen.

Unstreitiger Ausgangspunkt aller Diskussionen um den „digitalen Nachlass" ist § 1922 BGB (Universalsukzession). Insoweit wird allgemein die Ansicht vertreten, das alle vermögenswerten Rechte und Rechtsstellungen inklusive der vermögenswerten Bestandteile des allgemeinen Persönlichkeitsrechts vererblich sind, wohingegen höchstpersönliche Rechte ohne Vermögenswert (insbesondere das allgemeine Persönlichkeitsrecht in seinen ideellen Komponenten) unvererblich sind.[888]

c. Vererblichkeit eines E-Mail-Accounts sowie Accounts sozialer Netzwerke

In der Literatur vielfach und ausführlich problematisiert wird die Frage der Vererblichkeit eines E-Mail-Accounts. Insoweit wird vertreten, dass es sich bei E-Mail-Accounts um schlichte Immaterialgüter handelt, bei denen sich die Rechte und Pflichten des Nutzers in der vertraglichen Rechtsbeziehung zwischen dem Nutzer und dem Provider erschöpfen und bei denen die Erben wie bei einem Girovertrag zumindest vorläufig in das Schuldverhältnis mit dem Provider eintreten und in der Nutzung der Accounts frei sind, solange sie das postmortale Persönlichkeitsrecht respektieren.[889]

Aus Sicht des *DAV* handelt es sich bei einem E-Mail-Servicevertrag um einen typengemischten Vertrag mit werk-, dienst- und mietvertraglichen Elementen. Auch der *DAV* zieht einen Vergleich mit dem Girovertrag und geht von einer

---

Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (291); *Deusch*, Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2 (8). Auch *Kutscher*, Der digitale Nachlass, Dissertation, Kiel, 2015; im Folgenden zitiert als *Kutscher* (Diss.), S. 174 hält eine gesetzliche Klarstellung für die Abwicklung des digitalen Nachlasses für wünschenswert.

[887] So insbesondere vom *DAV* bezüglich des Datenschutzrechts/ Fernmeldegeheimnisses − § 88 TKG, vgl. dazu im Folgenden noch ausführlich.

[888] *DAV*, Stellungnahme Nr. 34/2013, S. 16 f., 30 ff.; *Hoeren*, Der Tod und das Internet − Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers, NJW 2005, 2113 (2113); *Deusch*, Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2 (4); *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (262); *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (291); *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3746); *Martini*, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1147); *Pruns*, Keine Angst vor dem digitalen Nachlass! Erbrechtliche Grundlagen – Alte Probleme in einem neuen Gewand?, NWB 2013, 3161 (3163 f.), *Kutscher* (Diss.), S. 91; *Klas/ Möhrke-Sobolewski*, Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3473 f.).

[889] *Kutscher* (Diss.), S. 44, 102 (vorab mit rechtlicher Analyse von Accounts auf S. 21 ff.).

Übertragbarkeit im Wege der Gesamtrechtsnachfolge aus. Dem Erben stehe derselbe Anspruch auf Zurverfügungstellung der E-Mails als Hauptleistungspflicht zu wie zuvor dem Erblasser, da zum Eigentum auch die auf dem Abschluss von Verträgen beruhenden schuldrechtlichen Forderungen gehörten. Der *DAV* hat allerdings telekommunikationsrechtliche und verfassungsrechtliche Vorbehalte (Art. 10 GG, § 88 TKG), die diesen Anspruch nach Ansicht des *DAV* möglicherweise zu Fall bringen könnten (vgl. dazu noch gesondert unten).[890]

Auch ansonsten wird in der Literatur ein Übergang vertraglicher Rechte und Pflichten aus Online-Beziehungen jeglicher Art auf den Erben grundsätzlich bejaht.[891]

Sehr ausführlich und differenziert behandelt aktuell *Seidler* im Rahmen einer Dissertation die Frage der Übergangsfähigkeit eines E-Mail-Accounts[892] und differenziert insoweit zwischen der zugrundeliegenden Rechtsbeziehung (der Rechtsbeziehung zwischen dem Provider und dem Nutzer, also dem „E-Mail-Vertrag“), dem E-Mail-Account als solchem und den gespeicherten Inhalten.[893] Sie kommt dabei zu dem Ergebnis, dass an dem Account und den Nachrichten als solchen keine absoluten Rechte bestehen, sondern sich die Rechtspositionen des Nutzers in der vertraglichen Rahmenbeziehung erschöpfen.[894] Der Account stellt danach zwar eine tatsächliche Position dar, der jedoch keine über die schuldrechtliche Rahmenbeziehung hinausgehende Rechtsqualität beizumessen sei.[895] Bei den E-Mails stehe neben der rechtlichen Rahmenbeziehung das Problem des Rechts auf Einsichtnahme.[896] Im Rahmen der Behandlung der Frage der Übergangsfähigkeit dieser Rechtspositionen kommt auch sie dazu, dass sowohl die vertraglich ausgestaltete Accountinhaberschaft als auch das Einsichtsrecht übergangsfähig sind.[897]

---

[890] *DAV*, Stellungnahme Nr. 34/2013, S. 17-19, 36 ff. (insbesondere S. 51 f.).
[891] *Steiner/Holzer,* Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263); *Herzog,* Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3749); *Pruns,* Keine Angst vor dem digitalen Nachlass! Erbrechtliche Grundlagen – Alte Probleme in einem neuen Gewand?, NWB 2013, 3161 (3165); ebenso *Hoeren,* Der Tod und das Internet − Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers, NJW 2005, 2113 (2114), der der Ansicht ist, dass zivilrechtlich Auskunftsansprüche gegen Provider in Bezug auf Passworte/ Zugangsdaten auf den Erben übergehen (etwa Paypal, eBay, Amazon, Zalando), wobei etwas anderes nur gelte, wenn ein entgegenstehender, ausdrücklicher oder mutmaßlicher Wille des Erblassers bestehe. *Hoeren* hält (anders als der *DAV*) das Fernmeldegeheimnis nicht für einschlägig, sodass Art. 10 GG, §§ 202, 202a, 206 StGB und § 88 TKG nicht entgegenstünden.
[892] *Seidler,* Digitaler Nachlass – Das postmortale Schicksal elektronischer Kommunikation, Dissertation, 2016, im Folgenden zitiert als *Seidler* (Diss.).
[893] *Seidler* (Diss.), S. 61 -81.
[894] *Seidler* (Diss.), S. 80.
[895] *Seidler* (Diss.), S. 72 f..
[896] *Seidler* (Diss.), S. 80.
[897] *Seidler* (Diss.), S. 95, 101.

Im Hinblick auf Verträge zwischen sozialen Netzwerken und ihren Mitgliedern wird in der Literatur vereinzelt erwogen, sie unter Schuldverhältnisse mit überwiegendem Personenbezug einzuordnen, wenn die Hauptleistung personenbezogen sei, da in diesem Fall gute Gründe für eine Unvererblichkeit sprächen.[898]

Auch im Hinblick auf Accounts, welche die Nutzung sozialer Netzwerke betreffen, wird hingegen ganz überwiegend vertreten, dass auch derartige Accounts vererblich sind.[899] Generalisierend wird für den digitalen Nachlass insoweit vertreten, dass die Vertragsbeziehung lediglich dann unvererblich ist, wenn ihr Inhalt so stark auf die Person des Berechtigten oder des Verpflichteten zugeschnitten ist, dass sie bei einem Gläubiger- oder Schuldnerwechsel in ihrem Wesen verändert würde, bzw. wenn die Leistungen des Providers individuell auf die Inhalte und Bedürfnisse des Nutzers zugeschnitten sind; insoweit wird auch der Rechtsgedanke des § 399 Alt. 1 BGB herangezogen.[900] Konkret für soziale Netzwerke wird dabei ausgeführt, dass hier im Regelfall der Inhalt des Rechts nicht in einem solchen Maße auf die Person des Berechtigten oder des Verpflichteten zugeschnitten sei, dass bei einem Subjektwechsel die Leistung in ihrem Wesen verändert würde, denn die Hauptleistungspflicht des Providers sei die Bereitstellung der Plattform und die Ermöglichung der Nutzung. Zudem wird darauf verwiesen, dass die Provider regelmäßig ohne Rücksicht auf die Person des Nutzers, meist auch ohne nähere Prüfung der Personenidentität, die Nutzungsverträge abschließen würden, sodass auch deshalb ein besonderer Personenbezug ausscheiden müsse. Auch die Nutzer nähmen kein persönliches Vertrauen in Anspruch. Auch bei persönlichkeitsrechtlich geprägten Nutzungsverträgen, wie bei sozialen Netzwerken, seien nur die Inhalte persönlichkeitsrechtlich relevant, die Leistungen des Providers seien aber nicht individuell auf die Inhalte und Bedürfnisse des Nutzers zugeschnitten.[901] *Seidler* betont, dass zwischen Persönlichkeitswerten und ihrer etwaigen Verkörperung zu unterscheiden sei – auch der Inhalt eines Tagebuchs

---

[898] *Klas/Möhrke-Sobolewski*, Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3474).

[899] *Kutscher* (Diss.), S. 156 f.; *Brinkert/Stolze/Heidrich*, Der Tod und das soziale Netzwerk, ZD 2013, 153 (155); *Martini*, Digitaler Nachlass und postmortaler Persönlichkeitsschutz im Internet, JZ 2012, 1145 (1147); *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263); *Seidler* (Diss.), S. 139; ebenso nun das LG Berlin, Urt. v. 17. 12. 2015 – 20 O 172/15, Rn. 28 (juris), jedenfalls bezüglich der Gewährung des Zugangs zu dem Account (dort: Facebook).

[900] *DAV*, Stellungnahme Nr. 34/2013, S. 35; *Kutscher* (Diss.), S. 156 f.; *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3747 f.); *Martini*, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1147); LG Berlin, Urt. v. 17. 12. 2015 − Az. 20 O 172/15, Rn. 28 (juris); *Brinkert/Stolze/Heidrich*, Der Tod und das soziale Netzwerk, ZD 2013, 153 (155).

[901] *Kutscher* (Diss.), S. 156 f.; ebenso mit gleicher Begründung: *Martini*, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1147), und *Brinkert/Stolze/Heidrich*, Der Tod und das soziale Netzwerk, ZD 2013, 153 (155); ebenso: *Seidler* (Diss.), S. 134-136.

unterfalle dem Schutz des postmortalen Persönlichkeitsrechts, ebenso wie Fotografien in einem Fotoalbum; gleichwohl werde hierdurch die verkörpernde Hülle des Sacheigentums nicht zu einer höchstpersönlichen Rechtsposition. Ebenso wenig sei die Höchstpersönlichkeit der dem Profil zugrundeliegenden Vertragsbeziehung anzunehmen.[902] *Seidler* untersucht zudem die Übergangsfähigkeit getrennt für die Kontoinhaberschaft und das Einsichtsrecht, gelangt aber für beide Positionen zu dem Ergebnis, dass sie auf den Erben übergehen.[903]

Allerdings gibt es in der analogen Welt Fälle, in denen eine Unvererblichkeit wegen der Höchstpersönlichkeit der Leistungsbeziehung angenommen wurde, die möglicherweise auf Fälle des digitalen Nachlasses übertragen werden könnten. So wurde in der Rechtsprechung für Partnerschaftsvermittlungsverträge[904] und für Heimpflegeverträge[905] entschieden, dass diese unvererblich sind.[906] Das Amtsgericht Dortmund hat hinsichtlich Partnerschaftsvermittlungsverträgen ausgeführt, dass das Vertragsverhältnis auf Seiten des Dienstberechtigten höchstpersönlicher Art sei, sodass der Sinn und Zweck des Vertragsverhältnisses nur so lange gegeben sei, wie der Verstorbene die Leistung in Anspruch habe nehmen können. Die zu erbringenden Vermittlungsdienste könnten nur in der Person des Dienstberechtigten, des Verstorbenen, ihren Sinn und ihre Erfüllung finden, denn der Sinn und Zweck eines Partnerschaftsvermittlungsvertrags, dem Vertragspartner einen Partner zu vermitteln, werde hinfällig, wenn der Vertragspartner versterbe.[907] Das Landgericht Düsseldorf hat die Beendigung eines Heimpflegevertrages mit dem Todesfall damit begründet, dass es sich dabei um ein Dienstleistungsverhältnis mit derart höchstpersönlichem Charakter handele, dass die Fortsetzung der Dienstleistung für die Angehörigen und Erben des Dienstberechtigten nicht in Betracht komme, sondern wegen nachträglicher Unmöglichkeit mit dem Tode des Dienstberechtigten ende.[908]

d. Vererblichkeit der E-Mails und möglicher Konflikt mit dem Telekommunikationsgesetz

Weiter wird in der Literatur die Frage der Vererblichkeit konkreter E-Mails diskutiert und dabei zwischen bereits abgerufenen E-Mails, die sich auf dem Rechner des Erblassers befinden und noch nicht abgerufenen E-Mails, die sich auf dem Server des Providers befinden, differenziert. In diesem Zusammenhang stellen

---

[902] *Seidler* (Diss.), S. 136.
[903] *Seidler* (Diss.), S. 139 (mit ausführlicher Herleitung auf S. 134-139).
[904] AG Dortmund, Urt. v. 18.9.1990 – 128 C 413/89, NJW-RR 1991, 689; zustimmend *Kutscher* (Diss.), S. 156 f..
[905] LG Düsseldorf, Urt. v. 7.9.1990 – 22 S 329/89, NJW-RR 1991, 184 (185): Das Dienstleistungsverhältnis weise einen derart höchstpersönlichen Charakter auf, dass die Fortsetzung der Dienstleistung für die Angehörigen und Erben des Dienstberechtigten nicht in Betracht komme.
[906] Weitere Beispiele, in denen auch in der Literatur die Unvererblichkeit jedenfalls diskutiert wird (etwa Haftpflichtversicherungsvertrag, Reisevertrag), finden sich bei *Seidler* (Diss.), S. 89 m. w. N.
[907] AG Dortmund, Urt. v. 18.9.1990 – 128 C 413/89, NJW-RR 1991, 689.
[908] LG Düsseldorf, Urt. v. 7.9.1990 – 22 S 329/89, NJW-RR 1991, 184 (185).

sich auch Probleme in Verbindung mit dem Telekommunikationsgesetz (TKG, dort § 88) sowie mit Art. 10 GG. Als Sonderproblem wird diskutiert, ob nach dem Inhalt der E-Mails (geschäftlicher oder privater Inhalt) zu differenzieren ist und in diesem Zusammenhang, ob bei privaten E-Mails (und sonstigen privaten Daten) der Erbe oder die nächsten Angehörigen berechtigt sein sollen.

Unproblematisch sind insoweit die auf der Festplatte des Rechners oder sonstigen Speichermedien des Erblassers gespeicherten E-Mails, die allgemein als vererblich angesehen werden.[909] Dies wird damit begründet, dass diese E-Mails aufgrund der Speicherung verkörperter, physischer Bestandteil einer vermögenswerten Sache sind bzw. dass sie in erbrechtlicher Hinsicht das Schicksal des Datenträgers als körperliche Sache teilen.[910]

Problematischer stellt sich die Situation bei E-Mails dar, die sich noch auf dem Server des Providers befinden und nicht auf einem Speichermedium des Erblassers. In dieser Konstellation kann der Erbe nicht über eine Vererbung von Eigentum am Datenträger Inhaber auch dieser Daten werden.[911] Wie oben bereits dargestellt tritt allerdings der Erbe nach allgemeiner Ansicht in das Vertragsverhältnis mit dem Provider ein. Wenn ein Passwort vorhanden ist, wird daher angenommen, dass der Erbe sich auch des Inhalts bedienen kann, da es sich bei dem Passwort letztlich um einen „digitalen Schlüssel" handele; insoweit wird auch argumentiert, dass bei Überlassen der Zugangsdaten seitens des Erblassers eine konkludente Übertragung der Wahrnehmungsrechte im Online-Bereich vorliegt.[912]

Wenn aber kein Passwort vorhanden ist, stellt sich das Problem, ob der Erbe einen Anspruch gegen den Provider auf Zugang zu den E-Mails bzw. Mitteilung des Passworts hat. Zivilrechtlich hat der Erbe wegen der Vererblichkeit der Vertragsbeziehung mit dem E-Mail-Anbieter einen Anspruch auf Zugang zu den E-Mails gegen den Provider.[913]

Seitens des *DAV* wurden aber Bedenken hinsichtlich eines Verstoßes gegen das durch § 88 TKG geschützte Fernmeldegeheimnisses geäußert,[914] die seitdem vielfach diskutiert, aber in der Literatur ganz überwiegend nicht geteilt werden. Ein Konflikt des Erbrechts mit dem Telekommunikationsrecht wird nicht gesehen

---

[909] *DAV*, Stellungnahme Nr. 34/2013, S. 19 ff., 48 ff., 66 ff.; *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263) (Eigentum an der Hardware wird vererbt, einschließlich der darauf gespeicherten Daten); ebenso *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3749), und *Kutscher* (Diss.), S. 100; *Ludyga*, Der digitale Nachlass – zivilrechtliche Aspekte, juris Die Monatszeitschrift 2016, 442 (443).

[910] *DAV*, Stellungnahme Nr. 34/2013, S. 19 ff., 48 ff., 66 ff.; *Ludyga*, Der digitale Nachlass – zivilrechtliche Aspekte, juris Die Monatszeitschrift 2016, 442 (443).

[911] *DAV*, Stellungnahme Nr. 34/2013, S. 51.

[912] *DAV*, Stellungnahme Nr. 34/2013, S. 50; *Kutscher* (Diss.), S. 128 f.

[913] *DAV*, Stellungnahme Nr. 34/2013, S. 51 *Ludyga*, Der digitale Nachlass – zivilrechtliche Aspekte, juris Die Monatszeitschrift 2016, 442 (444).

[914] *DAV*, Stellungnahme Nr. 34/2013, S. 66 ff.

bzw. vertreten, dass jedenfalls eine Lösung bereits mit dem geltenden Recht möglich ist. Im Einzelnen:

Der *DAV* sieht trotz des zivilrechtlichen Bestehens eines Anspruchs auf Zugang der Erben zu den E-Mails gegen Provider faktisch indes einen drohenden Verstoß gegen das durch § 88 TKG geschützte Fernmeldegeheimnis (jedenfalls der weiteren an der Kommunikation Beteiligten), weswegen er gesetzgeberischen Regelungsbedarf sieht und hierzu einen Regelungsvorschlag hinsichtlich eines neuen Absatzes 5 des § 88 TKG unterbreitet. [915]

Hoeren hält hingegen das Fernmeldegeheimnis nicht für einschlägig, sodass Art. 10 GG, §§ 202, 202a, 206 StGB und § 88 TKG nicht entgegenstünden.[916] Auch *Steiner/Holzer* sehen keinen Konflikt mit dem Telekommunikationsrecht. Der Provider erfülle lediglich eine vertragliche Pflicht und verschaffe dem Erben Zugang „im zur geschäftlichen Erbringung von Telekommunikationsdiensten erforderlichen Maße", was § 88 Abs. 3 S. 1 TKG erlaube. Zudem sei der Erbe kein „anderer" i. S. v. § 88 Abs. 3 TKG und man müsse in den meisten Fällen (insbesondere im geschäftlichen Bereich) ohnehin von einer mutmaßlichen Einwilligung des Absenders gegenüber den Erben ausgehen.[917] *Solmecke/Köbrich/Schmitt* sehen zwar den Konflikt, meinen aber, dass dieser Konflikt auch ohne gesetzgeberisches Handeln zu lösen sei und zwar im Wege der praktischen Konkordanz (verfassungsrechtliche Güterabwägung) bei Überwiegen des von Art. 14 GG umfassten Erbrechts.[918] Auch *Klas/Möhrke-Sobolewski* sehen keinen Verstoß gegen § 88 TKG bei Weitergabe der Daten und die Lösung ebenfalls im Wege der praktischen Konkordanz.[919] In der telekommunikationsrechtlichen Kommentarliteratur gibt es bislang – soweit ersichtlich – lediglich eine Auseinandersetzung mit der vom *DAV* aufgeworfenen Problematik: *Graulich* vertritt dabei ebenfalls die Auffassung, dass kein Verstoß gegen § 88 TKG in Betracht komme – dem Provider werde andernfalls eine Rolle als Wächter über die Einhaltung des Fernmeldegeheimnisses zugewiesen, die es in der Offline-Welt nicht gebe. Allerdings wird auch hier aus Gründen der Rechtssicherheit eine Klarstellung seitens des Gesetzgebers für vorzugswürdig gehalten.[920]

Kutscher setzt sich sehr ausführlich mit der Problematik auseinander und differenziert zwischen den Angeboten der Provider (Telekommunikationsdienste,

---

[915] *DAV*, Stellungnahme Nr. 34/2013, S. 66 ff. (sowie Regelungsvorschlag auf S. 6).
[916] *Hoeren,* Der Tod und das Internet − Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers, NJW 2005, 2113 (2114 f.).
[917] *Steiner/Holzer,* Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263 f.).
[918] *Solmecke/Köbrich/Schmitt,* Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (292).
[919] *Klas/Möhrke-Sobolewski,* Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3477 f.).
[920] Arndt/Fetzer/Scherer/*Graulich,* TKG § 88 Rn. 74.

die ganz oder überwiegend der Übertragung von Signalen über Telekommunikationsnetze dienen, § 3 Nr. 24 TKG), für die das Telekommunikationsgesetz gilt, und Telemedien, bei denen es sich um elektronische Informations- und Kommunikationsdienste handelt, für die das Telemediengesetz gilt (mit Vorrang des TKG gem. § 11 Abs. 3 TMG). Sie verweist darauf, dass das Datenschutzrecht mit dem Tod erlischt (kein postmortaler Datenschutz durch das BDSG) und im Anwendungsbereich des Fernmeldegeheimnisses das TKG als spezielle Regelung das allgemeine Datenschutzrecht verdrängt. Auch sie sieht allein beim Fernmeldegeheimnis in seiner einfachgesetzlichen Ausgestaltung in § 88 TKG mögliche Probleme im Hinblick auf das Fernmeldegeheimnis der Kommunikationspartner, kommt aber im Ergebnis nach einer Gegenüberstellung mit der vergleichbaren Regelung in § 39 PostG ebenfalls zu dem Schluss, dass § 88 TKG den Ansprüchen der Erben nicht entgegenstehe.[921] Auch für E-Mails, die erst nach dem Tod des Erblassers zugehen, sieht *Kutscher* kein Problem, da man die Erben aufgrund einer „erbrechtlichen Fiktion" als Adressaten der Einwilligung des Absenders ansehen könne; andernfalls müsse man von einer mutmaßlichen Einwilligung des Absenders ausgehen.[922] Dem Zugangsrecht des Erben stehe auch das Fernmeldegeheimnis nicht im Wege. Die Kommunikationspartner hätten bereits mit Absendung und Zugang ihrer Nachricht beim Erblasser ihre Verfügungsbefugnis über den Inhalt der Nachricht verloren und auf den Erblasser übertragen. Für Nachrichten, die erst nach dem Tode des Erblassers zugingen, würden die Grundsätze der mutmaßlichen Einwilligung gelten.[923] Auch *Kutscher* hält wegen der bestehenden Rechtsunsicherheit eine gesetzgeberische Klarstellung aber für wünschenswert.[924]

Auch *Seidler* setzt sich mit der Ansicht des *DAV* auseinander und kommt zu dem Ergebnis, dass sich aus den Wertungen des TKG keine Verschwiegenheitsverpflichtung des Providers ergebe.[925] Ein Erbe des verstorbenen Nutzers sei von vornherein nicht als „anderer" i. S. d. § 39 Abs. 3 S. 1 PostG anzusehen und auch im Bereich des telekommunikationsrechtlichen Fernmeldegeheimnisses könne nichts Abweichendes gelten.[926]

e. Berechtigung der Erben oder der nächsten Angehörigen in Bezug auf E-Mails und Problematik der Differenzierung zwischen E-Mails mit vermögenswertem und privatem Inhalt

In der Fachliteratur wird vielfach diskutiert, wer bei E-Mails (und sonstigen Daten) der Berechtigte im Erbfall ist: der/die Erbe(n) oder die nächsten Angehörigen. Dabei wird insbesondere diskutiert, ob zwischen E-Mails (bzw. auch sonstigen

---

[921] *Kutscher* (Diss.), S. 130-146.
[922] *Kutscher* (Diss.), S. 145 f.
[923] *Kutscher* (Diss.), S. 148.
[924] *Kutscher* (Diss.), S. 167 f.
[925] *Seidler* (Diss.), S. 115.
[926] *Seidler* (Diss.), S. 114.

Daten) mit vermögenswertem Inhalt und privatem Inhalt differenziert werden muss.

Der *DAV* hält eine Differenzierung nicht für erforderlich. Bei E-Mails (auf dem Rechner des Erblassers) besteht nach Ansicht des *DAV* nur eine Berechtigung des Erben. Den Angehörigen steht nur die Wahrnehmung des postmortalen Persönlichkeitsrechts des Erblassers zu (bloßes Abwehrrecht, das treuhänderisch für den verstorbenen Angehörigen geltend gemacht werde). Geschützt wird dadurch aber allein die Menschenwürde, sodass nur ein enger Anwendungsbereich besteht. Nur in dem Fall, dass die Erben dieses postmortale Persönlichkeitsrecht verletzten, bestünden Abwehransprüche, welche die nahen Angehörigen für den Verstorbenen geltend machen könnten. Bei Aufsplittung nach wirtschaftlichen und privaten Inhalten würde es andernfalls schon bei der Frage, wer entscheiden sollte, welche E-Mails geschäftlich und welche privat sind, unlösbare Probleme geben.[927]

Eine solche Differenzierung nimmt aber *Hoeren* (auch bei bereits abgerufenen E-Mails) vor, da die E-Mails, die keinen vermögensrechtlichen Bezug hätten, nicht vererbbar und daher den nächsten Angehörigen zuzuleiten seien, die dann die Persönlichkeitsrechte des Erblassers treuhänderisch wahrnähmen.[928] *Martini* teilt zwar zunächst aus rein zivilrechtlicher Sicht die Ansicht, dass den Erben die Daten zustünden.[929] Indes sieht er dies durch Datenschutzrecht und insbesondere das postmortale Persönlichkeitsrecht überlagert und kommt so zu dem Schluss, dass (wie von *Hoeren* vertreten) zwischen überwiegend die Vermögenssphäre betreffenden und überwiegend höchstpersönliche Sachverhalte betreffenden Daten unterschieden werden müsse. Die Trennung müsse durch treuhänderische Einschaltung eines neutralen Dritten erfolgen, etwa des Diensteanbieters. Dies würde jenem zwar einigen Aufwand abverlangen, den er aber in sein Geschäftsmodell einpreisen werde (müssen).[930] *Brinkert/Stolze/Heidrich* sehen wegen des postmortalen Persönlichkeitsrechts bei sozialen Netzwerken (Facebook etc.) eine lediglich eingeschränkte Rechtsstellung der Erben und lehnen einen uneingeschränkten Zugriff der Erben auf alle Inhalte eines Accounts ab, folgen also für soziale Netzwerke der Ansicht von *Martini* und *Hoeren*.[931]

In der aktuellen Literatur werden diese Ansätze ganz überwiegend abgelehnt und (der Ansicht des *DAV* folgend) vertreten, dass eine derartige Differenzierung nicht vorzunehmen sei. Das Erbrecht unterscheide gerade nicht zwischen privatem und vermögensbezogenem Nachlass – insoweit wird auf die etwas versteckten gesetzgeberischen Wertungen in §§ 2047 und 2373 BGB verwiesen. Richtigerweise

---

[927] *DAV*, Stellungnahme Nr. 34/2013, S. 23 ff., 49 ff. (insbesondere S. 52 f. und 56).
[928] *Hoeren*, Der Tod und das Internet − Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers, NJW 2005, 2113 (2114).
[929] *Martini*, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1147).
[930] *Martini*, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1147 ff., insbesondere 1152).
[931] *Brinkert/Stolze/Heidrich*, Der Tod und das soziale Netzwerk, ZD 2013, 153 (155 f.).

stünden dem Erben sämtliche Daten des Erblassers zu und die Angehörigen hätten lediglich Abwehransprüche, etwa bei Menschenwürdeverletzungen.[932]

f. Nachweis der Erbenstellung gegenüber Providern bei Geltendmachung eines Auskunftsanspruchs (insbesondere Frage der Wirksamkeit entsprechender AGB-Klauseln)

In der Literatur wird darauf hingewiesen, dass die Erben häufig vor dem Problem stehen, überhaupt klären zu müssen, welche Vertragsverhältnisse des Erblassers bestehen, da diese oft online abgeschlossen und auch Rechnungen nur per E-Mail versandt wurden. Ein Auskunftsanspruch wird in der Literatur für erforderlich gehalten und z. T. aus § 34 BDSG hergeleitet,[933] überwiegend aber als ein vertraglicher Nebenanspruch auf Auskunft bezüglich Passwörter und Zugangsdaten, der mit dem Providervertrag auf die Erben übergeht, begründet.[934]

Solmecke/Köbrich/Schmitt werfen in diesem Zusammenhang die Frage auf, welche Nachweise über das Erbrecht dabei von den Erben verlangt werden dürfen, insbesondere ob ein Erbschein verlangt werden könne. Gesetzlich sei Letzteres nicht erforderlich. Vertraglich sei dies zwar an sich möglich, aber über die Rechtsprechung des BGH im Bankrecht für entsprechende vertragliche Regelungen eingeschränkt worden. Zudem erscheine es unbillig, an den digitalen Nachlass die Maßstäbe des Bankrechts oder des Grundbuchrechts anzuwenden, zumal ein Erbscheinsantrag eine Annahme der Erbschaft darstelle und Auskunftsansprüche gerade vor der Annahme bestehen sollten, um vermögensrechtliche Verhältnisse für

---

[932] *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263); *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (291); ausführlich *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3747 ff.), und *Pruns*, Keine Angst vor dem digitalen Nachlass! Erbrechtliche Grundlagen – Alte Probleme in einem neuen Gewand?, NWB 2013, 3161 (3166); sehr ausführlich *Kutscher* (Diss.), S. 113 ff. (mit Darstellung des Streitstandes ab S. 102 ff.); ausführlich auch *Seidler* (Diss.), S. 96-101, ebenfalls mit dem Ergebnis des Übergangs des Einsichtsrechts auf die Erben (ohne dass nach etwaigem Vermögenswert zu differenzieren wäre), da stets von der Möglichkeit enthaltener vermögensrelevanter Inhalte auszugehen sei. Auch sie verweist (auf S. 122 f.) auf §§ 2047 Abs. 2, 2373 S. 2 BGB und kommt aufgrund der Annahme einer planwidrigen Regelungslücke zu einer analogen Anwendung dieser Vorschriften auf moderne Datenträger.

[933] *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (292 f.).

[934] Vgl. etwa *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3749); *Kutscher* (Diss.), S. 116; *DAV*, Stellungnahme Nr. 34/2013, S. 51 f., *Klas/Möhrke-Sobolewski*, Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3474) diese insoweit auch mit ausführlichen dogmatischen Bedenken gegen die Heranziehung von § 34 BDSG (S. 3475 f.).

[934] *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (294).

die Frage der Annahme/Ausschlagung zu klären. Sie kommen vor diesem Hintergrund zu dem Ergebnis, dass ein Erbschein zur Legitimation des Erben generell nicht gefordert, sondern der Nachweis durch Sterbeurkunde und jeweilige Ausweisdokumente bzw. für den Fall der gewillkürten Erbfolge durch Testament oder Erbvertrag erbracht werden könne.[935]

Herzog vertritt hingegen ohne nähere Begründung die Auffassung, dass die Provider i. d. R. zum Nachweis der Erbenstellung den Erbschein verlangen können.[936] Auch der *DAV* ist der Ansicht, dass der Erbschein verlangt werden könne, da entsprechende AGB-Klauseln in Parallele zu den Bankrechtsfällen wirksam seien.[937]

Vielfach wird in der Literatur bei dieser Diskussion der Fokus auf die Frage gelegt, ob AGB-Klauseln der Provider für den Fall des Todes des Kunden wirksam sind.

Insoweit werden insbesondere Kündigungsklauseln, Legitimationsklauseln und Abwicklungsklauseln diskutiert:

(1) Kündigungsklauseln

Hinsichtlich Kündigungsklauseln (die Kündigungsrechte im Todesfall des Nutzers des Accounts regeln) ist der *DAV* der Ansicht, dass ein außerordentliches Kündigungsrecht beim Tod des Kunden allenfalls beidseitig, d. h. für Provider und Erben, vereinbart werden könne. Ein einseitiges Kündigungsrecht sei nicht möglich. Es sei zweifelhaft, ob ein beidseitiges Kündigungsrecht vereinbart werden könne. Im Dienstvertrag werde eine solche Möglichkeit gerade abgelehnt. Möglicherweise müsse eine Differenzierung nach Vertragsgegenstand vorgenommen werden. In der Regel seien aber entsprechende AGB-Regeln wohl unwirksam.[938]

Kutscher verweist zwar auf die einseitigen Kündigungsrechte bei unentgeltlichen Verträgen (§ 671 Abs. 1 BGB für Auftrag und § 604 Abs. 3 BGB für Leihe), hier läge aber trotz Unentgeltlichkeit im geldwerten Sinne kein Auftragsverhältnis sondern ein synallagmatischer Vertrag vor, da der Nutzer persönliche Daten zur Verfügung stelle und sich mit dem Erhalt von Werbung einverstanden erkläre. Eine außerordentliche Kündigung gem. § 314 BGB komme mangels besonderen Vertrauensverhältnisses nicht in Betracht. Der Account gehe jedenfalls vorläufig auf die Erben über, Daten dürften nicht einfach gelöscht werden, sondern seien an Erben herauszugeben und dann zu löschen. In allen Fällen müsse der bloße

---

[935] *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (294).

[936] *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750 f.).

[937] *DAV*, Stellungnahme Nr. 34/2013, S. 62-64.

[938] *DAV*, Stellungnahme Nr. 34/2013, S. 59 ff. (insbesondere S. 62), unter Verweis auf OLG Koblenz, Urt. v. 30.10.2003 – 2 U 504/03, MMR 2004, 106, und OLG Koblenz, Urt. v. 30.9.2010 – 2 U 1388/09, CR 2011, 471 (473).

Zugriff zunächst gewährt werden. Ein außerordentliches Kündigungsrecht bei wichtigem Grund müsse beiden Vertragsparteien zugestanden werden, ein einseitiges Interesse des Providers an einer solchen Kündigung sei hier nicht anzunehmen.[939]

Auch *Seidler* hält einseitige Beendigungsklauseln wegen eines Verstoßes gegen § 307 Abs. 2 S. 1 BGB für unwirksam, da sie mit dem wesentlichen Grundgedanken des § 1922 Abs. 1 BGB, wonach zu Lebzeiten erworbene Rechtspositionen des Erblassers im Regelfall auch nach seinem Tod fortbestehen, nicht vereinbar seien.[940]

(2) Legitimationsklauseln

Im Hinblick auf die bereits oben erwähnten Legitimationsklauseln (Klauseln, die den Nachweis der Erbenstellung regeln) ist der *DAV* unter Verweis auf Bankrecht und Rechtsprechung des BGH der Ansicht, dass, soweit Erbscheinsvorlage von Banken in AGB gefordert werde, dies wirksam sei, darüber Hinausgehendes hingegen nicht. Ob eine Herabsetzung der Anforderungen an den Nachweis möglich sei, sei streitig. Die Problematik sei den Fällen von Banken-AGB vergleichbar und damit die dazu bestehende BGH-Rechtsprechung übertragbar auf Provider. Vor diesem Hintergrund seien alle vom DAV untersuchten verwendeten Klauseln unwirksam.[941] *Kutscher* verweist ebenfalls auf eine Parallele zum Bankrecht und die diesbezügliche BGH-Rechtsprechung und hält diese für übertragbar auf Internetprovider. Klauseln, die generell und unabhängig davon, ob im Einzelfall das Erbrecht zweifelhaft sei oder durch andere Dokumente einfacher und/oder kostengünstiger nachgewiesen werden könne, zwingend auf der Vorlage eines Erbscheins bestünden, seien daher unwirksam. Höhere Anforderungen dürften erst recht nicht gestellt werden. Zur Löschung die Vorlage einer Sterbeurkunde oder Traueranzeige ausreichen zu lassen, dürfe rechtswidrig sein, weil in diesem Fall nicht sichergestellt sei, dass Erben über Schicksal des Accounts entscheiden.[942] *Seidler* ist ebenfalls der Ansicht, dass die BGH-Rechtsprechung zu Banken-AGB auf den Übergang von E-Maildiensten und sozialen Netzwerken übertragbar sei und daher eine Klausel, aufgrund derer der Nachweis allein mittels Erbschein geführt werden könne, unwirksam sei.[943] Gleiches gilt ihrer Ansicht nach für das Verlangen nach einer gerichtlichen Entscheidung in AGB.[944] Sie hält indes Klauseln, nach denen die Vorlage einer Traueranzeige oder einer Sterbeurkunde zur Legitimation ausreiche, für wirksam. Solche Klauseln gingen allenfalls zu Lasten des Providers als Verwender solcher AGB, dem eine Haftung drohe, falls er Unbefugten die Zugangsdaten übermittelt. Da aber die Inhaltskontrolle

---

939 *Kutscher* (Diss.), S. 123 ff.
940 *Seidler* (Diss.), S. 144-146.
941 *DAV*, Stellungnahme Nr. 34/2013, S. 62-64.
942 *Kutscher* (Diss.), S. 124 f.
943 *Seidler* (Diss.), S. 146-148.
944 *Seidler* (Diss.), S. 148 f.

maßgeblich auf die Schutzbedürftigkeit des Vertragspartners abstelle, sei im Rahmen des § 307 Abs. 1 S. 1 BGB lediglich entscheidend, ob die jeweilige Klausel den Vertragspartner – also hier den Nutzer – unangemessen benachteilige, was hier aber gerade nicht der Fall sei.[945]

(3) Abwicklungsklauseln (Klauseln bezüglich der Abwicklung von Providerverträgen):

Der *DAV* führt aus, dass nach übereinstimmender Meinung die Pflicht zur Datenherausgabe (bzw. zur Schaffung der Möglichkeit des Kunden, sich Daten zu kopieren und die Daten zu löschen) bestehe. Im Fall der Löschung bestünden Schadensersatzansprüche. Ein Ausschluss des Herausgaberechts oder des Löschungsrechts in AGB sei gem. § 307 Abs. 2 Nr. 2 BGB unwirksam. Zulässig seien hingegen Modifikationen (Art und Weise der Herausgabe). Die Herausgabe von Vorgängen, die dem Fernmeldegeheimnis unterlägen, dürfe der Provider von Einverständniserklärungen des oder der Absender(s) abhängig machen (mehr aber nicht). Viele vom *DAV* untersuchte Klauseln seien unwirksam.[946]

Kutscher folgt dieser Ansicht[947] und beschäftigt sich zudem mit der Frage, ob die Verträge der Provider als höchstpersönliche ausgestaltet werden könnten, sodass eine Vererbung ausgeschlossen werden könnte, verneint dies aber für den Regelfall mangels Zuschnitt des Rechts auf die Person des Berechtigten in einem solchen Umfang, als dass bei einem Subjektwechsel die Leistung in ihrem Wesen verändert würde und damit Unvererblichkeit angenommen werden könnte.[948]

Weiter beschäftigt sich *Kutscher* mit der Frage, ob ein Provider den Vertrag unter einer Befristung auf den Tod des Nutzers abschließen kann und verneint dies für den Fall, dass dies in den AGB einseitig durch den Provider festgelegt ist, da dies mit wesentlichen Grundgedanken des BGB, insbesondere § 1922 BGB, und auch § 28 UrhG nicht vereinbar sei. Wenn der Provider dem Nutzer aber die Möglichkeit lasse, selbst zu entscheiden, wie mit seinen Daten nach seinem Tod umzugehen sei, könne darin keine unangemessene Benachteiligung entgegen Treu und Glauben (§ 307 Abs. 1 S. 1 BGB) gesehen werden. Die Löschung entspreche dann dem Erblasserwillen und der Erbe könne sich nicht wehren, da das Erbrecht erst mit dem Tod des Erblassers entstehe und dem Erben auch kein Anwartschaftsrecht zustehe.[949] *Steiner/Holzer* weisen auf uneindeutige AGB der großen Anbieter bzgl. der Vererbbarkeit von Nutzungsrechten bei E-Books, Musik- und Video-Downloads hin, ohne konkrete rechtliche Standpunkte zu vertreten.[950]

---

[945] *Seidler* (Diss.), S. 149.
[946] *DAV*, Stellungnahme Nr. 34/2013, S. 64 f.
[947] *Kutscher* (Diss.), S. 126-128.
[948] *Kutscher* (Diss.), S. 155- 157.
[949] *Kutscher* (Diss.), S. 158 f.
[950] *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (265).

g. Übertragung positiver Bewertungen (etwa auf eBay) auf die Erben

Ein der Nutzung eines Verkaufsportals zugrundliegender Vertrag (z. B. der *eBay*-Account) geht nach den bereits oben dargelegten Grundsätzen (vorbehaltlich etwaiger wirksamer vertraglicher abweichender Regelungen) auf den Rechtsnachfolger über. Fraglich ist jedoch, ob etwaige auf dem Verkäuferprofil (ggf. auch Käuferprofil) gespeicherte Bewertungen des Erblassers ebenfalls mit der Vertragsstellung auf den Erben übergehen, er sich diese also zu Nutzen machen kann. Dies wird vereinzelt mit einem pauschalen Hinweis darauf, dass bei der Vererbung eines Unternehmens auch der verkörperte Goodwill mit übergehe, bejaht.[951]

3. Stellungnahme

a. Vererblichkeit eines Accounts

Die grundsätzliche Frage, ob ein Account vererblich ist, wird in der Literatur zu Recht durchweg in dem Sinne bejaht, dass der Account als vertragliche Beziehung auf den Erben übergeht und so auch die vertraglichen Rechte und Pflichten auf den Erben übergehen, wobei im Falle der Fortführung des Vertrages ein eigener (neuer) Vertrag mit dem Erben zustande kommt (wie es auch beim Girovertrag der Fall ist). Da der Erbe also in die Providerverträge eintritt, stehen ihm die Ansprüche aus dem Vertrag (Übermittlung der E-Mails bzw. Zugänglichmachung durch Passwortübermittlung) zu. Die Arbeitsgruppe ist in diesem Zusammenhang noch vertieft der Frage nachgegangen, ob dies auch für Accounts bezüglich sozialer Netzwerke wie „Facebook“, „Xing“ oder „LinkedIn“ gilt. Die oben dargestellte weit überwiegende Ansicht in der Literatur, der sich auch das Landgericht Berlin[952] angeschlossen hat, wonach Vererblichkeit auch bei allen Accounts grundsätzlich gegeben ist, ist nach Ansicht der Arbeitsgruppe im Hinblick auf Accounts bezüglich sozialer Netzwerke wie „Facebook“, „Xing“ oder „LinkedIn“ zutreffend.

Das in der Literatur verwendete generelle Abgrenzungskriterium, wonach Unvererblichkeit anzunehmen ist, wenn der Inhalt der Vertragsbeziehung so stark auf die Person des Berechtigten oder des Verpflichteten zugeschnitten ist, dass sie bei einem Gläubiger- oder Schuldnerwechsel in ihrem Wesen verändert würde (Rechtsgedanke des § 399 Alt. 1 BGB), hat den großen Vorteil, dass es gleichermaßen als Kriterium für nicht digitale Sachverhalte angewandt wird, wie es auch bei den hier zu untersuchenden digitalen Fallkonstellationen sachgerecht erscheint. Es ermöglicht so den Gleichlauf von vergleichbaren nicht-digitalen und digitalen Sachverhalten. Die Anwendung dieser generalisierenden Abgrenzungskriterien führt dazu, dass auch bei Verträgen über die Accounts von sozialen Netzwerken wie „Facebook“, „Xing“ oder „LinkedIn“ Vererblichkeit gegeben ist. Auch bei diesen Verträgen ist die vom Anbieter zu erbringende Leistung in aller Regel nicht in einem solchen Maß auf die Person des Berechtigten zugeschnitten,

---

[951] *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750).
[952] LG Berlin, Urt. v. 17.12.2015 – 20 O 172/15, MDR 2016, 165.

dass ein Subjektwechsel die Leistung in ihrem Wesen verändern würde. Nur die *Inhalte*, die mittels dieser Accounts vom Nutzer geschaffen oder kommuniziert werden, sind in vielen Fällen persönlichkeitsrechtsrelevant, nicht aber die Leistungen des Providers im Rahmen der Vertragsbeziehung.

Durch den Vertragsschluss verpflichtet sich der Anbieter eines sozialen Netzwerks, dem Vertragspartner die Nutzung seiner „IT-Infrastruktur" zu gestatten.[953] Der Schwerpunkt der Leistungen bei sozialen Netzwerken liegt darin, eine technische Plattform zur Verfügung zu stellen, die es dem Kunden ermöglicht, sich selbst darzustellen und mit andern Nutzern in Kontakt zu treten.[954] Diese Leistungspflichten ändern sich aber gerade nicht, wenn an die Stelle des bisherigen Nutzers sein Rechtsnachfolger tritt. Der Provider war bei derartigen sozialen Netzwerken auch zu Lebzeiten des bisherigen Nutzers nicht etwa verpflichtet, dessen Profil zu individualisieren. Er stellt dem Nutzer lediglich die technischen Einrichtungen zur Verfügung, damit dieser selbst seine Profilseite gestalten und mit Inhalten füllen kann. Die Leistungspflichten des Providers unterscheiden sich damit nicht von Mitglied zu Mitglied, sondern sind stets gleich. Dies gilt sowohl für private als auch für beruflich genutzte Netzwerke.

Ein anderes ergibt sich auch nicht dadurch, dass der Nutzer im Rahmen seiner Nutzung selbst private Inhalte generiert, also die ihm zur Verfügung gestellte Profilseite selbst gestaltet. Auch dies führt nämlich nicht dazu, dass die zu erbringende Leistung in einem solchen Maß auf die Person des Berechtigten zugeschnitten wäre, dass ein Subjektwechsel sie in ihrem Wesen verändern würde. Die Vertragsbeziehung mit ihren Rechten und Pflichten besteht vom Grundsatz her unabhängig von den Inhalten, die der Nutzer auf der ihm zur Verfügung gestellten Seite einstellt. Von den Inhalten, die der Erblasser auf dieser Seite eingestellt hat, kann nicht auf eine Unvererblichkeit geschlossen werden, denn sie sind in jedem Fall individuell und niemals Gegenstand der Leistungspflichten aus dem Vertragsverhältnis, dessen Übergang zu prüfen ist. Eine Unvererblichkeit wegen der Höchstpersönlichkeit des Rechtsverhältnisses dürfte damit auch bei sozialen Netzwerken in aller Regel ausscheiden, sodass auch diese Vertragsbeziehungen dem Grunde nach vererblich sind.

Auch aus einer etwaigen Unzumutbarkeit der Fortsetzung der Vertragsbeziehung für den Provider lässt sich bei Verträgen über soziale Netzwerke in aller Regel keine Beendigung der Vertragsbeziehung mit dem Tod des Nutzers begründen, da – worauf in der Literatur, wie oben dargestellt, vielfach hingewiesen wird – die Provider die Nutzungsverträge regelmäßig ohne Rücksicht auf die Person des Nutzers, meist auch ohne nähere Prüfung der Personenidentität, abschließen.

Allerdings sind in Einzelfällen Vertragsgestaltungen zu Accounts denkbar, bei denen die Leistungspflichten derart auf den Nutzer zugeschnitten sind, dass eine

---

[953] *Bräutigam*, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635 (640).
[954] *Redeker*, IT-Recht, Rn. 1173.

Vererblichkeit aufgrund des höchstpersönlichen Charakters ausscheiden muss. Insoweit dürfte sich die Rechtsprechung aus der „analogen Welt“ zu den Partnerschaftsvermittlungsverträgen auf Online-Partnerschaftsvermittlungsverträge (Internet-Partnerschaftsbörsen wie „Parship“ etc.) übertragen lassen. Eine Vertragsbeziehung, in der ein Anbieter für einen Nutzer Partnerschaften anbahnen, also insbesondere Kontakte zu potentiell passenden Partnern herstellen soll, ist bereits per se auf den jeweils Suchenden höchstpersönlich zugeschnitten. Partnervorschläge müssen individuell und auf die Eigenschaften und Suchkriterien des Nutzers zugeschnitten sein. Aufgrund der Materie selbst liegt hier ein höchstpersönlicher Charakter vor. Hier kommt es auch inhaltlich in der Vertragsbeziehung auf die Person des Partnersuchenden selbst an, denn es liegt auf der Hand, dass der Anbieter die gegenüber dem Erblasser geschuldete, auf diesen notwendigerweise individuell zugeschnittene Leistung nicht gegenüber dem Erben fortsetzen kann. In derartigen Ausnahmefällen kommt eine Unvererblichkeit aufgrund des höchstpersönlichen Charakters der Leistungspflicht in Betracht – nicht jedoch generell bei Accounts von sozialen Netzwerken. Auch bei sozialen Netzwerken ist im Einzelfall eine Unvererblichkeit denkbar, nämlich wenn die Pflichten des Anbieters im Hinblick auf den Nutzer individualisiert sind. Das wird sich allerdings nur im Einzelfall bei besonderen (sehr seltenen und eher theoretisch vorstellbaren) Fallkonstellationen feststellen lassen. Für die „großen“ Anbieter von Accounts sozialer Netzwerke wie „Facebook“, „Xing“ oder „LinkedIn“ trifft dies indes nicht zu. Die Abgrenzung kann anhand des abstrakt-generellen Kriteriums des individuellen Zuschnitts der Leistungspflichten erfolgen.

Obwohl die Vertragsbeziehung „Account“ damit auch bei sozialen Netzwerken auf den Erben übergeht, dürften im Hinblick auf eine weitere Nutzung durch den Erben aber wohl (unabhängig von allgemeinen Geschäftsbedingungen der Anbieter) Einschränkungen gelten. Jedenfalls im Bereich privater Accounts dürfte die Profilseite an den Rechtsnachfolger anzupassen sein. Andernfalls könnte das postmortale Persönlichkeitsrecht des Erblassers verletzt werden. Wird durch die Fortführung des Accounts ohne Kenntlichmachung des Todes des Inhabers etwa suggeriert, der Erblasser sei noch am Leben und sei es selbst, der die Einträge vornehme, könnte hierin eine hinreichend schwere Persönlichkeitsrechtsverletzung liegen, die die wahrnehmungsberechtigten Angehörigen des Erblassers berechtigen könnte, Unterlassungsansprüche geltend zu machen (Stichwort: Lebensbildverzerrung). Damit dürfte (ähnlich den Bankverträgen) hier die Vertragsbeziehung übergehen, aber für eine Fortsetzung der Nutzung ein Eintritt des Erben in das Vertragsverhältnis (mit Anpassung des Accounts auf den Erben) erforderlich sein. Den Anspruch auf Gewährung des Zugangs zu dem Account bzw. auf Zurverfügungstellung der dortigen Inhalte schränkt dies indes nicht ein.

Nach alldem wird in diesem Punkt *kein* gesetzgeberischer Regelungsbedarf gesehen. Wäre eine Unvererblichkeit bei sozialen Netzwerken gegeben, bestünde für die Erben das Problem, dass sie nicht an die dort enthaltenen – möglicherweise für die Frage der Ausschlagung der Erbschaft mangels Werthaltigkeit relevanten – Informationen gelangten. Bei Annahme von Unvererblichkeit hätten die Erben

nämlich auch keinerlei Auskunftsansprüche zur Ermittlung des digitalen Nachlasses, da die Folge ein Erlöschen der Rechte wäre[955], sodass Auskunftsansprüche von vornherein ausscheiden würden. Da aber eine Vererblichkeit anzunehmen ist, stellt sich dieses Problem nicht. Bei den wenigen derartig höchstpersönlichen Vertragsbeziehungen, wie einer Online-Partnervermittlung, dürfte der Zugang zu dem Account für die Erben zwecks Ermittlung des Nachlasses eher irrelevant sein.

Würde man eine Regelung treffen, wonach Providerverträge *immer* auf den Rechtsnachfolger des verstorbenen Nutzers übergehen, hätte dies zur Konsequenz, dass auch solche Vertragsbeziehungen, aus denen ausnahmsweise höchstpersönliche Leistungspflichten folgen, den Tod des Nutzers überdauern würden. Dies würde aber gerade im Vergleich zu Schuldverhältnissen der „analogen Welt" zu widersprüchlichen Ergebnissen führen. So wäre es nicht sachgerecht, würde etwa der online geschlossene Partnervermittlungsvertrag auf den Erben des Nutzers übergehen, während das analog zustande gekommene Vertragsverhältnis mit dem Tod des Nutzers enden würde. Tatsächlich lässt sich die Frage nach dem Fortbestand solcher Verträge nach dem Tod des Nutzers aber mit den gleichen Instrumentarien wie bei analogen Schuldverhältnissen lösen.

Auch eine Regelung, wonach Providerverträge *im Zweifel* auf den Rechtsnachfolger des verstorbenen Nutzers übergehen, erscheint nicht erforderlich. Eine gesetzgeberische Regelung wäre aufgrund der dargestellten, ohnehin auch bei Accounts bezüglich sozialer Netzwerke bestehenden, Vererblichkeit lediglich deklaratorischer Natur. Zwar hat die Arbeitsgruppe festgestellt, dass der tatsächliche Befund bei allen großen Anbietern nicht der Rechtslage entspricht. Dies lag allerdings nicht an einem AGB-mäßigen Ausschluss der Vererblichkeit, sondern daran, dass keiner der untersuchten Anbieter die Übernahme des Vertrages durch die Erben vorsah. Vielmehr besteht kein genereller Widerspruch zwischen den allgemeinen Geschäftsbedingungen und der Rechtslage. Sofern in Einzelfällen allgemeine Geschäftsbedingungen die Rechte der Erben in unzulässiger Weise verkürzen, stellt sich die Frage nach dem Eingreifen von § 307 BGB und etwaigen Regelungsbedarfs in §§ 308, 309 BGB im Hinblick auf die jeweilige konkrete AGB-Regelung. Eine deklaratorische Regelung, wonach Vertragsbeziehungen über Accounts vererblich sind, erscheint überflüssig.

b. Erbrechtlicher Übergang von E-Mails und Problematik der Differenzierung zwischen Daten mit Vermögenscharakter und höchstpersönlichen Daten

Als allgemeine Meinung kann zugrunde gelegt werden, dass der Grundsatz der Universalsukzession den Ausgangspunkt bildet. Als eher unproblematisch stellt sich dabei der erbrechtliche Übergang bereits abgerufener E-Mails dar.

---

[955] *Herzog,* Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3747).

(1) Bereits abgerufene E-Mails

Bei bereits abgerufenen E-Mails stellt sich die derzeit geltende Rechtslage eindeutig so dar, dass der Erbe die auf der Hardware gespeicherten E-Mails miterbt, da das Eigentum an der Hardware (Festplatte) auf den Erben übergeht und die Daten auf dieser verkörpert sind. Dies entspricht auch der oben dargestellten allgemeinen Ansicht in der Literatur.

Eine Trennung zwischen persönlichen und geschäftlichen E-Mails ist de lege lata nicht durchzuführen, vielmehr stehen alle E-Mails dem Erben zu. Eine solche Trennung wird zwar (trotz des unstreitigen Ausgangspunkts der Universalsukzession) in der Literatur vertreten, sie entspricht aber nicht geltendem Recht.

Dass der Rechner (bzw. sonstige körperliche Speichermedien, wie externe Festplatten, USB-Sticks etc.) den Erben zusteht (§ 1922 BGB, Universalsukzession) ist unstreitig und gesichert. An Inhalten, die in Gegenständen verkörpert sind, an denen die Erben Eigentum erworben haben, stehen aber nach geltendem Recht den nächsten Angehörigen nie eigene Ansprüche zu. Sie können lediglich das postmortale Persönlichkeitsrecht des Verstorbenen als Wahrnehmungsberechtigte geltend machen und auch insofern lediglich Unterlassungsansprüche (und äußerungsrechtlich ggf. Berichtigungsansprüche) durchsetzen.

Nach der Rechtsprechung des BVerfG ist Maßstab beim postmortalen Persönlichkeitsrecht die Unverletzlichkeit der Menschenwürde.[956] Dem Wahrnehmungsberechtigten stehen nach gefestigter Rechtsprechung des BGH – bei einer Verletzung des postmortalen Persönlichkeitsrechts – lediglich Abwehransprüche, nicht aber Schadensersatzansprüche[957] und auch kein Anspruch auf Geldentschädigung[958] zu.

Damit steht den Wahrnehmungsberechtigten, welches oft die nächsten Angehörigen sein werden (wenn der Erblasser keine konkrete andere Person hierzu bestimmt hat), aber nur ein Abwehranspruch bei Menschenwürdeverletzungen zu. Einen Anspruch auf Herausgabe von E-Mails kann man mit dem postmortalen Persönlichkeitsrecht daher nicht herleiten (auch nicht im Zusammenspiel mit Datenschutzrecht).

Die gegenteilige, in der Literatur vertretene Ansicht (zurückgehend auf *Hoeren*) überzeugt daher bereits rechtlich nicht. Aus treuhänderisch für den Verstorbenen wahrzunehmenden Abwehransprüchen bei Menschenwürdeverletzungen kann kein eigener Auskunfts- und Herausgabeanspruch der nächsten Angehörigen hergeleitet werden, den diese allein wegen der „Privatheit“ der Daten hätten.

Aber auch in tatsächlicher Hinsicht würde diese Ansicht zu unlösbaren Problemen führen, da ja ein Dritter die E-Mails nach geschäftlichen und persönlichen sortieren müsste. Bei bereits abgerufenen E-Mails müsste der Rechner zunächst einem

---

[956] BVerfG, Nichtannahmebeschl. v. 5.4.2001 – 1 BvR 932/94, NJW 2001, 2957 (2958 f.).
[957] BGH, Urt. v. 6.12.2005 – VI ZR 265/04, Rn. 11 m. w. N. (juris).
[958] BGH, Urt. v. 6.12.2005 – VI ZR 265/04, Rn. 13 (juris).

Dritten zwecks Analyse und Aufteilung der Daten zur Verfügung gestellt werden, was kaum praktikabel sein dürfte. Aber auch bei nicht abgerufenen E-Mails erscheint es fragwürdig, dem Provider dies aufzuerlegen. Auch in der Sache wird sich die Differenzierung nicht durchhalten lassen. Die Annahme einer Infektion der geschäftlichen E-Mails durch persönliche Inhalte würde das Erbrecht aushöhlen und wäre in Fällen trivialer privater Inhalte gänzlich unangemessen.

Damit steht allein die Ansicht, wonach die E-Mails, die sich auf dem Server befinden, den Erben zustehen, im Einklang mit der geltenden Rechtslage und ist auch allein praktikabel.

De lege ferenda gilt nichts anderes, sodass auch an dieser Stelle *kein Regelungsbedarf* gesehen wird. Allein der Umstand, dass sich auch private Inhalte in den E-Mails befinden, rechtfertigt keine abweichende gesetzliche Regelung. Solche privaten Inhalte (Briefe, Tagebuchaufzeichnungen, Fotos etc.) gab es auch in der „Offline-Welt“ schon immer und sie gehören unzweifelhaft zum Nachlass. Dafür, dass dies bei digitalen Inhalten anders sein sollte, ist kein hinreichender Grund ersichtlich. Zudem fallen Erben und nächste Angehörige im Fall des Eingreifens des gesetzlichen Erbrechts auch gar nicht auseinander – ebenso wenig, wenn der Erblasser die nächsten Angehörigen testamentarisch als Erben einsetzt (etwa weil er im Detail abweichende Regelungen treffen will). Bei Auseinanderfallen von nächsten Angehörigen und Erben dürfte dies nicht selten auch ein Indiz für ein schwieriges Verhältnis zu den nächsten Angehörigen sein (wenn auch nicht notwendigerweise). Ihnen dann weitgehende Ansprüche im Hinblick auf persönliche Daten des Erblassers zuzuerkennen, erscheint nicht sinnvoll.

Bei den bereits abgerufenen E-Mails ist der Telekommunikationsvorgang auch bereits abgeschlossen, sodass sich keine Probleme mit dem TKG bzw. dem Fernmeldegeheimnis stellen. Bereits vom Erblasser abgerufene, geöffnete Daten (insbesondere E-Mails) unterfallen nicht mehr dem Fernmeldegeheimnis.

(2) Nicht abgerufene E-Mails

Bei den noch nicht abgerufenen E-Mails besteht ein durch den Erbfall erworbener vertraglicher Anspruch des Erben gegen den Diensteanbieter auf Zugang zu den seitens des Diensteanbieters vereinbarungsgemäß gespeicherten Daten des Erblassers oder auf Überlassung dieser Daten. Es stellt sich aber die Frage, ob der Vererblichkeit dieses Anspruchs § 88 Abs. 3 Satz 1 TKG entgegensteht.

Entscheidend für die Beantwortung dieser Frage ist, ob die Gewährung des Zugangs zum E-Mail-Account des Erblassers bzw. die Herausgabe nicht abgerufener E-Mails an den Erben den Tatbestand des § 88 Abs. 3 S. 1 TKG erfüllen würde.

Bei näherer Betrachtung des Gesetzeswortlauts spitzt sich diese Frage auf das Tatbestandsmerkmal der Kenntnisverschaffung eines „anderen“ zu, also darauf, ob der Erbe als „anderer“ i. S. d. § 88 Abs. 3 S. 1 TKG anzusehen ist. Der Wortlaut lässt eine Verneinung des Merkmals durchaus zu. Zwar wäre es naheliegend, dass man im alltagssprachlichen Sinne Erben und Erblasser als voneinander verschie-

dene Individuen, mithin als „andere Personen“, bezeichnet. Bei einem explizit juristischen Sprachgebrauch ist es aber für den unbefangenen Leser ohne Weiteres nachvollziehbar, das Merkmal „andere“ Person in Fällen der Gesamtrechtsnachfolge, die bspw. ja auch bei juristischen Personen (z. B. bei Verschmelzungsvorgängen im Gesellschaftsrecht) eintreten können, als nicht erfüllt anzusehen. Der Wortlaut des § 88 Abs. 3 Satz 1 TKG gibt mithin kein Ergebnis zwingend vor, schließt aber auch keines aus. Auch aus den Gesetzesmaterialien lassen sich diesbezüglich keine Erkenntnisse gewinnen.[959]

Was die systematische Auslegung angeht, so sind binnensystematische Aspekte nicht ersichtlich. Auch ein spezifisch erbrechtliches Begriffsverständnis des Merkmals „sich oder anderen“ führt unter dem Gesichtspunkt der systematischen Auslegung zu keinem eindeutigen Ergebnis, da die erbrechtliche Terminologie für die Auslegung des öffentlich-rechtlichen TKG nicht ohne Weiteres maßgeblich sein dürfte.[960] Unter systematischer Auslegung könnte man die in der Literatur diskutierte Erwägung verorten, dass eine Lösung dahingehend, dass die Überlassung des E-Mail-Accounts des Erblassers an einen Erben gegen das Fernmeldegeheimnis der Beteiligten am Telekommunikationsvorgang verstieße, im Widerspruch zur anerkannten Rechtslage im PostG stünde, wonach die Post verpflichtet sei, dem Erben Erblasserbriefpost zuzustellen oder Zugang zu dessen Briefpostfach zu verschaffen.[961] Gegen diesen Gedanken wird eingewandt, die Rechtslage im Bereich der Briefpost sei insoweit anders, als § 39 Abs. 3 S. 4 PostG im Gegensatz zu § 88 TKG den Dienstleister ermächtigt, in seinen AGB Vereinbarungen zur Auslieferung von Postsendungen an *Ersatzempfänger* zu treffen. Diese Kritik mindert die Beachtlichkeit des Vergleichs des Fernmeldegeheimnisses mit dem Postgeheimnis nicht, da dem Erben die Briefpost des Erblassers gerade nicht in Vertretung des Erblassers als „Ersatzempfänger“ zugestellt wird, sondern an dessen Stelle als seinem Gesamtrechtsnachfolger.[962]

In teleologischer Hinsicht ist zu beachten, dass § 88 TKG dem Schutz des Fernmeldegeheimnisses gemäß Art. 10 GG dient und als dessen einfachgesetzliche Ausprägung fungieren soll.[963] Dabei zielte der Gesetzgeber vielmehr im Zuge der Liberalisierung des Marktes der Telekommunikation darauf ab, den bis dahin durch Art. 10 GG gewährleisteten Schutz des Fernmeldegeheimnisses zur Ver-

---

[959] Vgl. BT-Drs. 13/3609, S. 53 f.; BT-Drs. 15/2316, S. 87.
[960] Vgl. Kroiß/Horn/Solomon/*Herzog*, Nachfolgerecht, Rn. 65.
[961] *Klas/Möhrke-Sobolewski*, Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3477); *Gloser*, „Digitale Erblasser" und "digitale Vorsorgefälle" − Herausforderungen der Online-Welt in der notariellen Praxis − Teil I, MittBayNot 2016, 12 (17 f.); *Kutscher* (Diss.), S. 140.
[962] Im Ergebnis ebenso *Kutscher* (Diss.), S. 141, die § 39 Abs. 3 S. 4 PostG als „für den Erbfall nicht einschlägig“ wertet.
[963] Beck-OK/*Bock*, TKG, § 88 Rn. 1; Spindler/Schuster/*Eckhardt*, § 88 TKG Rn. 1 f.

meidung einer Absenkung des Schutzniveaus durch einfachgesetzliche Verpflichtung auf die privaten Diensteerbringer zu übertragen.[964] Dies hat zur Folge, dass § 88 TKG entsprechend Art. 10 GG auszulegen ist.[965]

Dabei ist, was den durch Art. 10 GG geschützten Personenkreis anbelangt, in Bezug auf etwaige noch nicht abgeschlossene Kommunikationsvorgänge sowohl an den Absender der elektronischen Post als auch an den Erblasser als Empfänger der noch nicht abgerufenen E-Mails zu denken.

In Bezug auf den Absender der aus dem Erblasseraccount noch nicht abgerufenen E-Mails ist ein Eingriff in Art. 10 GG zu verneinen, weil dessen „Verfügungsbefugnis“ über den Kommunikationsvorgang (Inhalt und Verkehrsdaten) mit dem Zugang im E-Mail-Postfach des Empfängers auf diesen übergeht.[966] Insoweit weist ein E-Mail-Postfach funktional und wertungsmäßig keine relevanten Unterschiede zu einem Briefpostfach auf, bei dem der Absender stets damit rechnen muss, dass der Empfänger dritten Personen den Zugang zum Postfach und zur Kenntnisnahme seiner Post gestattet.[967]

Die teilweise vertretene Gegenansicht, wonach *jeglicher* nicht durch die Einwilligung des Absenders gedeckte Zugang des Erben zum Erblasseracount einen Eingriff in Art. 10 GG darstellt[968], überzeugt nicht. Sie beruft sich auf die mit dem Telekommunikationsvorgang verbundene grundrechtstypische Gefährdungslage.[969] Diese Argumentation verkennt, dass die für E-Mails bejahte „spezifische Gefährdungslage“, die sich aus den „Rahmenbedingungen des Kommunikationsvorgangs“ ergibt, nämlich der „räumlichen Distanz“ der Kommunikationspartner und des Dazwischentretens eines technischen Übermittlungsvorgangs, „der nicht ausschließlich im Einflussbereich“ der Kommunikationspartner liegt[970], zwar in Bezug auf die Gefahr des Zugriffs durch unbefugte Dritte unmittelbar einsichtig ist, nicht aber bei von Seiten des Empfängers legitimierten Personen. Denn die Zugriffsgewährung ist in diesen Fällen alleine der durch den Empfänger beherrschten Sphäre zuzurechnen und steht in keinem Zusammenhang mit dem

---

[964] Spindler/Schuster/*Eckhardt*, § 88 TKG Rn. 2; vgl. BT-Drs. 13/3609, S. 1 f.
[965] Spindler/Schuster/*Eckhardt*, § 88 TKG Rn. 4; vgl. auch in: Maunz/Dürig/*Durner*, Art. 10 GG Rn. 117-120. Aufgrund dieser einfachgesetzlichen Ausgestaltung des § 88 TKG dürfte auch die im Rahmen der Auslegung des § 88 TKG gelegentlich thematisierte Problematik der mittelbaren Grundrechtsbindung Privater (Stichwort: „Fraport-Entscheidung des BVerfG“) keine Rolle spielen (a.A. etwa: *DAV*, Stellungnahme Nr. 34/2013, S. 71 f., der eine gesteigerte Grundrechtsbindung privater Provider an Art. 10 GG bejaht).
[966] *Gloser*, „Digitale Erblasser" und "digitale Vorsorgefälle" − Herausforderungen der Online-Welt in der notariellen Praxis − Teil I, MittBayNot 2016, 12 (18)*;* Kroiß/Horn/Solomon/*Herzog*, Nachfolgerecht, Rn. 68; *Kutscher* (Diss.), S. 142.
[967] *Gloser*, „Digitale Erblasser" und "digitale Vorsorgefälle" − Herausforderungen der Online-Welt in der notariellen Praxis − Teil I, MittBayNot 2016, 12 (18); Kroiß/Horn/Solomon/*Herzog*, Nachfolgerecht, Rn. 68; *Kutscher* (Diss.), S. 142.
[968] *DAV*, Stellungnahme Nr. 34/2013, S. 72 ff.
[969] *DAV*, Stellungnahme Nr. 34/2013, S. 72 f.
[970] *DAV*, Stellungnahme Nr. 34/2013, S. 72.

Übermittlungsvorgang. Gleiches gilt in Bezug auf Zugriffsrechte von Gesamtrechtsnachfolgern, die ebenfalls in keinem spezifischen Zusammenhang mit dem Übermittlungsvorgang stehen, sondern alleine der Sphäre des Empfängers zuzuordnen sind. Überdies bietet sich auch hier ein Vergleich mit der Briefpost an: Auch das Ablegen der Briefpost in einem Postfach oder einem Briefkasten des Empfängers begründet die seitens des Absenders nicht mehr beeinflussbare „Gefahr" des Zugriffs durch andere Personen als dem Empfänger selbst. Diese Gefahr besteht auch bei im Machtbereich des Empfängers verwahrter Briefpost fort. Es liegt auf der Hand, dass der Absender insoweit den Zugriff dritter, vom Empfänger hierzu legitimierter Personen nicht unter Berufung auf Art. 10 GG von seiner Zustimmung abhängig machen kann.[971] Es ist nicht einzusehen, warum für elektronische Nachrichten etwas anderes gelten sollte.[972]

Aber auch in Bezug auf die Empfängerseite geht mit der Zugriffsgewährung an den Erben kein Eingriff in Art. 10 GG einher. Dies ergibt sich schon daraus, dass als Grundrechtsträger des Art. 10 GG auf Empfängerseite, wenn man vom Erben absieht, nur der Erblasser in Betracht kommt. Träger des Grundrechts aus Art. 10 GG kann aber nur der „tatsächliche Kommunikationsteilnehmer"[973] sein. Ist die E-Mail noch nicht abgerufen, so kommt der Erblasser als Kommunikationsteilnehmer nicht mehr in Betracht. Er scheidet mangels Grundrechtsfähigkeit, die bei natürlichen Personen grundsätzlich mit dem Tod endet[974], als Betroffener eines Grundrechtseingriffs aus. Für einen nachwirkenden, postmortalen Grundrechtsschutz, wie er jedenfalls in Bezug auf Art. 1 Abs. 1 GG anerkannt ist, der aber bei bereichsspezifischen Grundrechten regelmäßig Handlungsfähigkeit erfordert[975], ist in Bezug auf Art. 10 GG mangels tatsächlicher Beteiligung des Erblassers an einem Kommunikationsvorgang tatbestandlich kein Raum. Dies ergibt sich auch aus dem Sinn und Zweck des Art. 10 GG. Die den Kommunikationsvorgang betreffende Gefährdungslage (Aufhebung der Vertraulichkeit des Kommunikationsvorgangs durch Kenntnisnahme durch den Staat oder sonstige Dritte) ist erkennbar nicht mehr gegeben, wenn ein Kommunikationspartner vor Abschluss des Kommunikationsvorgangs verstirbt und ein legitimierter Gesamtrechtsnachfolger in die Funktion des Adressaten einrückt. Oder um es anders auszudrücken: Art. 10 GG schützt den Erblasser vor der Kenntnisnahme des Kommunikationsvorgangs durch den Staat oder unbefugte dritte Personen, nicht aber gegenüber seinen Erben.[976] Ist aber Art. 10 GG bei Zugriffsgewährung des Erben auf das

---

[971] *Kutscher* (Diss.), S. 143.
[972] *Kutscher* (Diss.), S. 143.
[973] Maunz/Dürig/*Durner*, Art. 10 Rn. 100.
[974] *Tonikidis*, Die Grundrechtsfähigkeit und Grundrechtsberechtigung natürlicher Personen, JA 2013, 38 (39).
[975] *Tonikidis*, Die Grundrechtsfähigkeit und Grundrechtsberechtigung natürlicher Personen, JA 2013, 38 (40).
[976] Vgl. *Gloser*, „Digitale Erblasser" und "digitale Vorsorgefälle" − Herausforderungen der Online-Welt in der notariellen Praxis − Teil I, MittBayNot 2016, 12 (18). So im Ergebnis auch für

E-Mailkonto tatbestandlich nicht verwirklicht, so mögen andere Grundrechte zum Zuge kommen, die der bei tatbestandlichem Eingreifen ansonsten speziellere Art. 10 GG verdrängt. Hierbei ist insbesondere an das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1, Art. 1 Abs. 1 GG) zu denken.[977] Dies kann dahinstehen, da § 88 TKG dem Schutz des Art. 10 GG zu dienen bestimmt ist, sodass die Regelung diesbezüglicher Grundrechtsbetroffenheit gesetzessystematisch andernorts zu verorten wäre.[978]

Nach alledem sprechen Systematik und Sinn und Zweck des § 88 Abs. 3 S. 1 TKG dafür, das Merkmal „sich oder anderen" in Bezug auf den Erben des Inhabers eines E-Mail-Accounts zu verneinen.

Es bleibt mithin die Frage, ob anwendungsvorrangiges EU-Recht, insbesondere die ab dem 25. Mai 2018 geltende EU-DSGVO[979], eine anderweitige Auslegung des § 88 Abs. 3 S. 1 TKG gebieten oder der Anwendung der Vorschrift entgegenstehen wird.

Es ist fraglich, ob die EU-DGSVO überhaupt auf die prüfungsgegenständliche Thematik anwendbar ist. Hiergegen sprechen Art. 1 Abs. 1, 2 EU-DSGVO, wonach die Verordnung nur dem Schutz „natürlicher Personen" dient und als solche nur lebende Menschen anzusehen sind.[980] Für diese Auslegung spricht auch Erwägungsgrund 27 EU-DGSVO, wonach die Verordnung nicht für personenbezogene Daten Verstorbener gilt und die Mitgliedstaaten eigene Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen können. Die noch nicht abgerufenen Nachrichten des Erblassers stellen personenbezogene Daten Verstorbener da, sodass die Zugangsgewährung zu einem Erblasser-Account zu Gunsten des Erben nicht in den Anwendungsbereich der EU-DSGVO fällt.

Formal hiervon unberührt bleibt, ob sich dies auf etwaige Rechtspositionen des Kommunikationspartners des Erblassers auswirkt. Geht man mit der diesseits zur

---

§ 88 TKG *Lange/Holtwiesche*, Digitaler Nachlass − eine Herausforderung für Wissenschaft und Praxis (Teil 2), ZErb 2016, 157 (159).

[977] Maunz/Dürig/*Durner*, Art. 10 Rn. 209.

[978] So auch *Lange/Holtwiesche*, Digitaler Nachlass - eine Herausforderung für Wissenschaft und Praxis (Teil 2), ZErb 2016, 157 (159 ff.), die § 88 Abs. 3 S. 1 TKG nach Systematik und Zweck nicht auf den Schutz personenbezogener Daten nach dem Tod eines Kommunikationspartners abzielen. Insoweit halten sie, im Einklang mit der hier vertretenen Auffassung, allenfalls postmortalen Schutz durch das allgemeine Persönlichkeitsrecht für einschlägig und verorten diese Rechtsfragen im Erbrecht.

[979] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L. 119 vom 4.5.2016, S. 1.

[980] *Weichert*, Postmortaler Datenschutz – Auskunftsansprüche von Erben und Angehörigen zu personenbezogenen Internetdaten eines Verstorbenen, S. 16, abrufbar unter http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_08_postmortds.pdf (letzter Abruf: 4.4.2017); *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, S. 21.

Auslegung des Art. 10 GG vertretenen Auffassung davon aus, dass der Kommunikationsvorgang zwar bis zum Abruf der Nachricht noch nicht abgeschlossen ist[981], der Absender aber mit dem Eintreffen der Nachricht in der Empfängersphäre seine „Verfügungsbefugnis" über den Kommunikationsvorgang (Inhalt und Verkehrsdaten) gegenüber der Empfängerseite verloren hat, so spricht Vieles dafür, von einem *umfassenden* Anwendungsausschluss der EU-DSGVO auf die Frage der Zugriffsrechte der Erben auf gespeicherte Kommunikationsdaten des Verstorbenen auszugehen.[982] Denn der Verlust der Verfügungsbefugnis über den Kommunikationsvorgang gegenüber der Empfängerseite umfasst auch Zugriffsrechte von Seiten des Empfängers beauftragter Dritter sowie von Erben. Überdies wird dieses Ergebnis dem Umstand gerecht, dass die Verordnung ersichtlich die Gesamtrechtsnachfolge von Todes wegen nicht regeln sollte, was unterlaufen würde, wenn die Daten Verstorbener unter dem Gesichtspunkt etwaiger Rechte des Absenders doch dem Anwendungsbereich der EU-DSGVO zugeordnet werden.[983]

Geht man vorsorglich gleichwohl von der Möglichkeit des Eingreifens der EU-DSGVO aus, so kommt ein umfassender Anwendungsausschluss der EU-DSGVO gemäß Art. 95 EU-DSGVO wegen Anwendungsvorrangs der spezielleren Richtlinie 2002/58/EG des Europäischen Parlaments und des Rats vom 12. Juli 2002 („Datenschutzrichtlinie für die elektronische Kommunikation")[984] in Betracht. Art. 95 EU-DSGVO bestimmt hierzu, dass die EU-DSGVO natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen der Union keine „zusätzlichen Pflichten" auferlegt, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

Der Wortlaut dieser Bestimmung deutet noch nicht zwingend auf einen Anwendungsvorrang der Richtlinie 2002/58/EG gegenüber der EU-DSGVO hin, sondern könnte auch so verstanden werden, dass aus der EU-DSGVO keine Verschärfung der in der Richtlinie normierten Pflichten abgeleitet werden darf.[985] Allerdings ist der Wortlaut des Art. 95 EU-DSGVO im Lichte des Erwägungsgrundes 173 EU-DSGVO auszulegen, der einen Anwendungsvorrang der Richtlinie

---

[981] *Weichert*, Postmortaler Datenschutz – Auskunftsansprüche von Erben und Angehörigen zu personenbezogenen Internetdaten eines Verstorbenen, S. 7, abrufbar unter http://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_08_postmortds.pdf (letzter Abruf: 4.4.2017).

[982] Im Ergebnis ähnlich *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, S. 21.

[983] Im Ergebnis ähnlich *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, S. 21.

[984] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation („Datenschutzrichtlinie für die elektronische Kommunikation"), ABl. L. 201 vom 31.7.2002, S. 37.

[985] *DAV*, Stellungnahme Nr. 8/2013, S. 11.

2002/58/EG vor der EU-DSGVO statuieren will[986]. Dabei gilt es indes für die Zukunft zu beachten, dass in Erwägungsgrund 173 eine Änderung der Richtlinie 2002/58/EG mit dem Ziel angekündigt ist, das Verhältnis der EU-DSGVO und der Richtlinie klarzustellen und um die Kohärenz mit der Verordnung zu gewährleisten. Da eine Überarbeitung der Richtlinie 2002/58/EG zu erwarten ist[987], sollte deren Neufassung zu gegebener Zeit daraufhin überprüft werden, ob sich aus ihr Anlass für eine anderweitige Bewertung ergibt.

Auch wenn § 88 Abs. 3 Satz 1 TKG nach alledem einer Zugriffsgewährung des Erben durch den Diensteanbieter auf den Erblasseraccount bzw. einer Überlassung der Daten des Erblasseraccounts an den Erben nicht entgegensteht, erschwert der Umstand, dass der Wortlaut des § 88 Abs. 3 TKG nicht unmittelbar auf § 1922 BGB Bezug nimmt – mithin für den Rechtsanwender nicht ohne Weiteres ersichtlich ist, ob und inwieweit Erbrecht und Telekommunikationsrecht aufeinander abgestimmt sind – die Rechtsanwendung. Von daher besteht zwar mit Blick auf das Ergebnis der vorstehenden Prüfung kein zwingender gesetzgeberischer Handlungsbedarf, wohl aber ist anzunehmen, dass eine klarstellende Regelung die Rechtsanwendung erheblich erleichtern würde.[988]

Eine derartige Regelung wäre auch, wie die vorstehende Prüfung im Zusammenhang mit der Auslegung des § 88 Abs. 3 TKG ergeben hat, mit Art. 10 GG[989], Art. 7 GRC, Art. 8 EMRK, der EU-DSGVO sowie mit der Richtlinie 2002/58/EG vereinbar. Da allerdings eine Überarbeitung der vorgenannten Richtlinie zum Zwecke ihrer Abgrenzung zur EU-DSGVO bevorsteht, müssten etwaige Änderungen der Richtlinie mit einem Gesetzesvorhaben erneut abgeglichen werden.

---

[986] *DAV*, Stellungnahme Nr. 8/2013, S. 11.

[987] Vgl. Erwägungsgrund 173 der EU-DSGVO: „Um das Verhältnis zwischen der vorliegenden Verordnung und der Richtlinie 2002/58/EG klarzustellen, sollte die Richtlinie entsprechend geändert werden. Sobald diese Verordnung angenommen ist, sollte die Richtlinie 2002/58/EG einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit dieser Verordnung zu gewährleisten."

[988] *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (264); *Deusch*, Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2 (5), der indes eine Änderung für geboten erachtet.

[989] Auch soweit, anders als hier, die Schutzbereichseröffnung des Art. 10 GG bei Zugangsgewährung des Erben zum Erblasseraccount bejaht wird, geht die h. M. von einer Grundrechtskollision mit Art. 14 GG aus und bejaht im Ergebnis überzeugend, dass Art. 14 GG sich vor Art. 10 GG im Wege der praktischen Konkordanz durchsetzen muss, da der Erbe zur Nachlasssicherung auf die Sichtung der Erblasserkorrespondenz angewiesen ist: Kroiß/Horn/Solomon/*Herzog*, Nachfolgerecht, Rn. 64; *DAV*, Stellungnahme Nr. 34/2013, S. 78 ff.; *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (292); *Klas/Möhrke-Sobolewski*, Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3478).

c. Anspruch auf Herausgabe der Daten bei Beendigung der Vertragsbeziehung

Aus dem vorstehend unter a. Gesagten ergibt sich, dass ein derartiger Anspruch auch derzeit jedenfalls zivilrechtlich besteht und zwar als vertragliche Hauptpflicht aus dem Providervertrag, der im Wege der Universalsukzession auf den Erben übergeht. Allein ein Konflikt mit § 88 TKG könnte bestehen, der eine gesetzliche Regelung sinnvoll erscheinen lässt (siehe oben). Dieser Anspruch ist von zentraler Bedeutung für den Erben.

Insofern kommt dem E-Mail-Konto eine Schlüsselfunktion zu, da sich rein faktisch über den Zugriff zum E-Mail-Konto zahlreiche Passwörter anderer Dienste zurücksetzen lassen und so ein Zugriff auch auf andere Accounts des Erblassers faktisch möglich wird.[990]

Ob das E-Mail-Konto oder Accounts in sozialen Netzwerken vom Erben fortgesetzt werden können, ist für den Erben eine weit weniger entscheidende Frage, als die, ob er zunächst schnell Zugriff auf die aufgelaufenen Kommunikationen bekommen kann. Das Interesse, Accounts des Erblassers fortzuführen (E-Mails, soziale Netzwerke), dürfte sich jedenfalls bei privat genutzten E-Mail-Accounts in engen Grenzen halten. Der Anspruch auf schnellen Zugriff auf die noch nicht abgerufenen Daten hingegen ist (gerade für die Ermittlung der Werthaltigkeit des Nachlasses) von großem Interesse für den Erben.

Für den Erben ist es von fundamentaler Bedeutung, sich möglichst schnell einen umfassenden Überblick über die vertraglichen Beziehungen des Erblassers zu verschaffen. Da heute in der Realität viele Verträge online verhandelt und geschlossen werden und viele Rechnungen auch lediglich per E-Mail versandt werden, ist ohne Zugriff auf den aktuellen Stand des E-Mail-Postfachs heute kaum noch gewährleistet, dass sich der Erbe über Forderungen und Verbindlichkeiten (einschließlich laufender Dauerschuldverhältnisse) abschließende Klarheit verschaffen kann.

So können sich auch in den noch nicht abgerufenen E-Mails des Erblassers (auf dem Server des Providers) noch an den Erblasser gerichtete Rechnungen befinden bzw. auch E-Mails, aus denen sich offene Forderungen des Erblassers (bzw. die Höhe, in der diese aktuell offen sind) ergeben. In diesem Zusammenhang sind etwa auch Accounts bei Paypal und ähnlichen Anbietern für Internetbezahlsysteme besonders relevant.

Derartige Informationen sind für den Erben aber von fundamentaler Bedeutung, da er innerhalb der Ausschlagungsfrist von sechs Wochen ab Kenntniserlangung vom Anfall und dem Grunde der Berufung (§ 1944 Abs. 1, 2 BGB) beurteilen muss, ob er die Erbschaft ausschlagen möchte (insbesondere wegen Überschuldung des Nachlasses).

---

[990] So auch *Pruns*, Keine Angst vor dem digitalen Nachlass! Erbrechtliche Grundlagen – Alte Probleme in einem neuen Gewand?, NWB 2013, 3161 (3162).

Aufgrund der besonderen Bedeutung des Auskunftsanspruchs erscheint es möglicherweise erwägenswert, ob insoweit eine gesetzgeberische Klarstellung erfolgen sollte, damit für alle Beteiligten Rechtssicherheit dahingehend besteht, dass der Provider verpflichtet ist, dem Erben den Zugang zu den E-Mails zu verschaffen (wozu er allerdings nach überwiegender und zutreffender Ansicht ohnehin auch nach derzeit geltender Rechtslage aus übergegangener Verpflichtung aus dem Providervertrag verpflichtet ist).

Hinsichtlich Auskunftsansprüchen bzw. Ansprüchen auf Übermittlung der Daten gegen den Provider stellt sich ein weiteres Problem, wenn nicht eine Person Erbe ist, sondern mehrere (etwa durch testamentarische Einsetzung mehrerer Erben oder im Fall mehrerer gesetzlicher Erben bei gesetzlicher Erbfolge). Insoweit besteht eine ungeteilte Erbengemeinschaft (§ 2032 BGB), deren Mitglieder bei der Geltendmachung nachlasszugehöriger Ansprüche grundsätzlich nur Leistung an alle verlangen können (§ 2039 S. 1 BGB) und gegenüber der die Ansprüche nur einheitlich erfüllt werden können (§ 2039 S. 1 BGB). Dies erschwert die praktische Durchführbarkeit von Auskunftsansprüchen. Da dies aber in gleicher Weise für alle Auskunftsansprüche auch im nicht-digitalen Bereich gilt, dürfte insoweit kein spezieller Regelungsbedarf für den digitalen Nachlass bestehen.

d. AGB-Regelungen bezüglich des Accounts im Todesfall

Die Rechtsprechung hat sich mit dieser konkreten Problematik, soweit ersichtlich, noch nicht beschäftigt; es gibt lediglich Rechtsprechung zur Frage der AGB-rechtlichen Zulässigkeit von einseitigen Kündigungsrechten im Online-Bereich, ohne dass dies aber Bezug zum Erbfall hätte, sowie zu Ansprüchen von Erben bei Giroverträgen. Ausgangspunkt sind daher die gesetzlichen Regelungen und die bereits geschilderten (insoweit auch eher raren) Stimmen aus der Literatur.

(1) Prüfungsmaßstab

Die hier näher beleuchteten Klauseln verstoßen weder gegen ein gesetzliches Verbot noch gegen die guten Sitten. Eine Nichtigkeit nach § 134 BGB bzw. § 138 Abs. 1 BGB scheidet daher aus. Sie wird – soweit ersichtlich – auch in der Literatur nirgends vertreten. Die Wirksamkeit der in allgemeinen Geschäftsbedingungen enthaltenen Kündigungs-, Legitimations- und Abwicklungsklauseln ist daher an §§ 307 ff. BGB zu messen.[991] Dabei ist – wie bereits oben dargestellt – zugrunde zu legen, dass ein Account (E-Mail, aber auch Facebook etc.) vererblich ist. Mithin wirken sich die in den AGB enthaltenen Regelungen nicht nur auf die Position des Erblassers aus. Sie berühren vielmehr grundsätzlich auch den Rechts- und Pflichtenkreis des in die Verträge eintretenden Erben. Der Anwendungsbereich der §§ 307 ff. BGB ist daher eröffnet.

---

[991] Für die weitere Prüfung wird unterstellt, dass AGB vorliegen, die vom Provider als Verwender einseitig gestellt und wirksam in den Vertrag einbezogen wurden.

Zu prüfen ist, ob der Ausschlusstatbestand des § 307 Abs. 3 BGB erfüllt ist. Nach § 307 Abs. 3 BGB unterliegen unter anderem nur solche AGB der offenen Inhaltskontrolle gem. §§ 307 ff. BGB, durch die eine Regelung getroffen wird, welche von Rechtsvorschriften entweder abweicht oder sie ergänzt.[992] Klauseln, die lediglich die einschlägige gesetzliche Regelung wiedergeben („deklaratorische" Klauseln), sind hingegen kontrollfest.[993]

Es ist daher zu ermitteln, ob die Rechtsordnung eine dem Regelungsgehalt der zu überprüfenden Klausel entsprechende (inhaltsgleiche) Regelung bereithält.[994] Zu diesem Zwecke ist festzustellen, welche Normen auf Providerverträge Anwendung finden. Deren rechtliche Einordnung ist im Einzelnen umstritten.[995] Angesichts der Vielgestaltigkeit der Regelungen dürfte sich eine allgemeine rechtliche Zuordnung von vorneherein verbieten. Festzuhalten ist jedoch, dass Providerverträge als solche gesetzlich nicht geregelt sind und in der Regel Elemente verschiedener Vertragstypen enthalten. Klauseln, die die gesetzlich nicht geregelten Vertragstypen ausgestalten, sind nicht von vorneherein von der Inhaltskontrolle ausgeschlossen.[996] Für die vorliegende Untersuchung kann daher grundsätzlich davon ausgegangen werden, dass Kündigungs-, Legitimations- und Abwicklungsklauseln für den Todesfall der Inhaltskontrolle unterfallen.

Da Klauselverbote gem. §§ 308, 309 BGB nicht einschlägig sind, kann de lege lata nur auf die Generalklausel des § 307 Abs. 1, 2 BGB abgestellt werden.

Gemäß § 307 Abs. 1 BGB sind Bestimmungen in AGB unwirksam, wenn sie den Vertragspartner des Verwenders entgegen den Geboten von Treu und Glauben unangemessen benachteiligen. Eine unangemessene Benachteiligung kann sich auch daraus ergeben, dass die Bestimmung nicht klar und verständlich ist. Gemäß § 307 Abs. 2 BGB – der vorrangig zu prüfen ist[997] - ist eine unangemessene Benachteiligung im Zweifel anzunehmen, wenn eine Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist oder wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrags ergeben, so einschränkt, dass die Erreichung des Vertragszwecks gefährdet ist. § 307 Abs. 2 BGB enthält Regelbeispiele, deren Erfüllung das Vorliegen einer unangemessenen Benachteiligung des Vertragspartners widerleglich vermuten lässt. Beide Regelbeispiele sind ihrerseits wieder von generalklauselartiger

---

[992] MüKo/*Wurmnest,* BGB, § 307 Rn. 1.
[993] BeckOK/*H. Schmidt*, BGB, § 307 Rn. 70.
[994] MüKo/*Wurmnest*, BGB, § 307 Rn. 6.
[995] Vgl. für Accessproviderverträge BGH, Urt. v. 23.3.2005 − III ZR 338/04, NJW 2005, 2076 (Dienstvertrag). Vgl. MüKo/*Busche*, BGB, § 631 Rn. 279 (Providervertrag mit einem Access-/Netz-Provider, der auf die Eröffnung einer Kommunikation mittels eines Hosts/Servers gerichtet ist: Vertrag sui generis; bei Verträgen über E-Mail-Dienste, die allerdings häufig Teil eines Access-/Netz-Providervertrags seien: Vertragsinhalt entscheidend).
[996] Vgl. MüKo/*Wurmnest*, BGB, § 307 Rn. 7.
[997] Vgl. Palandt/*Grüneberg*, BGB, § 307 Rn. 2.

Weite. Anwendungsbereich und -grundlagen decken sich mit denjenigen des Abs. 1 der Vorschrift.[998]

Auszugehen ist von den Vorschriften des dispositiven Rechts, die ohne die Klausel gelten würden. Die Anwendung von § 307 BGB setzt voraus, dass die Abweichung vom dispositiven Recht Nachteile von einigem Gewicht begründet. Unangemessen ist die Benachteiligung, wenn der Verwender durch einseitige Vertragsgestaltung missbräuchlich eigene Interessen auf Kosten seines Vertragspartners durchzusetzen versucht, ohne von vorneherein auch dessen Belange hinreichend zu berücksichtigen und ihm einen angemessenen Ausgleich zuzugestehen. Zur Beurteilung bedarf es einer umfassenden Würdigung, in die die Art des konkreten Vertrages, die typischen Interessen beider Parteien, die Anschauungen der beteiligten Verkehrskreise und die sich aus der Gesamtheit der Rechtsordnung ergebenden Bewertungskriterien einzubeziehen sind. Auszugehen ist von Gegenstand, Zweck und Eigenart des Vertrages. Zu berücksichtigen sind auch Rationalisierungsinteressen des Verwenders und sein Interesse an einer Vereinfachung der Arbeitsabläufe, wenn diese auch gegenüber höherrangigen Interessen des Kunden zurücktreten müssen.[999]

Durch die Anfügung des § 307 Abs. 1 S. 2 BGB ist nunmehr in den Gesetzestext aufgenommen, dass eine unangemessene Benachteiligung auch dadurch begründet werden kann, dass die beiderseitigen Rechte und Pflichten nicht klar und hinreichend deutlich umschrieben sind (Transparenzgebot). Das Transparenzgebot verpflichtet den Verwender, die Rechte und Pflichten des Vertragspartners so klar wie möglich (und nötig) zu formulieren und durchschaubar darzustellen. Ziel ist es, die Regelungen für den durchschnittlichen Vertragspartner verständlich zu gestalten und darüber hinaus die wirtschaftlichen Nachteile und Belastungen des Vertragspartners, die sich aus der Klausel (auch im Zusammenwirken mit anderen Regelungen) ergeben, so deutlich werden zu lassen, wie es nach den Umständen gefordert werden kann. Die Umschreibung muss dabei so klar sein, dass keine ungerechtfertigten Auslegungsspielräume, die der Verwender für sich nutzen könnte, verbleiben. Als Einzelausprägungen des Transparenzgebots, die sich teils überschneiden, sind zu nennen: Das Gebot, die Rechte und Pflichten des Vertragspartners klar und durchschaubar sowie verständlich zu umschreiben. Dazu gehört nicht nur, dass die einzelne Regelung für sich genommen klar formuliert ist und dass zusammengehörende Regelungen auch im Zusammenhang erscheinen und nicht über den gesamten Inhalt der AGB verstreut, ja in anderen Teilregelungen „versteckt“ werden. Wenn sich die Rechtsposition der Vertragspartner aus verschiedenen Einzelregelungen erst in der Zusammenschau ergibt, muss auch dies (ggf. durch Verweise in konkrete Klauseln) deutlich werden.[1000] An diesen Maßstäben sind die vorkommenden AGB der Anbieter zu messen.

---

[998] BeckOK/*H. Schmidt*, BGB, § 307 Rn. 50.
[999] Vgl. Palandt/*Grüneberg*, BGB, § 307 Rn. 12.
[1000] BeckOK/*H. Schmidt*, BGB, § 307 Rn. 43 m. w. N.

(2) (Einseitige) Kündigungsrechte für den Todesfall

Die Wirksamkeit von Kündigungsklauseln für den Fall des Todes eines Kunden ist in der Literatur diskutiert worden. Diesbezüglich wird zur Vermeidung von Wiederholungen auf die obigen Ausführungen Bezug genommen.

Soweit das Vorliegen unentgeltlicher Verträge bzw. die Anwendbarkeit der §§ 564 S. 2, 580 BGB verneint werden, sieht das dispositive Recht lediglich in § 314 BGB ein außerordentliches Kündigungsrecht vor. Danach kann bei Dauerschuldverhältnissen jeder Vertragsteil aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist kündigen. Ein wichtiger Grund liegt vor, wenn dem kündigenden Teil unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der beiderseitigen Interessen die Fortsetzung des Vertragsverhältnisses bis zur vereinbarten Beendigung oder bis zum Ablauf einer Kündigungsfrist nicht zugemutet werden kann. Bei der notwendigen umfassenden Würdigung sind die Besonderheiten des jeweiligen Vertragstyps zu berücksichtigen.[1001] Internetprovider bieten ihre Leistungen regelmäßig einer unbestimmten Vielzahl von Personen an. Die Leistungen sind ihrer Art nach nicht auf den speziellen Bedarf bestimmter Kunden zugeschnitten. Das Interesse des Anbieters an der Zurverfügungstellung seiner Leistung ist daher nicht an bestimmte Personen geknüpft. Ein Kündigungsrecht nach § 314 BGB besteht daher – jedenfalls im Regelfall – nicht.

Zu prüfen ist weiter, ob die festgestellte Abweichung von den Regeln des dispositiven Rechts zu einer unangemessenen Benachteiligung ihres Adressaten führt. Der in den Vertrag eintretende Erbe hat zunächst ein Interesse daran, die angefallenen Daten, insbesondere E-Mails oder sonst für den Verstorbenen bestimmte Mitteilungen, zu erhalten. Dieses Interesse wird jedoch durch die Frage der Zulässigkeit von Kündigungsklauseln in den AGB der Provider nicht unmittelbar berührt. Die Herausgabe von Daten betrifft vielmehr lediglich die Abwicklung eines wirksam beendeten Vertrages.

Ein – die Wirksamkeit von Kündigungsklauseln allein betreffendes – Interesse des Erben, den Account unverändert weiterzuführen, kann regelmäßig nur aus rein tatsächlichen Gründen – nämlich im Hinblick auf eine vereinfachte Abwicklung des Nachlasses – folgen.

Dem steht ein Interesse des Providers gegenüber, den Account des Erblassers nach dessen Tod nicht als solchen weiterführen zu müssen. Könnte der Account dauerhaft unverändert fortgeführt werden, so wäre dem Missbrauch Tür und Tor geöffnet, zumindest aber lägen Verwirrungen im Rechtsverkehr nahe. Denn der Internetaccount oder die sonstige Internetpräsenz einer Person wird von weiten Teilen des Rechtsverkehrs erfahrungsgemäß mit deren digitaler Identität gleichgesetzt, ein Erbe könnte quasi „als der Verstorbene“ auftreten, dritte Personen könnten daher fälschlich davon ausgehen, weiterhin mit dem Verstorbenen selbst

---

[1001] Palandt/*Grüneberg*, BGB, § 314 Rn. 7.

zu kommunizieren. Ein Interesse jedes Providers, die Kennung eines Nutzers stillzulegen, von dem er weiß, dass er verstorben ist, erscheint daher nachvollziehbar.

Dem Interesse des Erben an einer Abwicklung des Erbes kann demgegenüber nicht nur durch eine unveränderte Fortführung des Accounts entsprochen werden. Vielmehr ist es dem Erben – privat wie im geschäftlichen Verkehr – zuzumuten, sich als solcher zu offenbaren und deutlich zu machen, als Rechtsnachfolger des Verstorbenen zu agieren. Dies entspricht auch dem Interesse der außerhalb der Vertragsbeziehung zwischen Provider und Erben stehenden dritten Personen und den Anschauungen der beteiligten Verkehrskreise. Es ist daher nicht davon auszugehen, dass Kündigungsklauseln im Hinblick auf eine mögliche Beeinträchtigung der Testierfreiheit den Verstorbenen selbst oder aber den in den Vertrag eintretenden Erben unangemessen benachteiligen.

Der Annahme einer Wirksamkeit ein- oder beiderseitiger Kündigungsrechte des Internetproviders steht auch das Urteil des Oberlandesgerichts Koblenz vom 30. September 2010[1002] nicht entgegen, da dieses Urteil eine andere Fallgestaltung betrifft. Das Oberlandesgericht Koblenz hat einen Verstoß gegen § 307 Abs. 1 BGB angenommen, allerdings nicht in einem Fall mit Bezug zum Erbrecht, sondern lediglich in Fällen mit einseitigen Kündigungsklauseln bei Webhostingverträgen/Internetproviderverträgen mit Mindestvertragslaufzeiten. Die jederzeitige Kündigungsmöglichkeit des Providers ist aber mit einem Erlöschen im Todeszeitpunkt nicht vergleichbar, sodass diese Rechtsprechung nicht einfach übertragen werden kann. Im Ergebnis sind ein- oder beidseitige Kündigungsrechte in AGB der Provider de lege lata wirksam.

Die Wirksamkeit ein- oder beidseitiger Kündigungsrechte in AGB der Provider entspricht den beiderseitigen Interessen der Vertragsparteien. Einer Gesetzesänderung bedarf es bei entsprechender Ausgestaltung der Abwicklung des Rechtsverhältnisses bei Vertragsbeendigung nicht.

(3) Legitimationsklauseln

Die Wirksamkeit verschiedener Legitimationsklauseln zum Nachweis der Erbenstellung ist in der Literatur diskutiert worden. Diesbezüglich wird auf die obigen Ausführungen verwiesen. Zusammenfassend ist festzuhalten, dass Parallelen zu den Regelungen im Bankrecht gezogen werden und entsprechende Rechtsprechung des BGH für anwendbar gehalten wird.

Nach deutschem Recht ist der Erbe nicht verpflichtet, sein Erbrecht durch einen Erbschein nachzuweisen; er hat auch die Möglichkeit, den Nachweis seines Erbrechts in anderer Form zu erbringen.[1003] Danach dürften Regelungen in AGB, welche an den Nachweis der Erbenstellung keine besonderen bzw. Anforderungen unterhalb der Vorlage eines Erbscheins stellen, zulässig bzw. gem. § 307 Abs. 3 BGB einer Inhaltskontrolle bereits entzogen sein.

[1002] OLG Koblenz, Urt. v. 30.10.2010 − 2 U 1388/09, Rn 54 f. (juris).
[1003] BGH, Urt. v. 17.6.2004 − I ZR 136/01, NJW 2005, 599 ff. (600) m. w. N.

Zu prüfen ist weiter, ob zum Nachweis der Erbenstellung die Pflicht zur Vorlage eines Erbscheins bzw. sogar darüber hinausgehender Unterlagen in AGB wirksam begründet werden kann. Weitergehende Nachweise als den Erbschein sieht das deutsche Recht nicht vor. Für die Aufstellung weitergehender Anforderungen besteht – auch aus Sicht der Provider – kein Bedürfnis, da die Erbenstellung jedenfalls durch Vorlage eines Erbscheins ausreichend nachgewiesen werden kann.[1004] Die verpflichtende Vorlage weiterer Unterlagen ist demgegenüber regelmäßig geeignet, dem Erben einen erheblichen Mehraufwand zu verursachen. Ein entsprechendes Erfordernis widerspricht dem Interesse des Erben an einer möglichst raschen und kostengünstigen Abwicklung des Nachlasses[1005] und benachteiligt diesen unangemessen. Mit der ganz herrschenden Ansicht in der Literatur ist daher davon auszugehen, dass Klauseln in AGB, welche über die Vorlage des Erbscheins hinausgehende Anforderungen aufstellen, nach § 307 BGB unwirksam sind.

Zu prüfen bleibt, ob die Vorlage eines Erbscheins in den AGB der Internetdiensteanbieter gefordert werden kann. Einschlägige Rechtsprechung zu dieser Frage gibt es – soweit ersichtlich – bislang nicht. Den hierzu veröffentlichten Stimmen in der Literatur ist jedoch darin beizupflichten, dass sich ein Vergleich mit der Rechtslage im Bankrecht anbietet, da sich die Interessenlagen der Beteiligten weitestgehend entsprechen. Soweit hieraus jedoch abgeleitet wird, AGB, welche die Vorlage eines Erbscheins verlangten, seien grundsätzlich wirksam, ist dies so nicht zutreffend.

Vielmehr hat der BGH geurteilt, folgende dem Muster von Nr. 5 I AGB-Sparkassen nachgebildete Klausel einer Sparkasse sei im Verkehr mit Verbrauchern nach § 307 Abs. 1, Abs. 2 Nr. 1 BGB unwirksam:[1006]

> *„Nach dem Tode des Kunden kann die Sparkasse zur Klärung der rechtsgeschäftlichen Berechtigung die Vorlegung eines Erbscheins, eines Testamentsvollstreckerzeugnisses oder ähnlicher gerichtlicher Zeugnisse verlangen; fremdsprachige Urkunden sind auf Verlangen der Sparkasse mit deutscher Übersetzung vorzulegen. Die Sparkasse kann auf die Vorlegung eines Erbscheins oder eines Testamentsvollstreckerzeugnisses verzichten, wenn ihr eine Ausfertigung oder eine beglaubigte Abschrift vom Testament oder Erbvertrag des Kunden sowie der Niederschrift über die zugehörige Eröffnungsverhandlung vorgelegt wird.“*

Sinngemäß führt der BGH hierzu aus, das uneingeschränkte Recht, zur Klärung der rechtsgeschäftlichen Berechtigung die Vorlegung eines Erbscheins zu verlangen bzw. in bestimmten Situationen darauf zu verzichten, sei mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen werde, nicht zu

---

[1004] Siehe hierzu nur die Regelungen der §§ 2365-2367 BGB.
[1005] Vgl. hierzu BGH, Urt. v. 8.10.2013 – XI ZR 401/12, NJW 2013, 3716 (3718).
[1006] Vgl. hierzu BGH, Urt. v. 8.10.2013 – XI ZR 401/12, NJW 2013, 3716.

vereinbaren (§ 307 Abs. 2 Nr. 1 BGB) und benachteilige die Kunden entgegen den Geboten von Treu und Glauben unangemessen. Gemäß § 35 Abs. 1 S. 1 GBO könne zwar der Nachweis der Erbfolge gegenüber dem Grundbuchamt in der Regel nur durch einen Erbschein geführt werden. Beruhe jedoch die Erbfolge auf einer Verfügung von Todes wegen, die in einer öffentlichen Urkunde enthalten ist, so genüge es nach § 35 Abs. 1 S. 2 Hs. 1 GBO, wenn an Stelle des Erbscheins die Verfügung und die Niederschrift über deren Eröffnung vorgelegt würden. Nur wenn das Grundbuchamt die Erbfolge durch diese Urkunden nicht für nachgewiesen erachte, könne es die Vorlegung eines Erbscheins verlangen (§ 35 Abs. 1 S. 2 Hs. 2 GBO). Das Grundbuchamt habe demnach bei Vorliegen etwa eines – eröffneten – öffentlichen Testaments (§ 2232 BGB) grundsätzlich hierauf zu vertrauen und dürfe lediglich dann einen Erbschein verlangen, wenn sich bei der Prüfung der letztwilligen Verfügung hinsichtlich des behaupteten Erbrechts begründete (konkrete) Zweifel ergäben, die nur durch weitere, allein dem Nachlassgericht mögliche Ermittlungen über den tatsächlichen Willen des Erblassers oder über sonstige tatsächliche Verhältnisse geklärt werden könnten. Dem liege zu Grunde, dass beim öffentlichen – anders als beim eigenhändigen (§ 2247 BGB) – Testament vor der Beurkundung vom Notar die Identität und Geschäftsfähigkeit des Erblassers festgestellt (§§ 10, 11, 28 BeurkG), dessen letzter Wille erforscht und dieser klar und unzweideutig wiedergegeben würde (§ 17 BeurkG), was zu einem gesteigerten Beweiswert führe. Abweichend hiervon gestatteten die zu prüfenden AGB, selbst bei Vorliegen eines öffentlichen Testaments und Fehlen jeglicher Zweifel an der Erbfolge, auf der Vorlage eines Erbscheins zu bestehen. Es werde auch nicht danach differenziert, welche Art von Testament errichtet worden sei. Vielmehr werde die Entscheidung über die Art des verlangten Nachweises generell in das Ermessen des Instituts gestellt. Die Klausel knüpfe damit – obwohl ein eröffnetes öffentliches Testament in der Regel als ausreichender Nachweis für die Rechtsnachfolge anzusehen sei – sogar höhere Anforderungen an den Erbfolgenachweis, als sie im ohnehin sensiblen Bereich des Grundbuchrechts von Gesetzes wegen bestünden.

Die unangemessene Benachteiligung i. S. d. § 307 Abs. 1 S. 1 BGB werde durch den Verstoß gegen wesentliche Grundgedanken der Rechtsordnung indiziert. Gründe, die die Klausel nach Treu und Glauben gleichwohl als angemessen erscheinen ließen, lägen nicht vor. Daran, auch in klaren Erbfolgefällen allein zur Erlangung des Gutglaubensschutzes der §§ 2366, 2367 BGB stets auf einem Erbschein bestehen und damit öffentliche Urkunden leichter als z. B. das Grundbuchamt zurückweisen zu können, habe die Bank kein schutzwürdiges Interesse. Im Gegenteil seien die Interessen des (wahren) Erben, der im Wege der Universalsukzession (§ 1922 BGB) in die Stellung des Erblassers als Vertragspartner der Sparkasse eingerückt sei, vorrangig. Ihm sei regelmäßig nicht daran gelegen, auch in Fällen, in denen er sein Erbrecht unproblematisch anders als durch Vorlage eines Erbscheins nachweisen könne, das unnütze Kosten verursachende und zu

einer Verzögerung der Nachlassregulierung führende Erbscheinsverfahren anstrengen zu müssen.[1007]

In seinem Urteil vom 5. April 2016 hat der BGH die Erforderlichkeit des Nachweises der Erbenstellung durch Erbschein gegenüber einer Bank auch für den Fall, dass „nur" ein eröffnetes privatschriftliches Testament vorliegt, verneint.[1008]

De lege lata dürften daher jedenfalls AGB der Internetdienstanbieter im Hinblick auf die Vergleichbarkeit der Sach- und Interessenlage gem. § 307 Abs. 2 Nr. 1 BGB unzulässig sein, soweit diese ausnahmslos die Vorlage eines Erbscheins verlangen oder die Entscheidung über die Art des verlangten Nachweises generell in das Ermessen des Internetdienstanbieters stellen.

Ob de lege ferenda eine Regelung sinnvoll erscheint, nach welcher ein Erbschein auch dann nicht verlangt werden darf, wenn der Erbe eine in einer öffentlichen Urkunde enthaltene Verfügung von Todes wegen nicht vorlegt oder wenn an deren Gültigkeit konkrete Zweifel bestehen, ist fraglich.

Für eine solche gesetzliche Regelung sprechen im Wesentlichen die Eilbedürftigkeit und die Tatsache, dass nach der Rechtsprechung schon in der Stellung des Erbscheinsantrages die Annahme der Erbschaft durch schlüssiges Verhalten gesehen wird.

Dafür, dass es zulässig sein sollte, einen Erbschein zum Nachweis der Erbenstellung zu verlangen, kann ins Feld geführt werden, dass unterhalb der Ebene des Erbscheins die Nachweise der Erbfolge von fraglicher Tragfähigkeit sind und mit der Zuweisung an Daten (bzw. der Entgegennahme einer Löschungsanweisung) regelmäßig vollendete Tatsachen geschaffen werden, wenn der Provider oder derjenige, der die Daten ohne Erbschein bekommen hat, diese löscht. Verlangt man keinen Nachweis durch Erbschein, besteht die (erhöhte) Gefahr, dass die Daten an einen Nichtberechtigten ausgehändigt werden oder auf Veranlassung eines Nichtberechtigten gelöscht werden könnten. Zu berücksichtigen ist in diesem Bereich zudem das Persönlichkeitsrecht des Erblassers, welches in besonderer Weise berührt werden kann, wenn einem Dritten Zugangsrechte zu einem Account gewährt werden.

Letztlich besteht jedoch auch insoweit eine dem Bankrecht vergleichbare Interessenlage. In diesem Bereich hat man bislang eine gesetzliche Regelung nicht für erforderlich gehalten. Zwingende Gründe, die für eine entsprechende gesetzliche Regelung sprechen, sind auch tatsächlich nicht ersichtlich. Ein spezieller Regelungsbedarf für den Bereich des digitalen Nachlasses besteht ebenfalls nicht. Konsequenterweise sollte davon abgesehen werden, eine solche Regelung für den Bereich der Providerverträge zu schaffen.

[1007] Vgl. im Einzelnen BGH, Urt. v. 8.10.2013 – XI ZR 401/12, NJW 2013, 3716 (3718).
[1008] BGH, Urt. v. 5.4.2016 − XI ZR 440/15, NJW 2016, 2409.

(4) Abwicklungsklauseln

Zunächst ist die Lage nach geltendem Recht festzustellen. Wie bereits dargestellt, sind Vertragsbeziehungen über Online-Dienstleistungen einschließlich Telekommunikationsverträge vererblich, wobei Gleiches auch für die Daten gilt, die sich auf einem dem Erblasser gehörenden Speichermedium befinden.

Noch nicht abschließend geklärt ist hingegen die Frage, wie es sich bei nicht abgerufenen E-Mails verhält, die sich noch auf dem Server des Providers befinden. Auch dieses Problem wurde in der Literatur bereits diskutiert.

Ausgangspunkt der Überlegungen ist § 1922 BGB, der Grundsatz der Universalsukzession. Da nach diesem Grundsatz der schuldrechtliche Vertrag zum Provider mit Rechten und Pflichten auf den Erben übergeht, steht dem Erben zivilrechtlich ein Anspruch auf Zurverfügungstellung der E-Mails als Hauptleistungspflicht zu. Darüber hinaus besteht die vertragliche Nebenpflicht des Internetdiensteanbieters, dem Erben bestehende Passwörter mitzuteilen bzw. neue Passwörter zur Verfügung zu stellen. Diesbezüglich wird zur Vermeidung von Wiederholungen auf die obigen Ausführungen verwiesen. Diesem Anspruch steht im Ergebnis auch nicht das Telekommunikationsrecht entgegen. Auf die obigen Ausführungen wird diesbezüglich verwiesen. Zusammenfassend ist daher festzustellen, dass nach geltendem Recht ein zivilrechtlicher Anspruch auf Herausgabe der Daten besteht.

Gemäß § 307 Abs. 2 Nr. 2 BGB ist eine unangemessene Benachteiligung i. S. d. Absatzes 1 der Norm im Zweifel anzunehmen, wenn eine Klausel in AGB wesentliche Rechte oder Pflichten, die sich aus der Natur des Vertrages ergeben, so einschränkt, dass der Vertragszweck gefährdet ist. Wichtigster Anwendungsfall des § 307 Abs. 2 Nr. 2 BGB ist die Freizeichnung von Kardinalpflichten.[1009]

Unabhängig von der Frage, welchem Vertragstypus man Providerverträge zuordnet und ob man das Vorliegen eines entgeltlichen Vertrages annimmt, ist vertragliche Hauptpflicht des Internetdiensteanbieters, seinem Vertragspartner (und nach dessen Tode seinem Erben) Zugang zu den ihn interessierenden Daten zu gewähren. Eine Klausel, mit der ein Provider die entsprechenden Herausgabe- oder Auskunftsrechte in AGB explizit ausschließt, beinhaltet mithin eine Freizeichnung von Kardinalpflichten, die zu einer Gefährdung des Vertragszweckes führt. Die Voraussetzungen der Vertragszweckgefährdung gem. § 307 Abs. 2 Nr. 2 BGB liegen mithin vor. Ist dies der Fall, so wird das Vorliegen einer unangemessenen Benachteiligung i. S. d. § 307 Absatz 1 S. 1 BGB widerleglich vermutet.[1010] Gründe, die die Klausel nach Treu und Glauben gleichwohl als angemessen erscheinen lassen, liegen nicht vor. Ein schützenswertes Interesse des Providers, die Daten nicht herauszugeben, ist nicht ersichtlich.

[1009] Palandt/*Grüneberg*, BGB, § 307 Rn. 37.
[1010] Palandt/*Grüneberg*, BGB, § 307 Rn. 28.

Demgegenüber würde eine derartige Klausel die Rechtsstellungen des Erblassers wie auch des Erben in ganz erheblicher Weise beschränken. Der Erblasser wäre in seiner Testierfreiheit beeinträchtigt, da Daten aus einem Zeitraum zwischen seinem letzten Zugriff/Abruf und der Sperrung des Accounts bei entsprechender Vertragsgestaltung unwiederbringlich verloren wären. Eine derartige Klausel griffe aber auch in die Rechte des Erben ein, da sich aus den Daten wesentliche Informationen für die Frage der Werthaltigkeit des Nachlasses ergeben könnten. Wenn die Zugriffsmöglichkeit auf die Daten wirksam durch AGB abbedungen werden könnte, wäre dies für Erben fatal, weil ihnen dann jede Möglichkeit genommen wäre, den digitalen Nachlass zu ermitteln. Eine solche Klausel widerspricht daher nicht zuletzt dem Interesse des Erben an einer möglichst raschen und kostengünstigen Abwicklung des Nachlasses.

Wie gezeigt, besteht ein zivilrechtlicher Anspruch auf Herausgabe der Daten. AGB, die einen solchen Anspruch beschränken, sind aufgrund der nicht entkräfteten Vermutungswirkung des § 307 Abs. 2 Nr. 2 BGB unwirksam.

Eine Notwendigkeit, entsprechende Klauselverbote ausdrücklich in §§ 308, 309 BGB aufzunehmen, besteht schon mangels eines entsprechenden Klärungsbedarfes nicht. Eine Aufnahme aller oder einer Vielzahl von Klauseln, die – noch dazu deutlich erkennbar – bereits nach § 307 BGB unwirksam sind, würde zu einer äußerst kleinteiligen Regelung führen und das Gesamtgefüge der §§ 307 ff. BGB sprengen. Der Anwendungsbereich der §§ 308 f. BGB drohte, uferlos zu werden. Sollten sich die Provider trotz der eindeutigen Rechtslage dennoch auf die Wirksamkeit entsprechender AGB berufen, kann eine Klärung der Rechtsprechung vorbehalten werden.

e. Übertragbarkeit positiver Bewertungen eines Verkäufers auf seine Erben

Hinsichtlich des Übergangs positiver Bewertungen (eBay etc.) wird, wie oben dargestellt, vereinzelt unter Verweis darauf, dass bei Vererbung eines Unternehmens auch der verkörperte Goodwill mit übergeht, vertreten, dass nichts anderes für Bewertungen eines eBay-Händlers gelten könne.[1011]

Diese Ansicht ist indes abzulehnen. Auch ist fraglich, ob eine solche Übertragbarkeit überhaupt sinnvoll erscheint.

Ansatzpunkt ist insoweit wieder die Frage, ob positive Bewertungen überhaupt vererblich sein können oder ob sie zu den unvererblichen Rechten gehören. Vererblich sind alle vermögenswerten Rechte und Rechtsstellungen inklusive der vermögenswerten Bestandteile des allgemeinen Persönlichkeitsrechts, unvererblich (mit der Folge des Untergangs des Rechts im Erbfall) sind höchstpersönliche Rechte ohne Vermögenswert.[1012] Unvererbliche höchstpersönliche Rechte in die-

---

[1011] *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750).
[1012] Vgl. *DAV*, Stellungnahme Nr. 34/2013, S. 16 ff., 30 ff.

sem Sinne sind etwa der Name, die ideellen Bestandteile des allgemeinen Persönlichkeitsrechts und Familienrechte wie die elterliche Sorge.[1013] Die Unvererblichkeit stellt im Sinne der Rechtssicherheit und eines Kontinuitätsgedankens die Ausnahme dar, die gesetzlich in Sondervorschriften fixiert oder gewohnheitsrechtlich anerkannt sein oder sich aus der Natur der Sache ergeben muss, was wiederum durch Auslegung zu ermitteln ist.[1014]

Hier besteht das Problem, dass es sich um ein höchstpersönliches Recht handelt, dem man aber durchaus Vermögenswert zusprechen kann, denn einer positiven Bewertung als eBay-Händler bzw. einer vergleichbaren Bewertung kann durchaus absatzfördernde Wirkung zukommen. Dies könnte dafür sprechen, dass es sich um ein vermögenswertes Recht handelt, das vergleichbar den vermögenswerten Bestandteilen des allgemeinen Persönlichkeitsrechts vererbbar ist. Auch ist die Unvererblichkeit derartiger Bewertungen weder gesetzlich in Sondervorschriften fixiert noch gewohnheitsrechtlich anerkannt.

Allerdings greift hier eine Ausnahme, die sich aus der Natur der Sache ergibt, ein. Insoweit ist zu berücksichtigen, dass (positive) Bewertungen einer natürlichen Person im Rahmen von Plattformen wie eBay und ähnlichem gerade auf eine konkrete natürliche Person (den Erblasser) bezogen sind. Sie basieren auf Bewertungen von Personen, die mit dem Erblasser unmittelbar in geschäftlichem Kontakt gestanden haben. Diese Bewertungen sind damit unmittelbar mit der Person des Erblassers verknüpft. Sie bewerten das persönliche Verhalten (insbesondere die Lauterkeit und Zuverlässigkeit) des Erblassers im Rahmen von Vertragsabwicklungen. Sie lassen sich gerade nicht von der Person trennen, auf die sie sich beziehen. Es handelt sich vielmehr um persönliche Bewertungen, die untrennbar mit der Person des Erblassers verknüpft sind. Die Bewertung von Käufer- und Verkäuferverhalten ist zudem kein Selbstzweck und dient nicht dazu, bei dem Bewerteten eine verkehrsfähige Vermögensposition zu generieren. Sie dient vielmehr der Sicherheit im Geschäftsverkehr in diesen Portalen und damit allen dort am Geschäftsleben Teilnehmenden. Eine Vererblichkeit von positiven Bewertungen würde den Sinn und Zweck derartiger Bewertungen vollständig unterlaufen. Hieraus folgt die Unvererblichkeit solcher Bewertungen kraft Natur der Sache wegen der Höchstpersönlichkeit der Bewertung in Verbindung mit dem Sinn und Zweck dieser Bewertungen im Rahmen des Vertragszwecks. Dies gilt gleichermaßen für Verkäufer– wie auch Nutzerbewertungen.

Dies ist nicht nur de lege lata anzunehmen – eine andere Rechtslage wäre auch de lege ferenda nicht wünschenswert.

Der Rechtsverkehr vertraut in gewissem Umfang auf die positive Bewertung eines eBay-Verkäufers (und ähnliche Bewertungen), die sich aber aus gewonnenen Erfahrungen mit dieser Person speisen. Sie einfach auf den Erben zu übertragen ist nicht gerechtfertigt, da es in der Natur der Sache liegt, dass die Erfahrungen mit

---

[1013] Vgl. Palandt/*Weidlich*, BGB, § 1922 Rn. 36.
[1014] Vgl. *DAV*, Stellungnahme Nr. 34/2013, S. 31.

einer Person (Integrität, Zuverlässigkeit etc.) nicht einfach auf einen Erben (der im Fall gewillkürter Erbfolge jeder beliebige sein kann) übertragbar sind. Bildhaft gesprochen: Der zuverlässige und geschäftlich seriöse Erblasser kann von einer hochgradig unzuverlässigen und geschäftlich unseriösen Person beerbt werden. Der Rechtsverkehr, der auf die Bewertung vertraut, würde irregeführt und getäuscht.

Dies wird noch deutlicher bei Bewertungen in Portalen, in denen Berufsgruppen bewertet werden (etwa Ärzte), bei denen eine Übertragung des „Goodwill" von vornherein aus der Natur der Sache ausscheiden muss, zumal wenn der Erbe nicht zu derselben Berufsgruppe gehört. Aber auch ansonsten liegt bei derartigen Bewertungen auf der Hand, dass sie derart persönlich sind, dass sie nicht vererblich sein können. Gleiches muss für Bewertungen als eBay-Verkäufer und ähnlichen Portalen gelten. Im Übrigen müsste man andernfalls wohl konsequenterweise auch vertreten, dass negative (bzw. „nicht uneingeschränkt positive") Bewertungen ebenfalls auf den Erben übergehen würden, was einen zuverlässigen Erben ungerechtfertigt belasten würde.

Anderes muss allerdings gelten, wenn nicht eine Person, sondern ein Unternehmen bewertet wird und dieses Unternehmen vererbt wird. In diesem Fall betrifft die Bewertung nicht den Erblasser als Person, sondern ein Unternehmen, das nach dem Tod des Erblassers weiter fortbesteht. Unternehmensbewertungen dürften als wertbildender Faktor eines Unternehmens mit diesem verknüpft sein und mit diesem auf den Erben des Unternehmens übergehen. In diesem Fall ist daher von Vererblichkeit auszugehen, da hier die Ausnahme kraft Natur der Sache aufgrund von Höchstpersönlichkeit gerade nicht gegeben ist und auch der Sinn und Zweck der Bewertung bei ihrem Fortbestand weiter eingreift, da der Rechtsträger nicht untergegangen ist. Regelungsbedarf ergibt sich hieraus aber nicht, da die jeweiligen Ergebnisse nach der geltenden Rechtlage zu interessengerechten Ergebnisse führen dürften.

Zwar liegt hierin eine Ungleichbehandlung zu juristischen Personen. Indes ist diese sachlich begründet, da die juristische Person, die bewertet wird, nicht verstirbt. Bei Änderung des Personenbestandes, der für die juristische Person handelt, werden sich – für den Fall, dass die positiven Bewertungen nicht mehr gerechtfertigt sein sollten – jedenfalls im Laufe der Zeit die Bewertungen ändern.

Vor diesem Hintergrund kommt die Arbeitsgemeinschaft zu dem Ergebnis, dass es sich bei positiven eBay-Bewertungen und ähnlichen Verkäuferbewertungen im Hinblick auf natürliche Personen um unvererbliche Positionen kraft Natur der Sache handelt und dass dies auch berechtigt ist und nicht durch Reformüberlegungen geändert werden sollte, sodass auch hier *kein Regelungsbedarf* gesehen wird.

II. Themenkreis testamentarische Regelung

1. Fragestellung

Zum Themenkreis der testamentarischen Regelung hat die Arbeitsgruppe folgende Fragen als wesentlich erkannt und bearbeitet:

- Sollte der Erblasser den Umgang mit den in seinen Accounts abgelegten persönlichen Daten testamentarisch regeln können?
- Sind Daten ein Vermögensgegenstand?
- Sollte analog zur Bestattungsanordnung Art und Weise der digitalen Bestattung angeordnet werden können?

2. Diskussionsstand

Steiner/Holzer gehen als selbstverständlich von der Möglichkeit aus, derartige testamentarische Regelungen zu treffen und machen konkrete Formulierungsvorschläge. Falls erreicht werden solle, dass Erben in bestimmte Teile des digitalen Nachlasses keine Einsicht haben sollen, schlagen sie die Anordnung einer Testamentsvollstreckung über den digitalen Nachlass vor.[1015] *Kutscher* setzt sich mit der Möglichkeit auseinander, dass Provider in ihren AGB den Nutzern die Möglichkeit schaffen könnten, auch durch aktives Setzen von Häkchen zwischen mehreren vorgeschlagenen Formulartexten zu wählen (individualvertragliche Vereinbarungen hält sie für faktisch nicht durchführbar) und stellt sich die Frage nach AGB, die einer Inhaltskontrolle standhalten.[1016] Wenn sie transparent ausgestaltet seien und ein Wahlrecht des Nutzers beinhalteten, seien derartige Vereinbarungen wirksam; unwirksam sei hingegen wegen unangemessener Benachteiligung (§ 307 Abs. 1 S. 1 BGB) eine Regelung, in der der Provider in den AGB einseitig eine Befristung auf den Tod des Nutzers vorsehe.[1017] *Seidler* weist auf die Gestaltungsmöglichkeiten mittels Verfügungen von Todes wegen hin und verweist insoweit auf die Möglichkeiten der Teilungsanordnung und des (Voraus-)Vermächtnisses ggf. in Kombination mit einer Auflage.[1018] Sie zeigt weiter auf, dass der Erblasser durch Errichtung eines Vermächtnisses in Verbindung mit einer Auflage auch die Möglichkeit hat, die Zugangsberechtigung zu einem Account (ausschließlich) einer Person zu übertragen, die nicht zugleich Erbe ist, und mittels Auflage auch verhindern kann, dass überhaupt Einsicht in einen Account genommen werden kann, was durch Anordnung einer Testamentsvollstreckung abgesichert werden könnte.[1019] Schließlich verweist sie auf die Möglichkeit der postmortalen Vollmacht, die sie wegen der Gefahr eines Widerrufs durch die Erben

---

[1015] *Steiner/Holzer,* Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (266).
[1016] *Kutscher* (Diss.), S. 151 f. (mit intensiver Auseinandersetzung mit dem Interactive Account Manager von Google auf S. 153 f., 157 f.).
[1017] *Kutscher* (Diss.), S. 157-159.
[1018] *Seidler* (Diss.), S. 151 f.
[1019] *Seidler* (Diss.), S. 153 f..

allerdings für das weniger geeignete Mittel hält.[1020] Sie plädiert für eine Sensibilisierung der Bevölkerung insbesondere durch die Beratungs- und Gestaltungspraxis sowie durch Provider, hält aber eine gesetzliche Verpflichtung hierzu für Provider nicht für erforderlich.[1021]

3. Stellungnahme

Es ist einem Erblasser bereits nach derzeit geltender Rechtslage möglich, testamentarische Regelungen über den Umgang mit den in seinen Accounts abgelegten persönlichen Daten zu treffen, wenn auch mangels eines absoluten Rechts an Daten nicht unmittelbar über die Daten als solche verfügt werden kann.

Auch de lege ferenda sollte dies unzweifelhaft gewährleistet bleiben: Hätte der Erblasser keine Möglichkeit dies zu tun, würde ihn dies bereits zu Lebzeiten in seinem allgemeinen Persönlichkeitsrecht, seinem informationellen Selbstbestimmungsrecht und in seiner Testierfreiheit einschränken. Wenn man sich zu Lebzeiten bewusst sein müsste, dass man keinen Einfluss darauf nehmen kann, was im Todesfall mit den persönlichen Daten passiert, dann wäre man deutlich gehemmter im Umgang mit persönlichen Daten. Zudem wäre eine Nichtregelbarkeit im Hinblick auf die von Art. 14 GG geschützte Testierfreiheit hochproblematisch.

Zunächst aber zur geltenden Rechtslage: Ein Erblasser kann entsprechende letztwillige Verfügungen bezüglich seiner Daten treffen. Er kann die in seinen Accounts abgelegten persönlichen Daten testamentarisch jemandem zuwenden. Der eingesetzte Erbe erbt mit der Hardware die dort verkörperten Daten und mit dem Eintritt in die entsprechenden Providerverträge den jeweiligen Anspruch auf Zurverfügungstellung der bisherigen, noch nicht abgerufenen Daten bzw. eines Passworts, durch das Zugriff auf diese Kommunikation genommen werden kann (siehe oben unter B. I. 3.).

Im Hinblick auf das postmortale Persönlichkeitsrecht greifen die Grundsätze ein, die für dieses Recht durch die Rechtsprechung entwickelt wurden. Testamentarische Regelungen des Erblassers dürften diese nicht ausweiten können, sondern sie sind lediglich bei der Auslegung seines Willens im Rahmen der Ausübung des postmortalen Persönlichkeitsrechts durch die nächsten Angehörigen oder sonstigen vom Erblasser bestimmten Wahrnehmenden maßgeblich zu berücksichtigen.

Auch für die Fälle, dass der Erblasser zwar seinen digitalen Datenbestand einem Erben überlassen will, hiervon jedoch einzelne Daten ausnehmen möchte, oder wenn der Erblasser hinsichtlich seines digitalen Nachlasses eine differenzierte Nachlassregelung treffen möchte, etwa unterschiedliche Datenbestände an unterschiedliche Erben vererben möchte und ggf. bestimmte Datenbestände überhaupt nicht vererben, sondern sie löschen lassen möchte, bietet das bestehende Erbrecht faktisch auch für den digitalen Nachlass Gestaltungsmöglichkeiten.

[1020] *Seidler* (Diss.), S. 154-157.
[1021] *Seidler* (Diss.), S. 160 f.

Die Differenzierung nach unterschiedlichen Datenbeständen, die unterschiedlichen Erben zukommen sollen, ist erbrechtlich auch nach derzeitiger Rechtslage unproblematisch möglich; insoweit gibt es erbrechtlich verschiedene Möglichkeiten. So kann der Erblasser dies durch Erbeinsetzung mehrerer Erben mit Teilungsanordnung (§ 2048 BGB) oder Vorausvermächtnis an einzelne Erben gem. § 2150 BGB erreichen. Sollen Datenbestände Personen zugeordnet werden, die nicht Erbe werden sollen, besteht die Möglichkeit eines Vermächtnisses (§§ 2147 ff. BGB). In beiden Fällen ist zwar nicht die besondere Zuordnung der konkreten Datenbestände möglich, wohl aber die Steuerung, wem die Datenbestände zufallen, da sie entweder mit der Hardware (Computer, Laptop, Handy, Tablet, USB-Stick, externe Festplatte sowie sonstige Speichermedien) übergehen oder im Wege des Eintritts in laufende Verträge. Diese Rechtspositionen (Eigentum am Computer etc. und vertragliche Beziehungen zum Provider) sind wie dargestellt vererblich und können auch Gegenstand eines Vermächtnisses sein. Vermächtnis ist gem. § 1939 BGB die Zuwendung eines Vermögensvorteils an einen anderen, ohne ihn als Erben einzusetzen. Bei der Übertragung von Hardware samt den darauf befindlichen Daten ist dies unzweifelhaft möglich. Die Zuwendung einer Vertragsbeziehung zu einem Provider kann als Vermögensvorteil gewertet werden (Zugriffsmöglichkeit auf Daten als Vermögensvorteil), jedenfalls wenn keine Entgeltzahlungspflicht des Nutzers besteht.

Bei letztwilligen Verfügungen in diesem Zusammenhang dürfte es sich für einen Erblasser allerdings anbieten, bei der testamentarischen Verfügung klarzustellen, dass die Teilungsanordnung bzw. das Vermächtnis sich auf die Hardware bzw. auf den Übergang der Vertragsbeziehung auch und gerade im Hinblick auf die dort gespeicherten Daten bezieht, um Missverständnissen oder Streit vorzubeugen. Eine Regelungslücke im Hinblick auf testamentarische Gestaltungsspielräume ergibt sich daraus aber nicht.

Aber auch wenn der Erblasser bestimmte Datenbestände dem Zugriff der Erben (und überhaupt aller Personen) entziehen will, er also Datenbestände überhaupt nicht vererben, sondern ihre Löschung erreichen möchte, bietet das geltende Recht Gestaltungsmöglichkeiten mit der Auflage (§§ 1940, 2191 ff. BGB). Durch eine Auflage gem. § 1940 BGB wird der Erbe oder Vermächtnisnehmer zu einer Leistung verpflichtet. Gegenstand einer Auflage kann ein jedes Tun oder Unterlassen sein, das Gegenstand eines Schuldverhältnisses sein kann.[1022]

Damit dürfte die Zuwendung von Datenbeständen (im Wege der Zuwendung des Eigentums am Computer oder sonstigen Speichermedium oder im Wege der Zuwendung der vertraglichen Beziehung zum Provider) mit der Auflage, bestimmte

---

[1022] Vgl. Palandt/*Weidlich*, BGB, § 2192 Rn. 3.

Datenbestände zu löschen, rechtlich unproblematisch möglich sein. In der Literatur finden sich Formulierungsvorschläge für die Anordnung von „Auflagen und Vermächtnissen“ beim digitalen Nachlass.[1023]

Dass derartige Auflagen keine Garantie dafür sind, dass sie auch befolgt werden, zeigt das aus vor-digitaler Zeit stammende Beispiel der testamentarischen Verfügung von Franz Kafka, der (erfolglos) verfügt hatte, dass seine unveröffentlichten Manuskripte verbrannt werden sollten. [1024] Insoweit wäre allerdings die Anordnung einer Testamentsvollstreckung (§§ 2197 ff. BGB) denkbar.

Ein gesetzgeberischer Handlungsbedarf zur Sicherung des Erblasserwillens in Bezug auf Daten besteht nicht – die genannte Problematik stellt sich in gleicher Weise auch bei nicht-digitalen Informationen. Wenn der Erblasser keine Löschung/Vernichtung zu Lebzeiten vornimmt, besteht (online wie offline) keine 100%-ige Sicherheit, dass eine Löschung tatsächlich stattfindet.

Indes könnten bezüglich des Problems der Durchsetzung des Erblasserwillens gerade lebzeitige, vertragliche Vereinbarungen für den Todesfall (auch in Form von AGB mit Auswahlmöglichkeiten durch Setzen von Häkchen bei alternativ formulierten AGB) mit den jeweiligen Providern helfen.[1025] Wenn etwa der Erblasser die Möglichkeit hätte, bei der Verwaltung seines Accounts festzulegen, dass nach seinem Ableben bestimmte (oder alle) Daten gelöscht werden sollen, dürfte hierin die (wirksame) Erteilung einer postmortalen Vollmacht und einer postmortalen Weisung im Vertragsverhältnis zu sehen sein, durch die der Erblasser den Erben den Zugriff auf Daten entziehen könnte. Erbrechtlich übergehen dürften nach derzeitiger Rechtslage lediglich Ansprüche auf Übertragung von E-Mails und Passwörtern. Wenn der Erblasser aber selbst durch postmortale Vollmacht eine Löschung angeordnet hat, entzieht er damit wirkungsvoll diese Daten dem Zugriff der Erben, da das Vertragsverhältnis nur so übergeht, wie es mit dem Provider ausgestaltet ist.

Ein solches Vorgehen des Erblassers funktioniert aber lediglich auf vertraglicher Basis. Es stellt sich insoweit auf gesetzgeberischer Ebene die Frage, ob die Provider verpflichtet werden könnten und sollten, entsprechende Regelungen vorzusehen und auf entsprechende Möglichkeiten hinzuweisen. Dies betrifft die folgenden Fragestellungen zu III. (vgl. dazu sogleich). Einen Regelungsbedarf konkret zu dem Themenkreis „testamentarische Regelung“ sieht die Arbeitsgruppe indes nicht.

[1023] Vgl. bei *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (266).

[1024] Auf dieses Beispiel weist *Martini*, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1154), hin.

[1025] Ebenso *Kutscher* (Diss.), S. 157-160, die dort auch Formulierungsvorschläge macht.

III. Themenkreis Vorsorge

1. Fragestellungen

Mit Blick auf die Vorsorge stellten sich insbesondere folgende Fragen:

- Sollten Nutzer bei Anlegung des Accounts auf die für den Todesfall geltenden Regeln ausdrücklich hingewiesen werden müssen?
- Sollte hier bereits eine Auswahlmöglichkeit für den postmortalen Umgang mit den Daten bestehen müssen?

2. Diskussionsstand

Soweit ersichtlich, hat sich mit dieser Frage in der Literatur noch niemand explizit beschäftigt.

3. Stellungnahme

De lege lata gibt es weder eine solche Hinweispflicht noch eine Verpflichtung der Provider, eine Auswahlmöglichkeit für den postmortalen Umgang mit den Daten bereitzustellen. Es stellt sich also die Frage nach einem entsprechenden Regelungsbedarf.

a. Verpflichtung der Provider, eine Auswahlmöglichkeit für den postmortalen Umgang mit den Daten bereitzustellen

Vor dem Hintergrund alles bisher Gesagten besteht eine Notwendigkeit, den Provider zu verpflichten, eine Auswahlmöglichkeit für den postmortalen Umgang mit den Daten bereitzustellen, nach Ansicht der Arbeitsgruppe jedenfalls nicht zwingend. Eine derartige gesetzliche Regelung würde in die Vertragsfreiheit eingreifen, da sie sinnvollerweise Vorgaben über den Vertragsinhalt machen müsste, bspw. welche Gestaltungsmöglichkeiten für den Todesfall vorgesehen sein müssen (Mindestinhalte verschiedener Alternativen). Solche Vorgaben macht das Zivilrecht derzeit bei Dauerschuldverhältnissen aber auch ansonsten nicht. Es gibt nur ganz ausnahmsweise Sonderregelungen für Dauerschuldverhältnisse für den Todesfall (§§ 563 ff. BGB für das Mietrecht, allerdings gerade nicht als Auswahlmöglichkeit des Erblassers).

Für einen gesetzgeberischen Eingriff besteht kein Anlass, da der Erblasser entsprechende Rechtsfolgen nach derzeitiger Rechtslage – wie dargestellt – auch im erbrechtlichen Wege herbeiführen kann. Unter der Prämisse, dass der Erbe auch die Vertragsbeziehung zum Provider erbt und insoweit einen Herausgabeanspruch bezüglich der aufgelaufenen E-Mails (und auf Mitteilung des Passworts) hat, gehen sämtliche Daten auf den Erben über. Der Erblasser kann dies durch testamentarische Verfügungen – wie oben ausgeführt – aber auch anders gestalten (siehe oben unter II.).

Soweit die Daten nicht beim Provider liegen, sondern beim Erblasser (verkörpert auf Speichermedien), was etwa bei E-Mail-Accounts regelmäßig der Fall sein wird, spielen derartige Erwägungen ohnehin bereits vom Ansatz her keine Rolle.

Sie betreffen nur die beim Provider vorgehaltenen Daten. Auch von daher relativiert sich ein etwaiger Regelungsbedarf.

Soweit allerdings Provider entsprechende Angebote in ihren AGB machen, wie beim Interactive Account Manager von Google, (etwa durch Anklicken verschiedener Vorgehensweisen im Hinblick auf den Todesfall bzw. auch allgemein den Fall länger andauernder Inaktivität), können in diesen durchaus sinnvolle vertragliche Gestaltungsmöglichkeiten liegen. Diese wären in jedem Fall am AGB-Recht (§ 307 BGB) zu messen, insoweit insbesondere am Transparenzgebot.

b. Verpflichtung der Provider, Nutzer bei Anlegung des Accounts auf die für den Todesfall geltenden Regeln ausdrücklich hinzuweisen

Nach Ansicht der Arbeitsgemeinschaft ist auch eine Verpflichtung der Provider, Nutzer bei Anlegung des Accounts auf die für den Todesfall geltenden Regeln ausdrücklich hinzuweisen, nicht erforderlich. Wenn man eine Verpflichtung der Provider, eine Auswahlmöglichkeit für den postmortalen Umgang mit den Daten bereitzustellen, nicht schaffen möchte (so die Einschätzung der Arbeitsgruppe, siehe oben unter a.), dann würde eine Hinweispflicht sich lediglich auf die geltende erbrechtliche Rechtslage beziehen. Eine solche Hinweispflicht ist im Zivilrecht auch ansonsten nicht vorgesehen und sollte auch hier nicht verlangt werden. Wer sich über die geltende Rechtslage im Hinblick auf das Erbrecht im Unklaren ist, kann sich Rechtsrat einholen. Vertragspartnern von Dauerschuldverhältnissen wird auch im übrigen Zivilrecht nicht abverlangt, auf die geltende erbrechtliche Rechtslage hinzuweisen.

IV. Themenkreis Annahme und Ausschlagung des Erbes

1. Fragestellungen

Daten zu Vermögensverhältnissen des Erblassers sind zunehmend (nur) online verfügbar, sodass sich die Frage stellt, wie der Erbe über Annahme oder Ausschlagung des Erbes entscheiden können soll, wenn er Zugang zu diesen Informationen nur mit Erbschein erhält.

2. Diskussionsstand

Diese konkrete Thematik wird in der Literatur kaum diskutiert; Überschneidungen gibt es hinsichtlich der Diskussion zu der (insbesondere bezüglich AGB der Provider diskutierten) Frage, welche Legitimationsnachweise von den Erben verlangt werden dürfen (siehe insoweit bereits den Diskussionsstand oben unter I. 2.).[1026] *Solmecke/Köbrich/Schmitt* weisen auf das Problem hin, dass der Erb-

[1026] Insoweit Beiträge von *Solmecke/Köbrich/Schmitt,* Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (294), wonach der Erbschein nicht verlangt werden kann, und *Herzog,* Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem,

scheinsantrag die Annahme der Erbschaft darstellt, Auskunftsansprüche aber gerade vor der Annahme bestehen sollten, um vermögensrechtliche Verhältnisse für die Frage der Annahme/Ausschlagung zu klären.[1027] Hierzu ist zu bedenken, dass die Annahmeerklärung eine Willenserklärung ist, die formfrei wirksam und dem Gesetzeswortlaut nach nicht gegenüber einer bestimmten Person bzw. Behörde abgegeben werden muss. Gleichwohl geht die h.M. davon aus, dass es dem Sinn und Zweck des § 1943 BGB entspricht, den objektiven Tatbestand einer Willenserklärung grundsätzlich nur zu bejahen, wenn die Erklärung gegenüber einem Nachlassbeteiligten abgegeben wird.[1028] Als taugliche „Nachlassbeteiligte" werden Miterben, Nachlassgläubiger, Nachlasspfleger, Nachlassverwalter, Testamentsvollstrecker sowie das Nachlassgericht angeführt.[1029] Nach der Dogmatik der Rechtsgeschäftslehre bedarf es ferner zur Bejahung einer Willenserklärung einer Handlung, die dem objektiven Erklärungswert nach darauf gerichtet ist, dass der vorläufige Erbe endgültig Erbe sein und die Erbschaft behalten will.[1030] Eines korrespondierenden subjektiven Annahmewillens bedarf es nicht.[1031] In der Literatur wird bezüglich der an den Annahmewillen zu stellenden Anforderungen vertreten, mit Blick auf die Kürze der Ausschlagungsfrist und die Rechtsfolgen sei es geboten, bei der Bejahung des Annahmewillens im Falle konkludenten Verhaltens im Zweifelsfall zurückhaltend zu verfahren.[1032] Demgemäß wurde in der Rechtsprechung eine Auskunftsklage des vorläufigen Erben gegen den Testamentsvollstrecker, die ausdrücklich zu dem Zweck erfolgte, die Entscheidung über die Annahme der Erbschaft sachgerecht vorzubereiten und auf eine hinreichend gesicherte Tatsachengrundlage über den Nachlass zu stellen, nicht als konkludente Annahmeerklärung gewertet.[1033] Unumstritten ist aber, dass der beim Nachlassgericht gestellte oder eingereichte Antrag auf Erbscheinserteilung als Erbschaftsannahme zu werten ist, zumal er regelmäßig auch mit der Erklärung verbunden wird, dass der Antragsteller das Erbe angenommen hat.[1034] Wird mithin im Erbfall Auskunft über gespeicherte Daten des Erblassers oder Zugang zu in elektronischen Postfächern abrufbaren Informationen begehrt, so werden sich die vorläufigen Erben regelmäßig vom Vertragspartner des Erblassers auf die Vorlage eines Erbscheins verweisen lassen und zur Erlangung der benötigten Auskunft das Erbe annehmen müssen.

NJW 2013, 3745 (3750 f.) sowie des *DAV*, Stellungnahme Nr. 34/2013, S. 62-64, wonach der Erbschein als Nachweis verlangt werden kann.

[1027] *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (294).

[1028] Palandt/*Weidlich*, BGB, § 1942 Rn. 1.

[1029] MüKo/*Leipold*, BGB, § 1943 Rn. 3.

[1030] Palandt/*Weidlich*, BGB, § 1942 Rn. 2.

[1031] Palandt/*Weidlich*, BGB, § 1942 Rn. 2.

[1032] MüKo/*Leipold*, BGB, § 1943 Rn. 5.

[1033] BayObLG, Beschl. v. 8.9.2004 – 1Z BR 59/04, NJW-RR 2005, 232.

[1034] MüKo/*Leipold*, BGB, § 1943 Rn. 5; Palandt/*Weidlich*, BGB, § 1943 Rn. 2.

3. Stellungnahme

a. Rechtsnormen des geltenden Rechts, die die Rechtsfolgen der Annahmeerklärung bei Annahme der Erbschaft durch Beantragung eines Erbscheins zum Zwecke der Auskunftserlangung abmildern können

(1) Irrtumsanfechtung wegen Irrtums über eine verkehrswesentliche Eigenschaft des Nachlasses (§§ 1954, 119 Abs. 2 BGB)

Es ist anerkannt, dass die Anfechtung der Annahme der Erbschaft (§§ 1954 ff. BGB) auf die in §§ 119, 120, 123 BGB geregelten Anfechtungsgründe gestützt werden kann.[1035] Ebenso ist anerkannt, dass der Nachlass als „Sache" i. S. d. § 119 Abs. 2 BGB zu werten ist.[1036] Schließlich entspricht es der h.M., dass die Überschuldung des Nachlasses als „verkehrswesentliche Eigenschaft" des Nachlasses zur Anfechtung gemäß § 119 Abs. 2 BGB berechtigt, wenn der Irrtum auf Fehlvorstellungen oder Unkenntnis der Zusammensetzung des Nachlasses hinsichtlich des Bestands an Aktiva oder Passiva und nicht auf einer Fehleinschätzung über den Wert der dem Erben bekannten nachlasszugehörigen Gegenstände beruht.[1037] Demgegenüber vertritt eine Mindermeinung, auch die reine Unkenntnis der Überschuldung des Nachlasses stelle einen zur Anfechtung berechtigenden Eigenschaftsirrtum dar.[1038] Eine Stellungnahme zu diesem Streit kann vorliegend dahinstehen, da für den Fall eines auf der Unkenntnis des Erben über den Nachlassbestand beruhenden Irrtums über die Überschuldung des Nachlasses nach übereinstimmender Auffassung ein Anfechtungsgrund gemäß § 119 Abs. 2 BGB gegeben ist.[1039] Der vorläufige Erbe, der zur Ermittlung des Nachlassbestands ohne Vorlage eines Erbscheins nicht in der Lage war und in der irrigen Hoffnung die Erbschaft annimmt, dass der Nachlass nicht überschuldet ist, ist demgemäß nach § 119 Abs. 2 BGB zur Anfechtung der Erbschaftsannahme berechtigt.

Unklarer stellt sich die Rechtslage dar, wenn der Nachlass nicht überschuldet ist, aber Verbindlichkeiten aufweist, deren Regulierung „lästig" ist, weil sie entweder kritischer Prüfung, ggf. im Einzelfall auch der Durchführung von Prozessen, bedarf, oder mit anderweitigen straf- und/oder disziplinarrechtlichen Gefahren verbunden ist, weil es sich z. B. bei den Nachlassverbindlichkeiten um Steuerschulden aus nicht ordnungsgemäß versteuertem Auslandsvermögen handelt.[1040] Eine Mindermeinung vertritt dazu, dass, sofern keine Überschuldung vorliege, irrtümliche Annahmen über die Zusammensetzung des Nachlasses nicht als Irrtum gemäß §§ 1954, 119 Abs. 2 BGB zu werten seien, da Verkehrsanschauungen über

---

[1035] Palandt/*Weidlich*, BGB, § 1954 Rn. 1.
[1036] Vgl. statt vieler MüKo/*Leipold*, BGB, § 1954 Rn. 11.
[1037] OLG München, Beschl. v. 8.7.2015 − 31 Wx 54/15, NJW-RR 2015, 1418 m. w. N.
[1038] Lange/Kuchinke, S. 220.
[1039] OLG Düsseldorf, Urt. v. 18.11.1998 − 11 U 49/98, ZEV 2000, 64.
[1040] Zu letzterer Konstellation vgl. etwa *Schaub*, Schwarzgeld im Nachlass: Ratschläge für Erben, ZEV 2011, 624-627.

die Wesentlichkeit von Nachlasszusammensetzungen nicht zu ermitteln seien.[1041] Demgegenüber vertritt die h. M., die Vorstellung über das Nichtbestehen erheblicher Verbindlichkeiten oder einer im Verhältnis zum Nachlasswert wesentlichen Verschuldung sei zwar grundsätzlich als „verkehrswesentliche Eigenschaft“ zu werten.[1042] Eine Anfechtung könne indes an der Kausalität des Irrtums für die Annahmeerklärung, also daran scheitern, dass der Erbe die Erbschaft auch in Kenntnis der Schulden angenommen hätte, was angenommen wird, wenn trotz der dem Erben bei Annahme unbekannten Verbindlichkeiten ein erheblicher Aktivnachlass verbleibt.[1043] Dabei ist nach der Rechtsprechung in die Überlegungen miteinzubeziehen, wie der Annehmende sich entschieden hätte, wenn er die Möglichkeiten der Haftungsbeschränkung verständig erwogen hätte.[1044] Ferner wird im Falle einer Erbengemeinschaft berücksichtigt, dass für Nachlassverbindlichkeiten eine gesamtschuldnerische Haftung besteht, sodass der Miterbe bei voller Haftung im Außenverhältnis von den übrigen Miterben gemäß § 426 Abs. 1 S. 1 BGB entsprechend den von ihnen zu tragenden Anteilen Ausgleich verlangen kann, wobei er schon vor der Leistung an den Gläubiger über einen Befreiungsanspruch verfügt.[1045] Dabei wird ihm im Rahmen der Prüfung der Voraussetzungen des § 119 Abs. 2 BGB die Darlegungs- und Beweislast für die fehlende Werthaltigkeit des Freistellungs- bzw. Ausgleichsanspruchs gegenüber dem/den Miterben zugewiesen.[1046] Diese Prüfungsmaßstäbe können selbst bei erheblichen Verbindlichkeiten und Haftungsrisiken dazu führen, dass die Bejahung eines für die Annahme ursächlichen Irrtums verneint wird, wenn ein nach Bereinigung der Verbindlichkeiten verbleibender Reinnachlass von wenigen tausend Euro verbleibt. So hatte etwa das OLG Zweibrücken einen errechneten anteiligen Reinnachlass eines Miterben, der sich erheblichen Steuerverbindlichkeiten ausgesetzt sah, von 2.814,29 DM für die Verneinung eines annahmeursächlichen Irrtums gemäß § 119 Abs. 2 BGB mit der Begründung ausreichen lassen, es entspreche der allgemeinen Lebenserfahrung, dass man im Allgemeinen bei verständiger Würdigung auch kleinere Erbschaften anzunehmen pflege.[1047] Ebenso wenig werden bei nicht überschuldeten Nachlässen die mit der Regulierung der Nachlassverbindlichkeiten für den Erben verbundenen Unannehmlichkeiten (wie z. B. Selbstanzeige bei nicht versteuertem Vermögen) als „verkehrswesentliche“ Eigenschaften gewertet.[1048]

[1041] Staudinger/*Otte*, § 1954 Rn. 16.
[1042] Lange/Kuchinke, S. 218-221.
[1043] BeckOKG/*Heinemann*, BGB, § 1954 Rn. 42; BayObLG, Beschl. v. 11.1.1999 − 1 Z BR 113/98, NJW-RR 1999, 59; OLG Zweibrücken, Beschl. v. 16.2.1996 – 3 W 260/95.
[1044] OLG Zweibrücken, Beschl. v. 16.2.1996 – 3 W 260/95.
[1045] BayObLG, Beschl. v. 11.1.1999 − 1 Z BR 113/98, NJW-RR 1999, 59; OLG Zweibrücken, Beschl. v. 16.2.1996 – 3 W 260/95.
[1046] OLG Zweibrücken, Beschl. v. 16.2.1996 – 3 W 260/95.
[1047] OLG Zweibrücken Beschl. v. 16.2.1996 – 3 W 260/95.
[1048] *Schaub*, Schwarzgeld im Nachlass: Ratschläge für Erben, ZEV 2011, 624 (625).

(2) Haftungsbeschränkungsmöglichkeiten in Bezug auf „nicht-kaufmännische“ Nachlässe[1049]

(a) Haftungsbeschränkungsmöglichkeiten des Alleinerben

Bis zur Erbschaftsannahme ist der vorläufige Erbe durch § 1958 BGB prozessual vor einer persönlichen gerichtlichen Inanspruchnahme wegen einer Nachlassverbindlichkeit[1050] geschützt. Auch vor Zwangsvollstreckungsmaßnahmen in das Eigenvermögen ist er in der Schwebezeit durch § 778 Abs. 1 ZPO geschützt. Der endgültige Erbe haftet gemäß § 1967 BGB „vorläufig“[1051] unbeschränkt, d. h. „mit Nachlass und Eigenvermögen“[1052], aber unter Einräumung gesetzlicher Beschränkungsmöglichkeiten „beschränkbar“.[1053] Allerdings genießt auch der endgültige Erbe nach der Erbschaftsannahme temporären Schutz: Er wird durch Einreden innerhalb zeitlich limitierter „Schonfristen“ (§ 2014 BGB: „Dreimonatseinrede“; § 2015 BGB: Einrede des Aufgebotsverfahrens bei Beantragung des Aufgebots innerhalb eines Jahres nach Erbschaftsannahme), sofern er nicht bereits unbeschränkt haftet (§ 2016 Abs. 1 BGB), dahingehend geschützt, dass lediglich eine unter dem Vorbehalt der beschränkten Haftung ergehende Verurteilung (§ 305 ZPO) erfolgen kann, wobei die Einreden im Vollstreckungsfall seitens des Erben gemäß § 785 ZPO geltend gemacht werden können.[1054] Ist das Aufgebotsverfahren rechtskräftig ausgeschlossen, bewirkt es gegenüber den ausgeschlossenen Gläubigern eine Haftungsbeschränkung auf den Nachlass nach Maßgabe des § 1973 BGB.[1055] Diese außerordentliche Haftungsbeschränkung kann der Erbe auch gegenüber denjenigen Nachlassgläubigern geltend machen, die ihre Forderung später als fünf Jahre nach dem Erbfall gegenüber Erben geltend gemacht haben (§ 1974 BGB). Gegenüber diesen aufschiebenden oder partiellen Verteidigungs- und Beschränkungsmöglichkeiten stellen die Inventarerrichtung und die eidesstattliche Versicherung gemäß § 1993 ff. BGB keine Haftungsbeschränkungsmöglichkeiten des Erben dar. Sie werden vielmehr überwiegend als „Angriffswaffen“[1056] der Nachlassgläubiger betrachtet, die entweder auf deren Antrag zu erfolgen haben (§ 2006 Abs. 1 BGB) oder jedenfalls bei Versäumung einer hierzu gerichtlich gesetzten Frist oder bei Verweigerung der Abgabe die unbeschränkte Haftung zur Folge haben (§ 1994 Abs. 1 S. 2 BGB, § 2006 Abs. 3 BGB).

[1049] Da die zu untersuchende Fragestellung sich auf ein allgemeines erbrechtliches Problem bezieht, werden die das Handels- und Gesellschaftsrecht berührenden Konstellationen der Vererbung eines Handelsgeschäfts oder eines Gesellschaftsanteils im Folgenden zur Beschränkung des Prüfungsgegenstands nicht in die Prüfung einbezogen.

[1050] Palandt/*Weidlich*, BGB, § 1958 Rn. 1.

[1051] Palandt/*Weidlich*, BGB, Einf v § 1967 Rn. 1.

[1052] *Graf,* Möglichkeiten der Haftungsbeschränkung für Nachlaßverbindlichkeiten, ZEV 2000, 125.

[1053] Palandt/*Weidlich*, BGB, § 1958 Rn. 1.

[1054] MüKo/*Küpper,* BGB, § 2014 Rn. 4.

[1055] Palandt/*Weidlich*, BGB, § 1973 Rn. 1.

[1056] *Graf,* Möglichkeiten der Haftungsbeschränkung für Nachlaßverbindlichkeiten, ZEV 2000, 125 (127).

Unbeschränkte Haftung tritt überdies ein, wenn der Erbe absichtlich eine erhebliche Unvollständigkeit der im Inventar enthaltenen Angabe der Nachlassgegenstände herbeiführt (§ 2005 Abs. 1 BGB).

Eine rechtssichere Haftungsbeschränkung gegenüber allen Nachlassgläubigern mit der Folge haftungsrechtlicher Sonderung von Eigenvermögen und Nachlass kann der – zu diesem Zeitpunkt noch nicht endgültig unbeschränkt haftende – Erbe nur durch die Herbeiführung der Anordnung von Nachlassverwaltung und Nachlassinsolvenz erreichen (§ 1975 BGB).[1057] Dabei steht dem Erben das Recht zur Beantragung der Nachlassverwaltung voraussetzungslos und zeitlich unbeschränkt zu und ermöglicht ihm bei „unübersichtlicher" Haftungslage eine geordnete Befriedigung der Nachlassgläubiger unter Vermeidung von Gefahren für das Eigenvermögen.[1058] Ist die Nachlassverwaltung durch Befriedigung aller bekannten Nachlassgläubiger beendet, so wirkt die einmal eingetretene Haftungsbeschränkung über das Nachlassverwaltungsverfahren hinaus fort, sodass der Erbe bei späterer Inanspruchnahme durch einen weiteren Nachlassgläubiger diesen grundsätzlich auf die Befriedigung aus dem Nachlassüberschuss verweisen kann, ohne hierzu erneut die Anordnung einer Nachlassverwaltung beantragen zu müssen.[1059]

Auch zur Beantragung des Nachlassinsolvenzverfahrens ist der Erbe berechtigt und bei Kenntniserlangung von Zahlungsunfähigkeit oder Nachlassüberschuldung verpflichtet. Außer den Eröffnungsgründen „Zahlungsfähigkeit" und „Nachlassüberschuldung" (§ 320 Satz 1 InsO) genügt bei Antrag des Erben[1060] ausnahmsweise auch drohende Zahlungsunfähigkeit des Nachlasses zur Verfahrenseröffnung (§ 320 S. 2 InsO).[1061]

Ist eine die Kosten des Verfahrens deckende Masse im Nachlass nicht vorhanden, so wird die Anordnung der Nachlassverwaltung abgelehnt (§ 1982 BGB) bzw. der Antrag auf Eröffnung des Nachlassinsolvenzverfahrens abgewiesen (§ 26 Abs. 1 S. 1 InsO). In diesem Fall mutet das Gesetz dem Erben zur Herbeiführung der Haftungsbeschränkung nicht zu, aus Eigenmitteln die Verfahrenskosten zu tragen, sondern gestattet ihm, sofern er nicht bereits aus anderen Gründen unbeschränkt haftet, sich gegenüber den Nachlassgläubigern auf die Dürftigkeitseinrede gemäß § 1990 Abs. 1 S. 1 BGB zu berufen. Dies hat zur Folge, dass der endgültige Erbe die Nachlassgläubiger auf die Befriedigung aus dem Nachlass verweisen kann (§ 1990 Abs. 1 S. 1 BGB), den er zum Zwecke der Befriedigung im Wege der Zwangsvollstreckung herauszugeben hat (§ 1990 Abs. 1 S. 2 BGB),

---

[1057] *Lettmann*, RNotZ 2002,Die Beschränkung der Erbenhaftung, 537 (542); *Herzog*, Haftung des Erben für Miet- und WEG-Schulden, NZM 2013, 175 (177); MüKo/*Küpper,* BGB, Vorb. v. § 1967 Rn. 2.

[1058] *Lettmann*, Die Beschränkung der Erbenhaftung, RNotZ 2002, 537 (545).

[1059] *Lettmann*, Die Beschränkung der Erbenhaftung, RNotZ 2002, 537 (545).

[1060] Ferner sind bei drohender Zahlungsunfähigkeit antragsberechtigt der Nachlassverwalter, sonstige Nachlasspfleger oder der Testamentsvollstrecker (§ 320 S. 2 InsO).

[1061] *Lettmann*, Die Beschränkung der Erbenhaftung, RNotZ 2002, 537 (547).

ohne dass er dabei wie bei einem Insolvenzverfahren verpflichtet wäre, auf eine gleichmäßige Befriedigung der Nachlassgläubiger hinzuwirken.[1062]

Ungeachtet dessen muss der gerichtlich wegen Nachlassverbindlichkeiten in Anspruch genommene Erbe, sofern er nicht ohnehin bereits endgültig unbeschränkt haften sollte, die Beschränkung der Erbenhaftung einredeweise geltend machen, damit sie im Urteilstenor vorbehalten wird, da sie anderenfalls im Zwangsvollstreckungsverfahren nicht mehr eingewendet werden kann (§§ 780, 781 ZPO). Der Nachlassgläubiger kann die Aufnahme des Vorbehalts in den Urteilstenor nur dadurch abwenden, dass er darlegt und im Bestreitensfall beweist, dass der Erbe bereits unbeschränkbar haftet.[1063] Vollstreckt der Nachlassgläubiger aus einem Titel in das Eigenvermögen des Erben, kann der Erbe, sofern der Vorbehalt in den Titel aufgenommen wurde, durch eine Vollstreckungsgegenklage (§§ 785, 767 ZPO) die materiell-rechtliche Haftungsbeschränkung, die in diesem Verfahren geprüft wird, prozessual durchsetzen.[1064]

(b) Haftungsbeschränkungsmöglichkeiten von Miterben

Die vorläufige unbeschränkbare Haftung des Erben für Nachlassverbindlichkeiten gemäß § 1967 BGB hat bei Miterben eine gesamtschuldnerische (Außen-)Haftung (§ 2058 BGB) für gemeinschaftliche Nachlassverbindlichkeiten zur Folge. Bei Inanspruchnahme eines Miterben wegen gemeinschaftlicher Nachlassverbindlichkeiten gelten grundsätzlich, d. h. soweit in den §§ 2058 ff. BGB nichts Abweichendes geregelt ist, die gleichen Regeln wie bei der Inanspruchnahme eines Alleinerben.

Eine maßgebliche Zäsur hinsichtlich der Frage, welche Besonderheiten bei der Haftung(-sbeschränkung) der Miterben gelten, stellt die Teilung des Nachlasses dar. Dies wird vor dem Hintergrund verständlich, dass bei der Erbschaft mehrerer Personen die Erbengemeinschaft – eine „Gesamthandsgemeinschaft“ – entsteht, die als geschlossenes Sondervermögen vom Eigenvermögen der Erben getrennt ist und auf das sie – bildlich gesprochen wie bei einem „zugebundenen Sack, in dem die Erbschaft steckt“[1065] – nur sehr beschränkte Zugriffsmöglichkeiten haben.[1066] Diese strikte Trennung der Vermögensmassen entfällt mit der Auseinandersetzung der Erbengemeinschaft. Daher sieht § 2046 Abs. 1 S. 1 BGB vor, dass die Miterben voneinander verlangen können, dass vor der Auseinandersetzung die Nachlassverbindlichkeiten berichtigt werden. Sind einzelne Nachlassverbindlichkeiten noch nicht fällig oder streitig, so ist das zu ihrer Erfüllung Erforderliche zurückzubehalten (§ 2046 Abs. 1 S. 2 BGB). Demgemäß bestimmt § 2059 BGB,

---

[1062] *Lettmann*, Die Beschränkung der Erbenhaftung, RNotZ 2002, 537 (549); *Herzog*, Haftung des Erben für Miet- und WEG-Schulden, NZM 2013, 175 (177).
[1063] *Klinger*, Vorbehalt der beschränkten Erbenhaftung als Regressfalle, NJW-Spezial 2005, 541.
[1064] *Klinger*, Vorbehalt der beschränkten Erbenhaftung als Regressfalle, NJW-Spezial 2005, 541.
[1065] So wörtlich Kroiß/Ann/Mayer/*Kick*, BGB, § 2058 Rn. 2.
[1066] Kroiß/Ann/Mayer/*Kick*, BGB, § 2058 Rn. 2.

dass jeder noch nicht unbeschränkt haftende Miterbe bis zur Nachlassteilung Gläubigern den Zugriff auf sein Eigenvermögen wegen einer Nachlassverbindlichkeit verweigern darf. Ab der Nachlassteilung ist der Miterbe mithin wegen Nachlassverbindlichkeiten dem Zugriff auf sein Eigenvermögen ausgesetzt. Dabei gilt gegenüber der Alleinerbschaft die Besonderheit, dass die Nachlassverwaltung als Möglichkeit der Haftungsbeschränkung ab der Nachlassteilung, die auch insoweit Zäsurwirkung hat, entfällt (§ 2062 2. Hs. BGB). Aber auch bis zur Nachlassteilung steht die Nachlassverwaltung dem Miterben als Mittel der Haftungsbeschränkung insoweit nur eingeschränkt zur Verfügung als sie von den Miterben nur gemeinschaftlich beantragt werden kann (§ 2062 1. Hs. BGB). Dabei genügt zur Herbeiführung eines Antrags auch kein Mehrheitsbeschluss. Vielmehr muss der Antrag einvernehmlich durch sämtliche Miterben erfolgen[1067] und wird nach h.M. überdies bereits dann unzulässig, wenn auch nur einer der Miterben unbeschränkt haftet.[1068] Demgegenüber kann die Nachlassinsolvenzverwaltung bei Vorliegen der Voraussetzungen von jedem Miterben einzeln (§ 317 Abs. 2 S. 1 InsO[1069]) sowohl vor als auch nach der Teilung des Nachlasses beantragt werden (§ 316 Abs. 2 InsO). Überdies kann der nicht unbeschränkbar haftende Miterbe nach der Teilung des Nachlasses durch das Aufgebotsverfahren bzw. bei Geltendmachung einer Nachlassverbindlichkeit später als fünf Jahre nach dem Erbfall die Haftung gegenüber den ausgeschlossenen Gläubigern bzw. gegenüber den ihre Verbindlichkeit verspätet geltend machenden Nachlassgläubigern die Haftung durch die Berufung auf die Einreden aus §§ 1973, 1974 BGB beschränken. Darüber hinaus kann er in diesen Fällen, also insbesondere infolge der Durchführung des Aufgebotsverfahrens, gegenüber diesen Gläubigern gemäß § 2060 BGB die Reduzierung der Haftung der Höhe nach von der Gesamtschuld auf eine seiner Erbquote entsprechende Teilschuld bewirken.[1070] Der Vorteil der Umwandlung der gesamtschuldnerischen in teilschuldnerische Haftung kommt im Falle des Aufgebotsverfahrens allen Miterben, also auch solchen zugute, die keinen Antrag auf Durchführung des Aufgebotsverfahrens gestellt haben (§ 460 Abs. 1 S. 1 FamFG). Neben dem gerichtlichen Aufgebotsverfahren (§ 2060 Nr. 1 BGB) eröffnet § 2061 BGB die Möglichkeit der Durchführung eines Privataufgebotsverfahrens, das weniger aufwändig ist, dafür allerdings „lediglich“ zu Gunsten aller Miterben eine Beschränkung der Haftung betreffend die ausgeschlossenen Gläubiger auf eine Teilschuld herbeiführt, also eine Beschränkung der Haftung der Höhe nach, nicht aber bezüglich des haftenden Vermögens.[1071]

[1067] MüKo/*Ann*, BGB, § 2062 Rn. 3; Palandt/*Weidlich*, BGB, § 2062 Rn. 1; Kroiß/Ann/Mayer/*Kick*, BGB, § 2062 Rn. 13.

[1068] MüKo/*Ann*, BGB, § 2062 Rn. 3; Palandt/*Weidlich*, BGB, § 2062 Rn. 1; Kroiß/Ann/Mayer/*Kick*, BGB, § 2062 Rn. 4.

[1069] Die Zulässigkeit des Antrages erfordert die Glaubhaftmachung des Eröffnungsgrundes durch den Miterben.

[1070] Keidel/*Zimmermann*, FamFG, § 460 Rn. 4.

[1071] MüKo/*Ann*, BGB, § 2061 Rn. 6; *Mayer*, MittBayNot 2010, 345 (350).

b. Bewertung der Schutzmöglichkeiten des geltenden Rechts im Hinblick auf einen bestehenden gesetzgeberischen Handlungsbedarf betreffend des „analogen Nachlasses“

(1) Irrtumsanfechtung wegen Irrtums über eine verkehrswesentliche Eigenschaft des Nachlasses (§§ 1954, 119 Abs. 2 BGB)

Die Möglichkeit der Anfechtung der Annahmeerklärung (§ 119 Abs. 2 BGB) mildert die Folgen der Erbschaftsannahme durch die Beantragung eines Erbscheins zum Zwecke der Auskunftserlangung allerdings wesentlich ab, da hierdurch in dem Fall, dass zuvor unbekannte Nachlassverbindlichkeiten nach Ablauf der Ausschlagungsfrist bzw. nach Erbschaftsannahme bekannt werden, die zur Überschuldung des Nachlasses führen, eine Haftung des Erben mit seinem Eigenvermögen verhindert werden kann.

Eine Überschuldung des Nachlasses berechtigt zur Anfechtung gemäß § 119 Abs. 2 BGB, wenn die Erbschaftsannahme durch die Beantragung eines Erbscheins erfolgt ist, der zum Zwecke der Auskunftserlangung über den Nachlassbestand beantragt worden ist, weil der vorläufige Erbe, der in Unkenntnis des Nachlassbestandes einen Erbschein beantragt hat, um den Nachlassbestand zu ermitteln, sich über die Werthaltigkeit des Nachlasses Gedanken gemacht, auf einen Reinerlös vertraut und keine anderweitige Möglichkeit zur Aufklärung des ungewissen Sachverhalts als die Beantragung des Erbscheins hatte.

In dem Fall, dass der Nachlass nicht überschuldet ist, aber mit erheblichen oder sonst für den Erben „lästigen“ Verbindlichkeiten belastet ist, besteht, insbesondere bei Erbengemeinschaften, auch bei verhältnismäßig geringen anteiligen Reinerlöserwartungen, denen im Außenverhältnis erhebliche gesamtschuldnerische Verbindlichkeiten gegenüber stehen, allerdings die Möglichkeit, dass eine Anfechtung gemäß § 119 Abs. 2 BGB keinen Erfolg verspricht, da entweder bereits das Vorliegen eines Anfechtungsgrundes oder aber jedenfalls die Kausalität zwischen Irrtum und Annahmeerklärung mit der Begründung verneint wird, dass es der allgemeinen Lebenserfahrung entspreche, dass man im allgemeinen bei verständiger Würdigung auch kleinere Erbschaften anzunehmen pflege. Ist der Nachlass hingegen überschuldet, so besteht die oben dargestellte Möglichkeit der Anfechtung stets uneingeschränkt.

(2) Haftungsbeschränkungsmöglichkeiten des Alleinerben

Soweit es um die Haftung des Alleinerben geht, ist zudem das System der Erbenhaftung mit seinen verschiedenen Beschränkungsmöglichkeiten und dem Zusammenspiel von materiellem Recht und Prozessrecht (§§ 780, 781 ZPO) zwar unübersichtlich geregelt, letztlich aber so ausgestaltet, dass es den Erben bei sorgfältiger rechtlicher Beratung, deren Einholung ihm mit Rücksicht auf die berechtigten Nachlassgläubigerinteressen zugemutet werden kann, zuverlässig vor einer Haftung für Nachlassverbindlichkeiten mit seinem Eigenvermögen bewahren kann. Auch wenn der Erbe vor der Erbschaftsannahme keine zuverlässige Auskunft über die Zusammensetzung des Nachlasses und etwaige Nachlassverbind-

lichkeiten erlangen kann, geht der Rat der wegen etwaiger Ausschlagungswünsche aufgesuchten Notare häufig dahin, die Erbschaft anzunehmen und den risikoarmen Weg der Beantragung einer Nachlassverwaltung zu gehen, die voraussetzungslos angeordnet wird und gerade bei unübersichtlichen Nachlässen eine geordnete Befriedigung der Nachlassgläubiger unter Vermeidung der Eigenhaftung des Erben ermöglicht.[1072] Alternativ kann der Erbe, wenn er das Verfahren der Nachlassverwaltung zunächst vermeiden will, das kostengünstigere Aufgebotsverfahren wählen, um vor weiteren Schritten Aufschluss darüber zu erlangen, mit welchen Nachlassverbindlichkeiten er rechnen muss.[1073] Ergeben sich Anhaltspunkte für eine Nachlassüberschuldung, steht der Weg zur Einleitung des Nachlassinsolvenzverfahrens, das zur Beschränkung der Erbenhaftung führt, offen. Diese Möglichkeiten bieten auch dem Alleinerben, der sich vor der Erbschaftsannahme keine hinreichenden Informationen über den Nachlassbestand verschaffen konnte, einen hinreichenden Schutz vor der Haftung mit seinem Eigenvermögen. Auch die Notwendigkeit der Bedienung lediglich „lästiger" Verbindlichkeiten wird ihm durch das Verfahren der Nachlassverwaltung bei Bedarf abgenommen. Im Hinblick auf die gesetzlichen Möglichkeiten der Beschränkung der Erbenhaftung besteht mithin in Bezug auf den Alleinerben grundsätzlich kein gesetzgeberischer Handlungsbedarf zur Verbesserung der Auskunftsmöglichkeiten vor der Erbschaftsannahme. Eine etwaige Verschärfung der Problematik durch die Zunahme „digitaler Nachlässe" vermag hieran nichts zu ändern.

(3) Haftungsbeschränkungsmöglichkeiten des Miterben

Für den Miterben sind die Möglichkeiten der Haftungsbeschränkung weniger komfortabel. Er ist nur, sofern er bis zu diesem Zeitpunkt noch nicht unbeschränkbar haftet, bis zur Nachlassteilung vor Zugriffen auf sein Eigenvermögen wegen Nachlassverbindlichkeiten sicher (§ 2059 BGB). Nach der Auseinandersetzung der Erbengemeinschaft droht ihm dagegen eine grundsätzlich gesamtschuldnerische Haftung mit den übrigen Miterben für die gemeinschaftlichen Nachlassverbindlichkeiten (§ 2058 BGB). Wird er insoweit nach der Teilung in voller Höhe alleine in Anspruch genommen, kann er zwar bei den Miterben Rückgriff nehmen. Insoweit trägt er aber ggf. die – bei großen Erbengemeinschaften unter Umständen erhebliche - Last der Beitreibung des Ausgleichsanspruchs sowie das Insolvenzrisiko bezüglich seiner Miterben.[1074] Demgegenüber ist dem Miterben der Weg der Haftungsbeschränkung auf den Nachlass durch Herbeiführung der Anordnung der Nachlassverwaltung erschwert bzw. versperrt, weil er vor der Nachlassteilung hierzu auf die Mitwirkung *aller* Miterben angewiesen ist, was bei mit-

---

[1072] *Lettmann*, Die Beschränkung der Erbenhaftung, RNotZ 2002, 537 (545, 557); *Herzog*, Haftung des Erben für Miet- und WEG-Schulden, NZM 2013, 175 (177).
[1073] *Lettmann*, Die Beschränkung der Erbenhaftung, RNotZ 2002, 537 (557); *Graf*, Möglichkeiten der Haftungsbeschränkung für Nachlaßverbindlichkeiten, ZEV 2000, 125 (131).
[1074] *Mayer*, Teilung bricht Gesamthand − Praktische Fälle der Erbauseinandersetzung, MittBayNot 2010, 345 (350).

wirkungsunwilligen Miterben und großen Erbengemeinschaften ein unüberwindbares Problem darstellen kann und eine Nachlassverwaltung nach Nachlassteilung unzulässig ist (§ 2062 2. Hs. BGB). Demnach bleibt dem Miterben, der den Nachlassbestand vor der Erbschaftsannahme nicht kennt und die Erbschaft nicht ausgeschlagen hat, zur Vermeidung untragbarer Haftungsrisiken für den Nachlass nur die Möglichkeit, vor der Auseinandersetzung der Erbengemeinschaft auf der Durchführung eines gerichtlichen Aufgebotsverfahrens und der Berichtigung aller im Aufgebotsverfahren bekannt gewordenen Nachlassverbindlichkeiten vor der Nachlassteilung zu bestehen, was er wegen §§ 2045, 2046 BGB gegenüber den anderen Miterben auch durchsetzen kann, um ggf. je nach Ergebnis des Aufgebotsverfahrens einen Antrag auf Durchführung eines Nachlassinsolvenzverfahrens zu stellen.[1075] Dies kann den gut beratenen Laien zwar im Ergebnis effektiv vor der Haftung für Nachlassverbindlichkeiten mit seinem Eigenvermögen bewahren (§§ 1973, 1974, 1990, 2060 BGB), ihn allerdings bei einer Vielzahl von Nachlassverbindlichkeiten und Ungewissheit bezüglich des genauen Umfangs des Nachlasses mit erheblichem Prüfungsaufwand belasten. Die Entscheidung darüber, ob der Miterbe sich diesem erheblichen Zeit- und Arbeitsaufwand und den ggf. damit verbundenen Beratungskosten, die unter Umständen in einem deutlichen Missverhältnis zu dem erwartenden Reinnachlass stehen können, aussetzen will, kann der Miterbe, wenn er vor der Erbschaftsannahme keinen hinreichenden Einblick in den Nachlass, die Kontenbewegungen und die Geschäftskorrespondenz des Erblassers nehmen konnte, nicht fundiert treffen. Damit könnte ein Miterbe, der derartige Risiken nicht auszuschließen vermag und sicher vermeiden will, zu einer ggf. vorschnellen Ausschlagung motiviert werden. Dies könnte dafür sprechen, die Haftungssituation des Miterben durch gesetzgeberische Maßnahmen zu verbessern oder Auskunftsansprüche auszuweiten.

c. Bewertung gesetzgeberischen Handlungsbedarfs in Bezug auf den „digitalen Nachlass“

Bei analogen Nachlässen haben die vorläufigen Erben vor der Annahme der Erbschaft vielfach Zugriff auf die Briefpost sowie im Haushalt des Erblassers vorhandene Geschäfts- und Bankunterlagen.[1076] Mit zunehmender Ersetzung der Briefpost durch elektronische Post und zunehmender Verlagerung von Geschäftsaktivitäten auf elektronische „Vertriebskanäle“ wird diese faktische Zugangsmöglichkeit abnehmen.[1077] Stellt man sich den Extremfall eines Erblassers vor, der nur oder ganz überwiegend per elektronischer Post kommuniziert und die

---

[1075] *Mayer*, Teilung bricht Gesamthand − Praktische Fälle der Erbauseinandersetzung, MittBayNot 2010, 345 (351).

[1076] Vgl. zu dem Vergleich betreffend die rechtlichen Zugangsmöglichkeiten zu Briefpost und elektronischer Post: *Gloser*, "Digitale Vorsorge" in der notariellen Praxis, DNotZ 2015, 4 (6); *Solmecke/Köbrich/Schmitt*, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291; *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3749) m. w. N.

[1077] Vgl. *Gloser*, "Digitale Vorsorge" in der notariellen Praxis, DNotZ 2015, 4 (6).

Mehrzahl seiner Geschäftsaktivitäten über elektronische Diensteanbieter und Onlinebanking abwickelt, so entfällt diese Möglichkeit vollständig. Kenntnisse über noch offen stehende per E-Mail übermittelte Rechnungen, noch zu erfüllende Verträge und die Geschäftspartner des Erblassers kann sich der vorläufige Erbe in diesem Fall nur durch Zugang zum digitalen Datenbestand des Erblassers, insbesondere zu seinen E-Mailkonten, verschaffen.[1078] Überdies ist es in diesem Zusammenhang auch ratsam zu prüfen, ob illegale Online-Aktivitäten des Erblassers (wie z. B. illegale Downloads etc.) den Nachlass mit Haftungsrisiken belegen und rasches Handeln (z. B. Löschen rechtswidriger Inhalte auf Websites) nahelegen.[1079] Liegt der Erbfolge dann keine notariell beurkundete Verfügung von Todes wegen zu Grunde, so ist der vorläufige Erbe, der sich einen Überblick über den Nachlassbestand verschaffen will, um eine sachgerechte Entscheidung über die Annahme/Ausschlagung der Erbschaft treffen zu können, nach derzeitiger Rechtslage häufig auf die Beantragung eines Erbscheins und mithin auf die Annahme der Erbschaft angewiesen. Da der vorläufige Erbe bei Erblassern, die ihre Korrespondenz und/oder geschäftliche Aktivitäten ganz oder überwiegend digital abgewickelt haben, auf den Zugang zu den Erblasseraccounts zur Sichtung des Nachlasses angewiesen ist,[1080] könnte dies für einen gesetzgeberischen Handlungsbedarf sprechen.

Dies wird nicht durch die in der kautelarjuristischen Literatur aufgezeigten Vorsorgemöglichkeiten (Stichworte: Vorsorgevollmacht; Auflagen und Vermächtnisse in letztwilligen Verfügungen; Hinterlegung von Passwörtern etc.)[1081] ausgeräumt. Denn einerseits ist die „digitale“ Vorsorge schwierig, da sich stets die Frage stellt, wie Passwörter etc. zu Lebzeiten des Erblassers sicher vor dem Zugriff Dritter (einschließlich etwaiger Vorsorgebevollmächtigter etc.) verwahrt und zugleich hinreichend aktualisiert werden können. Aber selbst wenn man diese Probleme zu lösen vermag, bedarf die „digitale“ Vorsorge, auf die der Erbe ja keinen Einfluss nehmen kann, die aber letztlich in seinem Interesse erfolgt, eines Erblassers, der hierzu bereit ist. Da dies gesetzgeberisch nicht gewährleistet wer-

---

[1078] *Brinkert/Stolze/Heidrich*, Der Tod und das soziale Netzwerk, ZD 2013, 153 (154); *Klas/Möhrke-Sobolewski*, Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3474); *Gloser*, „Digitale Erblasser" und "digitale Vorsorgefälle" - Herausforderungen der Online-Welt in der notariellen Praxis − Teil I, MittBayNot 2016, 12 (14).

[1079] *Deusch*, Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2 (7 f.).

[1080] *Deusch*, Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2 (7 f.); *Gloser*, „Digitale Erblasser" und "digitale Vorsorgefälle" − Herausforderungen der Online-Welt in der notariellen Praxis − Teil II, MittBayNot 2016, 101 (108).

[1081] *Brinkert/Stolze/Heidrich*, Der Tod und das soziale Netzwerk, ZD 2013, 153 (156 f.); *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (265 f.); *Gloser*, "Digitale Vorsorge" in der notariellen Praxis, DNotZ 2015, 4; *ders.*, „Digitale Erblasser" und "digitale Vorsorgefälle" − Herausforderungen der Online-Welt in der notariellen Praxis − Teil II, MittBayNot 2016, 101 (104 ff.).

den kann, ist „digitale“ Vorsorge zwar wichtig und unterstützenswert, aber letztlich nicht dazu geeignet, die sich für den Miterben stellenden Probleme umfassend zu lösen.

d. Gesamtbewertung/Fazit

Gesetzgeberischer Handlungsbedarf besteht jedenfalls nicht für Alleinerben, denn dort ist das System der Erbenhaftung, wie oben ausgeführt, bereits unabhängig von der Möglichkeit der Anfechtung einer Erbschaftsannahme so ausgestaltet, dass es den Erben zuverlässig vor einer Haftung für Nachlassverbindlichkeiten bewahren kann.

Allein in Bezug auf Miterben könnte daher gesetzgeberischer Handlungsbedarf erwogen werden. Insoweit käme zum einen die Stärkung der Rechtsposition des vorläufigen Erben vor Erbschaftsannahme in Betracht, insbesondere die Verlängerung der Ausschlagungsfrist des § 1944 Abs. 1 BGB und die Stärkung der Auskunftsrechte vorläufiger Erben.[1082] Allerdings würde die Schaffung gesetzlicher Informationsrechte vor der Erbschaftsannahme einen besonders weitreichenden Eingriff in das bestehende System des BGB darstellen. Im Übrigen hätte diese Lösung den Nachteil, dass sie auch zu Gunsten des Alleinerben eingreifen würde, für den aber, wie dargelegt, bereits vom Ansatz her kein gesetzgeberischer Handlungsbedarf besteht.

Vor diesem Hintergrund könnte an Lösungen gedacht werden, die bei den Haftungserleichterungen für Miterben ansetzen. Denkbar erschiene insoweit eine Änderung des § 2062 BGB, wobei in Betracht kommen könnte, jedem Miterben ein selbständiges Recht auf Beantragung der Nachlassverwaltung zuzubilligen. Es bestünde auch die Möglichkeit, gesetzlich zu regeln, dass die Anordnung der Nachlassverwaltung so lange zulässig bleibt, wie nicht alle Miterben unbeschränkt haften. Zudem könnte die Anordnung der Nachlassverwaltung auch noch für die Zeit nach der Nachlassteilung gesetzlich zugelassen werden.

Letztlich dürften aber die derzeit bestehenden Möglichkeiten der Anfechtung wegen Irrtums über eine verkehrswesentliche Eigenschaft des Nachlasses (§§ 1954, 119 Abs. 2 BGB) in Kombination mit der Möglichkeit, zur Vermeidung von Haftungsrisiken vor der Auseinandersetzung der Erbengemeinschaft auf der Durchführung eines gerichtlichen Aufgebotsverfahrens und der Berichtigung aller dort bekannt gewordenen Verbindlichkeiten zu bestehen, auch den Miterben so effek-

---

[1082] Diesen auf *Röthel* (*Röthel*, Gutachten A zum 68. Deutschen Juristentag Berlin 2010, A 48 und A 108) und *Mayer* (*Mayer*, Referat zum 68. Deutschen Juristentag Berlin 2010, L 121 sowie L 122 f.) zurückgehenden Forderungen beim 68. Deutschen Juristentag in Berlin hat der Deutsche Juristentag damals zugestimmt, vgl.
http://www.djt.de/fileadmin/downloads/68/68_djt_beschluesse.pdf (angenommen mit 63:9:5) sowie
http://www.djt.de/fileadmin/downloads/68/68_djt_beschluesse.pdf (angenommen mit 59:7:9).

tiv vor einer Haftung mit seinem Eigenvermögen bewahren, dass im Ergebnis gesetzgeberischer Handlungsbedarf bei der Haftung der Miterben auch im Hinblick auf den „digitalen Nachlass“ nicht anzunehmen ist.

Insoweit sollte aber die weitere Entwicklung beobachtet werden. Sollten künftig verstärkt Fälle von Haftungsproblemen von Miterben im Zusammenhang mit digitalen Nachlässen auftreten, könnte eine Stärkung der Rechte der Miterben durch Schaffung von Auskunftsrechten und Verlängerung der Ausschlagungsfrist oder durch Reform von § 2062 BGB mit den oben genannten Möglichkeiten der Haftungserleichterungen erwogen werden. Derzeit erscheint dies aber nicht erforderlich.

V. Themenkreis postmortales Persönlichkeitsrecht (Recht der Angehörigen, Zugriffe auf persönliche Daten des Verstorbenen zu verhindern)

1. Fragestellungen

Zum Themenkreis postmortales Persönlichkeitsrecht wurden folgende Fragestellungen aufgeworfen:

- Sollten die Angehörigen (nicht die Erben) ein Recht auf wenigstens vorläufige Sperrung eines Social-Media-Accounts haben, um Zugriff auf persönliche Daten des Verstorbenen zu verhindern?
- Steht das Recht auf Entscheidung über die „digitale Bestattung“ den Erben oder den Angehörigen zu (vgl. § 1968 BGB)?

2. Diskussionsstand

Letztlich handelt es sich bei diesen Fragestellungen um dieselbe Problematik wie bei E-Mail-Accounts bezüglich der Frage, ob diese den Erben oder den nächsten Angehörigen zustehen. Zwar handelt es sich bei einem Social-Media-Account um eine Form des Accounts, der oft dadurch geprägt ist, dass persönliche Daten ausgetauscht werden, sodass der Aspekt der „privaten Daten“ hier stärker ausgeprägt ist. Indes gibt es auch Social-Media-Accounts, die eher geschäftliche Kontakte betreffen (etwa Xing).

Der Diskussionsstand über die Frage, ob der Zugriff auf E-Mails des Erblassers den Erben oder den nächsten Angehörigen zusteht, ist damit tendenziell auf die vorliegende Frage bezüglich Social-Media-Accounts übertragbar, zumal die Diskussion oft anhand des Beispiels der E-Mail-Konten geführt wird, regelmäßig aber in dieser Diskussion offen als Frage des Zugriffsrechts/der Zuordnung von Accounts/Accountdaten aller Arten bezeichnet wird: So benennen *Steiner/Holzer*[1083] gerade auch soziale Netzwerke als Beispiel. *Solmecke/Köbrich/Schmitt*

[1083] *Steiner/Holzer,* Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263).

bezeichnen das E-Mail-Konto ausdrücklich nur als Beispiel.[1084] *Herzog, Pruns* und *Kutscher* sprechen allgemein von Daten oder verwenden den Begriff „Accountdaten" als Oberbegriff.[1085] Explizit zu Social-Media-Accounts haben sich *Brinkert/Stolze/Heidrich* geäußert und insoweit die Meinung vertreten, dass ein uneingeschränkter Zugriff der Erben auf alle Inhalte eines Accounts abzulehnen sei.[1086] Auch *Seidler* beschäftigt sich ausführlich mit dem postmortalen Schicksal sozialer Netzwerke. Sie kommt dabei indes unter Verweis auf ihre Ausführungen zu den E-Mail-Accounts zu dem Ergebnis, dass sowohl die Kontoinhaberschaft, als auch das Einsichtsrecht mangels Höchstpersönlichkeit auf den Erben übergehen und die Rechtspositionen eines verstorbenen Nutzers uneingeschränkt zum Nachlass zählen.[1087]

Allgemein zu der Frage, ob Ansprüche aus Providerverträgen betreffend soziale Netzwerke wie Facebook, Twitter etc. auf die Erben übergehen, finden sich einige Quellen in der Literatur. Der *DAV* geht davon aus, dass Ansprüche auf Löschung von Daten auf Homepages, Facebook und Twitter vererblich sind, da auch diese mit dem Vertragsverhältnis auf die Erben übergehen.[1088] Auch *Steiner/Holzer* vertreten, dass vertragliche Rechte und Pflichten aus Online-Beziehungen jeder Art auf die Erben übergehen, namentlich die Beziehungen zu sozialen Netzwerken wie Facebook oder Twitter sowie Cloud-Anbietern. Insoweit bestehe ein Kündigungsrecht, ein Recht darauf, das Profil samt Inhalten sperren bzw. löschen zu lassen (sofern keine abweichende Verfügung des Erblassers existiert), ein Anspruch auf Zugang zum Konto und Herausgabe der dort gespeicherten Inhalte und ein Anspruch auf Auskunft über die Vertragsdaten.[1089] *Brinkert/Stolze/Heidrich* gehen (unter Hinweis darauf, dass insoweit auch Auftragsrecht im Hinblick auf teilweise vertretene Unentgeltlichkeit der Verträge vertreten wird) von typengemischten Verträgen mit überwiegend dienst-, miet- und werkvertraglichen Elementen aus.[1090] Sie nehmen (wie *Hoeren* und *Martini* bezüglich E-Mails) wegen des postmortalen Persönlichkeitsrechts ein Erbrecht und ein Zugriffsrecht der Erben nur bezüglich vermögensrechtlicher Positionen an, nicht aber bezüglich persönlicher/privater Inhalte.[1091] Bei *Kutscher* findet sich ein Aufriss zum Streitstand, ob es sich bei den sozialen Netzwerken um entgeltliche Verträge (eigener

---

[1084] *Solmecke/Köbrich/Schmitt,* Der digitale Nachlass – haben Erben einen Auskunftsanspruch? – Überblick über den rechtssicheren Umgang mit den Daten von Verstorbenen, MMR 2015, 291 (291).

[1085] *Herzog,* Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3747 ff.); *Pruns,* Keine Angst vor dem digitalen Nachlass! Erbrechtliche Grundlagen – Alte Probleme in einem neuen Gewand?, NWB 2013, 3161 (3166); *Kutscher* (Diss.), S. 102 ff.

[1086] *Brinkert/Stolze/Heidrich,* Der Tod und das soziale Netzwerk, ZD 2013, 153 (155).

[1087] *Seidler* (Diss.), S. 126-139.

[1088] *DAV,* Stellungnahme Nr. 34/2013, S. 55 f.; ebenso *Herzog,* Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750).

[1089] *Steiner/Holzer,* Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263).

[1090] *Brinkert/Stolze/Heidrich,* Der Tod und das soziale Netzwerk, ZD 2013, 153 (154).

[1091] *Brinkert/Stolze/Heidrich,* Der Tod und das soziale Netzwerk, ZD 2013, 153 (155 f.).

Art oder typengemischte Verträge) oder unentgeltliche Verträge (Auftragsrecht mangels Entgeltlichkeit) handelt, wobei die Frage diskutiert wird, ob die Einräumung der Nutzung personenbezogener Daten zu Werbezwecken dazu führt, dass synallagmatische Verträge vorliegen (was *Kutscher* mit der Begründung eines Bezahlens mit personenbezogenen Daten und der Einwilligung, während der Nutzung Werbung eingeblendet zu bekommen bejaht).[1092] *Klas/Möhrke-Sobolewski* vertreten den Standpunkt, dass es sich bei Verträgen zwischen sozialen Netzwerken und ihren Mitgliedern um Schuldverhältnisse mit überwiegendem Personenbezug handeln dürfte, sodass sie nicht vererblich seien.[1093]

Konkret zu der Frage, ob das Recht auf Entscheidung über die „digitale Bestattung" den Erben oder den Angehörigen zusteht, findet sich soweit ersichtlich in der Literatur nichts.

3. Stellungnahme

Die Gründe, die im Rahmen der Beurteilung von E-Mail-Accounts dazu führen, dass der Erbe umfassend in die Rechtsposition des Erblassers eintritt und die nächsten Angehörigen nur Abwehrrechte aus dem postmortalen Persönlichkeitsrecht bei Menschenwürdeverletzungen für den Erblasser geltend machen können, gelten auch für Social-Media-Accounts. Diese mögen zwar regelmäßig stärkeren Bezug zu privaten Umständen des Erblassers haben. Dennoch muss hier aus den bereits ausgeführten Gründen de lege lata (umfassende Rechtsstellung der Erben nach dem deutschen Erbrecht, nur Abwehrrecht der nächsten Angehörigen treuhänderisch für den Erblasser bei Menschenwürdeverletzungen, faktische Undurchführbarkeit einer Trennung zwischen vermögensbezogenen und persönlichen Daten) ein Anspruch der nächsten Angehörigen auf Löschung ausscheiden. Ein solcher Anspruch würde lediglich den Erben zustehen. Die insoweit für diese Rechtsverhältnisse von *Brinkert/Stolze/Heidrich* vertretene Ansicht, dass eine entsprechende Differenzierung vorzunehmen wäre[1094], ist aus den genannten Gründen abzulehnen. Vielmehr tritt allein der Erbe in die Rechtsbeziehung zu dem Anbieter ein, sodass ihm die Rechte aus dieser Vertragsbeziehung zustehen.[1095] Soweit *Klas/Möhrke-Sobolewski* vertreten, dass eine Vererblichkeit wegen des Personenbezugs nicht gegeben ist,[1096] erscheint dies fraglich, da der Vertrag als solcher keinen besonderen persönlichen Zuschnitt aufweisen dürfte.

[1092] *Kutscher* (Diss.), S. 45/46; zur vertragsrechtlichen Einordnung von „Daten als Entgelt" siehe Kapitel 3, Abschnitt G.

[1093] *Klas/Möhrke-Sobolewski,* Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3474).

[1094] *Brinkert/Stolze/Heidrich,* Der Tod und das soziale Netzwerk, ZD 2013, 153 (155 f.).

[1095] Ebenso wie hier der *DAV,* Stellungnahme Nr. 34/2013, S. 55 f., *Herzog,* Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750); *Steiner/Holzer,* Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263).

[1096] *Klas/Möhrke-Sobolewski,* Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3474).

Die Vertragsbeziehung als solche dürfte aber für die Frage der Vererbbarkeit maßgeblich sein, sodass mit der ganz überwiegenden Ansicht in der Literatur von einer Vererbbarkeit auszugehen ist.

Auch de lege ferenda wäre ein solcher Anspruch der Angehörigen nicht sinnvoll. Wenn der Erblasser gerade nicht seine nächsten Angehörigen als Erben eingesetzt hat (die aber gesetzliche Erben gewesen wären), sondern Dritte, dann ist dies jedenfalls ein Indiz hinsichtlich des Verhältnisses zu den nächsten Angehörigen. Ihnen dann Löschungsrechte bezüglich Accounts gleich welcher Art des Erblassers zuzuerkennen, erscheint jedenfalls auf den ersten Blick bedenklich. Zudem würde ein solcher Anspruch mit dem Erbrecht der Erben kollidieren, in das eingegriffen würde (ggf. könnten auch für den Erben relevante Daten dabei verloren gehen). All dies spricht deutlich dagegen, dass die nächsten Angehörigen einen solchen Anspruch haben sollten. Die bloße Sperrung des Accounts würde auch nicht bedeuten, dass die Angehörigen ein Recht auf Zugang zu persönlichen Daten hätten. Es träte vielmehr eine Art Stillstand ein, da die nächsten Angehörigen die Rechte der Erben blockiert hätten. Auch für eine vorläufige Sperrung durch die nächsten Angehörigen ist kein praktisches Bedürfnis ersichtlich. Eine solche Sperrung würde dem Erben vorübergehend den Zugang zu sämtlichen Inhalten (auch den vermögensrelevanten) verwehren, was im Hinblick auf die kurze Ausschlagungsfrist von sechs Wochen fragwürdig erscheint und auf der anderen Seite den nächsten Angehörigen nichts bringen würde (denn sie hätten damit weder Zugriff, noch die Möglichkeit endgültiger Löschung).

Hinsichtlich der Frage, ob das Recht auf Entscheidung über die „digitale Bestattung“ den Erben oder den Angehörigen zusteht, muss zunächst geklärt werden, was eigentlich unter „digitaler Bestattung“ zu verstehen ist.

Hierbei geht es nicht um das Recht der Totenfürsorge (privatrechtliches Recht nichtvermögensrechtlicher Art, das Entscheidungen über die Art der Bestattung, den Ort der letzten Ruhestätte, das Grabmal, eine eventuelle Umbettung oder Exhumierung betrifft).[1097] Vielmehr geht es bei dieser Fragestellung um das Recht, die Löschung sämtlicher im Rahmen der Nutzung des Internets hinterlassener (persönlicher und geschäftlicher) Daten zu beantragen und durchzuführen. Die begriffliche Parallele zur Bestattung des Leichnams des Betroffenen mit der Regelung der Kostentragung für die Beerdigung in § 1968 BGB und zum Recht der Totenfürsorge führt daher nicht zu einer inhaltlichen Parallele.

Damit geht es in der Sache bei der Frage der „digitalen Bestattung“ faktisch lediglich um die Rechte an den Verträgen mit den Providern. De lege lata sind diese recht eindeutig ausschließlich den Erben zugewiesen (s. o.). Die Rechte und Pflichten aus diesen Vertragsverhältnissen, zu denen gerade auch das Recht der Kündigung des Vertrages und der Löschung von Inhalten gehört, unterliegen der Universalsukzession nach § 1922 BGB. Insoweit gelten hier die gleichen Erwägungen wie zur Frage der Vererblichkeit eines E-Mail-Accounts und sonstiger

---

[1097] Vgl. *DAV,* Stellungnahme Nr. 34/2013, S. 39 f.

Accounts (s. o.). Daraus folgt, dass das geltende Recht die Entscheidung über die „digitale Bestattung“ gerade nicht den Angehörigen zuweist, sondern den Erben, die in die Verträge eintreten.

Auch de lege ferenda besteht eher kein Bedürfnis dafür, die „digitale Bestattung“ in Form von Sonderregelungen – etwa analog zu den Vorschriften über die Bestattung des Leichnams – auszugestalten. Eine derartige Zuordnung würde entweder den Erben gerade die Rechte entziehen, die ihnen eigentlich gem. § 1922 BGB (Universalsukzession) zustehen oder bei Aufteilung der Rechte die Probleme der „Splittung“ des Zugriffsrechts auf Accountdaten wieder auf den Tisch bringen. Zudem gilt auch hier der bereits soeben angeführte Gedanke, dass die Erbeinsetzung gerade anderer als der nächsten Angehörigen jedenfalls ein Indiz dafür sein kann, dass das Verhältnis des Erblassers zu letzteren problematisch gewesen sein könnte, was dagegen spricht, ihnen weitgehende Rechte im Hinblick auf Daten des Erblassers zuzuerkennen.

VI. Themenkreis „Vererbbarkeit einer Website des Verstorbenen“

1. Fragestellung

Im Verlauf der Bearbeitung ist die Frage aufgekommen, ob eine Website des Verstorbenen vererblich ist.

2. Diskussionsstand

Nach Ansicht des *DAV* ist das Nutzungsrecht an einer Domain insoweit vererblich als der Erbe in das Schuldverhältnis des Erblassers mit der Deutsches Netzwerk Information Center e.G. (DENIC e.G.) eintritt.[1098] Ähnlich vererblich ist danach ein Anspruch auf Löschung von Daten auf Homepages, da auch diese mit dem Vertragsverhältnis auf Erben übergehen.[1099] Nach Ansicht von *Hoeren*, der sich hiermit ausführlicher als der *DAV* beschäftigt, geht die Inhaberschaft und damit das Nutzungsrecht an einer Domain auf den Erben über, da es eine eigentumsfähige Position darstelle (rechtlich geschützten Vermögenswert, damit vererbbar), die aus dem Vertragsschluss mit der DENIC e.G. folge. Der Erbe trete auch in das Rechtsverhältnis mit der DENIC e.G. ein. Die Stellung als administrativer Kontakt (admin-c) ist nicht vererblich. Der Erbe kann die Domain weiter betreiben oder kündigen.[1100] *Hoeren* verweist bezüglich des Übergangs einer Website auf verschiedene rechtliche Probleme: Bei Änderungen der Website sind §§ 14, 23 UrhG zu beachten (kann unberechtigte Entstellung/ Bearbeitung/ Umgestaltung darstellen). Wenn das Urheberrecht an der Website dem Erblasser zustand, geht

---

[1098] *DAV*, Stellungnahme Nr. 34/2013, S. 48 f.; ebenso *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750).
[1099] *DAV*, Stellungnahme Nr. 34/2013, S. 55 f.
[1100] *Hoeren*, Der Tod und das Internet - Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers, NJW 2005, 2113 (2115 f.); ebenso: *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (263).

dies auf Erben über (§ 28 UrhG); Impressumspflicht, § 6 TDG, binnen sechs Wochen nach Todesfall ist Impressum zu ändern (Verletzung der Änderungspflicht ist Ordnungswidrigkeit § 12 TDG). *Martini* ist der Ansicht, dass auch bei öffentlich verfügbaren personenbezogenen Daten wie denen einer eigenen Homepage oder eines Internet-Blogs die Angehören das datenschutzrechtliche Totenfürsorgerecht wahrnähmen und die Vererbbarkeit der Rechtspositionen ausgeschlossen sei.[1101]

3. Stellungnahme

Insoweit gelten grundsätzlich zunächst die gleichen Ausgangspunkte wie bei den oben behandelten E-Mail-Accounts und auch den Accounts sozialer Netzwerke. Eine Trennung zwischen persönlichen und sonstigen Inhalten (wie sie *Martini* vorschlägt) ist auch hier nicht vorzunehmen. Auch insoweit ist wiederum der Ansatzpunkt des *DAV*[1102] zutreffend, dass das Nutzungsrecht an einer Domain insoweit vererblich ist, als der Erbe in das Schuldverhältnis des Erblassers mit der DENIC e.G. eintritt. Insoweit dürfte (vergleichbar mit dem Girovertrag, wie hier auch bezüglich E-Mail-Providerverträgen vertreten) bei Fortführung ein eigener Vertrag mit der DENIC e.G. zustande kommen. Aus den zutreffenden Hinweisen von *Hoeren*[1103] bezüglich des Umstandes, dass etwaige Urheberrechte Dritter und die Impressumspflicht beachtet werden müssen, ergibt sich kein gesetzgeberischer Handlungsbedarf. Es gelten die gleichen Erwägungen wie bei E-Mails mit dem Unterschied, dass hier in der Regel keine Passwortproblematik bestehen dürfte und die Dringlichkeit des Zugriffs geringer ist.

VII. Themenkreis Vererbbarkeit von Nutzungsrechten bei E-Books, Musik- und Video-Downloads

1. Fragestellung

Die Arbeitsgruppe hat sich ausführlich mit der Frage auseinandergesetzt, ob Nutzungsrechte wie etwa bei E-Books, Musik- und Video-Downloads vererblich sind und inwieweit dies durch vertragliche (insbesondere AGB-) Regelungen eingeschränkt werden kann. In diesem Zusammenhang spielen urheberrechtliche Fragen (insbesondere die Frage des Eingreifens des sog. „Erschöpfungsgrundsatzes“) eine wichtige Rolle. Insoweit hat sich die Arbeitsgruppe insbesondere gefragt, ob eine gesetzliche Regelung angezeigt ist, die in jedem Fall die Vererblichkeit derartiger Nutzungsrechte sicherstellt.

2. Diskussionsstand

In erster Linie wird die Problematik der Übertragung von Nutzungsrechten im Hinblick auf die Frage der Übertragbarkeit von Nutzungsrechten unter Lebenden

---

[1101] *Martini,* Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1153 f.).
[1102] *DAV,* Stellungnahme Nr. 34/2013, S. 48 f..
[1103] *Hoeren,* Der Tod und das Internet - Rechtliche Fragen zur Verwendung von E-Mail- und WWW-Accounts nach dem Tode des Inhabers, NJW 2005, 2113 (2115 f.).

diskutiert. Bei dieser Frage handelt es sich vom Ansatz her um eine urheberrechtliche Problematik. Insoweit geht es um die urheberrechtliche Frage der „Erschöpfung“, wonach der Erwerber eines körperlichen Werkstücks dieses zustimmungsfrei auf einen Dritten übertragen kann. In allgemeinen Geschäftsbedingungen der Anbieter von E-Books oder Musik-Downloads ist z.T. vorgesehen, dass das Nutzungsrecht nicht übertragbar ist. Deutsche Gerichte hatten zu prüfen, ob dies gegen die Generalklausel des § 307 BGB verstößt. Ein zentrales Argument für das Vorliegen eines solchen Verstoßes wäre, wenn der Erschöpfungsgrundsatz (§ 17 Abs. 2 UrhG) nicht nur für den Erwerb von körperlichen Werkstücken, sondern auch für den Erwerb von Nutzungsrechten in digitaler Form gelten würde. In diesem Fall würde die Zweifelsregelung des § 307 Abs. 2 Nr. 1 BGB eingreifen, da dann entsprechende allgemeine Geschäftsbedingungen mit dem wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht vereinbar wären. Greift der Erschöpfungsgrundsatz im Hinblick auf digitale Erwerbsformen hingegen nicht, fällt dieses zentrale Argument für einen Verstoß gegen die Generalklausel des § 307 BGB weg. In diesem Zusammenhang existiert ein Grundsatzurteil des EuGH für Computerprogramme, wonach für diese der Erschöpfungsgrundsatz auch gilt, wenn sie via Internet-Download veräußert wurden.[1104] Die Instanzenrechtsprechung in Deutschland lehnt eine Übertragung dieser Entscheidung auf andere Werkformen (wie Musik-Downloads oder E-Books) allerdings ab und gelangt so zu einer Wirksamkeit entsprechender allgemeiner Geschäftsbedingungen, die eine Übertragbarkeit ausschließen.[1105] Die Ablehnung der Anwendung des Urteils des EuGH („Used-Soft“) auf andere Werkformen wird damit begründet, dass sich diese Entscheidung ausdrücklich und ausschließlich auf das Verbreitungsrecht nach § 69d Abs. 1 UrhG und die dem zugrunde liegende gemeinschaftsrechtliche Bestimmung in Art. 4 Abs. 2 der Richtlinie 2009/24/EG beziehe, die speziell den Schutz von Computerprogrammen betreffe und im Verhältnis zur Richtlinie 2001/29/EG (InfoSoc Richtlinie) lex specialis sei; zudem wird auf die ausdrückliche Argumentation in dem Urteil des EuGH selbst hingewiesen.[1106] Auch in der Literatur wird die Anwendung des Erschöpfungsgrundsatzes auf E-Books, den Download von Musikdateien/Filmen oder den

---

[1104] EuGH, Urt. v. 3.7.2012, NJW 2012, 2565 (2568) Rn. 72 (UsedSoft).

[1105] Vgl. etwa grundlegend und ausführlich: OLG Hamm, Urt. v. 15.5.2014 – I-22 U 60/13, ZUM 2014, 715 ff. (juris, dort Rn. 39 ff., insbes. Rn. 45 ff., zur o. g. Rechtsprechung des EuGH Rn. 107 ff., insbes. Rn. 121 ff.; OLG Hamburg, Beschl. v. 4.12.2014 – 10 U 5/11, CR 2015, 534 (535 f.) m. w. N. mit ausdrücklicher Auseinandersetzung mit der o. g. Rechtsprechung des EuGH; LG Bielefeld Urt. v. 5.3.2013 – 4 O 191/11, juris Rn. 62 ff. m. w. N. aus der obergerichtlichen Rechtsprechung in Rn. 67, explizit zum EuGH Rn. 75 ff.; weitere Nachweise auch bei *Steiner/Holzer,* Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 ff. Fn 34 und 35.

[1106] OLG Hamburg, Beschl. v. 4.12.2014 – 10 U 5/11, CR 2015, 534 (535) unter Verweis auf Rn. 56 und 60 des o. g. EuGH-Urteils, ausführlich OLG Hamm, Urt. v. 15.5.2014 – I-22 U 60/13, juris Rn. 107 ff.

Online-Vertrieb von Computerspielen überwiegend abgelehnt,[1107] teilweise aber auch befürwortet.[1108]

Ein wesentliches Argument, das gegen eine (analoge) Anwendung des Erschöpfungsgrundsatzes auf Nutzungsrechte angeführt wird, ist das Risiko eines unkontrollierbaren Sekundärmarktes aufgrund der Gefahr rechtswidriger Mehrfachübertragungen ohne die erforderliche Löschung beim Ersterwerber.[1109] Die von der obergerichtlichen Rechtsprechung konstatierten häufig geringen Preisunterschiede zwischen dem Erwerb einer körperlichen Werkkopie und einem digitalen Produkt begründen hingegen nach Ansicht dieser Gerichte keine den Vertragszweck mitbestimmende Erwartung.[1110]

Rechtspolitisch wird de lege ferenda zum Teil die Forderung erhoben, das Urheberrecht zu ändern und die Übertragbarkeit unter Lebenden zu gewährleisten.[1111] In diesem Zusammenhang wird auf die bereits derzeit bestehenden technischen Schutzmöglichkeiten vor unkontrollierbaren Vervielfältigungen hingewiesen.[1112]

Diese Erwägungen betreffen indes die Frage der Übertragung unter Lebenden und nicht die Frage der Vererblichkeit. In der Literatur, die sich mit Fragen des digitalen Nachlasses beschäftigt, wird dieses Thema nur von wenigen und auch nur sehr knapp behandelt.

Herzog vertritt insoweit recht apodiktisch die Ansicht, dass auch Lizenzverträge und sonstige Nutzungsrechte des Erben an Programmen oder Ähnlichem nach § 1922 BGB mit übergehen,[1113] ohne allerdings auf die Fragestellungen im Hinblick auf den Erschöpfungsgrundsatz einzugehen. Auch *Kutscher* erörtert die

---

[1107] Dreier/*Schulze*, UrhG, § 17 Rn. 30 m. w. N.; zahlreiche Literaturnachweise auch bei Wandtke/Bullinger/*Heema*, UrhG, § 17 Rn. 27, der selbst eine differenzierte Ansicht vertritt, wonach der Erschöpfungsgrundsatz zwar nicht per se gilt, aber die körperliche Weitergabe desselben Werkstücks auch bei Online erworbenen Daten möglich ist, wenn die Festplatte des Computers oder das sonstige Speichermedium veräußert wird (Rn. 28).

[1108] Vgl. etwa BeckOGK/*Mössner*, BGB, § 90 Rn. 90 m. w. N. und mit umfangreichen Nachweisen zum Streitstand in Literatur und Rechtsprechung in Fn. 635; differenzierend: Wandtke/Bullinger/*Heema*, UrhG, § 17 Rn. 28.

[1109] Vgl. *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 265 mit Nachweisen in Fn. 39; OLG Hamburg, Beschl. v. 4.12.2014 – 10 U 5/11, CR 2015, 534 (535 f.); *Kreutzer*, Weiterveräußerungsfähigkeit von digitalen Gütern (Studie im Auftrag des Ministeriums für ländlichen Raum und Verbraucherschutz des Landes Baden-Württemberg), zitiert dies als eines der Hauptargumente, S. 35 f.

[1110] OLG Hamm, Urt. v. 15.5.2014 – I-22 U 60/13, juris Rn. 133; ebenso OLG Hamburg, Beschl. v. 4.12.2014 – 10 U 5/11, CR 2015, 534 (536 f.).

[1111] *Kreutzer*, Weiterveräußerungsfähigkeit von digitalen Gütern (Studie im Auftrag des Ministeriums für ländlichen Raum und Verbraucherschutz des Landes Baden-Württemberg), S. 65 ff.

[1112] *Keutzer*, Weiterveräußerungsfähigkeit von digitalen Gütern (Studie im Auftrag des Ministeriums für ländlichen Raum und Verbraucherschutz des Landes Baden-Württemberg), S. 50 f., 57 ff.

[1113] *Herzog*, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750).

Problematik der Nutzungsrechte. Sie ordnet Nutzungen, die lediglich zum Abruf im Internet zur Verfügung gestellt werden (E-Books, Streaming, Video- und Audio-on-Demand), z. T. als Kaufverträge mit lizenzrechtlichem Einschlag ein; bei Anlegen eines Accounts als gemischter Vertrag sui generis mit dienst-, werk- und mietvertraglichen Elementen.[1114] Sie konstatiert, dass aufgrund des weiten Vermögensbegriffs des § 1922 BGB im Zweifel Vererblichkeit bejaht werden müsse; gerade Musik-Accounts und E-Books hätten ggf. großen wirtschaftlichen Wert, sodass man sie als Bestandteile des Vermögens ansehen müsse.[1115] Allerdings hält sie AGB-rechtlich die Deaktivierung des Accounts nach gewisser Inaktivitätszeit für zulässig, wenn die Frist nicht zu kurz bemessen und der Nutzer informiert worden sei, da andernfalls der Provider der Vielzahl an digitalen „Müllaccounts" kaum noch Herr werden könne.[1116] *Steiner/Holzer* stellen den Streitstand im Hinblick auf die Geltung des urheberrechtlichen Erschöpfungsgrundsatzes bezüglich Übertragungen unter Lebenden dar[1117] und erläutern den Zusammenhang der Geltung des Erschöpfungsgrundsatzes für die Möglichkeit des vertraglichen Ausschlusses der Vererbbarkeit (bei Nichtgeltung des Erschöpfungsgrundsatzes mögliche zeitliche Befristung der Übertragung des Nutzungsrechts).[1118] Zu einem eindeutigen Ergebnis kommen sie nicht. Sie konstatieren, dass sich darüber streiten lasse, ob Regelungen in allgemeinen Geschäftsbedingungen die Vererbbarkeit des Nutzungsrechts tatsächlich wirksam ausschließen würden. Mit dem Weiterverkauf oder einer sonstigen Übertragung an Dritte könne das Vererben eines Nutzungsrechts wohl auf jeden Fall nicht gleichgesetzt werden, da das zentrale Argument gegen die Erschöpfungswirkung, die Gefahr eines unkontrollierbaren Sekundärmarktes, für digitale Werkexemplare bei einer Übertragung an den Rechtsnachfolger des Erstnutzers nicht gegeben sei.[1119] Rechtsprechung zu dieser speziellen Frage existiert, soweit ersichtlich, nicht.

Auch in diesem Zusammenhang ist die dargestellte Problematik der Geltung des urheberrechtlichen Erschöpfungsgrundsatzes von erheblicher Bedeutung. Für im Nachlass enthaltene Nutzungsrechte gilt zwar, dass sie grundsätzlich ohne Zustimmung des Rechteinhabers vererbbar sind, da § 34 UrhG nur die Übertragung unter Lebenden regelt – allerdings kann die Vererbbarkeit vertraglich ausgeschlossen werden, so wie auch der Anbieter das Nutzungsrecht insgesamt zeitlich begrenzen kann (§ 31 Abs. 1 S. 2 UrhG).[1120] De lege lata ist damit der vertragliche Ausschluss der Vererbbarkeit möglich, da er eine Befristung der Übertragung des

---

[1114] *Kutscher* (Diss.), S. 55 f..
[1115] *Kutscher* (Diss.), S. 55 f. (vertragsrechtliche Einordnung), S. 120 f. sowie S. 127 f. (Inhaltskontrolle von AGB).
[1116] *Kutscher* (Diss.), S. 127 f..
[1117] *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (264 f.).
[1118] *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (265).
[1119] *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (265).
[1120] Vgl. *Steiner/Holzer*, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (265).

Nutzungsrechts auf Lebenszeit im Sinne einer Begrenzung gem. § 31 Abs. 1 S. 2 UrhG bedeuten würde.

Auch ein Urteil des EuGH aufgrund eines Vorlageverfahrens aus den Niederlanden (Vereniging Openbare Bibliotheken), bei dem es um diverse Vorlagefragen ging, die die Geltung des Erschöpfungsgrundsatzes im Hinblick auf urheberrechtlich geschützte digitale Bücher betreffen, hat die Frage der Anwendbarkeit des Erschöpfungsgrundsatzes auf digitale Kopien nicht endgültig geklärt. Die Vorlagefragen betrafen in erster Linie Fragen des Verleihens digitaler Kopien eines Werkes und insofern die Auslegung der Richtlinie 2006/115 EG vom 12. Dezember 2006 zum Vermietrecht und Verleihrecht sowie zu bestimmten dem Urheberrecht verwandten Schutzrechten im Bereich des geistigen Eigentums und nicht unmittelbar die InfoSoc Richtlinie (2001/29/ EG), in der die Reichweite des Erschöpfungsgrundsatzes bei digitalen Inhalten beschränkt wird.[1121] Der EuGH hat in diesem Urteil entschieden, dass die Vorschriften aus der Richtlinie 2006/115/EG dahin auszulegen sind, dass der Begriff „Verleihen“ das digitale Verleihen einer Kopie eines Buches erfasst, wenn dieses Verleihen so erfolgt, dass die in Rede stehende Kopie auf dem Server einer öffentlichen Bibliothek abgelegt ist und es dem betreffenden Nutzer ermöglicht wird, diese durch Herunterladen auf seinem Computer zu reproduzieren, wobei nur eine einzige Kopie während der Leihfrist heruntergeladen werden kann und der Nutzer nach Ablauf dieser Frist die von ihm heruntergeladene Kopie nicht mehr nutzen kann. Insoweit hat der EuGH ausgeführt, dass das Unionsrecht, namentlich Art. 6 dieser Richtlinie dahin auszulegen ist, dass es einen Mitgliedstaat nicht daran hindert, die Anwendung von Art. 6 Abs. 1 dieser Richtlinie mit der Bedingung zu verknüpfen, dass die von der öffentlichen Bibliothek zur Verfügung gestellte digitale Kopie eines Buches durch einen Erstkauf oder eine andere erstmalige Eigentumsübertragung dieser Kopie oder mit Zustimmung i. S. v. Art. 4 Abs. 2 der Richtlinie 2001/29/EG (InfoSoc Richtlinie) in Verkehr gebracht wurde und weiter, dass Art. 6 Abs. 1 dieser Richtlinie der Anwendung der dort geregelten Ausnahme auf das Verleihwesen entgegensteht, wenn die Kopie aus einer illegalen Quelle stammt.[1122] Der EuGH führt ausdrücklich aus, dass Art. 4 Abs. 2 der Richtlinie 2001/29/EG für die Auslegung von Art. 6 Abs. 1 der Richtlinie 2006/115/EG nicht maßgeblich ist, da aus Art. 1 Abs. 2 Buchst. b der Richtlinie 2001/29/EG folge, dass sie die unionsrechtlichen Bestimmungen über das Verleihrecht unberührt lasse.[1123] Eine Klärung der Fragen der Geltung des Erschöpfungsgrundsatzes für digitale Kopien nach der Richtlinie 2001/29/EG hat diese Entscheidung damit nicht herbeigeführt. Der dargestellte Inhalt der Entscheidung spricht indes eher dagegen, dass der EuGH den Erschöpfungsgrundsatzes auf digitale Kopien anwenden möchte.

[1121] Dabei handelt es sich um das Urteil des EuGH vom 10.11.2016 − Rs. C-174/15 (Vereniging Openbare Bibliotheken), GRUR 2016, 1266, hier zitiert nach juris.

[1122] EuGH, Urt. v. 10.11.2016 − Rs. C-174/15, Leitsätze zu 1. bis 3. sowie juris Rn. 54, 65 und 72.

[1123] EuGH, Urt. v. 10.11.2016 − Rs. C-174/15, juris Rn. 56 f.

3. Überblick über die derzeit vorhandenen AGB-Regelungen

Ein stichprobenhafter empirischer Überblick über vorhandene AGB-Regelungen ergibt, dass sich in Deutschland in den allgemeinen Geschäftsbedingungen der Anbieter von digitalen Inhalten (E-Books, Musik, Filmen) ganz überwiegend keine expliziten Regelungen dazu finden, was mit den erworbenen digitalen Inhalten im Todesfall des Erwerbers geschieht. Eine derartige Regelung findet sich bei Apple für die Nutzer der „apple icloud", wo es heißt:

> *„Sofern gesetzlich nichts anderes vorgeschrieben ist, stimmen Sie zu, dass Ihr Account nicht übertragbar ist und dass alle Rechte an Ihrer Apple ID oder Ihren Inhalten innerhalb Ihres Accounts im Falle Ihres Todes enden. Bei Erhalt einer Kopie Ihrer Sterbeurkunde können Ihr Account aufgelöst und sämtliche Inhalte innerhalb Ihres Accounts gelöscht werden. Wenden Sie sich an den iCloud Support unter www.apple.com/support/icloud, wenn Sie weitere Unterstützung wünschen."*[1124]

Diese Regelung führt (unter der Prämisse ihrer Wirksamkeit) dazu, dass die digitalen Inhalte, die der Erblasser erworben hat, nicht vererblich sind, sondern das Nutzungsrecht mit dem Tode des Erblassers erlischt. Weiter heißt es dort

> *„Sie stimmen zu, dass Sie den Dienst (oder Teile davon) nicht vervielfältigen, kopieren, duplizieren, verkaufen, weiterverkaufen, vermieten oder eintauschen werden, egal für welchen Zweck."*[1125]

Bei Apple allgemein für „iTunes" und bei sämtlichen anderen untersuchten Anbietern finden sich keine expliziten Regelungen dazu, ob die digitalen Inhalte vererbt werden können, sondern lediglich allgemeine Ausführungen zur Übertragung.[1126]

Zusammenfassend lässt sich damit sagen, dass überwiegend in den allgemeinen Geschäftsbedingungen klargestellt wird, dass bei einem Download kein Eigentum übertragen wird, sondern nur einfache Nutzungsrechte eingeräumt werden, die nicht übertragen werden dürfen. Ob dies auch für eine Übertragung von Todes wegen gilt, wird in den allgemeinen Geschäftsbedingungen (bis auf icloud, s. o.) nicht thematisiert. Z. T. sind die Formulierungen eindeutig auf Übertragungen

---

[1124] Vgl. http://www.apple.com/legal/internet-services/icloud/de/terms.html, dort unter IV. D.
[1125] Vgl. http://www.apple.com/legal/internet-services/icloud/de/terms.html, dort unter IV. E.
[1126] So etwa bei Apple für „iTunes", vgl. unter http://www.apple.com/legal/internet-services/itunes/de/terms.html, dort unter B. (iv); bei Musicload (Dixero Media GmbH): https://www.musicload.de/web/static?id=agb, dort unter Ziffer 4.3; bei Amazon für den Kindle unter https://www.amazon.de/gp/help/customer/display.html?nodeId=200506200, dort unter 1., bei e.book.de unter http://www.ebook.de/de/category/59411/agb.html unter § 5, 1) und 3); bei Thalia.de unter http://www.thalia.de/shop/hilfe-agb/show/?intid=amc143591276427005, dort unter III. 1. § 3; bei bücher.de unter http://www.buecher.de/show/service/unternehmensinformationen/agb/458802/.

unter Lebenden bezogen, z. T. sind die Formulierungen abstrakt gehalten. Faktisch stellt sich derzeit das Problem einer vertraglichen Beschränkung der Übertragung auf die Lebenszeit des Nutzers lediglich für Nutzer der „apple icloud".

4. Stellungnahme

Bei dieser Fragestellung geht es ganz konkret um wirtschaftliche Werte, die auch erheblich sein können (Literatur-, Musik- und Videosammlungen in digitaler Form).

Es ist von dem Grundsatz auszugehen, dass die Nutzungsrechte vererblich sind. Auch faktisch ist in der Praxis die Vererbbarkeit derzeit in der Regel nicht ausgeschlossen. Die meisten allgemeinen Geschäftsbedingungen der Anbieter von E-Books und Downloads von Musik und Filmen enthalten wie dargestellt jedenfalls derzeit keinen eindeutigen Ausschluss der Vererbbarkeit (Ausnahme: Apple bezüglich der „icloud", s. o.). Ein solcher Ausschluss wäre de lege lata aber wohl möglich. Anders ist dies bei reiner Software, da insoweit der Erschöpfungsgrundsatz nach der zitierten Rechtsprechung des EuGH Anwendung findet, sodass die Vererblichkeit nicht durch AGB ausgeschlossen werden kann. Bezüglich Software besteht daher jedenfalls kein Regelungsbedarf.

Anders als bei Software stellt sich die Situation bei sonstigen in digitaler Form erworbenen Nutzungsrechten wie E-Books, Musik und Videos dar. Hier gilt der Erschöpfungsgrundsatz nach der derzeitigen ständigen Rechtsprechung in Deutschland nicht. De lege lata dürfte daher eine Regelung, die ein Erlöschen mit dem Tode vorsieht, auch durch allgemeine Geschäftsbedingungen wirksam sein. §§ 308 und 309 BGB enthalten hierzu keine Regelungen. Ein Verstoß gegen § 307 BGB dürfte nicht gegeben sein, da die Zweifelsregelung des § 307 Abs. 2 Nr. 1 BGB mangels Verstoß gegen den Erschöpfungsgrundsatz nicht eingreift, da nicht von wesentlichen Grundgedanken einer gesetzlichen Regelung abgewichen wird. Denkbar erscheint hingegen, dass – jedenfalls derzeit – von einer allgemeinen Erwartungshaltung auf Seiten der Nutzer auszugehen sein könnte, aufgrund derer eine Klausel in allgemeinen Geschäftsbedingungen, die die Nutzung auf Lebenszeit befristet, sich als überraschende Klausel i. S. d. § 305c BGB darstellen könnte und daher nach dieser Vorschrift bereits nicht Vertragsbestandteil wird. Rechtsprechung zu dieser speziellen Frage ist soweit ersichtlich aber noch nicht ergangen.

Die Möglichkeit für Anbieter, Nutzungsrechte befristet auf Lebzeiten zu übertragen, kann zu misslichen Konsequenzen für den Erben führen. Ein Erbe müsste, um sich rechtstreu zu verhalten und um keine Urheberrechte zu verletzen, für sämtliche auf von ihm ererbter Hardware vorhandenen, möglicherweise urheberrechtlich geschützten Daten ermitteln, von welchem Anbieter sie stammen, wie dessen allgemeine Geschäftsbedingungen ausgestaltet sind und ob er daher die Daten weiter nutzen darf oder löschen muss. Rein faktisch wird dies kaum jemand tun und dürfte dies auch kaum zu leisten sein. Wenn der Erblasser lediglich die Musikdatei etc. ohne weitere Angaben auf einem Datenträger gespeichert hat, ist die Ermittlung der Quelle (illegaler Download, legaler Download von einer

Quelle mit erbrechtsbeschränkenden AGB, legaler Download von einer Quelle ohne erbrechtsbeschränkende AGB) nicht möglich.

Wegen der fehlenden Übertragbarkeit unter Lebenden und der Möglichkeit, dass auch durch allgemeine Geschäftsbedingungen die Vererblichkeit ausgeschlossen werden kann, droht insoweit bei E-Books sowie Downloads von Musik und Videos ein „Erwerb zweiter Klasse“.

Diese Nachteile werden auch nicht durch die vertragliche Gestaltung, insbesondere durch niedrigere Preise beim Erwerb digitaler Inhalte, kompensiert. Besonders augenfällig ist dies im Bereich der E-Books im Hinblick auf das am 1. September 2016 in Kraft getretene Buchpreisbindungsgesetz, durch das die bisher für gedruckte Bücher geltende Buchpreisbindung ausdrücklich auf elektronische Bücher ausgedehnt wird.[1127] Faktisch wurde die Buchpreisbindung bereits zuvor auch auf E-Books angewandt,[1128] das Buchpreisbindungsgesetz wurde lediglich entsprechend angepasst. Die Preise für E-Books und legale, kostenpflichtige Downloads von Musik unterscheiden sich regelmäßig nicht erheblich von den Preisen für CDs und Bücher.[1129]

Da die Argumente der Gefahr eines unkontrollierbaren Zweitmarktes und der Gefahr rechtswidriger Mehrfachübertragungen, ohne die erforderliche Löschung beim Ersterwerber, bei der Übertragung im Wege der Gesamtrechtsnachfolge gerade nicht greifen, spricht auch unter Berücksichtigung dieser Gefahren nichts dagegen, gesetzlich vorzusehen, dass die Vererbbarkeit von Nutzungsrechten nicht vertraglich ausgeschlossen werden kann. Allerdings stellen sich angesichts der verschiedenen Regelungsmöglichkeiten hier nicht unerhebliche Probleme, auf die im Folgenden jeweils gesondert einzugehen sein wird.

[1127] Vgl. etwa die Pressemitteilung der Bundesregierung: https://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2016/02/2016-02-03-bkm-buchpreisbindung.html.

[1128] Vgl. etwa https://de.wikipedia.org/wiki/Buchpreisbindung; http://www.spiegel.de/kultur/literatur/buchpreisbindung-fuer-e-books-bundeskabinett-beschliesst-gesetzesentwurf-a-1075453.html;
http://www.boersenverein.de/de/portal/Preisbindung/158315;
http://www.internetrecht-rostock.de/e-book-buchpreisbindung.htm.

[1129] Stichprobenhafte Untersuchung der Angebote auf amazon.de und musicload.de zeigen gängige Preise von 9,99 € bis 14,99 € für ein neuerschienenes Musikalbum und Bestseller, was sich nicht erheblich von Ladenpreisen für CDs unterscheidet. Auf eBook.de wird häufig zum Vergleich des E-Book-Preises der Preis für das gedruckte Buch angegeben und liegt regelmäßig einige Euro unter dem Verkaufspreis für das gedruckte Buch, allerdings in der Regel nicht wesentlich niedriger als dieses. Bereits im Jahr 2010 wurde in der „Zeit“ auf die Problematik hingewiesen; danach sind E-Books in der Regel 10 bis 20% günstiger als das gedruckte Buch; Quelle: http://www.zeit.de/digital/mobil/2010-09/ebooks-preisbindung-ereader.

Es bestehen im Kern vier Möglichkeiten.

- *Große Lösung im Urheberrecht:* Neufassung von § 17 Abs. 2 UrhG. Ausweitung des Erschöpfungsgrundsatzes generell auch auf nichtkörperliche Werkstücke (Nutzungsrechte) (a.).
- *Lösung im BGB:* Regelung in § 308 BGB oder § 309 BGB, die eine Befristung auf den Tod des Erblassers und damit eine Unvererblichkeit in allgemeinen Geschäftsbedingungen ausschließt (ggf. beschränkt auf bestimmte Fälle, etwa Verträge mit Verbrauchern) (b.).
- *Kleine Lösung im Urheberrecht:* Neufassung von § 31 Abs. 1 S. 2 UrhG, Einschränkung der Möglichkeit der zeitlichen Befristung dahingehend, dass eine Befristung auf die Lebenszeit nicht vereinbart werden kann (ggf. beschränkt auf bestimmte Fälle, etwa Verträge mit Verbrauchern) (c.).
- *Verzicht auf eine Neuregelung* (d.).

a. Große Lösung im Urheberrecht

Die große Lösung im Urheberrecht (Ausweitung des Erschöpfungsgrundsatzes generell auch auf nichtkörperliche Werkstücke) würde dem festgestellten Bedürfnis umfassend Rechnung tragen, dass auch digitale Inhalte, die beim Erblasser gespeichert sind, uneingeschränkt auf den Erben übergehen. Es würde umfassend sichergestellt, dass diese nicht vor dem kaum lösbaren Problem stehen, dass sie zwecks Klärung der Frage, ob sie berechtigt sind, die Inhalte weiter zu nutzen, die Quelle der digitalen Inhalte ermitteln und die Vertragsbeziehungen kontrollieren müssten. Weiter hätte sie den Vorteil, dass sie Friktionen des Zivilrechts mit dem Urheberrecht oder innerhalb des Urheberrechts von vornherein vermeidet (vgl. zu diesem Problem ausführlich unter b. und c.).

Allerdings hätte dieser Lösungsansatz erhebliche Auswirkungen auf das Vertragsrecht. Er würde umfassend die Weiterveräußerung gebrauchter, digitaler Inhalte ermöglichen. Gegen eine derart weitgehende Regelung sprechen verschiedene Umstände: Zum einen lehnt die Rechtsprechung in Deutschland eine Anwendung des Erschöpfungsgrundsatzes auf digitale Inhalte ab. Zwar handelt es sich insoweit naturgemäß um eine Ablehnung de lege lata. Allerdings werden von der Rechtsprechung und der herrschenden Lehre hierfür auch Argumente angeführt, die de lege ferenda gleichfalls Geltung beanspruchen würden, nämlich insbesondere die Missbrauchsgefahr und das Entstehen eines unkontrollierbaren Zweitmarktes. Zudem hält es auch die EU-Kommission derzeit für verfrüht, an dieses Thema heranzugehen; man will dort die Problematik weiter beobachten.[1130]

[1130] European Commission, White Paper: A copyright Policy for Creativity and Innovation in the European Union, Juni 2004, netzpolitik.org/wp-upload/White-Paper-EC-Copyright-Reform.pdf, dort S. 7; vgl. ausführlich zu den legislative Initiativen auf EU-Ebene bei *Kreutzer*, Weiterveräußerungsfähigkeit von digitalen Gütern (Studie im Auftrag des Ministeriums für ländlichen Raum und Verbraucherschutz des Landes Baden-Württemberg), S. 40 f., der dort zu

Vor dem Hintergrund der bestehenden europarechtlichen Vorgaben zum Erschöpfungsgrundsatz (Art. 3 Abs. 3 (für die öffentliche Wiedergabe), Art. 4 Abs. 2 (für die Verbreitung) jeweils in Verbindung mit Erwägungsgrund Nr. 29 der Richtlinie 2001/29/EG (InfoSoc-Richtlinie)), erscheint es zudem zweifelhaft, ob eine nationale Regelung derzeit überhaupt möglich ist. Insoweit gehen die Meinungen in der Literatur auseinander.[1131] In dieser Situation spricht deutlich mehr gegen als für die große Lösung im Urheberrecht. Sinnvoll (und möglicherweise allein möglich) wäre eine derartig grundlegende und weitreichende Neuregelung angesichts grenzüberschreitender Märkte im Online-Handel auch ohnehin allein auf europäischer Ebene.

b. Lösung im BGB

Die Lösung im BGB (Regelung in § 308 oder § 309 BGB, die eine Befristung auf den Tod des Erblassers und damit eine Unvererblichkeit ausschließt, ggf. beschränkt auf bestimmte Fälle, etwa Verträge mit Verbrauchern) löst das erbrechtliche Problem nicht so umfassend wie die große Lösung im Urheberrecht. Es bliebe die Möglichkeit, dass der Erblasser individualvertraglich die Nutzung befristet auf seinen Tod abgeschlossen hat. Außerdem bestünde die Möglichkeit, dass dem Erblasser das Nutzungsrecht mit einer Befristung übertragen wurde, die wirksam ist, weil sie einen bestimmten Zeitraum festlegt, also das Nutzungsrecht künftig enden wird. Wurde ein Nutzungsrecht nur auf Zeit übertragen, wird der Anbieter Vorkehrungen getroffen haben, um die Nutzung über den vereinbarten Zeitraum hinaus zu unterbinden. Andernfalls wird er zum Fristablauf eine Kontaktaufnahme unternehmen und dabei selbst erkennen, dass ein Erbfall eingetreten ist. Daraufhin wird er im Bedarfsfall selbst aktiv werden und auf den Erben zugehen. Unklare Rechtslagen würden vermieden.

Auch der Umstand, dass nur Regelungen in allgemeinen Geschäftsbedingungen unwirksam wären, nicht aber individualvertragliche, wäre nicht schwerwiegend. Entsprechende Befristungen werden in aller Regel in allgemeinen Geschäftsbedingungen enthalten sein. Der ganz überwiegende Teil der möglichen Fälle würde erfasst werden, denn individualvertraglich wird bei der Übertragung von Nutzungsrechten an Verbraucher kaum je eine Befristung erfolgen, da diese Verträge als Massengeschäfte unter Verwendung allgemeiner Geschäftsbedingungen ausgestaltet sind. Die dargestellte Problematik betrifft aber gerade Erbfälle, bei denen derartige Nutzungsrechte an Verbraucher übertragen wurden, sodass die wesentlichen Fälle durch eine Regelung innerhalb von §§ 308, 309 BGB erfasst würden.

---

dem Schluss kommt, dass dem Thema derzeit bei den EU-Instanzen keine hohe Relevanz zugeschrieben wird.

[1131] Nachweise etwa bei *Kreutzer*, Weiterveräußerungsfähigkeit von digitalen Gütern (Studie im Auftrag des Ministeriums für ländlichen Raum und Verbraucherschutz des Landes Baden-Württemberg), Fn. 128 f. (S. 45).

Hier stellen sich aber andere Probleme und zwar in Bezug auf § 31 Abs. 1 S. 2 UrhG. Diese Vorschrift regelt, dass das Nutzungsrecht auch räumlich, zeitlich oder inhaltlich beschränkt eingeräumt werden kann. *Das Gesetz selbst* sieht damit ausdrücklich die Möglichkeit einer Befristung vor. Gem. § 307 Abs. 3 S. 1 BGB gelten § 307 Abs. 1 und Abs. 2 sowie §§ 308 und 309 BGB indes nur für Bestimmungen in allgemeinen Geschäftsbedingungen, durch die von Rechtsvorschriften abweichende oder diese ergänzende Regelungen vereinbart werden. Damit ist zweifelhaft, ob eine Regelung in §§ 308, 309 BGB vor dem Hintergrund der Vorschrift des § 31 Abs. 1 S. 2 UrhG überhaupt möglich ist. Ein Abweichen liegt vor, wenn der Regelungsgehalt der allgemeinen Geschäftsbedingungen mit dem Inhalt der einschlägigen Rechtsvorschrift nicht übereinstimmt.[1132] Dies ist im vorliegenden Fall nicht gegeben, da die AGB-Regelungen bei Vereinbarung einer Befristung gerade mit § 31 Abs. 1 S. 2 UrhG übereinstimmen, der diese Möglichkeit ausdrücklich vorsieht. Allerdings könnte hier eine Regelung anzunehmen sein, die i. S. d. § 307 Abs. 3 S. 1 BGB Rechtsvorschriften ergänzt. Allgemeine Geschäftsbedingungen, die im Vollzug eines ergänzungsbedürftigen Gesetzes den gesetzlich vorgegebenen Rahmen ausfüllen, unterliegen der Inhaltskontrolle; ebenso Klauseln, die eine gesetzliche Regelung übernehmen, sie aber durch Zusatzregelungen ergänzen.[1133] Auch diese Konstellation dürfte hier aber nicht vorliegen. Vielmehr dürfte § 31 Abs. 1 S. 2 UrhG eine Erlaubnisnorm darstellen, die den Parteien Spielraum für vertragliche Gestaltungen lässt. Eine solche Konstellation ist in ihrer rechtlichen Einordnung problematisch und in der Literatur wird unterschiedlich beurteilt, ob hier eine Inhaltskontrolle möglich oder im Gegenteil ausgeschlossen ist [1134]. Damit bestünde bereits im Hinblick auf die Möglichkeit einer Regelung allein im AGB-Recht aber eine gewisse Rechtsunsicherheit. Gegen eine Regelung in § 308 oder § 309 BGB sprechen aber noch weitere Gesichtspunkte: Unabhängig von der Problematik des § 307 Abs. 3 S. 1 BGB würde eine solche Regelung zu einer Friktion des BGB im Verhältnis zum UrhG führen, wo Befristungen gerade ausdrücklich zugelassen sind. Zeitliche Beschränkungen sind bei der Einräumung von Urheberrechten üblich, sodass von einem Nutzer erwartet werden kann, er prüfe nicht nur, ob ein Nutzungsrecht besteht, sondern auch, dass

---

[1132] Palandt/*Grüneberg*, BGB, § 307 Rn. 52 m. w. N.

[1133] Palandt/*Grüneberg*, BGB, § 307 Rn. 53 m. w. N.; ebenso MüKo/*Wurmnest*, BGB, § 307 Rn. 9 m. w. N.

[1134] Für einen Ausschluss der Inhaltkontrolle in diesen Fällen: Palandt/*Grüneberg*, BGB, § 307 Rn. 53 f. m. w. N.; hingegen soll nach BeckOGK/*Schmidt*, BGB, § 307 Rn. 72. m. w. N., Kontrollfreiheit gegeben sein, wenn sich aus der Gesetzeshistorie eindeutig der Wille des Gesetzgebers herleiten lasse, dass die Erlaubnisnorm auch durch AGB solle genutzt werden können, er weist zudem darauf hin, dass in den Fällen, in denen eine Regelung nach § 309 BGB getroffen worden sei, sich die Fragestellung dahin verlagere, ob die Klausel, die sich an die Vorgaben konkreter Klauselverbote halte, damit auch nicht mehr nach § 307 BGB zu kontrollieren sei (was für eine Kontrollfähigkeit spricht); vgl. zudem ausführlich und differenzierend nach dem jeweiligen Zweck der Erlaubnisnorm MüKo/*Wurmnest*, BGB, § 307 Rn. 10 m. w. N.

es noch besteht.[1135] Zudem sind vereinzelt sogar Befristungen für Nutzungsrechte im Gesetz geregelt. Nach § 38 Abs. 1 UrhG erwirbt der Verleger einer periodisch erscheinenden Sammlung das ausschließliche Abdruckrecht an einem Beitrag grundsätzlich nur für die Zeit eines Jahres.[1136] Würde nun im BGB geregelt, dass im Rahmen von allgemeinen Geschäftsbedingungen eine vertragliche Regelung unwirksam ist, bei der gerade die für den Nutzer längst mögliche Befristung, nämlich die auf seine Lebenszeit, vereinbart ist, so besteht (unabhängig von der angeführten Problematik des § 307 Abs. 3 S. 1 BGB) eine Friktion zum Urheberrecht, in dem jegliche Befristung zulässig ist. Dass gerade die *längste* Befristung für den Nutzer durch allgemeine Geschäftsbedingungen nicht vereinbart werden kann, kürzere - wie etwa eine Befristung auf ein Jahr oder ähnliches - aber schon, stellt einen gewissen Widerspruch dar. Auch würden damit im BGB (für Regelungen durch allgemeine Geschäftsbedingungen) Vereinbarungen untersagt, die nach dem Urheberrecht gerade gesetzlich als Gestaltungsmöglichkeit vorgesehen sind. Dieser Widerspruch hindert zwar nicht in rechtlicher Hinsicht eine derartige Regelung, da ja die im Urheberrecht vorgesehene Gestaltungsmöglichkeit im BGB lediglich in dem Sonderfall für unzulässig erklärt wird, dass sie im Wege der allgemeinen Geschäftsbedingungen vereinbart wird. Dennoch bleibt ein gewisser Bruch, da eine Gestaltungsvariante mittels allgemeiner Geschäftsbedingungen im BGB für unzulässig erklärt würde, die im Urheberrecht gerade *gesetzlich vorgesehen* ist.

Bedenken hinsichtlich einer gesetzlichen Regelung in diesen Vorschriften bestehen auch vor dem Hintergrund, dass die bestehenden Verbote in §§ 308, 309 BGB durchweg einen höheren Abstraktionsgrad und einen allgemeineren, weiteren Anwendungsbereich haben, als dies bei einer Regelung der Fall wäre, mit der eine ganz spezielle Art der Befristung (auf Lebenszeit) für eine ganz spezielle Konstellation (Übertragung von Nutzungsrechten) ausgeschlossen werden würde. Diese Regelung im BGB würde allein urheberrechtlich relevante Sachverhalte betreffen. Eine solche Regelung würde sich aus diesen Gründen nicht gut in die Vorschriften der §§ 308, 309 BGB einfügen und es wäre höchst fraglich, ob die Ergänzung dieser Normen um eine Ziffer zur Regelung eines derartig speziellen urheberrechtlichen Falles rechtspolitisch durchsetzbar und überhaupt wünschenswert wäre.

Abschließend kommt noch hinzu, dass der Regelungsbedarf, soweit er ausschließlich das Gebiet des Erbrechts betrifft, also die Problematik der Geltung des Erschöpfungsgrundsatzes für digitale Inhalte ausklammert, eher in der Situation des Erben begründet ist. Nur bei ihm stellen sich die aufgezeigten Probleme, dass er

---

[1135] Dreier/*Schulze*, UrhG, § 31 Rn. 34 unter Berufung auf BGH, Urt. v. 12.2.1952 – I ZR 115/51, BGHZ 5, 116 (121), wo es allerdings um die Übertragung von Verfilmungsrechten ging, also um einen Rechtserwerb im geschäftlichen, professionellen Bereich und nicht durch Verbraucher. Ob sich dieses Postulat aus dem Jahr 1952 heute auf Fälle mit Verbraucherbeteiligung übertragen lässt, erscheint zweifelhaft.

[1136] Dreier/*Schulze*, UrhG, § 31 Rn. 35.

regelmäßig nicht in der Lage sein dürfte, die Quelle der auf ererbter Hardware vorgefundenen Musik, Filme und Bücher zu ermitteln, sodass er nicht feststellen kann, ob er nach den zugrunde liegenden Vertragsbeziehungen möglicherweise gar nicht berechtigt ist, auf diese Inhalte weiter zuzugreifen. Die Beschränkung des Erblassers durch die Nichtgeltung des Erschöpfungsgrundsatzes trifft diesen viel stärker dadurch, dass die Übertragung unter Lebenden (Veräußerung, Verschenken) bei digitalen Inhalten nicht möglich ist (also nicht im Hinblick auf die rein erbrechtlichen Aspekte des Problems). Im Hinblick auf die rein erbrechtliche Problematik der Übertragbarkeit ist das Regelungsbedürfnis eher ordnungspolitischer Natur und nimmt eher die Stellung der Erben in den Fokus, da eine klare Zuordnung von digitalen Inhalten zum Erben wünschenswert ist, um Rechtsunsicherheit im Erbfall zu vermeiden. Der Erblasser, der ein auf seine Lebenszeit beschränktes Nutzugsrecht erwirbt, wird in seiner Testierfreiheit hingegen gar nicht eingeschränkt, da er ja nie eine vererbbare Rechtsposition erworben hat. Dieser festgestellte Regelungsbedarf spricht ebenfalls gegen eine Regelung in §§ 308, 309 BGB, die ihrem Sinn und Zweck nach eher Regelungen darstellen, die den Schutz von strukturell unterlegenen Vertragsparteien bezwecken und gerade nicht allgemeine ordnungspolitische Ziele und den Schutz Dritter. Auch dies spricht gegen eine Regelung in §§ 308, 309 BGB.

Zwar erschiene es auch möglich, außerhalb des AGB-Rechts im BGB einen (zwingenden) schuldrechtlichen Anspruch zu schaffen, aufgrund dessen Verbraucher bei Erwerb digitaler Inhalte in die Lage versetzt werden müssen, diese Inhalte auch weiterveräußern zu dürfen. Dies würde ein gesetzliches Leitbild einer Übertragbarkeit digitaler Inhalte im BGB verankern, aufgrund dessen Abweichungen durch AGB gemäß § 307 Abs. 2 Nr. 1 BGB unwirksam wären.[1137] Allerdings würde eine solche Regelung im BGB den Regelungen des Urheberrechts diametral widersprechen und einen offen zu Tage tretenden grundlegenden Bruch in der Rechtsordnung verursachen. Auch würde eine solche Regelung nur zwischen den Vertragspartnern gelten, sodass, wenn der Veräußerer nicht über entsprechende Rechte verfügen würde, die Weiterveräußerung dennoch Urheberrechte verletzen würde und so die Verkehrsfähigkeit gerade nicht gesichert wäre. Dem Erwerber, der nun die erworbenen digitalen Inhalte doch nicht weiterveräußern dürfte, stünden lediglich Schadensersatzansprüche gegen den Veräußerer zu. Auch eine solche Regelung erscheint daher nicht sinnvoll.

c. Kleine Lösung im Urheberrecht

Die kleine Lösung im Urheberrecht (Neufassung von § 31 Abs. 1 S. 2 UrhG; Einschränkung der Möglichkeit der zeitlichen Befristung dahingehend, dass eine Be-

---

[1137] Auf diese Möglichkeit – aber auch ihre Nachteile – wies Prof. Dr. Gerald *Spindler* in seinem Vortrag im BMJV anlässlich der Vorstellung von Rechtsgutachten zu Fragestellungen im digitalen Vertragsrecht und zum Richtlinienentwurf für Verträge über digitale Inhalte am 2.5.2016 hin.

fristung auf den Lebenszeit nicht vereinbart werden kann, ggf. beschränkt auf bestimmte Fälle, etwa Verträge mit Verbrauchern) hätte gegenüber der Lösung im BGB (s. o. b.) den Vorteil, dass sich die diversen aufgezeigten Probleme im Zusammenhang mit den §§ 307 ff. BGB nicht stellen und auch eine Friktion zwischen UrhG und BGB vermieden würde. Des Weiteren hätte sie den Vorteil, dass sie mehr Rechtssicherheit bieten würde, als eine Regelung allein für allgemeine Geschäftsbedingungen, da sich ein Erbe bei dieser Lösung sicher sein könnte, dass mit dem Erbfall keine Nutzungsrechte erloschen (bzw. richtiger: dem Stammrecht wieder zugefallen[1138]) sind. Es bliebe das Problem sonstiger zeitlicher Befristungen (s. o.), das aber aus den oben genannten Gründen nicht besonders schwerwiegend sein dürfte.

Allerdings stellt sich wieder das Problem einer Friktion – in diesem Fall innerhalb des § 31 UrhG. In § 31 Abs. 1 S. 2 UrhG –, werden Befristungen ausdrücklich für zulässig erklärt. In einer Neuregelung würde in einem weiteren Satz oder Absatz eine Einschränkung dahingehend aufgenommen werden, dass eine Befristung auf den Todesfall des Nutzers nicht vereinbart werden darf – also gerade die *längstmögliche* und damit für den Nutzer *am wenigsten einschränkende* Befristung. Kürzere Befristungen dürften damit zu Lasten des Nutzers vereinbart werden, gerade die längst mögliche hingegen nicht. Dies würde eine gewisse Friktion innerhalb des § 31 UrhG selbst nach sich ziehen.

d. Absehen von einer Regelung

Vor dem Hintergrund, dass die oben genannten drei Lösungswege jeweils die dort genannten Probleme aufwerfen und dass allgemeine Geschäftsbedingungen, die explizit eine Vererblichkeit ausschließen (Befristung auf Lebzeiten) jedenfalls derzeit kaum vorkommen, könnte von einer Regelung derzeit – trotz der beschriebenen Probleme – abzusehen sein. Der Handlungsbedarf ist angesichts des empirischen Befundes mangels weiter Verbreitung entsprechender, auf den Todesfall befristender allgemeiner Geschäftsbedingungen jedenfalls nicht drängend. Zudem würden Brüche innerhalb unserer Rechtsordnung vermieden.

e. Vorschlag

Trotz der aufgezeigten Probleme empfiehlt die Arbeitsgruppe vor diesem Hintergrund daher, derzeit *keine gesetzliche Regelung* zu treffen. Alle drei aufgezeigten Regelungsmöglichkeiten unterliegen den jeweils dort aufgeführten nicht unerheblichen Unwägbarkeiten, Bedenken, Folgeproblemen und Kritikpunkten. Auch stellt sich angesichts des derzeitigen empirischen Befundes der Regelungsbedarf nicht als zwingend dar. Es bleibt abzuwarten, ob sich Probleme in dieser Hinsicht künftig überhaupt nennenswert stellen werden - etwa ob künftig vermehrt AGB-Regelungen, vergleichbar derjenigen für die icloud, Verwendung finden. Das Problem, das sich für die Erben stellt, ist zwar derzeit abstrakt vorhanden. In der

---

[1138] Vgl. Wandtke/Bullinger/*Wandtke/Grunert,* UrhG, § 31 Rn. 11.

Praxis dürfte es sich aufgrund der geringen Verbreitung solcher allgemeiner Geschäftsbedingungen aber eher selten stellen. Gerade bei der icloud sorgt der Anbieter, der von dem Erbfall erfährt, durch Löschung selbst für klare Verhältnisse, wozu er auch in der Lage ist, da sich die Daten an einem Speicherplatz befinden, den er selbst zur Verfügung stellt und kontrolliert. In dieser Situation, in der empirisch kein dringender Handlungsbedarf feststellbar ist und alle möglichen gesetzlichen Lösungen auch Probleme, Unsicherheiten, Friktionen oder sonstige Nachteile in sich tragen, erscheint es eher angebracht, von einer gesetzlichen Neuregelung zunächst abzusehen. Eine andere Frage ist es, ob derartige Klauseln in allgemeinen Geschäftsbedingungen (wie oben dargestellt) als so ungewöhnlich anzusehen sind, dass sie wegen § 305c BGB (überraschende Klausel) nicht Vertragsbestandteil werden. Gesetzgeberischer Regelungsbedarf bzw. Ansätze für ein gesetzgeberisches Tätigwerden ergeben sich aus dieser Problematik hingegen nicht. Hier bleibt die Entwicklung der Rechtsprechung abzuwarten.

VIII. Themenkreis Vererbbarkeit bei Online-Banking, PayPal etc. (online-Zahlungsverkehr)

1. Fragestellung

Die Arbeitsgruppe hat sich weiter mit der Frage beschäftigt, inwieweit eine Vererbbarkeit bei Online-Banking, PayPal etc. (online-Zahlungsverkehr) gewährleistet ist.

2. Diskussionsstand

Hier wird vertreten, dass auf Online-Banking §§ 675c ff. BGB anzuwenden seien. Internet-Bezahlsysteme wie PayPal seien entweder als virtuelles Konto und damit als Girovertrag (im Fall eines PrePaid-Kontos), sonst als Geschäftsbesorgungsvertrag mit werkvertragstypischen Erfolgspflichten gem. §§ 675, 631 Abs. 2 BGB einzuordnen.[1139]

3. Stellungnahme

Vom Ansatz her müssen hier dieselben Grundsätze gelten, wie für die Übertragbarkeit eines E-Mail-Accounts. Diese sind in der Literatur (zutreffend) in einer Parallele zu der Rechtsprechung aus dem Girovertrag gesehen worden. Online-Banking-Verträge sind Giroverträgen noch sehr viel vergleichbarer als E-Mail-Providerverträge (möglicherweise sogar identisch bzw. in einem Vertrag enthalten). Insoweit muss auch hier gelten, dass der Erbe zunächst in den Vertrag eintritt. Sofern keine der Parteien von etwaigen Kündigungsrechten Gebrauch macht und der Vertrag nicht nur abgewickelt, sondern fortgesetzt wird, wird man mit der Rechtsprechung zu Giroverträgen das Entstehen eines neuen eigenen Vertragsverhältnisses mit dem Erben annehmen müssen, was auch für Online-Banking wie

---

[1139] *Kutscher* (Diss.), S. 61 ff (insbes. S. 63).

für Giroverträge gleichermaßen interessengerecht ist. Für den Online-Zahlungsdienst PayPal dürfte Gleiches zu gelten haben. Es besteht daher kein Regelungsbedarf.

IX. Themenkreis Vererbbarkeit bei „virtuellen Gegenständen“ (Avatare etc.)

1. Fragestellung

Die Arbeitsgruppe hat sich zudem mit der Frage der Vererbbarkeit von „virtuellen Gegenständen“ (Avatare etc.) auseinandergesetzt.

2. Diskussionsstand

Dieses Problem wird in der Literatur lediglich bei *Kutscher* kurz angerissen. Insoweit geht es um Gegenstände, die nur in der virtuellen Welt einen Gebrauchswert haben. Virtuelle Gegenstände finden sich vor allem im Bereich der Online-Spiele. Sie werden indes auch auf dem freien Markt gegen reales Geld angeboten. Auch virtuelle Währungen (insbesondere wiederum innerhalb von Online-Spielen) werden in Online-Auktionshäusern gehandelt.[1140] Virtuelle Gegenstände – so Kutscher – seien danach bloße Immaterialgüterrechte, der Erblasser und damit auch sein Rechtsnachfolger habe nicht einmal eine absolute Rechtsposition, sie hätten keine eigenen Rechte an virtuellen Gegenständen.[1141]

3. Stellungnahme

Zwar trifft der Hinweis von *Kutscher* zu, dass es sich bei virtuellen Gegenständen nicht um absolute Rechtspositionen handelt, sodass eigene Rechte des Erblassers und der Erben unmittelbar an den Gegenständen selbst ausscheiden. Damit erschöpft sich allerdings die Frage der Vererblichkeit nicht. Vielmehr ist nach derzeit geltender Rechtslage diese Problematik wiederum über den Eintritt des Erben in vertragliche Beziehungen des Erblassers zu lösen. „Virtuelle Gegenstände“ sind lediglich in dem digitalen Kontext, in dem der Erblasser sie erworben hat, sinnvoll nutzbar, also insbesondere innerhalb von Online-Spielen. Innerhalb dieser können die virtuellen Gegenstände aber wirtschaftlich durchaus Werte darstellen – man denke an einen begeisterten Nutzer von Online-Spielen, der viel Geld in die kostenpflichtige virtuelle Optimierung seiner Spielfigur (Avatar) investiert hat. Die Übernahme dieser erkauften virtuellen Gegenstände könnte für einen Erben, der ebenfalls diese Spiele nutzen will, einen unmittelbaren wirtschaftlichen Wert darstellen.

Es handelt sich bei Online-Spielen auch nicht um eine höchstpersönliche Rechtsbeziehung, die bei einem Gläubiger- oder Schuldnerwechsel in ihrem Wesen verändert würde. Der Anbieter stellt lediglich (für jeden Nutzer in gleicher Weise) die Spielmöglichkeit zur Verfügung. Die individuelle Ausstattung digitaler Spielfiguren (Avatare) führt – wie auch die konkrete Ausgestaltung der Nutzerseiten

---

[1140] Vgl. zu alldem *Kutscher* (Diss.), S. 39.
[1141] *Kutscher* (Diss.), S. 42.

bei sozialen Netzwerken (s. o.) – nicht zu einer Unvererblichkeit aufgrund von Höchstpersönlichkeit. Der Erbe tritt daher in die Vertragsbeziehung ein, die aber in aller Regel hier mit der Pflicht zur Zahlung laufender Entgelte verbunden sein wird. Vor diesem Hintergrund sind hier Kündigungsfragen von besonderer Bedeutung (Möglichkeit beiderseitiger Kündigungen aus wichtigem Grund? Übertragbarkeit von in der Online-Umgebung erworbenen „virtuellen Gegenständen“ auf andere Accounts? Wirksamkeit von AGB-Klauseln, die ein Erlöschen der Rechte an den virtuellen Gegenständen mit dem Tod des Inhabers vorsehen?). Insoweit dürfte es maßgeblich auf die jeweiligen AGB ankommen, die anhand von § 307 BGB zu überprüfen sind.

Denkbar erschiene insoweit, dass ein Regelungsbedarf bezüglich Regelungen in allgemeinen Geschäftsbedingungen bestehen könnte (mögliche Schaffung von Regelungen in §§ 308, 309 BGB, etwa um Regelungen in allgemeinen Geschäftsbedingungen auszuschließen, die das Erlöschen derartiger Rechte zum Gegenstand haben). Im Ergebnis erscheint jedoch eine Regelung in §§ 308, 309 BGB speziell im Hinblick auf Avatare in Online-Spielen u. ä. nicht sinnvoll. Bei kostenpflichtigen Spielen dürfte der Erbe, der nicht selbst an dem Spiel teilnehmen will, selbst regelmäßig ein Interesse an der schnellstmöglichen Kündigung haben, um nicht für eine von ihm möglicherweise gar nicht gewollte Spielmöglichkeit dauerhafte laufende Kosten tragen zu müssen. Das Bestehen eines Interesses des Erben, gerade mit dem vom Erblasser kostenpflichtig verbesserten Avatar weiter an dem Spiel teilzunehmen, wird eine eher seltene Konstellation sein. Auch dürften in der Regel die in Rede stehenden eingesetzten Mittel des Erblassers, die dieser in die Optimierung des Avatars o. ä. investiert hat, überschaubar sein. Insbesondere aber handelt es sich bei derartigen Ausgaben nicht um Investitionen als Vermögensanlage, sondern zur Verfolgung eines eigenen Spielzwecks des Erblassers. Dieser Spielzweck hat sich in der Vergangenheit durch Nutzung des Erblassers ja auch verwirklicht (die Ausgabe hat sich also mehr oder weniger im Spiel „amortisiert“). Damit dürfte auch eine Regelung in allgemeinen Geschäftsbedingungen, die eine Beendigung des Accounts mit dem Tod des Erblassers oder ein beiderseitiges Kündigungsrecht im Todesfall des Nutzers vorsieht, eher nicht gegen § 307 BGB verstoßen und ein Bedürfnis nach einer Regelung ist §§ 308, 309 BGB stellt sich nicht. Eine Regelung in §§ 308, 309 BGB speziell im Hinblick auf Avatare in Online-Spielen u. ä. erscheint zudem jedenfalls vor dem Hintergrund, dass es sich um eine recht spezielle Materie handelt, nicht sinnvoll. Die Regelungskomplexe in §§ 308, 309 BGB haben, wie bereits oben dargestellt, einen höheren Abstraktionsgrad; die hier denkbaren Regelungen wären eng begrenzt und speziell.

X. Themenkreis Probleme des anwendbaren Rechts bei internationalem Bezug (etwa ausländische Provider)

1. Fragestellung

Die Arbeitsgruppe hat sich mit der Frage auseinandergesetzt, inwieweit Probleme hinsichtlich des anwendbaren Rechts bei internationalem Bezug (etwa bei ausländischen Providern) bestehen.

2. Diskussionsstand

Eine ausführliche Auseinandersetzung mit der Frage des anwendbaren Rechts findet sich bei *Kutscher*.[1142] Die Erbfolge richtet sich für Todesfälle ab dem 17. September 2015 nach der EuErbVO[1143], wonach der letzte gewöhnliche Aufenthalt des Erblassers ausschlaggebend ist und die gemäß ihrem Art. 22 eine beschränkte Rechtswahl ermöglicht.[1144] Im Hinblick auf vertragliche Regelungen (für den digitalen Nachlass relevant etwa bezüglich Accounts, die in den Nachlass fallen) greift Art. 3 Rom I-VO ein, wonach die Parteien im Ausgangspunkt das anwendbare Recht frei wählen können.[1145] Einschränkungen gelten insoweit für die Rechtswahl in AGB und insbesondere bei Verbraucherbeteiligung.[1146] Verträge ohne Rechtswahlklausel unterliegen nach Art. 6 Abs. 1 Rom I-VO dem Recht des Staates, in dem der Verbraucher seinen gewöhnlichen Aufenthalt hat. Bei Verbraucherverträgen mit Rechtswahlklausel gilt nach Art. 6 Abs. 2 Rom I-VO in dem Fall, dass nach deutschem zwingendem Verbraucherrecht der Verbraucher besser stünde als nach gewähltem Recht, das deutsche Verbraucherrecht (z. B. AGB-Recht).[1147] Ergänzt wird dieser Schutz durch Art. 46b EGBGB, etwa für den Fall, dass die Rom I-VO keine Anwendung findet.[1148] Wenn keine Rechtswahl getroffen wurde oder diese ungültig ist und kein besonderer Vertrag nach Art. 5-8 Rom I-VO vorliegt, richtet sich die objektive Anknüpfung im Rahmen des Vertragsstatuts nach den Kriterien von Art. 4 Rom I-VO.[1149]

[1142] *Kutscher* (Diss.), S. 67 ff.
[1143] Verordnung (EU) Nr. 650/2012 vom 4.7.2012 über die Zuständigkeit, das anzuwendende Recht, die Anerkennung und Vollstreckung von Entscheidungen und die Annahme und Vollstreckung öffentlicher Urkunden in Erbsachen sowie zur Einführung eines Europäischen Nachlasszeugnisses.
[1144] *Kutscher* (Diss.), S. 68 und 88 f. m. w. N.; für den Zeitraum davor galt nach Art. 25 Abs. 1 EGBGB das Recht der Staatsangehörigkeit des Erblassers.
[1145] *Kutscher* (Diss.), S. 74 f. m. w. N.
[1146] Art. 3 Abs. 5, 10 Rom I-VO und Art. 6 Rom I-VO; vgl. *Kutscher* (Diss.), S. 75 m. w. N.
[1147] *Kutscher* (Diss.), S. 82 ff. m. w. N.
[1148] Vgl. ausführlich hierzu bei *Kutscher* (Diss.), S. 84 f. m. w. N.
[1149] *Kutscher* (Diss.), S. 85 ff. m. w. N.

3. Stellungnahme

Vielfach werden die Provider als Vertragspartner ihren Sitz nicht in Deutschland haben. Da – wie dargestellt – insoweit die Rechte der Erben sich aus den übergehenden Vertragsbeziehungen ergeben, stellt sich dann die Frage des anzuwendenden Rechts. Da es um Vertragsbeziehungen geht, gilt das Vertragsstatut, insoweit enthalten die AGB der Provider in aller Regel Rechtswahlklauseln.[1150] Aufgrund von Art. 6 Rom I-VO bleiben bezüglich der Vertragsbeziehungen aber trotz Rechtswahl zwingende Verbraucherschutzvorschriften, die im jeweiligen Aufenthaltsstaat des Verbrauchers gelten, anwendbar; sie gelten, wenn sie für den Verbraucher günstiger sind, als das gewählte Recht. Im Bereich des digitalen Nachlasses bedeutet dies, dass soweit Verbraucher beteiligt sind, die ihren gewöhnlichen Aufenthaltsort in der Bundesrepublik Deutschland haben, insbesondere die Inhaltskontrolle nach §§ 307 ff. BGB eingreift – auch wenn der Provider im Ausland sitzt und eine andere Rechtswahl in seinen AGB getroffen hat.[1151] Ein konkreter Regelungsbedarf wird vor diesem Hintergrund nicht gesehen.

XI. Themenkreis Übergang von Telekommunikationsverträgen auf die Erben

1. Fragestellung

Die Arbeitsgruppe hat schließlich die Frage der Vererbbarkeit von Telekommunikationsverträgen vertieft bearbeitet.

2. Diskussionsstand

Der *DAV* weist auf das Problem hin, dass ein Telekommunikationsanschluss in der Regel pro Wohnung nur einmal zur Verfügung steht, sodass ein Übergang dieses Vertrages auf die Erben, wenn diese nicht zugleich Mitwohnungsinhaber sind, zu der misslichen Konsequenz führe, dass ein Vertrag nach § 1922 BGB auf die Erben übergehe, die tatsächliche Nutzung aber bei den bisherigen Nutzern verbleibe.[1152] Er schlägt insoweit vor, dass auf mietrechtliche Regelungen (§§ 563 ff. BGB) zurückgegriffen werden könne und macht einen Gesetzgebungsvorschlag (Neuschaffung von § 43c TKG-E). Danach soll der Ehegatte oder der eingetragene Lebenspartner, der mit einem Teilnehmer einen gemeinsamen Haushalt führt, bei Verträgen über Telekommunikationsdienste im Festnetz mit dem Tod des Teilnehmers in das Vertragsverhältnis eintreten. Tritt dieser Personenkreis nicht ein, so sollen Kinder oder andere Familienangehörige oder sonstige Personen eintreten, falls sie mit dem Erblasser in einem gemeinsamen Hausstand gelebt haben. Sie haben die Möglichkeit, binnen eines Monats den Nichteintritt in das Vertragsverhältnis zu erklären.

[1150] Vgl. *Kutscher* (Diss.), S. 89.
[1151] Vgl. *Kutscher* (Diss.), S. 89.
[1152] *DAV,* Stellungnahme Nr. 34/2013, S. 6, 8 f..

3. Stellungnahme

Der vom *DAV* insoweit gesehene Regelungsbedarf erscheint zwar nicht unplausibel. Diese Problematik stellt sich indes bereits seit Jahrzehnten in gleicher Weise allgemein für Telefonanschlüsse, ohne dass eine entsprechende gesetzgeberische Regelung erfolgt wäre. Ein Telekommunikationsanschluss (Providervertrag – in aller Regel gerade kombiniert mit einem Telefonvertrag) ist einem Mietverhältnis aber nicht vergleichbar, sodass es fraglich erscheint, ob hier Regelungen eingeführt werden sollten, die derartige Verträge im Erbfall wie Mietverträge behandeln. Ein Telekommunikationsanschluss kann leicht gekündigt und für den neuen Vertragspartner neu abgeschlossen werden. Die Situation ist nicht vergleichbar mit der des Mietverhältnisses bei Versterben des Mieters und Verbleiben von Angehörigen, die die Wohnung mitnutzen. Wäre dort ein Eintrittsrecht nicht gegeben, würden regelmäßig eine Wohnungssuche und ein Umzug im Raum stehen (mit ggf. erheblichem Aufwand und erheblichen Kosten, ungeachtet der möglicherweise auch erheblichen sozialen Folgen). Das ist bei Telekommunikationsverträgen sehr viel unproblematischer und schneller möglich und regelmäßig auch weder mit großem Aufwand, noch mit großen Kosten verbunden.

Der *DAV* sieht das Problem vor allem, wenn Erben nicht diejenigen sind, die mit dem Erblasser zusammen wohnen, sodass die faktischen Nutzer des Anschlusses mit demjenigen, der in den Vertrag eintritt, nicht identisch sind. Rein faktisch dürfte aber der Fall, dass der Erblasser mit Personen zusammenlebt, die weder gesetzliche Erben sind, noch von ihm als Erben eingesetzt sind, sondern er andere Personen zu Erben eingesetzt hat, jedenfalls nicht sehr häufig sein. Denkbar sind solche Fälle zwar (unverheiratetes Zusammenleben eines Erblassers mit einer Partnerin, ohne ein Testament aufgesetzt zu haben, Wohnungsgemeinschaften etc.). Die Problematik stellt sich aber jedenfalls nicht standardmäßig in der Masse der Erbfälle. Hinzu kommt insbesondere, dass derartige Problemfälle sich auch durch Vertragskündigungen und Neuabschlüsse binnen kürzester Zeit regeln lassen. Vor diesem Hintergrund sieht die Arbeitsgruppe insoweit keinen Regelungsbedarf.

C. Ergebnis

Ein grundlegender zwingender Regelungsbedarf im Bereich des digitalen Nachlasses besteht nach dem Ergebnis der Überprüfung der Rechtslage durch die Arbeitsgruppe nicht. Dem Erblasser stehen hinreichende rechtliche Mittel zur Verfügung, um auch differenzierte Regelungen zur Übertragung (oder Löschung) von Datenbeständen (E-Mails etc.) anzuordnen und zwar sowohl durch lebzeitige Regelungen, als auch durch entsprechende Regelungen von Todes wegen. Die Frage nach der Berechtigung der Erben oder der nächsten Angehörigen an Datenbeständen ist de lege lata eindeutig zugunsten der Erben zu beantworten. Dies erscheint auch sinnvoll und interessengerecht.

Hinsichtlich des Telekommunikationsrechts besteht zwar kein zwingendes Erfordernis einer Neuregelung, da § 88 TKG auch derzeit dem (bereits aus dem Vertragsverhältnis mit dem Provider bestehenden) Auskunftsanspruch des Erben nicht entgegensteht. Insoweit wäre indes zur Schaffung von Rechtssicherheit eine (klarstellende) gesetzliche Regelung innerhalb des TKG (unter Berücksichtigung der EU-DSGVO) sinnvoll, wie sie auch vielfach in der Literatur angeregt wird.

Im Hinblick auf etwaige sich im Rahmen von digitalen Nachlässen verschärfende Haftungsproblematiken für Miterben könnte sich zukünftig die Frage stellen, ob die Position der vorläufigen Miterben vor Erbschaftsannahme durch die Stärkung von Auskunftsrechten und die Verlängerung der Ausschlagungsfrist oder durch Haftungserleichterungen im Wege der aufgezeigten möglichen Änderungen des § 2062 BGB gestärkt werden sollte. Derzeit erscheint dies auch angesichts der Probleme des „digitalen Nachlasses“ nicht erforderlich. Die weitere Entwicklung sollte hier aber beobachtet werden.

Literaturverzeichnis

Arndt, Hans-Wolfgang/ Fetzer, Thomas/Scherer, Joachim/Graulich, Kurt — Telekommunikationsgesetz, Kommentar, 2. Auflage, Berlin 2015

Auer-Reinsdorff, Astrid/ Conrad, Isabell (Hrsg.) — Handbuch IT- und Datenschutzrecht, 2. Auflage, München 2016

Bamberger, Heinz-Georg/ Roth, Herbert — Beck'scher Online-Kommentar BGB, 38. Edition, Stand: 1.2.2016.

Baumgartner, Ulrich/ Ewald, Konstantin — Apps und Recht, 2. Auflage, München 2016

Bäumler, Helmut/ Mutius, Albert von — Anonymität im Internet - Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, 1. Auflage, Braunschweig/Wiesbaden 2003

Becker, Maximilian — Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, in: Festschrift für Karl-Heinz Fezer, hrsg. von Wolfgang Büscher, Jochen Glöckner, Axel Nordemann, Christian Osterrieth und Rudolf Rengier, München 2016, S. 815.

Bitkom e.V./ Bitkom Research GmbH — Soziale Netzwerke 2013 – Dritte, erweiterte Studie – Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet, Berlin 2013

Bitkom e.V./ Bitkom Research GmbH — Die Nutzung von E-Books, Studie, Berlin 2016

Borges, Georg/ Meents, Jan Geert (Hrsg.) — Cloud Computing Rechtshandbuch, Saarbrücken/München 2016

Bundeskartellamt — „Marktmacht von Plattformen und Netzwerken“ - Ergebnisse und Handlungsempfehlungen, Arbeitspapier, Bonn 2016

Conrad, Isabell/ Grützmacher, Malte (Hrsg.)	Recht der Daten und Datenbanken im Unternehmen, zugleich Festgabe Jochen Schneider zum 70. Geburtstag, Köln 2014
Deutscher Anwaltverein	Stellungnahme des Deutschen Anwaltsvereins durch die Ausschüsse Erbrecht, Informationsrecht und Verfassungsrecht und zum digitalen Nachlass, Stellungnahme Nr. 34, Berlin, Juni 2013.
Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)	Daten – Ware und Währung, Eine repräsentative Bevölkerungsbefragung, Studie, Hamburg 2014
Dreier, Thomas/ Schulze, Gernot	Urheberrechtsgesetz, Kommentar, 5. Auflage, München 2015
Erbs, Georg/ Kohlhaas, Max	Strafrechtliche Nebengesetze, Kommentar, 205. EL Oktober 2015
Erman	BGB, Kommentar, 14. Auflage, Köln 2014
Faust, Florian	Bürgerliches Gesetzbuch Allgemeiner Teil, 5. Auflage 2016
Geppert, Martin/Piepenbrock, Hermann-Josef/ Schütz, Raimund/Schuster, Fabian	Beck'scher Kommentar zum TKG, 4. Auflage 2013
Gola, Peter	DS-GVO, Kommentar, 1. Auflage 2017
Graef, Ralph Oliver	Recht der E-Books und des Electronic Publishing, München 2016
v. d. Groeben, Hans/ Schwarze, Jürgen/ Hatje, Armin (Hrsg.)	Europäisches Unionsrecht, Kommentar, 7. Auflage, Baden-Baden 2015
Große Ruse-Khan, Henning/Klass, Nadine/ von Lewinski, Silke (Hrsg.)	Nutzergenerierte Inhalte als Gegenstand des Privatrechts, Aktuelle Probleme des Web 2.0, Berlin/Heidelberg 2010

Gsell, Beate/ Krüger, Wolfgang/ Lorenz, Stephan/ Mayer, Jörg (Hrsg.)	beck-online.GROSSKOMMENTAR zum Bürgerlichen Gesetzbuch, München 2016
Härting, Niko	Internetrecht, 5. Auflage, Köln 2014
Herberger, Maximilian/ Martinek, Michael/ Rüßmann, Helmut/ Weth, Stephan (Hrsg.)	Juris Praxiskommentar zum Bürgerlichen Gesetzbuch, 7. Auflage, Saarbrücken 2014
Hilber, Marc (Hrsg.)	Handbuch Cloud Computing, Köln 2014
Hilgendorf, Eric (Hrsg.)	Robotik im Kontext von Recht und Moral, 2014
Hoeren, Thomas (Hrsg.)	Big Data und Recht, München 2014
Hoeren, Thomas/ Sieber, Ulrich/ Holznagel, Bernd (Hrsg.)	Handbuch Multimedia-Recht - Rechtsfragen des elektronischen Rechtsverkehrs, Münster/Freiburg 2016
Hoffmann, Christian/Luch, Anika/Schulz, Sönke/ Borchers, Corinna	Die digitale Dimension der Grundrechte - Das Grundgesetz im digitalen Zeitalter, Baden-Baden 2015
Hohlfeld, Ralf/ Godulla, Alexander	Das Phänomen der Sozialen Medien, in: Rechtshandbuch Social Media, hrsg. von Gerrit Hornung und Ralf Müller-Terpitz, Berlin/Heidelberg 2015, S. 11 ff.
Hornung, Gerrit/ Müller-Terpitz, Ralf (Hrsg.)	Rechtshandbuch Social Media, 1. Auflage, Berlin/Heidelberg 2015
Jauernig	Bürgerliches Gesetzbuch, Kommentar, 16. Auflage 2015
Kayser, Godehard/ Thole, Christoph (Hrsg.),	Insolvenzordnung, Kommentar, 8. Auflage, Heidelberg 2016
Keidel, Theodor	FamFG, Kommentar, 19. Auflage 2017
Köhler, Helmut	BGB Allgemeiner Teil, 40. Auflage 2016
Kreuzer, Till (iRights.Law)	Weiterveräußerungsfähigkeit von digitalen Gütern, Studie, 2015

Kroiß, Ludwig/Ann, Christoph, Mayer, Jörg	Kommentar zum Bürgerlichen Gesetzbuch, Band 5: Erbrecht, 4. Auflage 2014
Kroiß, Ludwig/ Horn, Claus-Henrik/ Solomon, Dennis	Nachfolgerecht, Kommentar, 1. Auflage 2015
Kühling, Jürgen/ Buchner, Benedikt	DS-GVO, Kommentar, 1. Auflage 2017
Kühling, Jürgen/ Martini, Mario et al.	Die DSGVO und das nationale Recht - Erste Überlegungen zum nationalen Regelungsbedarf, 2016
Kutscher, Antonia	Der digitale Nachlass, Dissertation, Kiel, 2015
Lange, Heinrich/ Kuchinke, Kurt	Erbrecht, Ein Lehrbuch, 5. Auflage 2001
Leible, Stefan/Lehmann, Matthias/Zech, Herbert (Hrsg.)	Unkörperliche Güter im Zivilrecht, Tübingen 2011
Maunz, Theodor/Dürig, Günter	Grundgesetz, Kommentar, 78. Auflage 2016
Müller-Broich, Jan D.	Telemediengesetz, 1. Auflage 2012
Münchener Kommentar zum Bürgerlichen Gesetzbuch	Band 1, 7. Auflage, München 2015; Band 2, 7. Auflage, München 2016; Band 4, 6. Auflage, München 2012; Band 5, 6. Auflage, München 2013; Band 9, 6. Auflage, München 2013
Münchener Kommentar zur Insolvenzordnung	Band 1, 3. Auflage, München 2013
Münchener Kommentar zur Zivilprozessordnung	Band 2, 4. Auflage, München 2012
Musielak, Hans-Joachim/ Voit, Wolfgang	Zivilprozessordnung, Kommentar, 13. Auflage, München 2016
Noerr LLP	Digitalisierte Wirtschaft/Industrie 4.0, Gutachten, 2015

Palandt, Otto	Bürgerliches Gesetzbuch, Kommentar, 76. Auflage, München 2017
Plath, Kai-Uwe (Hrsg.)	BDSG/DSGVO, Kommentar, 2. Auflage, Köln 2016
Prütting, Hanns/ Gehrlein, Markus	Zivilprozessordnung, Kommentar, 8. Auflage 2016
Redeker, Helmut	IT-Recht, 5. Auflage 2012
Rehbinder, Manfred/ Peukert, Alexander	Urheberrecht, 17. Auflage, München 2015
Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz (Hrsg.)	Verbraucher in der Digitalen Welt - Verbraucherpolitische Empfehlungen, Veröffentlichung, Berlin 2016
Säcker, Franz Jürgen	Berliner Kommentar zum TKG, 2. Auflage 2009
Scheuerle, Klaus-Dieter/ Mayen, Thomas	Telekommunikationsgesetz Kommentar, 2. Auflage, München 2008
Schmidt, Karsten	Insolvenzordnung, Kommentar, 19. Auflage, München 2016
Schulze, Reiner/Dörner, Heinrich/Ebert, Ina/ Hoeren, Thomas/Kemper, Rainer/ Saenger, Ingo/ Schreiber, Klaus/Schulte-Nölke, Hans/ Staudinger, Julius von	BGB Handkommentar, 9. Auflage 2016
Seidler, Katharina	Digitaler Nachlass – Das postmortale Schicksal elektronischer Kommunikation, Dissertation, Hamburg, 2016
Soergel, Hans-Theodor	Bürgerliches Gesetzbuch, Kommentar, Band 2, Allgemeiner Teil 2 (§§ 104 - 240), 13. Auflage, Stuttgart 1999

Sorge, Christoph	Softwareagenten. Vertragsschluss, Vertragsstrafe, Reugeld, Hochschulschrift in der Reihe Schriften des Zentrums für Angewandte Rechtswissenschaft der Universität Karlsuhe, Karlsruhe 2006
Spindler, Gerald/ Schuster, Fabian	Recht der elektronischen Medien, Kommentar, 3. Auflage 2015
Staudinger, Julius von	Kommentar zum BGB, Band 1: Allgemeiner Teil, Neubearbeitung 2012, Band 2: Recht der Schuldverhältnisse, Neubearbeitung 2012 bzw. 2015
Thomas, Heinz/ Putzo, Hans	Zivilprozessordnung, Kommentar, 37. Auflage, München 2016
Titze, Heinrich	Vom sogenannten Motivirrtum, Festschrift für Ernst Heymann (1940), Band 2, S. 70 ff.
Uhlenbruck, Wilhelm/ Hirte, Heribert/ Vallender, Heinz (Hrsg.)	Insolvenzordnung, Kommentar, 14. Auflage, München 2015
Vorwerk, Volkert/ Wolf, Christian	Beck'scher Online-Kommentar ZPO, 21. Edition, Stand: 1.7.2016
Wandtke, Artur-Axel/ Bullinger, Winfried	UrhR, Praxiskommentar zum Urheberrecht, 4. Auflage, München 2014
Weichert, Thilo	Postmortaler Datenschutz – Auskunftsansprüche von Erben und Angehörigen zu personenbezogenen Internetdaten eines Verstorbenen, Gutachten 2016
Wolf, Manfred/ Lindacher, Walter F./ Pfeiffer, Thomas	AGB-Recht, Kommentar, 5. Auflage, München 2009
Wolf, Manfred/ Neuner, Jörg	Allgemeiner Teil des Bürgerlichen Rechts, 11. Auflage 2016
Zech, Herbert	Information als Schutzgegenstand, Tübingen 2012
Zöller, Richard	Zivilprozessordnung, Kommentar, 31. Auflage, Köln 2016