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 ................................................................. 5

A. Allgemeines ................................................................................................. 5
B. Dateneigentum ............................................................................................ 7
C. Digitales Vertragsrecht ............................................................................ 11
D. Digitales Persönlichkeitsrecht .................................................................. 18
E. Digitaler Nachlass ..................................................................................... 22
F. Gesetzgeberischer Handlungsbedarf ......................................................... 24

Vorgehensweise der Arbeitsgruppe ................................................................. 26

Kapitel 1: Dateneigentum .............................................................................. 29

A. Vorbemerkung ............................................................................................ 29
B. Datenbegriff ............................................................................................... 29
   I. Definition .................................................................................................... 29
   II. Abgrenzung zum Speichermedium ......................................................... 30
   III. Abgrenzung zum Dateninhalt ................................................................. 31
C. Daten im geltenden Recht ......................................................................... 32
   I. Fehlende Sachqualität der Daten ............................................................. 32
   II. Daten als Gegenstände ......................................................................... 33
   III. Behandlung von Daten im geltenden Recht ......................................... 34
D. Ausgestaltung eines absoluten Rechts an Daten ...................................... 36
   I. Schutzumfang ........................................................................................... 36
   II. Dogmatische Verortung ......................................................................... 39
   III. Personelle Zuordnung ......................................................................... 42
   IV. Zwischenergebnis ................................................................................. 44
E. Regelungsbedarf im Einzelnen ................................................................. 44
   I. Daten als sonstiges Recht i. S. v. § 823 Abs. 1 BGB? ........................... 45
   II. Schutz der Daten gegen unberechtigten Zugriff .................................... 52
   III. Gesamt- und Einzelzwangsvollstreckung .......................................... 60
   IV. Handel mit Daten ................................................................................... 69
   V. Zuordnung automatisch generierter Daten ......................................... 74
VI. Zwangsvollstreckung in Datenbestände .................................. 84
F. Zusammenfassende Erwägungen zum Regelungsbedarf ..................... 88
   I. Schlussfolgerungen aus der Analyse einzelner Fallgruppen .......... 88
   II. Einschätzungen der Wissenschaft ........................................ 89
   III. Einschätzungen der Praxis .................................................. 94
   IV. Bestrebungen auf europäischer Ebene .................................. 96
   V. Ausblick .............................................................................. 97
G. Ergebnis .................................................................................. 98

Kapitel 2: Digitales Vertragsrecht .................................................. 99

A. Vorbemerkung ........................................................................... 99
B. Vertragsschluss durch Roboter .................................................. 100
   I. Untersuchungsgegenstand ....................................................... 100
   II. Maschinell ausgelöste Erklärungen als Willenserklärungen ........ 102
   III. Zugang von Erklärungen ....................................................... 104
   IV. Anwendbare Auslegungsgrundsätze ...................................... 105
   V. Anfechtung von maschinell ausgelösten Willenserklärungen .... 105
   VI. Empfehlung ........................................................................ 108
C. Haftungsrechtliche Fragen im Internet der Dinge ............................... 109
   I. Untersuchungsgegenstand ....................................................... 109
   II. Vertragliche Haftung .............................................................. 109
   III. Außervertragliche Haftung .................................................... 111
   IV. Empfehlungen ...................................................................... 119
D. Cloud Computing ...................................................................... 120
   I. Technische Grundlagen und ökonomische Bedeutung ............... 120
   II. Schuldrechtliche Einordnung .................................................. 128
   III. Vertragstypologische Einordnung ......................................... 138
   IV. Untersuchung einzelner Aspekte .......................................... 145
   V. Ergebnisse ............................................................................ 163
E. Streaming ................................................................................. 165
   I. Technische Grundlagen ......................................................... 165
   II. Ökonomische Bedeutung/Marktentwicklung ......................... 166
   III. Vertragsrechtliche Einordnung von Live-Streaming .................. 167
IV. Vertragsrechtliche Einordnung von On-Demand-Streaming ........... 174
V. Zwischenergebnis .................................................................................. 181
VI. Problemfelder/Praktische Fragestellungen ..................................... 182
VII. Ergebnisse .......................................................................................... 191
F. Soziale Netzwerke .................................................................................. 192
   I. Das Phänomen „Soziales Netzwerk“ ................................................. 192
   II. Rechtliche Problemfelder ................................................................. 194
   III. Vertragsrechtliche Fragestellungen und Lösungsansätze ............ 194
   IV. Empfehlungen .................................................................................. 198
G. „Bezahlen mit Daten“ am Beispiel der Sozialen Netzwerke ............ 199
   I. Untersuchungsgegenstand ............................................................... 199
   II. Schuldrechtliche Einordnung und Regelungsbedarf ..................... 199
   III. Empfehlungen ................................................................................ 225
H. Erwerb digitaler Inhalte im Wege des Downloads ......................... 226
   I. Untersuchungsgegenstand ............................................................... 226
   II. Gesellschaftliche und ökonomische Relevanz .............................. 227
   III. Bürgerlich-rechtliche Sonderregelungen ..................................... 229
   IV. Anwendbarkeit der allgemeinen Regelungen .............................. 236
   V. Umsetzbarkeit verbraucherpolitischer Ziele .................................. 241
   VI. Empfehlungen ................................................................................ 251
I. WAP-Billing und Zahlungswege im Internet ...................................... 252
   I. Allgemeines ...................................................................................... 252
   II. Bezahldienste .................................................................................. 252
   III. WAP-Billing ................................................................................... 253
   IV. In-App-Käufe .................................................................................. 259
   V. Empfehlungen .................................................................................. 260
J. Virtuelle Währungen ............................................................................. 261
   I. Allgemeines ...................................................................................... 261
   II. Technischer Hintergrund ............................................................... 262
   III. Problemfelder ................................................................................ 264
   IV. Ergebnisse ...................................................................................... 269
Kapitel 3: Digitales Persönlichkeitsrecht ............................................................... 270
A. Vorbemerkung ........................................................................................................ 270
B. Verbreitung von Tatsachen und Meinungen über Neue Medien .......................... 271
   I. Schutz des allgemeinen Persönlichkeitsrechts .................................................. 271
   II. Auskunft über die Identität von Tätern und Teilnehmern ............................... 276
   III. Unterlassung, Beseitigung (Löschung) und Widerruf ..................................... 278
   IV. Schadensersatz und Schmerzensgeld ............................................................... 304
   V. Internationale Zuständigkeit und anwendbares Recht ...................................... 307
C. Profilbildung und Verhaltensprognose durch „Big Data“-Analysen ..................... 308
D. Klarnamenpflicht im Internet ............................................................................... 312
E. Profildiebstahl ....................................................................................................... 314
F. Ausspähen von Daten ............................................................................................ 316
G. Ungewollte Einflüsse Dritter ............................................................................... 319
H. Ergebnisse .............................................................................................................. 321

Kapitel 4: Digitaler Nachlass .................................................................................. 324
A. Übersicht über die bearbeiteten Fragestellungen ............................................... 324
B. Die Themenkreise im Einzelnen .......................................................................... 324
   I. Vererbarkeit eines Accounts ............................................................................... 324
   II. Testamentarische Regelung ............................................................................... 363
   III. Vorsorge ........................................................................................................... 367
   IV. Annahme und Ausschlagung des Erbes ............................................................ 368
   V. Postmortales Persönlichkeitsrecht ..................................................................... 381
   VI. Vererbarkeit einer Website des Verstorbenen ................................................. 385
   VII. Vererbarkeit von Nutzungsrechten .................................................................. 386
   VIII. Vererbarkeit bei Online-Banking, PayPal etc. ............................................... 400
   IX. Vererbarkeit „virtueller Gegenständen“ ............................................................ 401
   X. Probleme des anwendbaren Rechts bei internationalem Bezug ....................... 403
   XI. Übergang von Telekommunikationsverträgen auf die Erben ......................... 404
C. Ergebnis ................................................................................................................ 406

Literaturverzeichnis ................................................................................................. 407
Zusammenfassung und Ergebnisse

A. Allgemeines


(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“.

(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

„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.


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;


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 Nutzung 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 versprechen. 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 auslösen, erscheinen derzeit nicht gegeben:


• 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, wer die Daten speichert, verarbeitet, verkauft oder löscht. 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 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 geregelt) 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 sächlichsten 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.


- 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.


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.


Vertragsschluss durch Roboter

Haftungsrechtliche Fragen im Internet der Dinge

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**

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**

Soziale Netzwerke


„Bezahlen mit Daten“


**Erwerb digitaler Inhalte im Wege des Downloads**


**WAP-Billing und Zahlungswege im Internet**

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

**Virtuelle Währungen**


**D. Digitales Persönlichkeitsrecht**

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.


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

- § 13 Abs. 6 TMG, wonach der Dienstanbieter 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.


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


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


Forderungen nach gesetzlichen Vorgaben für das Lösungsverfahren 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 Zustel-
lungsbevollmächtigten. Schon wegen des – auf bestimmte strafbewehrte Hand-
lungen – beschränkten Anwendungsbereichs erfüllt der Gesetzentwurf die Forde-
rung der Arbeitsgruppe nach einem einheitlichen und verbraucherfreundlichen
Lösungsverfahren 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 Prü-
fung des postmortalen Schicksals von Rechtspositionen, die der Erblasser auf-
grund elektronischer Kommunikation innehatte (bspw. Nutzer-Accounts oder Fo-
ren-Einträge). Auf der ersten Stufe sind die einzelnen Rechtspositionen nach ihrer
Übergangsähigkeit (Vererbbarkeit) abzugrenzen. Hinsichtlich der übergangsfä-
higen 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) Nachlassab-
wicklung 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 un-
terschiedlicher 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 zugrundelie-
genden Vertragsbeziehung so stark auf die Person des Berechtigten oder des Ver-
pflichteten zugeschnitten ist, dass sie bei einem Gläubiger- oder Schuldnerwech-
sel 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 er-
geben. 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 Subjekwechsel die Leistung in ihrem Wesen verändern würde. Nur die In-
halte, die mittels dieser Accounts vom Nutzer geschaffen oder kommuniziert wer-
den, sind in vielen Fällen höchstpersönlich, nicht aber die Leistungen des Provi-
ders im Rahmen der Vertragsbeziehung. Die Vertragsbeziehung mit ihren Rech-
ten 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 Spei-
chermedium 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 „anologen 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

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 verlängern, 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.


(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 ge richteten Anspruchs keine anderweitigen Ansprüche hergeleitet werden kön nen.

(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 Verbraucherrechtrechtlich Richtlinie umgesetzt worden ist, sollte erwogen werden, für Widerrufs Fälle ausdrücklich zu regeln, dass (auch) den Anbieter keine Wertsatzpflicht trifft.


(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 Lösungsverfahren 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


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.


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-

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.


- 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.


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 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).“


B. Datenbegriff

I. Definition

DIN 4430, Teil 2 Nr. 2.1.13 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. 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.

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.\textsuperscript{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.\textsuperscript{11}

Das BGB enthält in seiner geltenden Fassung in § 312f Abs. 3 BGB\textsuperscript{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\textsuperscript{13} fallen hierunter etwa Computerprogramme, Anwendungen (Apps), Spiele, Musik, Videos oder Texte. Ob die Daten heruntergeladen, gespeichert und hierarchisch sichtbar gemacht würden oder während des Herunterladens in Echtzeit sichtbar gemacht würden (Streaming), sei dabei unerheblich.


\section*{II. Abgrenzung zum Speichermedium}


\textsuperscript{10} Vgl. Becker, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, S. 815 (816).
\textsuperscript{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.
\textsuperscript{13} BT-Drs. 17/12637, S. 55.
\textsuperscript{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 Arbeitspeichern), 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


\(^{15}\) Näher aus technischer Sicht Hoppen, Sicherung von Eigentumsrechten an Daten, CR 2015, 802 (803 f.).


\(^{18}\) BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.

C. Daten im geltenden Recht


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.

Das trifft zwar auf typische Speichermedien wie Festplatten, CD-ROMs und USB-Sticks zu. Betrachtet man jedoch Daten insolvent, 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

Siehe unten (F.II.).

MüKol/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 Strom22 und von Software23 nach gel tendem 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 Gegenstands begriff. 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); MüKol/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.).
26 Vgl. MüKol/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-Mitgliedstaaten²⁸ – 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 Wirtschaftsgüter³⁰ 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

---


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 Auftraggeber erhält, bei Beendigung des Auftrags herauszugeben (§§ 667, 675 BGB).


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 ausge setzt, 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 Datennübermittlung 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,

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 auszustatten, 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 (I.) und die Immaterialgüterrechte (II.) 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).


36 Vgl. Palandt/Bassenge, BGB, § 903 Rn. 4 ff.
37 Vgl. Rehinder/Peukert, Urheberrecht, Rn. 126.
38 Vgl. Rehinder/Peukert, Urheberrecht, Rn. 142.
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 oder aber nur hinsichtlich einzelner Befugnisse begründet werden. Dazu könnten zählen:

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 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 Lösung 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 Hoen, 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.
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 Datenaanalyse 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 belassen.

b. Negative Rechte

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

---

44 Zech, "Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151 (1153 f.).
jeder Gebrauch der Sache ihre Nutzbarkeit durch andere potentielle Nutzer einschränkt und den Kreis der Nutzungsmöglichkeiten verkleinert.\textsuperscript{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 (nicht-rival), die aktuelle Nutzung durch eine Person beeinträchtigt also nicht die Nutzung durch beliebig viele andere Personen.\textsuperscript{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.\textsuperscript{48} Zu erwähnen ist schließlich, dass Daten, anders als die meisten Sachen, grundsätzlich nicht abnutzbar sind, woran die technische Abnutzung von Speichermedien nichts ändert.\textsuperscript{49}


\textsuperscript{49} Zech, Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (139 f.).
eine maßgebende Bedeutung zukäme, wenn man – unabhängig vom Dateninhalt und damit von der Schöpfungshöhe – jedes digitale Datum erfassen wollte.\textsuperscript{51}

Ob die Schaffung eines gänzlich neuen Rechts an Daten erforderlich und trotz des Grundsatzes des Numerus clausus der Sachenrechte\textsuperscript{52} dogmatisch umsetzbar wäre, bedarf eingehender Prüfung.\textsuperscript{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.\textsuperscript{54} Dafür sprechen die Rechtsklarheit\textsuperscript{55} und Rechtsicherheit, 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 Wertes personenbezogener Daten wird bereits heute die Weiterentwicklung des Datenschutzrechts diskutiert. Gegenstand dieser Diskussion sind insbesondere die Schaffung eines an das bestehende Urheberrecht angelehnten „Datennutzungsrechts“\textsuperscript{56} sowie die Rechtskonstruktion eines „immateriälgüterrechtlichen Eigentumsrechts an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten“\textsuperscript{57}. Hierbei handelt es sich allerdings


\textsuperscript{52} Dazu Staudinger/Seiler, BGB, Eckpfeiler des Zivilrechts, 2014, Sachenrecht – Allgemeine Lehren, Rn. 37.


\textsuperscript{54} Zech, Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 137 (146).


\textsuperscript{57} Fezer, Theorie des immateriälgüterrechtlichen 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.  

3. **Offene Fragen**

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

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.

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. 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.

**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...
dem Arbeitnehmer/Auftragnehmer oder dem Auftraggeber/Arbeitgeber zuzuordnen sind) 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). 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. 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


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

Skripturaktes wertungsgerechte Ausnahmen gelten, wenn der Eigentümer des Speichermittels die Skriptur nicht in irgendeiner Form mitveranlasst hat. Er folgt die Skriptur automatisch oder arbeitsteilig, soll nach der Wesentlichkeit des Beeinflussungsmoments abgegrenzt werden.

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.


IV. Zwischenergebnis

Als im Bedarfsfall näher zu überprüfende 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).
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 nämlichbspw. 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 Immateriagar-, 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

damit als Eigentum von § 823 Abs. 1 BGB erfasst. Ist der Berechtigte also Eigentümer des Datenträgers, sind auch die darauf abgelegten Daten deliktsrechtlich geschützt.\textsuperscript{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.\textsuperscript{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.\textsuperscript{78}

Wer Daten auf einem Datenträger ablegen, der weder in seinem Eigentum noch in seinem (berechtigten) Besitz steht, genießt danach grundsätzlich keinen deliktsrechtlichen 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 Driftschadensliquidation zu prüfen.\textsuperscript{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 Strafornormen) 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

\textsuperscript{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.

\textsuperscript{77} Statt vieler: Palandt/Sprau, BGB, § 823 Rn. 13 m. w. N.


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.\footnote{Herberger/Martinek/Rüßmann u.a./Lange/Schmidbauer, jurisPK-BGB, § 823 Rn. 18.} Anerkannt ist vielmehr, dass nur absolute, ausschließliche Rechte in Betracht kommen.\footnote{Statt vieler: Palandt/Sprau, BGB, § 823 Rn. 11.}

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.\footnote{Vgl. MüKo/Wagner, BGB, § 823 Rn. 205; BeckOGK/Spindler, BGB, § 823 Rn. 158.}


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

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. Dabei wird der Schutz teilweise auf qualifizierte Fälle beschränkt, etwa auf eine „Datensammlung von erheblicher Bedeutung“. In der Rechtsprechung und von der wohl überwiegenden Anzahl der Literaturstimmen wird die Anerkennung eines solchen sonstigen Rechts indes abgelehnt. Für beide Ansichten sprechen erhebliche Gründe:

a. Gründe für die Einordnung als sonstiges Recht


87 Vgl. MüKo/Wagner, BGB § 823 Rn. 207.
88 BeckOGK/Spindler, BGB, § 823 Rn. 183 a.E.
90 So Conrad/Grützmacher/Bartsch, Recht der Daten und Datenbanken im Unternehmen, S. 301; gegen eine derartige Einschränkung BeckOGK/Spindler, BGB, § 823 Rn. 186.
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 ver-
teilten Servern gespeichert sein mit der Folge, dass kaum oder gar nicht feststell-
bar 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 Wertungsgesichts-
punkt 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 zu-
kommen.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 überkomme-
nen, 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 ent-
sprechende Einordnung bei digitalen Daten nicht vor. Der Zugang zu Daten und

93 So etwa Conrad/Grützmacher/Bartsch, Recht der Daten und Datenbanken im Unternehmen,
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.

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 unzutragliche 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

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

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.


---


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:

Grundlegendste Schutzform ist der Integritätschutz 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 Be- stand 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

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.


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 Rückübertragung 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.\(^\text{111}\) 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.\(^\text{112}\) 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.\(^\text{113}\)

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).


(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 strafrechtlichen Schutzes von Daten (a), der deliksrechtliche 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.

(b) Deliksrechtlicher Schutz


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). Entsprechendes gilt für den deliksrechtlichen 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/Herberich, Nutzenergierende 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.
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


(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 hinzugekommen, 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

---

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

(b) Immaterialgüterrechte


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.).
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.\(^{127}\)


Diese Voraussetzungen dürften in vielen Fällen vorliegen, wenn unbefugt auf digitale Daten eines Unternehmens zugegriffen wird. 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.


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


III. Gesamt- und Einzelzwangsvollstreckung gegen Eigentümer des Speichermediums

1. Problemstellung


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.\textsuperscript{134}

Geht der Cloudbetreiber in die Insolvenz, kommt es zunächst auf die Ausübung des Wahlrechts des Insolvenzverwalters an.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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

\textsuperscript{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).
\textsuperscript{135} Dazu Bultmann, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (993).
\textsuperscript{136} Vgl. Jülicher, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063.
\textsuperscript{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.\(^\text{138}\)

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.\(^\text{139}\)

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:\(^\text{140}\)


\(^{138}\) 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 Kunden- 
daten und das Recht herauszugeben, diese Daten zu speichern und zu nutzen.

Bei einer Gesamtwürdigung aller Umstände sei, so das OLG Düsseldorf, zum ei-
en festzustellen, dass die Kunden, die sich bei dem Newsletter an- oder abge-
meldet hätten, im Rahmen ihres informationellen Selbstbestimmungsrechts und im 
Rahmen ihres sonstigen allgemeinen Persönlichkeitsrechts nur die Auftraggeber-
erin und nicht den Dienstleister ermächtigt hätten, die E-Mail-Adressen zum 
Zweck des Newsletter-Versands zu speichern und zu nutzen. Für die Auftraggeber-
erin seien diese, wenn auch von Seiten der Kunden jederzeit widerruflichen Er-
mächtigungen, ihre E-Mail-Adressen für den Newsletter-Versand zu speichern 
und zu nutzen, von erheblichem wirtschaftlichem Wert gewesen, weil sie auf die-
sem Wege ihre besonders interessierten Kunden gezielt habe bewerben können. 
Zum anderen habe die Auftraggeberin dem Dienstleister nur das von ihrer vorge-
nannten Rechtsstellung abgeleitete und nach dem Geschäftsbesorgungsvertrag je-
derzeit widerrufbare Recht eingeräumt, die E-Mail-Adressen insoweit zu spei-
ichern 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 Auf-
traggeberin eine Kopie seiner Daten zukommen lasse und gleichzeitig die Daten im 
eigenen Bestand lösche.\footnote{Vgl. zur Herausgabe von Daten Conrad/Grützmacher/Müller, Recht der Daten und Daten-
banken im Unternehmen, S. 313 ff. m. w. N.}

\textbf{b. Aussonderungsrecht bei Cloud Computing}

Die Entscheidung des OLG Düsseldorf,\footnote{OLG Düsseldorf, Urt. v. 27.9.2012 − I-6 U 241/11, CR 2012, 801, vgl. soeben a.} 
die in der Literatur zustimmend zitiert 
fügt sich in die insolvenzrechtliche Dogmatik ein:\footnote{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 Unter-
nehmen, 2014, S. 343.}

Die Aussonderung kann auf dingliche oder auf persönliche, also schuldba-
dliche Berechtigungen eines Dritten gestützt werden. Entscheidend ist, dass die Berech-
tigung dazu führt, dass der Gegenstand, dessen Aussonderung begehrt wird, als massefu-
rem anzusehen ist. Daher schließen sich Aus- und Absonderung gegen-
seitig aus, denn die abgesonderte Befriedigung kann nur in Bezug auf massezu-
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.\textsuperscript{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.\textsuperscript{146} Anders kann es bei schuldrechtlichen Herausgabeansprüche liegen.\textsuperscript{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.\textsuperscript{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.\textsuperscript{149} Ein solcher Anspruch ist regelmäßig gerichtet auf Herausgabe der Gegenstände, die der Geschäftsherr dem Geschäftsbesorger zur Ausführung des zu besorgenden Geschäfts übergeben hat.\textsuperscript{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.\textsuperscript{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

\textsuperscript{145} Uhlenbruck/Brinkmann, InsO, § 47 Rn. 9.
\textsuperscript{146} Vgl. MüKo/Ganter, InsO, § 47 Rn. 347.
\textsuperscript{147} Siehe nur MüKo/Ganter, InsO, § 47 Rn. 341 ff. m. w. N.
\textsuperscript{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).
\textsuperscript{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.
von § 823 Abs. 1 und 2 BGB geschützten Rechten/Rechtsgütern (u.a. allgemeines Persönlichkeitsrecht) und Straftatbeständen (etwa § 303a StGB) ergeben.¹⁵²


c. Rechtslage bei Vertragsketten


¹⁵² Näher Jülicher, Die Aussonderung von (Cloud-)Daten nach § 47 InsO, ZIP 2015, 2063 (2065); Bulthmann, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (995).
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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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, Drittwiderrufsverhältnisse nach § 771 ZPO zu erheben.


\textsuperscript{159} Vgl. \textit{Bultmann}, Aussonderung von Daten in der Insolvenz, ZInsO 2011, 992 (996).


\textsuperscript{161} Dazu BeckOGK/Spindler, BGB, § 823 Rn. 137; \textit{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


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


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.


5. \textbf{Zwischenergebnis}


IV. Handel mit Daten

1. Problemstellung


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.


---

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

3. Regelungsbedarf


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?


Auch sonst ist nicht erkennbar, dass der Datenhandel durch Einführung eines absoluten Rechts an Daten gefördert werden könnte. Vielmehr dürfte das Fehlen
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\textsuperscript{173} vorgeschlagen wird).


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


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


---

176 Näher oben unter B. 2. a.


c. Sonstige Erwägungen


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

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.\textsuperscript{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,


Gemeinsam ist allen diesen Fällen – die Liste ließe sich beliebig verlängern –, 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:


- 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. 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.).
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 Her-
steller in der Lage, dem Landwirt (kostenpflichtige) Dienstleistungen an-
zubieten. In Betracht käme auch eine Zuweisung der Daten an andere Be-
teiligte, etwa den Eigentümer der Flächen oder deren Pächter, an den Land-
wirt, 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 unmittel-
barsten veranlasst).  

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 mög-
lcherweise zu unerwünschten Ergebnissen führt. Nach einem Blick auf die gel-
tende Rechtslage (2.) wird daher zunächst noch einmal vertieft betrachtet, nach
welchen Kriterien automatisch generierte Daten rechtlich zugeordnet werden
können (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 zugrei-
fen kann, der sie also z. B. speichern, verarbeiten, verkaufen oder löschen kann.
Dies gilt allerdings nur vorbehaltlich etwaiger die Daten im Einzelfall betreffen-
der Rechtspositionen. In Betracht kommen insoweit weniger die Rechtsverhält-
nisse am Speichermedium. Daten werden nämlich nicht Bestandteil des Spei-
chermedium. Daten werden nämlich nicht Bestandteil des Spei-
chermedium zu klären.  

Die personelle Zuordnung kann sich aber aus dem Dateninhalt ergeben, etwa bei
personenbezogenen Daten (Datenschutzrecht, allgemeines Persönlichkeits-
recht)\textsuperscript{193}, bei Immateriagüterrechten (z. B. Urheberrecht) oder bei Daten, die Be-
triebs- oder Geschäftsgeheimnisse beinhalten. Ferner kann eine vertragliche Zu-
ordnung Bedeutung erlangen, etwa ein Kauf von Daten, ein Lizenzvertrag oder

\textsuperscript{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 Be-
tracht; ein nachvollziehbares Interesse habe fast jeder Beteiligte. Aus rechtlicher Perspektive
gebe es jedenfalls keine zwingende Antwort.

\textsuperscript{192} Vgl. BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.

\textsuperscript{193} Vgl. Specht, Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternati-
tiven – Eine Erläuterung des gegenwärtigen Meinungsstands und Gedanken für eine zukünftige
Ausgestaltung, CR 2016, 288 (292 f.).

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

---


\(^{195}\) 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.).


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, 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.

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


c. Sacheigentum


206 BGH, Urt. v. 10.7.2015 – V ZR 206/14, GRUR 2016, 109, Rn. 20.
entfernten Orten, weshalb die exakte Bestimmung des körperlichen Speichermittels an Bedeutung verliert.\textsuperscript{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), könnten 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.\textsuperscript{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-

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 Datenn mengen 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.\footnote{Vgl. Becker, Schutzrechte an Maschinendaten und die Schnittstelle zum Personendatenschutz, FS Fezer, 2016, S. 815 (823 f.).}

Das zeigt sich etwa bei den in der modernen Landwirtschaft generierten Daten, mit deren Hilfe der Landmaschinenhersteller dem Landwirt maßgeschneider 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\footnote{Monopolkommission, Sondergutachten zu „Herausforderung digitale Märkte“, BT-Drs. 18/5080, Ziff. 88 f.} empfiehlt, die Verfügungsrechte im Rahmen der Datenschutzregelungen zu konkretisieren. Eine Vergabe von eindeutigen, absoluten Rechten, wo immer möglich, sei wettbewerbspolitisch zu befürworten. Dabei sei
es aus ökonomischer Perspektive nicht eindeutig, welche Zuteilung der Verfü-
gungsrechte 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 ers-
scheint 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 ei-
nen 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, Immaterialgü-
terrechts, allgemeines Persönlichkeitsrecht, Schutz von Betriebs- und Geschäfts-
geheimnissen). Der Blick auf die in Betracht kommenden Zuordnungskriterien
hat gezeigt, dass ein einheitliches, allen vorgenannten Maßgaben gerecht werden-
des 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 betroffe-
nen Rechtsregimes vorgenommen werden. Verfügt bspw. ein PKW-Hersteller
über personenbezogene Daten des Fahrers, bietet das Datenschutzrecht grundsätz-
lich geeignetere Instrumente, als sie eine abstrakt-generelle Zuordnung eines ab-
soluten Rechts an den Daten ermöglichen würde. Entsprechendes gilt für die üb-
rigen 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 Zuord-
nung 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-

213 So auch Faust, Gutachten zum 71. Deutschen Juristentag, S. 56.
nelle Asymmetrien oder ein Marktversagen, dürfte das Kartellrecht eher für Abhilfe sorgen können als die Schaffung eines absoluten (Zivil-)Rechts an automatisch generierten Daten.\textsuperscript{215} Soweit ersichtlich, besteht insoweit – jedenfalls derzeit – allerdings kein vordringlicher Handlungsbedarf.\textsuperscript{216} Wie beispielsweise die zunehmend intensive Zusammenarbeit von Automobilindustrie und Internetwirtschaft zeigt, besteht hierfür ein Markt.\textsuperscript{217} Der Big-Data-Sektor wächst um 40\% pro Jahr und damit sieben Mal schneller als der IT-Markt insgesamt.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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 sachtäsigsten Instrumenten entgegentreten wird (z. B. AGB-Recht, Datenschutzrecht, Wettbewerbsrecht, Kartellrecht).

\textsuperscript{215} Näher Grützmacher, Dateneigentum – ein Flickenteppich – Wem gehören die Daten bei Industrie 4.0, Internet der Dinge und Connected Cars?, CR 2016, 485 (495).
\textsuperscript{216} Eingehend Dorner, Big Data und „Dateneigentum“, Grundfragen des modernen Daten- und Informationshandels, CR 2014, 617 (626 f.).
\textsuperscript{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 dessen, der faktisch auf automatisch generierte digitale Daten zugreifen kann; diese (speziellen) Rechtsbereiche kommen auch für die Korrektur etwaiger Fehlerentwicklungen 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 Regeln 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 insofern 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 hindern- des Recht i. S. v. § 771 ZPO berufen.


---

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


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

3. Folgerungen für die Zwangsvollstreckung in Daten


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.\textsuperscript{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


\textsuperscript{232} Vgl. Zöller/Stöber, ZPO, § 857 Rn. 12c m. w. N.

\textsuperscript{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 (verfügbaar bei beck-online).
faktische Ausschließlichkeit begründet aber grundsätzlich kein absolutes Recht i. S. v. § 857 Abs. 1 ZPO.\textsuperscript{234}


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,\textsuperscript{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.

\textsuperscript{234} Vgl. BGH, Beschl. v. 5.7.2005 – VII ZB 5/05, NJW 2005, 3353 f. (zu Internet-Domains).
\textsuperscript{235} Vgl. Zöller/Stöber, ZPO, § 857 Rn. 12c m. w. N.
\textsuperscript{236} LG Mönchengladbach, Beschl. v. 22.9.2004 – 5 T 445/04, MDR 2005, 118; Zöller/Stöber, ZPO, § 857 Rn. 12c.
\textsuperscript{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


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. 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.


**II. Einschätzungen der Wissenschaft**

Dieser Befund wird im Wesentlichen bestätigt durch die herangezogene Literatur.\(^\text{241}\) Nur vereinzelt wird die Schaffung eines absoluten Rechts an Daten (oder eine andere gesetzgeberische Maßnahme) vorgeschlagen.\(^\text{242}\) 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 Sachzusammenhängs 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.).


1. Erforderlichkeit eines neuen Schutzgesetzes


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

---

246 So etwa Wagner, eigene Mitschriften der Arbeitsgruppe.
247 Vgl. oben E. II.

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.

2. Schutzlücke bei Herausgabeansprüchen


3. Schaffung eines neuen Immaterialgüterrechts an Maschinendaten

Becker und Zech sprechen sich für die Schaffung eines neuen Immaterialgüterrechtes 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.


\(^{254}\) Vgl. oben E., insbesondere unter II. und III.

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

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. Im Übrigen sei wegen der wirtschaftlichen Bedeutung und der enormen Auswirkungen eines absoluten Datennutzungsrechts eine breite gesellschaftliche Diskussion geboten.

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 angelehnten „Datennutzungsrechts“ sowie die Rechtskonstruktion eines „immateri algorechtlichen Eigentumsrechts an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten“ diskutiert. Anders als die dem Prüfauftrag der Arbeitsgruppe geschuldete Perspektive in diesem Kapitel stellen diese Ansätze...
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 immateriellgüterrechtlichen 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, 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.


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 meint etwa, es solle „nicht vorzeitig nach dem Gesetzgeber gerufen werden, zu groß ist die Gefahr der verfehlten Monopolisierung von Informationen.“ Grünberger warnt vor unangemessen hohen Transaktionskosten, wenn bei der Verwendung von Daten stets das Schutzobjekt, sein Inhaber und die geschützten Verwertungshandlungen identifiziert werden müssten. Heymann hält die Konstruk-

---

263 Siehe oben B.III.
264 Schwartmann/Hentsch, Eigentum an Daten – Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV 2015, 221.
267 Heymann, Der Schutz von Daten bei der Cloud Verarbeitung, CR 2015, 807 (809 ff.).


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-, Zwangs- vollstreckungs- 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

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.

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 Verbraucherverbände279 wie auch der Verbände der Wirtschaft280 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.
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.\textsuperscript{283}

IV. Bestrebungen auf europäischer Ebene


Ob die gegenwärtigen Initiativen in die Begründung eines „europäischen Daten-eigentums“ 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

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.\textsuperscript{284}

V. Ausblick

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


Auch die Entwicklung der Wettbewerbsverhältnisse sollte beobachtet werden. Es gilt, eine verfehlte Monopolisierung von Daten zu verhindern.\textsuperscript{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 Marktzutritsschranken durch exklusive Datenherrschaft marktmächtiger Unternehmen hin.\textsuperscript{286} Im März 2016 hat das Bundeskartellamt ein Verfahren gegen Facebook wegen des Verdachts eröffnet, dass

\textsuperscript{284} Vgl. Becker, Rechte an Industrial Data und die DSM-Strategie, GRUR Newsletter 01/2016, S. 7 (11).

\textsuperscript{285} Dazu oben E. V. 4. a. (2).

durch die Ausgestaltung von Vertragsbedingungen zur Verwendung von Nutzerdaten eine mögliche marktbeherrschende Stellung auf dem Markt für soziale Netzwerke missbraucht worden sein könnte.\textsuperscript{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.\textsuperscript{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


\textsuperscript{287} Bundeskartellamt, Pressemitteilung vom 2.3.2016, http://www.bundeskartellamt.de/Shared-Docs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html.

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.


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**


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 computer-gesteuert ermöglicht, ohne dass der Mensch noch selbst eingreift.\footnote{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).} 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.

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 behelf, 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; Staedinger/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 wieder.\textsuperscript{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\textsuperscript{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 programstechnisch über Funktionen vorgegeben sind.\textsuperscript{298} Sie sind damit autonome Systeme.\textsuperscript{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-

\textsuperscript{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.

\textsuperscript{297} Sorge, Softwareagenten, Vertragsschluss, Vertragsstrafe, S. 42.


III. Zugang von Erklärungen, die von Maschinen in Empfang genom- men und autonom weiterverarbeitet werden


Problem und wird in der Praxis der vollautomatisierten Bestellverfahren mittels Computererklärung wohl kaum eine Rolle spielen, 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.


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:

---

306 Siehe nur MüKo/Busche, BGB, § 133 Rn. 12.
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**


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.
Die denkbaren Fallkonstellationen und Möglichkeiten lassen sich an dieser Stelle nicht abschließend darstellen. 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. 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.

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 sowohl wertungsmäßig als auch künstlerschaftlich um einen Fehler, der dem Erklärungsirrtum gleichsteht, da der Wille dann als bloßer Motivirrtum andererseits.

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. 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 Geschäftsirritümern (§§ 119 ff. BGB) einerseits und dem grundsätzlich nicht zur Anfechtung berechtigenden bloßen Motivirrtum andererseits. Die mitunter in Grenzfällen schwie-

---

316 Dazu Faust, Bürgerliches Gesetzbuch Allgemeiner Teil, § 21 Rn. 21, 23 (Fall 14b); MüKo/Säcker, BGB, Einl. Rn. 193 a.E.
317 Köhler, Die Problematica 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\textsuperscript{320} und des Kalkulationsirrtums\textsuperscript{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\textsuperscript{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 Regulierungsmodell der Rechtsgeschäftslehre des Bürgerlichen Gesetzbuches systemkonform zu konkretisieren. Vorauselnde 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.

---

\textsuperscript{320} Siehe hierzu die umfangreichen Nachweise und Ausführungen bei MüKo/Armbrüster, BGB, § 119 Rn. 81 ff.

\textsuperscript{321} Siehe hierzu die umfangreichen Nachweise und Ausführungen bei MüKo/Armbrüster, BGB, 119 Rn. 85 ff.

\textsuperscript{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“ 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 genannt:

- **Smart Products** verursachen Schäden beim Käufer (z. B. selbsfahrender Rasenmäher),
- **autonome Systeme** 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 – 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.
2. Anspruch auf Schadensersatz oder Ersatz vergeblicher Aufwendungen


3. Besonderheiten beim Einsatz von direkter M2M-Kommunikation?


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.


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 Horner/Kaulartz, Haftung 4.0 – Verschiebung des Sorgfaltsmaßstabs bei Herstellung und Nutzung autonomenter Systeme, CR 2016, 7 (8).
b. Anspruch aus § 823 Abs. 2 BGB


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. Es handelt sich dabei um eine verschuldensunabhängige Gefährdungshaftung (§ 1 Abs. 1 ProdHaftG), die einen Haftungshöchstbetrag bei Tod oder Körperschädigung (§ 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.

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

---

3. Haftungslücken beim Betrieb von autonomen Systemen


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

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. Für die Schadenszurechnung kommen mithin Hersteller und Betreiber in Betracht:


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


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


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


---


\(^{352}\) Horner/Kaulartz, Haftung 4.0 – Verschiebung des Sorgfaltmaßstabs bei Herstellung und Nutzung autonomer Systeme, CR 2016, 7 (13).

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 Gesetzebungskompetenz 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 Gemeinwohlninteresse 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**


c. **Lösungsansatz 3: Entwicklung eines neuen Haftungsregimes**


---

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 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“.


---

356 2015/2103(INL), Rn. 49.
357 2015/2103(INL), Rn. 51.
358 2015/2103(INL), Rn. 58.
IV. Empfehlungen


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.

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 in der allgemeingültigen Definition.\(^{361}\) Der Dachverband der digitalen Wirtschaft, Bitkom e.V., verwendet folgende Begriffsbestimmungen:


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 Entwicklung, 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.


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.  

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

   (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 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.

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


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


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

---

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.

(3) Hybrid Cloud


(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.\(^\text{371}\) 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.\(^\text{372}\)

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.\(^\text{373}\)

\(^{370}\) Vgl. Borges/Meents/Krcmar, Rechtshandbuch Cloud Computing, § 1 Rn. 50.
\(^{371}\) Borges/Meents/Krcmar, Rechtshandbuch Cloud Computing, § 1 Rn. 49.
\(^{373}\) Vgl. Borges/Meents/Krcmar, Rechtshandbuch Cloud Computing, § 1 Rn. 51 ff.

### 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]


b. „Platform as a Service“ [PaaS]

Kurzbeschreibung: Bereitstellung einer (Entwicklungs-)Plattform.

---

\(^{374}\) Borges/Meents/Krcmar, Rechtshandbuch Cloud Computing, § 1 Rn. 59 ff.


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. 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.

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.


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


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 Be- schaffung 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.
Verfügung gestellt, sondern diese vom Anbieter selbst eingesetzt, um eine vom Kunden definierte Leistung zu erbringen.\textsuperscript{380}

\section*{4. Akteure (Wertschöpfungsstrukturen)}

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

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{cloud_computing_akteure.png}
\caption{Wertschöpfungsstruktur des Cloud Computing}
\end{figure}

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

\begin{enumerate}
  \item \textbf{Nutzer / Konsument}
  Der Konsument (auch als „Kunde“ bezeichnet) kauft Dienstleistungen mittels unterschiedlicher Distributionskanäle, etwa direkt vom Serviceanbieter oder mittels einer Marktplattform.
  \item \textbf{Infrastrukturanbieter}
  Infrastrukturanbieter stellen die zum Betrieb von Anwendungen benötigten Computing- und Speicherlösungen bereit. Sie bilden somit das „technische Rückgrat“.
  \item \textbf{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.
\end{enumerate}

\textsuperscript{380} Hilber/Intveen/Hilber/Rabus, Handbuch Cloud Computing, Teil 2, Rn. 148.
\textsuperscript{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

Die zentralen Erkenntnisse fasst die Studie wie folgt zusammen:


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,\textsuperscript{385}
- Urheberrecht,
- Steuerrecht (u.a. bei steuerrechtlich relevanten Daten, §§ 146 ff. AO),\textsuperscript{386}

\textsuperscript{384} Computerwoche 2017-10-11 vom 6.3.2017, S. 6 f.
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


   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. 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

---


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:


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 Richtliniendruck vereinbart. Für das vorliegende Arbeitspapier ist er dennoch vor allem unter zwei Aspekten von besonderer Bedeutung:


b. Mitteilung und Konsultationen zur Schaffung einer Europäischen Datenwirtschaft

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 Dienstleistungs begriff 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. 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.

2. Vertragliche Pflichten / Schuldrechtliche Einordnung


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.
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“
➔ 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

---

b. Vertragstypologische Einordnung

(1) Ausgangspunkt


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 Mängelgeltungsteils400,
- 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

---

398 Borges/Meents/Krcmar, Rechtskonzepte Cloud Computing, § 2 Rn. 20.

- 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

(2) Typengemischte/Zusammengesetzte Verträge


\(\Rightarrow\) 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.

\(\Rightarrow\) 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
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 Vertrags-
typ „verschmolzen“, handelt es sich um einen sog. typengemischten Vertrag, 
bekommt gee. 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 Vertrags-
konstellation zugrunde:

Die Parteien waren durch einen sog. ASP-Vertrag (Application Service Provi-
ding/Bereitstellung von Softwareanwendungen und damit verbundenen Dienst-
leistungen) verbunden. Hiernach stellte der Anbieter (Kläger) dem Nutzer (Be-
klagten) auf einem zentralen Server installierte Buchhaltungs- und Warenwirt-
schaftssoftware zur Nutzung über das Internet zur Verfügung. Der Vertrag um-
fasste die „Miete der Software incl. Programmpflege, kostenlose Pro-
grammpdates, Nutzung bis zu 500 MB Datenvolumen/User, tägliche Datensi-
cherung, Hotlineservice“.

Der BGH bestätigte in der genannten Entscheidung die Vorinstanz, auf den zwi-
schen 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
derüber hinaus vereinbarte – Zurverfügungstellung von Speicherkapazitäten auf
dem Server des Anbieters zur Speicherung der vom Nutzer im Rahmen der Soft-
warennutzung 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 Män-
geln, MMR 2012, 783 (784); siehe hierzu auch die Übersicht bei Borges/Meents, Rechtshand-
buch 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 Vertragsarten (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


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.\textsuperscript{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)**


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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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

ein wichtiger Aspekt bei der vertragsrechtlichen Einordnung von Vereinbarungen über SaaS.\textsuperscript{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.\textsuperscript{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 träge. 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.\textsuperscript{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.\textsuperscript{418} Der BGH

\textsuperscript{415} Vgl. Zech, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3.
\textsuperscript{416} Hilber/Paul/Niemann, Handbuch Cloud Computing, Teil 3, Rn. 85.
\textsuperscript{417} Hilber/Paul/Niemann, Handbuch Cloud Computing, Teil 3, Rn. 128.
\textsuperscript{418} Hilber/Paul/Niemann, Handbuch Cloud Computing, Teil 3, Rn. 91; Wandtke/Bullinger/Grützmacher, Praxiskomentar zum Urheberrecht, § 69c Rn. 5.
stellt jedoch eine rein technische Betrachtung an, nach der derjenige ver-
viehfältigt, der die körperliche Festlegung technisch bewerkstelligt und
kontrolliert. Dies zugrunde gelegt ist es in aller Regel der Anbieter, dem
die Vervielfältigung zuzurechnen ist, nicht der Nutzer. Letzterer hat stan-
dardmäßig 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 bestimm-
mungsgemäße Nutzung der SaaS innerhalb der Cloud handelt.

- 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

- Die Erstellung von Backups im Rahmen von SaaS wird, wie oben darge-
estellt, durch den Anbieter innerhalb seiner Infrastruktur und nicht durch den
Nutzer vorgenommen. Einer Nutzungsrechteinräumung gegenüber dem
Nutzer bedarf es daher nicht. Diese Vervielfältigungshandlung seitens des
Anbieters ist von § 69d Abs. 2 UrhG gedeckt.

- 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) erfasst.

419 BGH, Urt. v. 22.4.2009 – I ZR 216/06, CR 2009, 598.
423 Hilber/Paul/Niemann, Handbuch Cloud Computing, Teil 3, Rn. 97.
424 Hilber/Paul/Niemann, Handbuch Cloud Computing, Teil 3, Rn. 147 f.
426 Wandtke/Bullinger/Grützmacher, Praxiskomentar 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.\(^\text{427}\) Dies bedeutet in letzter Konsequenz, dass auch auf diese Vertragsbeziehungen Mietvertragsrecht anzuwenden ist.


\(^{427}\) Hilber/Intveen/Hilber/Rabus, Handbuch Cloud Computing, Teil 2, Rn. 152.
\(^{428}\) Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 47.
\(^{430}\) Hoeren/Sieber/Holznagel/Redeker, Handbuch Multimedia-Recht, Teil 12, Rn. 387, 391.
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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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


\textsuperscript{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).

\textsuperscript{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).

\textsuperscript{435} Hilber/Intveen/Hilber/Rabus, Handbuch Cloud Computing, Teil 2, Rn. 167.

mit werkvertraglichem Charakter vorliegt und damit grundsätzlich Werkvertragsrecht nach §§ 631 ff. BGB zur Anwendung kommt. 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. 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.

4. Einordnung übriger Vertragsleistungen


5. Erleichterung vertragstypologischer Zuordnung durch Einfügung eines „§ 453 Abs. 1 BGB“ ins Mietrecht


---

438 Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 61.
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.“

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.


IV. Untersuchung einzelnener Aspekte unter Zugrundelegung einer vertragstypologischen Einordnung als Miet-, Dienst- oder Werkvertrag

1. Pflichten der Vertragsparteien


a. Mietvertrag

Die Hauptleistungspflicht des Cloud-Anbieters (Vermieters) besteht bei Anwendung von Mietvertragsrecht darin, dem Cloud-Nutzer (Mieter) den Cloud Service
während der Dauer des Vertrages in einem zum vertragsgemäßen Gebrauch ge- eigneten Zustand „bereitzustellen“ (Grundsatz der ständigen Verfügbarkeit).


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.

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.

In der Literatur wird die Frage nicht einheitlich beantwortet, ob zur Erhaltungspflicht des Cloud-Anbieters auch die Durchführung von Modernisierungs- oder Aktualisierungsmaßnahmen gehört.

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.

---

444 Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 73.
446 Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 76.
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


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


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.
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.

d. Vertragsänderungen/-anpassungen


2. Leistungsstörungen


Je nach vertragstypologischer Einordnung der geschuldeten Leistung können unterschiedliche Gewährleistungsrechte zur Anwendung kommen.

\paragraph*{a. Mietrecht}


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.).


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.


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.
Erfüllungsgehilfen.\textsuperscript{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.\textsuperscript{469} Den Cloud-Anbieter trifft demnach ein hohes Risiko.\textsuperscript{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.\textsuperscript{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. pauschalerer Schadensersatz, ausfallen soll.\textsuperscript{472} Die Vertragspartner können aber individualvertraglich weitgehende Haftungsbeschränkungen vereinbaren, solange diese nicht gänzlich hinter das gesetzliche Leitbild des Mietrechts zurückfallen.\textsuperscript{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.\textsuperscript{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.\textsuperscript{475}

\textsuperscript{468} A.A. wohl Kirn/Müller-Hengstenberg, Überfordert die digitale Welt der Industrie 4.0 die Vertragstypen des BGB?, NJW 2017, 433 (436).
\textsuperscript{469} BGH in st. Rspr., u.a. NJW 2000, 2344; NJW 2009, 142.
\textsuperscript{471} Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 94, 114.
\textsuperscript{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.\textsuperscript{476}

b. Dienstvertragsrecht


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.\textsuperscript{477}


\textsuperscript{476} Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 102.
\textsuperscript{477} Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 104.
\textsuperscript{478} Hilber/Intveen/Hilber/Rabus, Handbuch Cloud Computing, Teil 2, Rn. 225.
\textsuperscript{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. 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


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.


481 Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 84.
nicht arglistig verschwiegen oder eine Garantie für die Beschaffenheit des Werks übernommen hat (§ 639 BGB).\footnote{Vgl. zu allem Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 108 ff., 116.}


3. \textbf{Haftung}


\begin{enumerate}
\item \textbf{Haftungsbeschränkung in AGB}


zum Schutz des Verbrauchers eingeschränkt sind, sind häufig haftungsbeschränkende AGB unwirksam.\textsuperscript{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.\textsuperscript{488} Die Problematic 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 Vertragschluss unter Einbeziehung einseitig vorformulierter Klauseln typischerweise zu beobachten ist, stärker Berücksichtigung findet.\textsuperscript{489}


\hspace{1em}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.\textsuperscript{490} Hierbei ist


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.\textsuperscript{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 Kollosion 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.\textsuperscript{492}

c. Haftung des Cloud-Nutzers


d. Durchsetzbarkeit


\textsuperscript{491} Bohm, Herausforderungen von Cloud Computing-Verträgen: Vertragstypologische Einordnung, Haftung und Eigentum an Daten, ZEuP 2016, 358 (379).
4. Laufzeit / Beendigung


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).


- Weitere Beendigungsstatbestände 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:


496 Vgl. Palandt/Weidenkaff, BGB, § 542 Rn. 1 ff.


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 Verbraucher- 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.


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. 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.


---

den Zeitraum nach Vertragsschluss, aber vor Erbringung der ersten geschuldeten Leistung sinnvoll.\footnote{Borges/Meents, Rechtshandbuch Cloud Computing, § 4 Rn. 224.}

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;

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.\footnote{Schuster/Hunzinger, Vor- und nachvertragliche Pflichten beim IT-Vertrag – Teil II: Nachvertragliche Pflichten, CR 2015, 277 (278).}

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-

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.

505 Der Umfang der erforderlichen Migrationsunterstützung ist dabei letztlich einzelfallabhängig. So kann der Cloud-Anbieter auch verpflichtet sein, dem Cloud-Nutzer etwa eine Dokumentation des Know-how's zur Verfügung zu stellen, z. B. in Form von Prozessbeschreibungen, damit entweder der Cloud-Nutzer selbst oder der neue Anbieter leistungsfähig sind.

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.

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.

508 Borges/Mee, Rechtshandbuch Cloud Computing, § 4 Rn. 229.
509 Unabhängig davon können entsprechende Ansprüche in Bezug auf personenbezogene Daten aus datenschutzrechtlichen Gesichtspunkten bestehen.

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). Nutzt 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. zeintensiven 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.


\(^{511}\) 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.\footnote{Schuster/Hunzinger, Vor- und nachvertragliche Pflichten beim IT-Vertrag – Teil II: Nachvertragliche Pflichten, CR 2015, 277 (283 f.).}

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:


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


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


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


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 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.


III. Vertragsrechtliche Einordnung von Live-Streaming

Der hier nachzugehende 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“


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

---

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. 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.


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. Beispielsweise 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

---

der Öffentlichkeit viel diskutierten Fälle von kino.to\textsuperscript{524} und Redtube\textsuperscript{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.\textsuperscript{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.\textsuperscript{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\textsuperscript{528} – Werkgenuss, sondern bei der gebotenen objektiven Betrachtung um einen Eingriff in das Vervielfältigungsrecht (§ 16 UrhG).\textsuperscript{529} Daran ändert auch der Umstand nichts, dass es dem durchschnittlichen Benutzer nicht

\begin{footnotes}
\item[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 haben, 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.
\item[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).
\end{footnotes}
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.\footnote{Zech, Lizenzen für die Benutzung von Musik, Film und E-Books in der Cloud, ZUM 2014, 3 (6).}

Gleichwohl bedarf es mit Blick auf die Schrankenregelung des § 44a Nr. 2 UrhG im Ergebnis keiner Einräumung von Nutzungsrechten durch den Streaming-Anbieter.


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)\footnote{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.} 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-
abhängig von der Rechtmäßigkeit der Vorlage zu betrachten ist und es ausschließlich auf die Rechtmäßigkeit der Nutzung ankommt. 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.


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:


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.).

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 Abonnementvertrag 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).


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.


(3) Vertragsrechtliche Einordnung eines unentgeltlichen Vertrages über Live-Streaming


Der Begriff der Geschäftsbesorgung in § 662 BGB ist im Übrigen denkbar weit zu verstehen. Gegenstand eines Auftragsverhältnisses können Dienste jeder Art sein. 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. 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/Weißenkaff, BGB, § 611 Rn. 27.
543 MüKo/Müller-Glögge, BGB, § 611 Rn. 34.
Ungeachtet dessen, dass sich die vertragsrechtliche Einordnung grundsätzlich nach den Haupteistungspflichten 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.


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 dahin- stehen, 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.\textsuperscript{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-

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

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.


Für die Einordnung als Mietvertrag spricht schließlich auch der Vergleich mit der Miete eines Datenträgers (Bsp.: Film-DVD). Dies gibt auch mit Blick auf die folgenden, im Wesentlichen technisch bedingten Besonderheiten beim On-Demand-Streaming:

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 Hauptleistungs-pflicht betreffen.

Eine andere Beurteilung ergibt sich auch nicht daraus, dass für den Abspielsvorgang beim On-Demand-Streaming die Erstellung einer sequentiellen Kopie der Daten beim Clienten erforderlich ist. Bei einer Gesamtbetrachtung des Abspielsvorgangs ergeben sich angesichts der automatischen Lösung 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. Im Übrigen ist mit Blick auf die oben genannte ASP-

Rechtsprechung des BGH zu vermuten, dass sich die Rechtsprechung bei Fortgel- tung der bestehenden Rechtslage ebenfalls zur Anwendung mietrechtlicher Vor- schriften 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.


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.\textsuperscript{553} Soll Gegenstand des Leistungsbestimmungsrechts die Hauptleistungspflicht des Vermieters aus einem Mietertrag 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.“\textsuperscript{554}


\textsuperscript{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.
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


(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 Vertragstyps 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.

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.

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.


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 Gleichheit 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.

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


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


\(^{559}\) Nachfolgend RL-E.


2. Einzelne vertragsrechtliche Pflichten / Problemstellungen


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

---

hat. Im Falle einer Verletzung dieser Vertragspflicht drohen die (gesetzliche) Minderung der geschuldeten Miete oder anderweitige Gewährleistungsansprüche.


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


nicht durch Auslegung anhand des Vertragszwecks ermitteln lässt, ist der übliche Gebrauch zu gewähren.\textsuperscript{564}


Allerdings lässt sich dieses Problem – analog zu den obigen Überlegungen zur vertragstypologischen Einordnung sowie der Miete einer Film-DVD – durch eine entsprechende Konkretisierung der Haupleistungspflicht 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.\textsuperscript{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 mindesstens 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;

\textsuperscript{564} Vgl. MüKo/Häublein, BGB, § 535 Rn. 65.

\textsuperscript{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.


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


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 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


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.


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 Beendigungsstatbestände 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.


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.


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.


1. Begriff und Merkmale sozialer Netzwerke


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.
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.

2. Gesellschaftliche Bedeutung

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.\textsuperscript{580}

Das dominierende Geschäftsmodell\textsuperscript{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\textsuperscript{582} Aspekte im Vordergrund.

III. Vertragsrechtliche Fragestellungen und Lösungsansätze

\textsuperscript{580} Siehe oben I. 2.
\textsuperscript{581} Dieses Geschäftsmodell liegt u. a. Facebook, Google+ und Twitter zugrunde.
\textsuperscript{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.\(^5\)

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\(^6\). 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.\(^5\)

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


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


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

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 Netzerwerks 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.\textsuperscript{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\textsuperscript{590} auch eine Einordnung als Mietvertrag bzw. als mietvertragsähnliches Rechtsverhältnis.\textsuperscript{591}

Im Schrifttum wird des Weiteren eine Rechtsbeziehung mit miet- und dienstvertraglichen Elementen angenommen.\textsuperscript{592} In der instanzgerichtlichen Rechtsprechung\textsuperscript{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 zukunfts positive Regelung, die soziale Netzwerke vertragstypologisch einordnet, kaum möglich sein.

\textsuperscript{589} Vgl. zum Ganzen Bräutigam/Sonleithner, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 28 m. w. N. auch zur a. A.
\textsuperscript{590} BGH, Urt. v. 15.11.2006 – XII ZR 120/04, NJW 2007, 2394 ff.
\textsuperscript{591} Vgl. Bräutigam/Sonleithner, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 29f. m. w. N. zum Schrifttum.
\textsuperscript{592} Bräutigam, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635 (640); Bräutigam/Sonleithner, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 19.

Die Kündbarkeit des Vertrags dürfte sich nach den allgemeinen Regelungen und Grundsätzen für die Kündbarkeit von Dauerschuldverhältnissen bestimmen.

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.


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


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.


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

200 Stücke gleicher Gattung und Menge – fehlt. Auch die grundlegenden Funktionen von Geld erfüllen personenbezogene Daten nicht\textsuperscript{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 \textit{Entgelt} – zugewendet wird.\textsuperscript{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 ein wirtschaftlich zugänglich ist. Die tatsächlich schwierige Frage nach dem wirtschaftlichen Wert personenbezogener Daten, der auf fundamentalen Voraussetzungen beruht und je nach Kontext der beabsichtigten Datenverwendung sehr unterschiedlich sein kann, muss deshalb bei der schuldrechtlichen Einordnung nicht entschieden werden.\textsuperscript{603}

\textsuperscript{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 aufeinanderzutreffen 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.


\textsuperscript{602} Vgl. dazu ausführlich Staudinger/Olzen, BGB, § 241 Rn. 14 ff.

\textsuperscript{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.\textsuperscript{604}

Im Verhältnis zwischen dem Anbieter eines „kostenlosen“ sozialen Netzwerks und dessen Nutzer stehen sich vielmehr wechselseitige (nicht monetäre) Hauptleistungspflichten gegenüber.\textsuperscript{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 Synalagma vor.


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 Rechtsgeschäften 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).\textsuperscript{604}

\textsuperscript{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.

\textsuperscript{605} In diesem Sinne auch Benninghoff, Brauchen wir eine „Button“-Lösung für das Datenschutzrecht, VuR 2013, 361 f.

Geld. Personenbezogene Daten seien nicht identisch mit Geld, schon weil sie mehrfach weggelassen werden könnten und ihr Wert nicht messbar sei. Dienstanbieter 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 Verbraucherrechte. Es müsse deshalb vermieden werden, personenbezogene Daten als Ware wie jede andere zu behandeln.


Daten“ wäre es inkonsequent, bürgerlich-rechtliche Regelungen für dieses Phäno-
men, welche für die mit Daten „bezahlenden“ Personen ausschließlich vorteil-
haft 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, Rechts-
beziehungen unter bürgerlich-rechtlichen Aspekten zu regeln, bedarf es eines auf 
him aufbauenden Datenschuldrechts.

2. Art der Hauptleistung des Nutzers

Die Einordnung von Daten bzw. der Einwilligung in die wirtschaftliche Verwer-
tung von Daten als Gegenstand eines Leistungsaustauschs im Rahmen eines 
Schuldverhältnisses ist gegenwärtig weder auf EU-Ebene noch im deutschen Zi-
vilrecht geregelt. Es gibt bislang – auch in anderen Mitgliedstaaten – kein „Da-
tenschuldrrecht“ 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. identi-
fizierbarer 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 Da-
ten“ 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-Datenschutzrichtlinie607 zugrunde liegt, sind personenbezo-
gene Daten praktisch sämtliche Daten, die mit einer bestimmten bzw. bestimm-
baren Person in Verbindung stehen.608 Erfasst ist jede Information geistigen In-
halts 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 Nut-
zer bei der Registrierung ihren wahren Namen und wahre weitere persönliche In-
formationen angeben müssen.

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


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


---

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 abgestellt, 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


In einer die Internetwirtschaft unnötig beeinträchtigenden Weise zu weitgehend wäre ein Abstellen auf die aktive Datenhingabe deshalb, weil ein „Bezahlen mit Daten“ dann bereits vorliege, 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

---


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 Software618 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.

---

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 sächsgerecht, 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 sächs- 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 Rechswirkungen des Geschäfts von einem ungewissen zukünftigen Ereignis abhängig macht.\(^{619}\) Bei der auflösenden Bedingung wird das Fortbestehen der Rechswirkungen 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.


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 Netzerwerks 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.\(^{620}\)


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.


\(^{620}\) 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. 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.\textsuperscript{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\textsuperscript{623}, erscheint eine solche Regelung mit Bezug auf soziale Netzerwerke als nicht erforderlich.


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

\textsuperscript{622} So generell für Verbraucherverträge der Beschluss Ziffer 15 der Abteilung Zivilrecht des 71. Deutschen Juristentags 2016.


\textsuperscript{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.


5. Einordnung der Hauptleistung des Nutzers im System des Schuldrechts

Die vom Nutzer als Voraussetzung einer Nutzung des sozialen Netzwerks zu erzielende 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

---


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)


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.

Im Schrifttum wird der Aspekt der Datenqualität im Zusammenhang mit „Big Data“ diskutiert. Im Vordergrund steht dabei der Erwerb von Rohdaten und von Resultaten aus Big-Data-Anwendungen.


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.


---

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.
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. Bezugszeitpunkt: „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 beschrifft ist (sog. „Button-Lösung“).


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).

---


634 Siehe dazu oben unter I. 4. b. (2).
sondern die *rein zivilrechtliche Frage*, wie eine datenschutzrechtliche Einwilligung (datenschuldrechtlich) zum Bestandteil eines synallagmatischen Vertrags gemacht werden kann.

Ergänzend sollte § 312a Abs. 3 BGB um eine Regelung ergänzt werden, wonach eine Vereinbarung, die auf ein über das vereinbarte Entgelt hinausgehendes „Bezahlen mit Daten“ gerichtet ist, *ausdrücklich* getroffen werden muss.


Eine entsprechende Ergänzung empfiehlt sich für die Fallgestaltung, dass der Verbraucher eine datenschutzrechtliche Einwilligung als „Zusatzentgelt“ leisten soll, in § 312a Abs. 3 BGB.

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 Hauptleistungs-Pflicht – 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 Einfalls- tor 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.


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 Einwilligungs erfordernis 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 Geldbetrages durch A nicht dadurch zu einer Hauptleistungspflicht von B, weil ein von B vorgegebener formularmäßig Vertragstext als dessen vertragliche Hauptpflicht bestimmt, A durch die Entgegennahme des Geldbetrages 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.


Aus vorstehenden Erwägungen vermag – entgegen einer im Schrifttum geäußerten Befürchtung\textsuperscript{647} – auch Art. 6 Abs. 1 lit. f EU-DSGVO nicht das Einwilligungsverfahrens 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 „rechtsgeschäftigen 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 \textit{so selbstverständlich}, dass es \textit{keiner} darauf bezogenen \textit{Regelung} bedarf.

\textsuperscript{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 beismessen.

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.\textsuperscript{648}

Dass der Begriff „entgeltlich“ in § 312 Abs. 1 BGB weit ausgelegt werden muss und Verbraucherverträge auch dann als entgeltlich einzuarbeiten 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.\textsuperscript{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.


\textsuperscript{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.

\textsuperscript{649} Vgl. insoweit Brömke/Schmidt, Der Anwendungsbereich der Vorschriften über die besonderen Vertriebsformen nach Umsetzung der Verbraucherrechtsrichtlinie, VuR 2014, 3; dem folgend Palandt/Grüneberg, BGB, § 312 Rn. 3; ebenso jurisPK/Junker, BGB, § 312 Rn. 20.

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.“

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 mit Nachweisen zum aktuellen Schrifttum 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 folgt, 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.
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.


„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
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.


b. Verarbeitung personenbezogener Daten für eigene Zwecke als Leistung


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
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.\footnote{Zur Bedeutung von Kardinalpflichten und zur Inanspruchnahme besonderer Vertrauens bei § 307 Abs. 2 Nr. 2 BGB vgl. Palandt/Grüneberg, BGB, § 307 Rn. 48, 50.}

Soweit Fragen der Gefahrtragung, Gewährleistung und Haftung im Schrifttum vereinzelt thematisiert werden, wird eine Anwendbarkeit des allgemeinen Leistungsstörungsrechts (§§ 280 ff. BGB) angenommen.\footnote{Bräutigam/Sonnleithner, Vertragliche Aspekte der Social Media, in: Hornung/Müller-Terpitz, Rechtshandbuch Social Media, Rn. 25, auch zur Frage von Haftungserleichterungen.}

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.


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.
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 Werter satzpflicht 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.


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 im Wege des Streaming zu konsumieren. Verträgen über Streaming-Leistungen wird an anderer Stelle näher nachgegangen.

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 stehen—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“,...

657 Siehe dazu Kapitel 2 Abschnitt E.

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


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.“
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).
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.

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


zunehmend Verträge über die zeitlich begrenzte Einräumung von Nutzungsrechten.


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 (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.

---

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. 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 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 (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.

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.

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.


Widerrufsrecht mit Beginn der Ausführung des Vertrags verliert. Auch diese Bestätigung kann der Unternehmer über die genannte Schaltfläche einholen.\textsuperscript{675}

Den Beginn der Vertragsausführung seitens des Unternehmers wird man beim Erwerb digitaler Inhalte über das Internet im \textit{Beginn des Downloads} zu sehen haben.\textsuperscript{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.\textsuperscript{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.\textsuperscript{678}


\textsuperscript{675} Vgl. Graef, Recht der E-Books und des Electronic Publishing, Rn. 158.

\textsuperscript{676} Vgl. Graef, Recht der E-Books und des Electronic Publishing, Rn. 158.


\textsuperscript{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.

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.


(2) Diskutierte Änderungen

Der 71. Deutsche Juristentag 2016 fordert681, 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 Faust683 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.

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.


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.


Zu den Informationspflichten des Unternehmers gehört nach Art. 246a § 1 Abs. 1 S. 1 Nr. 15 EGBGB des Weiteren die Verpflichtung, den Verbraucher „gebenfalls, 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.\textsuperscript{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.\textsuperscript{686}

Ein Regelungsbedarf wird insoweit nicht thematisiert und ist auch nicht ersichtlich.

\textbf{IV. Anwendbarkeit der allgemeinen Regelungen des bürgerlichen Rechts auf den Erwerb digitaler Inhalte}


1. \textbf{Vertragsschluss und Minderjährigenschutz}

Der Abschluss eines Kaufvertrags über das Internet bestimmt sich nach den allgemeinen Regelungen (§§ 145 ff. BGB).\textsuperscript{687} Für den bürgerlich-rechtlichen Minderjährigenschutz gelten dabei keine besonderen Vorschriften.

a. \textbf{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\textsuperscript{688} hat in einem solchen Fall ein Handeln unter fremdem Namen angenommen, auf das die Regeln über die Stell-

\textsuperscript{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.
\textsuperscript{686} Vgl. – auch zu wettbewerbsrechtlichen Unterlassungsansprüchen und einem Unterlassungsklagerecht nach § 2 UKlAG – Erman/Koch, BGB, § 312a Rn. 34 und § 312d Rn. 68.
\textsuperscript{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.
\textsuperscript{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.\textsuperscript{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.


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 Vertrags schlüssen 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.

\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{694}

\textsuperscript{690} Zur Umsetzbarkeit verbraucherpolitischer Ziele im bürgerlichen Recht siehe unten V.
\textsuperscript{691} Vgl. Faust, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, II. 5.
\textsuperscript{693} Vgl. BGH, Urt. v. 15.11.2006 – XII ZR 120/04, Tz. 15, CR 2007, 75 f. m. v. w. N.
\textsuperscript{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.


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 erlangt696, gehört eine nicht konkret vereinbarte spätere Bereitstellung neuerer technischer Versionen i. S. v. „Updates“ der digitalen Inhalte nicht zu den Hauptleistungspflichten des Verkäufers.


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).  
694 Siehe dazu nachstehend unter IV. 5.  
695 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).  
696 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 Ergebnissen⁷⁰⁰.

---


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 passieren701;

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;


V. Bürgerlich-rechtliche Einordnung und Umsetzbarkeit verbraucherpolitischer Ziele mit Bezug auf Verträge über den Erwerb digitaler Inhalte


Eine Würdigung unter schuldbrechtlichen 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:


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."


„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.“


---


705 Siehe S. 5 des Berichts der DRM-Projektgruppe.
Eines Weiterveräußerungsrechts für rechtmäßig erworbene digitale Güter ausgesprochen.706


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:

---


• 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


a. Urheberrechtliche Aspekte


709 Siehe dazu oben unter V.
710 Vgl. Wandtke/Bullinger/Bullinger, UrhR, § 19a Rn. 10 f., 23.

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 erworbenen digitale Inhalte kopieren darf, sowie die gesondert untersuchte 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.


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, finden über § 453 Abs. 1 BGB auf den Erwerb digitaler Inhalte entsprechende Anwendung.

711 Siehe dazu nachfolgend die Ausführungen unter V. 2.
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 6121978.

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.


---


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 Ladenpunkten 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


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 – 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. 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. Aus solchen (Neben-)Pflichten können sich – auch wenn

§ 242 BGB selbst grundsätzlich keine Anspruchsgrundlage ist – klagbare Erfüllungsansprüche ergeben.


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 entschuldbbarer Weise über Bestehen oder Umfang seines Rechts im Ungewissen ist.


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 u. 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.

VII. Empfehlungen


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.


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 erworbbener digitaler Inhalte zum rezeptiven Werkgenuss würde sich nicht in das geltende Vertragsrecht einfügen.
I. WAP-Billing und Zahlungswege im Internet

I. Allgemeines


Von diesen Themenkomplexen wiederum zu trennen sind die virtuellen Währungen, die im nächsten Abschnitt beleuchtet werden.

II. Bezahldienste


Bei sog. Zahlungsauslösedienstleistern 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 Zahlungsdienst­richtlinie auch eine gesetzliche Grundlage geschaffen werden.\textsuperscript{722}

\textbf{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.\textsuperscript{723}

\textbf{1. Technischer Hintergrund}\textsuperscript{724}


\textbf{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,

\textsuperscript{722} Entwurf eines Gesetzes zur Umsetzung der Zweiten Zahlungsdienstrichtlinie, BR-Drs. 158/17.

\textsuperscript{723} Wegner, Betrugsstrafbarkeit bei Missbrauch des „WAP-Billing“-Verfahrens, NStZ 2016, 455.

\textsuperscript{724} Vgl. zu diesem Absatz Wegner, Betrugsstrafbarkeit bei Missbrauch des „WAP-Billing“-Verfahrens, NStZ 2016, 455.

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 schlüssigen 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:

§ 45k gewährt wird, wenn sie ihre Forderung auf die Telefonrechnung des Schuldners setzen lassen.“

3. Problemaufriss


\textsuperscript{725} YouGov 2016 – Verbraucherbefragung WAP-Billing/Ergebnisbericht für das BMJV, S. 4.
\textsuperscript{727} YouGov 2016 – Verbraucherbefragung WAP-Billing/Ergebnisbericht für das BMJV, S. 34.
\textsuperscript{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).

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 äußer 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.

4. Lösungsmöglichkeiten


Folgende Lösungsmöglichkeiten können in Betracht gezogen werden:

a. Voreinstellung einer Drittanbietersperre


730 BR-Drs. 436/16.

731 Vgl. Ziffer 3 der BR-Drs. 436/16 (B).


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.


Auch die Verbraucherschutzministerkonferenz sieht in der Einführung eines Widerspruchsrechts eine Möglichkeit, den Mechanismus der Abbuchung von unbe rechtigten Drittforderungen über die Telefonrechnung außer Kraft zu setzen (vgl. Beschluss der VSMK unter Ziffer 6).

IV. In-App-Käufe


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 Zahlungsrichtlinie in deutsches Recht – keinen gesetzgeberischen Handlungsbedarf. Zahlungsauslösedservice sollen künftig in Umsetzung der Zweiten Zahlungsdienerichten gesetzlich geregelt werden.


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 Geldwäscherrichtlinie 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. In Deutschland wurden bislang lediglich Bitcoin anerkannt. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ordnet Bitcoin als mit Devisen vergleichbare Rechnungseinheiten im Sinne des § 11 S. 1 Nr. 7 Kreditwesengesetz (KWG) ein. 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.

II. Technischer Hintergrund


---

739 Boehm/Pesch, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung – Eine erste juristische Einordnung, MMR 2014, 75.
740 Beck, Bitcoins als Geld im Rechtssinne, NJW 2015, 580.
742 Heine, Bitcoins und Botnetze – Strafbarkeit und Vermögensabschöpfung bei illegalem Bitcoin-Mining, NSiZ 2016, 441.
743 Beck, Bitcoins als Geld im Rechtssinne, NJW 2015, 580.
wird.\textsuperscript{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.\textsuperscript{746}


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

\textsuperscript{745} Kütük/Sorge, Bitcoin im deutschen Vollstreckungsrecht – Von der „Tulpenmanie“ zur „Bitcoinmanie“, MMR 2014, 643.

\textsuperscript{746} Boehm/Pesch, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung – Eine erste juristische Einordnung, MMR 2014, 75.

\textsuperscript{747} Kütük/Sorge, Bitcoin im deutschen Vollstreckungsrecht – Von der „Tulpenmanie“ zur „Bitcoinmanie“, MMR 2014, 643.

\textsuperscript{748} Beck, Bitcoins als Geld im Rechtssinne, NJW 2015, 580.

\textsuperscript{749} Vgl. zum gesamten Absatz Boehm/Pesch, Bitcoins: Rechtliche Herausforderungen einer virtuellen Währung – Eine erste juristische Einordnung, MMR 2014, 75.


**III. Problemfelder**


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).\footnote{Palandt/Grüneberg, BGB, Einl. v. § 241 Rn. 5.} Dies ist bei virtuellen Währungen jedoch nicht der Fall.

1. Online-Handel


Die Beantwortung dieser Fragen hängt von der Rechtsnatur der Bitcoins sowie der zugrundeliegenden schuldrechtlichen Verträge ab.

a. Kaufvertrag


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.


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.  

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.

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.

f. Zwischenergebnis


---

2. Haftungsrechtliche Probleme


3. Zwangsvollstreckung

Angesichts ihres Werts und ihrer zunehmenden Verkehrsfähigkeit stellt sich die Frage, ob und inwieweit auf Bitcoins im Rahmen der Zwangsvollstreckung zugreifen werden kann. Die Zwangsvollstreckung richtet sich nach den Regelungen der Zivilprozessordnung (ZPO).

a. Anwendbarkeit §§ 808 ff. und 829 ff. ZPO


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. § 857 ZPO beinhaltet eine Auffangnorm, um das Vermögen des Schuldners umfassend als Haftungsgrundlage zu erschließen. Nicht von § 857 ZPO erfasst und unpfändbar sind bloße Befugnisse

---

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 und tatsächliche Verhältnisse sowie Vermögensinbegriffe. 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


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.

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.


\textsuperscript{763} Richtlinie 2000/31/EG („Richtlinie über den elektronischen Geschäftsverkehr“).
\textsuperscript{764} Verordnung 2016/679/EU („EU-Datenschutzgrundverordnung“).
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 Gesetzesbedarf und hält es im Allgemeinen für vorzugs würdig, 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


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.


---


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 Entscheidungssohheit 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.\textsuperscript{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:

\textsuperscript{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.

\textsuperscript{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.


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.\textsuperscript{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 Unrechtmäßigkei der Verarbeitung, die anderweitige Rechtfertigung 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 Rechtfertigung oder der 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.


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

\textsuperscript{770} \textit{Boehme-Neßler}, Das Recht auf Vergessenwerden, NVwZ 2014, 825 (829).
beziehungsweise auf das auf der Öffnungsklausel des Art. 8 Abs. 1 S. 3 EU-DSGVO beruhende nationale Recht abzustellen.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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\textsuperscript{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


Grundsätzlich besteht allerdings de lege lata kein zivilrechtlicher Anspruch des Opfers einer Persönlichkeitsrechtsverletzung gegen den Dienstanbieter auf Auskunft über die Identität des Täters oder Teilnehmers. Ein zivilrechtlicher Auskunftsanspruch lässt sich zwar aus Treu und Glauben gem. § 242 BGB ableiten.

\textsuperscript{772} Kühling/Buchnet/Herbst, DS-GVO, Art. 17 Rn. 34.
\textsuperscript{773} Kühling/Buchnet/Herbst, DS-GVO, Art. 17 Rn. 35.
\textsuperscript{774} Gola/Nolte/Werkmeister, DS-GVO, Art. 17 Rn. 27.
\textsuperscript{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. 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.

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.


---

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.
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 Dienstanbietern 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 Richtertvorbehalt 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/Telefónica“ 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.


Hierfür spricht, dass die Inanspruchnahme auf Auskunft im Hinblick auf Bestands- und Nutzungsdaten dem Verhältnismäßigkeitsgrundsatz genügen muss. 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

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 rufschrädigenden Meinungsaussprüchen kann dem Verletzten auf negatorischer und deliktischer Grundlage zudem ein Anspruch auf Veröffentlichung einer strafbewehrten Unterlassungsverpflichtung des Verletzers zustehen, wenn die unzulässige Meinungsaussprache öffentlich erfolgt ist und die Publikation der Untersuchungserklärung 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 personlichkeitsrechtsverletzender 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.


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.
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.


Daneben kommen datenschutzrechtliche Ansprüche in Betracht. Zu unterscheiden ist zwischen Löschungsansprüchen auf datenschutzrechtlicher Grundlage nach

- nationalem Recht (Bundesdatenschutzgesetz und Landesdatenschutzgesetze) und

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


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.

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

---

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.\textsuperscript{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.\textsuperscript{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 persönlickeitsrechtsverletzenden Inhalten etc.).


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.

\textsuperscript{789} BGH, Urt. v. 27.3.2007 – VI ZR 101/06.


\textsuperscript{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.\footnote{OLG Hamburg, Urt. v. 7.7.2015 – 7 U 29/12.}

f. Online-Enzyklopädien


g. Host-Provider


Cloud-Provider werden in der Literatur teilweise Host-Providern gleichgestellt.\footnote{Neidinger, Anmerkung zur Entscheidung des BGH, Urt. v. 26.11.2015 – I ZR 174/14, CR 2016, 408 (410).}

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,


\subsubsection*{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.


j. Domain-Registrar

Streit besteht zur Haftung von Domain-Registern. Die Rechtsprechung hat Ansprüche gegen Domain-Registre 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).
⁸⁰¹ EuGH, Urt. v. 15. 9.2016 − Rs. C-484/14 (Mc Fadden).
⁸⁰² BR-Drs. 276/17.
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 erstrebt, 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 Ur sprungsbeitrags 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.

808 Vgl. z. B. BGH, Urt. v. 28.7.2015 – VI ZR 340/14, NJW 2016, 56, Rn. 27 m. w. N.
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“


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.\textsuperscript{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.\textsuperscript{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 Einzelfalls richtet. Geht der Intermediär den Hinweisen nicht nach, kann der Rechtsweg beschritten werden.\textsuperscript{814}

Inhaltlich geht die Rechtsprechung davon aus, dass bei unwahren Tatsachenbehauptungen die Abwägung grundsätzlich zu Gunsten des Betroffenen zu erfolgen habe.\textsuperscript{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“

\textsuperscript{812} Z. B. Erwägungsgrund 78 der EU-DSGVO einerseits, Erwägungsgrund 66 der EU-DSGVO andererseits.

\textsuperscript{813} Vgl. Art. 23 Abs. 1 Buchst. j. EU-DSGVO, Erwägungsgrund 73 der EU-DSGVO.

\textsuperscript{814} LG Heidelberg, Urt. v. 9.12.2004 – 2 O 162/13 (zu Google).

\textsuperscript{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 Verleumung,
- Recht auf Resozialisierung,
- Aggregation von Informationen aus verschiedenen Quellen und Lebensbereichen zu einem „Abbildung 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.


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:


\(^{816}\) *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.\textsuperscript{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)

Die Verfahren sind je nach Dienstanbieter 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:


\textsuperscript{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.


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 Lösung 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.


---

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.

• 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 Lösung sicherzustellen.

Die Arbeitsgruppe hat wünschenswerte Bestandteile eines sachgerechten Lösungsverfahrens 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 Lösungsverfahren 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


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.


(3) Anhörung

Grundsätzlich geboten ist eine Pflicht zur Anhörung der für den Beitrag 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 Dienstanbietern eine Art Schiedsrichterfunktion\textsuperscript{820} zueingerkennt:\textsuperscript{821}


- 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 gesetzt 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.\textsuperscript{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 Meinungsaussprache durch einen Angriff auf den zugrundeliegenden Sachverhalt relativiert.

\textsuperscript{820} Höch, Bewegung bei Bewertungsportalen – wie Unternehmen ihren Ruf im Netz besser schützen können, BB 2016, 1475 (1478).

\textsuperscript{821} BGH, Urt. v. 25.10.2011 – VI ZR 93/10, juris Rn. 26 f. („blogspot.com“).

\textsuperscript{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.


der Verordnung Nr. 1348/2000 anerkannt wurde, die bei Ablauf dem vorliegen-
den 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.\footnote{EuGH, Urt. v. 11.6.2009 – Rs. C-564/07.}

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 Unter-
richtung 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; al-
lerdings ist zu gewährleisten, dass der Beschuldigte tatsächlich über die volle Frist
für die Einlegung des Rechtsmittels verfügt.\footnote{EuGH, Urt. v. 15.10.2015 –
Rs. C-216/14.} Auch insofern sind nationale Re-
gelungen nur beschränkt sinnvoll.

Übersetzungspflichten sollten sich nach den allgemeinen Vorschriften richten.
Der Aufwand für die Vorlage einer Übersetzung erscheint angesichts des verfass-
sungsrechtlichen Gebots hinnehmbar.

Im Beschlussweg ergangene Unterlassungsverfügungen eines deutschen Gerichts
haben im Ausland nur beschränkte Wirkung. Mögliche Maßnahmen zur
Steigerung der Effizienz einstweiliger Verfügungen gegen ausländische Dienste-
anbieter sind derzeit jedoch nicht ersichtlich. In EU-Mitgliedsstaaten sind einst-
weilige Verfügungen nach Art. 42 Abs. 2 Brüssel-İa-VO (EU) 1215/2012 ohne
Exequaturverfahren vollstreckbar.

(b) Einführung eines Verbandsklagerechts

Mit dem Ende Februar 2016 in Kraft getretenen Gesetz zur Verbesserung der zivi-
relrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Da-
utschutzrechts 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.\footnote{Kühling/Buchnet/Bergt, DS-GVO, Art. 80 Rn. 13, 18;
Halfmeier, Die neue Datenschutzver-
bandsklage, NJW 2016, 1126; Schantz, Die Datenschutz-Grundverordnung, NJW 2016, 1841;
a.A. Gola/Werkmeister, DS-GVO, Art. 80 Rn. 18.}

Da das Datenschutzrecht seine Wurzeln im Recht auf informationelle Selbstbe-
stimmung 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 au-
ßerhalb verbraucherschützender Vorschriften des Datenschutzrechts wäre es sinn-
voll, ein Verbandsklagerecht für die Fälle einzurichten, in denen der Dienstean-
bieters nicht das geforderte Löschverfahren vorhält. Dies erscheint im Hinblick auf
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“


(d) Ergänzende öffentlich-rechtliche Rechtsdurchsetzung


(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. 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.


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 des 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

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 Mitgliedstaaten unberührt lässt, spezifische Anforderungen vorzuschreiben, die vor der Entfernung von Informationen oder der Sperrung des Zugangs unverzüglich zu erfüllen sind.


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.


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-

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.\footnote{Brunst, Umsetzungsprobleme der Impressumspflicht bei Webangeboten, MMR 2004, 8 (12 f); Müller-Broich, TMG, § 5 Rn. 17 ff.} Es könnte sich daher anbieten, dies für die deutsche Sprache entsprechend gesetzlich zu konkretisieren, wenn man das Lösungsverfahren 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.


(d) Mögliche Regelungsorte


Wie durch den Deutschen Bundestag in seiner Entscheidung 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...


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.\(^{837}\)

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.


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 ein Diensteanbieter eine Verweisung auf Internetseiten mit einem unschwer zu bejahenden persönlichkeitsrechtswidrigem Inhalt nicht dauerhaft entfernt, nachdem er hierauf hinreichend konkrekt 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;³³⁸

- 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 active Rolle spielen, die ihm eine Kenntnis von bestimmten Daten oder eine Kontrolle über sie verschaffen konnte.³³⁹

Nach der Rechtsprechung des EGMR kann eine von einem nationalen Gericht verhängte Entschädigungszahlung für die nicht automatische Lösung 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.³⁴⁰

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.³⁴¹

Insgesamt sieht die Arbeitsgruppe derzeit keinen über die geltende Rechtslage hinausgehenden Regelungsbedarf.

³³⁹ BGH, Urt. v. 19.3.2015 – I ZR 94/13, juris Ls. 3 (“Hotelbewertungsportal”).
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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{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.

\textsuperscript{843} BGH, Urt. v. 25.10.2011 – VI ZR 93/10, BGHZ 191, 219.
\textsuperscript{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.


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 Erlaubnisstatbestand 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, und durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden können. 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. 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.


- 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-


851 BGH, Urt. v. 28.1.2014 – VI ZR 156/13 (Schufa-Scoring); BVerfG, 1 BvR 756/14 (abhängig).
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. Das allgemeine Persönlichkeitsrecht beinhaltet nämlich auch das Recht, in gewählter Anonymität zu bleiben und die eigene Person nicht in der Öffentlichkeit dargestellt zu sehen. Das BVerfG hat sich mehrfach mit der Anonymisierung von Daten befasst.

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 Klarnamens 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.

Des Weiteren wird die Frage diskutiert, ob vor dem Hintergrund des Grundrechts schutzes, 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.
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.\textsuperscript{858} Grundlage der Diskussion ist die politische Forderung, dass Rechtsverletzungen im Internet besser verfolgbare sein sollten.\textsuperscript{859} Insbesondere zur Aufklärung schwerer Straftaten ist kürzlich der Zwang von Telekommunikationsanbietern zur Vorratsdatenspeicherung erneut eingeführt worden.\textsuperscript{860} Hiergegen ist jedoch von verschiedener Seite Verfassungsbeschwerde erhoben worden; eine Entscheidung darüber steht noch aus.\textsuperscript{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 Klarnamenszwang für Äußerungen im Internet vor dem Hintergrund zunehmender, teils justizierbarer 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.\textsuperscript{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 sensiblen Themen generell deaktiviert wird. Andererseits wird immer wieder darauf

\textsuperscript{858} Vgl. auch Härting, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065 (2068); Heckmann, Anonymität der IT-Nutzung und permanente Datenverknüpfung als Herausforderung für Ehreschutz 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“).


\textsuperscript{860} BT-Drs. 18/5088, dazu Nachbaur, Vorratsdatenspeicherung „light“ rechtswidrig und allenfalls bedingt von Nutzen, ZRP 2015, 215.


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.\footnote{Vgl. auch Härting, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065 (2068).}

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.

\section*{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 Profile, 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.
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.


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-


Vor diesem Hintergrund sieht die Arbeitsgruppe derzeit in diesem Themenbereich keinen Regelungsbedarf.

F. Ausspähen von Daten


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).

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.\footnote{Umfangreiche Darstellung: Roos/Schumacher, Botnetzes als Herausforderung für Recht und Gesellschaft – Zombies außer Kontrolle?, MMR 2014, 377.}

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.\footnote{BR-Drs. 338/16.}

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.


Die Anspruchslage, auch mit Blick auf Ansprüche gegenüber Dienstanbietern, wenn dort hinterlegte Daten durch Dritte ausgespäht werden, erscheint nach den bisherigen Recherchen der Arbeitsgruppe ungeklärt. Das BVerfG hat als Ausprü-
gung des allgemeinen Persönlichkeitsrechts ein Grundrecht auf Schutz der Integ-
rität und Vertraulichkeit informationstechnischer Systeme geschaffen. Das
Grundrecht ist drittschützend und damit im Verhältnis von Privaten zueinander
von Belang.  
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 Sicherheits-
vorkehrungen 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 Be-
seitigungsansprüche 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 Erstellen von Persönlichkeits- und Nutzungsprofilen, des
Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziel-
len Zwecken erhoben, verarbeitet oder genutzt werden. Art. 80 EU-DSGVO lässt
dies auch zukünftig zu.  
Hierzu ist darauf hinzuweisen, dass bspw. der Verbraucherzentrale Bundesver-
band (vzbv) zwischenzeitlich zum dritten Mal ein Klageverfahren gegen Face-
book angestrengt hat (u. a. wegen irreführender Werbung für einen angeblich
kostenlosen Dienst, kritischer Voreinstellungen sowie diverser Klauseln in den
Nutzungsbedingungen). Dass darüber hinaus auch die Einschaltung der Daten-
schutzbeauftragten dazu beitragen kann, den Interessen der Nutzer Gehör zu ver-
schaffen, scheint das jüngste Verhalten von Facebook zu belegen, wonach das
Unternehmen vor dem Hintergrund entsprechender Beanstandungen des
Hamburgischen, aber auch der britischen Datenschutzbeauftragten die Weiter-
gabe von Daten europäischer Whats-App-Nutzer vorerst gestoppt haben soll.

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 be-
steht.

---

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.
875 https://www.welt.de/wirtschaft/article159391467/Datenweitergabe-von-WhatsApp-an-Fa-
cebook-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-Website) 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. Die praktische Bedürfnis an einer dahingehenden Regelung erscheint aber zweifelhaft.


---

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.
Dass es Möglichkeiten der Rechtsdurchsetzung beim Erhalt ungewollter Werbung auch gegenüber Intermediären gibt, erscheint ebenfalls gesichert.878


Bislang hatte sich die Rechtsprechung hierzu unter lauterkrechtsrechtlichen Aspekten zu befassen. Ob Anbieten, Vertrieb und Bewerbung derartiger Werbeblocker lauterkrechtsrechtlich 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-find 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.
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.


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. Ombudsman 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 Dienstanbieter 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.

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.“


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. Bemerkenswert

\footnote{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).}

\footnote{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).}

\footnote{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/Möhre-Sobolewski, Digitaler Nachlass – Erbenschutz trotz Datenschutz, NJW 2015, 3473 (3473).}

\footnote{Ludyga, Der digitale Nachlass – zivilrechtliche Aspekte, juris Die Monatszeitschrift 2016, 442 (443).}

\footnote{Steiner/Holzer, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (266); Solmecke/Köbrich/Schmitt, Der digitale Nachlass – haben Erben einen Auskunftsanspruch? –}

Unstreitiger Ausgangspunkt aller Diskussionen um den „digitalen Nachlass“ ist § 1922 BGB (Universalsukzession). Insoweit wird allgemein die Ansicht vertreten, dass 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.

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.

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


So insbesondere vom DAV bezüglich des Datenschutzrechts/ Fernmeldegeheimnisses − § 88 TKG, vgl. dazu im Folgenden noch ausführlich.


88 Kutscher (Diss.), S. 44, 102 (vorab mit rechtlicher Analyse von Accounts auf S. 21 ff.).
Übertragbarkeit im Wege der Gesamtrechtsnachfolge aus. Dem Erben stehe der-
selbe Anspruch auf Zurverfügungstellung der E-Mails als Haupteinstellungspflicht zu wie zuvor dem Erblasser, da zum Eigentum auch die auf dem Abschluss von Verträgen beruhenden schuldrechtlichen Forderungen gehörten. Der DAV hat al-
erdings telekommunikationsrechtliche und verfassungsrechtliche Vorbehalte (Art. 10 GG, § 88 TKG), die diesen Anspruch nach Ansicht des DAV möglicher-
weise 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 be-
jaht.\(^{891}\)

Sehr ausführlich und differenziert behandelt aktuell Seidler im Rahmen einer Dis-
sertation die Frage der Übergangsfähigkeit eines E-Mail-Accounts\(^{892}\) und dif-
ferenziert insoweit zwischen der zugrundeliegenden Rechtsbeziehung (der Rechtsbeziehung zwischen dem Provider und dem Nutzer, also dem „E-Mail-Ver-
trag“), 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 schuldrecht-
liche 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 Über-
gangsfähigkeit dieser Rechtspositionen kommt auch sie dazu, dass sowohl die vertraglich ausgestaltete Accountinhaberschaft als auch das Einsichtsrecht über-
gangsfähig 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 Prob-
lem, NJW 2013, 3745 (3749); Pruns, Keine Angst vor dem digitalen Nachlass! Erbrechtliche Grundlagen – Alte Probleme in einem neuen Gewand?, NWB 2013, 3161 (3165); ebenso Hoe-
eren, 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 zivil-
rechtlich 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. Hoorer
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 Haupteistung personenbezogen sei, da in diesem Fall gute Gründe für eine Unvererblichkeit sprächen. Auch im Hinblick auf Accounts, welche die Nutzung sozialer Netzwerke betreffen, wird hingegen ganz überwiegend vertreten, dass auch derartige Accounts vererblich sind. 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. 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 Haupteistungspflicht 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. 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 postmortaler 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 postmortaler 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.\textsuperscript{902} Seidler untersucht zudem die Übergangsähigkeit getrennt für die Kontoinhaberschaft und das Einsichtsrecht, gelangt aber für beide Positionen zu dem Ergebnis, dass sie auf den Erben übergehen.\textsuperscript{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\textsuperscript{904} und für Heimpflegeverträge\textsuperscript{905} entschieden, dass diese unvererblich sind.\textsuperscript{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.\textsuperscript{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.\textsuperscript{908}

\textbf{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

\textsuperscript{902} Seidler (Diss.), S. 136.
\textsuperscript{903} Seidler (Diss.), S. 139 (mit ausführlicher Herleitung auf S. 134-139).
\textsuperscript{904} AG Dortmund, Urt. v. 18.9.1990 – 128 C 413/89, NJW-RR 1991, 689; zustimmend Kutscher (Diss.), S. 156 f.
\textsuperscript{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.
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. 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.


Seitens des DAV wurden aber Bedenken hinsichtlich eines Verstoßes gegen das durch § 88 TKG geschützte Fernmeldegeheimnisses geäußert, 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).


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,

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. 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.

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.


Eine solche Differenzierung nimmt aber Hoeren (auch bei bereits abgerufenen E-Mails) vor, da die E-Mails, die keinen vermögensrechtlichen Bezug hätten, nicht vererbarbar und daher den nächsten Angehörigen zuzuleiten seien, die dann die Persönlichkeitsrechte des Erblassers treuhänderisch wahrnehmen.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 Vermögensphäre betreffenden und überwiegend hochpersönliche Sachverhalte betreffenden Daten unterschieden werden müsse. Die Trennung müsse durch treuhänderische Eingriff eines neutralen Dritten erfolgen, etwa des Dienstanbieters. Dies würde jenem zwar einige 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).
929 Martini, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeits schutzes im Internet, JZ 2012, 1145 (1147).
930 Martini, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeits schutzes im Internet, JZ 2012, 1145 (1147 ff., insbesondere 1152).
931 Brinkert/Stolze/Heidrich, Der Tod und das soziale Netzwerk, ZD 2013, 153 (155 f.).

\f

Nachweis der Erbenstellung gegenüber Providern bei Geltendmachung eines Auskunftsanspruchs (insbesondere Frage der Wirksamkeit entsprechender AGB-Klauseln)


\f

\f

\f

\f

\f

\f

\f

\f

\f

\textit{Herzog} vertritt hingegen ohne nähere Begründung die Auffassung, dass die Provider i. d. R. zum Nachweis der Erbenstellung den Erbschein verlangen können.\footnote{Herzog, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750 f.).} Auch der DAV ist der Ansicht, dass der Erbschein verlangt werden könne, da entsprechende AGB-Klauseln in Parallele zu den Bankrechtsfällen wirksam seien.\footnote{DAV, Stellungnahme Nr. 34/2013, S. 62-64.}

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 Kündigungs­ und Abwicklungsklauseln diskutiert:

(1) Kündigungs­klauseln


\textit{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
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 erworbe Rechtspositionen des Erblassers im Regelfall auch nach seinem Tod fortbestehen, nicht vereinbar seien. 940

(2) Legitimationsklauseln


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.  

(3) Abwicklungsklauseln (Klauseln bezüglich der Abwicklung von Providerverträgen):


Kutscher folgt dieser Ansicht 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.


---

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 zugrundeliegender Vertrag (z. B. der eBay-Account) geht nach den bereits oben dargelegten Grundsätzen (vorbehaltlich etwaiger wirksamer vertraglicher abweichender Regelungen) auf den Rechtsnachfolger über. Fragens 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.\textsuperscript{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\textsuperscript{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,

\textsuperscript{951} Herzog, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750).

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.\textsuperscript{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.\textsuperscript{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. Der 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

\begin{footnotesize}
\textsuperscript{953} Bräutigam, Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, 635 (640).
\textsuperscript{954} Redeker, IT-Recht, Rn. 1173.
\end{footnotesize}


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


b. Erbrechtlicher Übergang von E-Mails und Problematik der Differenzierung zwischen Daten mit Vermögenscharakter und höchstpersönlichen Daten


\(^{955}\) 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.


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.).
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.


(2) Nicht abgerufene E-Mails

Bei den noch nicht abgerufenen E-Mails besteht ein durch den Erbfall erworbener vertraglicher Anspruch des Erben gegen den Dienstanbieter auf Zugang zu den seitens des Dienstanbieters 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 dahingeahnd, 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.
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 Dienstleister zu übertragen.\textsuperscript{964} Dies hat zur Folge, dass § 88 TKG entsprechend Art. 10 GG auszulegen ist.\textsuperscript{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 „Verfügungsbeauftragung“ über den Kommunikationsvorgang (Inhalt und Verkehrsdaten) mit dem Zugang im E-Mail-Postfach des Empfängers auf diesen übergeht.\textsuperscript{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.\textsuperscript{967}

Die teilweise vertretene Gegenansicht, wonach jeglicher nicht durch die Einwilligung des Absenders gedeckte Zugang des Erben zum Erblasseraccount einen Eingriff in Art. 10 GG darstellt\textsuperscript{968}, überzeugt nicht. Sie beruht auf die mit dem Telekommunikationsvorgang verbundene grundrechtstypische Gefährdungslage.\textsuperscript{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 Dazwischenetretens eines technischen Übermittlungsvorgangs, „der nicht ausschließlich im Einflussbereich“ der Kommunikationspartner liegt\textsuperscript{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

\textsuperscript{964} Spindler/Schuster/Eckhardt, § 88 TKG Rn. 2; vgl. BT-Drs. 13/3609, S. 1 f.
\textsuperscript{966} Gloser, „Digitale Erblasser“ und "digitale Vorsorgefälle“ – Herausforderungen der Online-Welt in der notariellen Praxis – Teil I, MittBayNot 2016, 12 (18); Kroiß/Horn/Solomon/Hertzog, Nachfolgerecht, Rn. 68; Kutscher (Diss.), S. 142.
\textsuperscript{967} Gloser, „Digitale Erblasser“ und "digitale Vorsorgefälle“ – Herausforderungen der Online-Welt in der notariellen Praxis – Teil I, MittBayNot 2016, 12 (18); Kroiß/Horn/Solomon/Hertzog, Nachfolgerecht, Rn. 68; Kutscher (Diss.), S. 142.
\textsuperscript{968} DAV, Stellungnahme Nr. 34/2013, S. 72 ff.
\textsuperscript{969} DAV, Stellungnahme Nr. 34/2013, S. 72 f.
\textsuperscript{970} DAV, Stellungnahme Nr. 34/2013, S. 72.


---

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).
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.\textsuperscript{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.\textsuperscript{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\textsuperscript{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.\textsuperscript{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

\textsuperscript{977} So auch Lange/Holtwiesche, Digitaler Nachlass – eine Herausforderung für Wissenschaft und Praxis (Teil 2), ZErb 2016, 157 (159).
Auslegung des Art. 10 GG vertretenen Auffassung davon aus, dass der Kommunikationsvorgang zwar bis zum Abruf der Nachricht noch nicht abgeschlossen ist\textsuperscript{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 \textit{umfassenden} Anwendungsausschluss der EU-DSGVO auf die Frage der Zugriffsrechte der Erben auf gespeicherte Kommunikationsdaten des Verstorbenen auszugehen.\textsuperscript{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.\textsuperscript{983}


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.\textsuperscript{985} Allerdings ist der Wortlaut des Art. 95 EU-DSGVO im Lichte des Erwägungsgrundes 173 EU-DSGVO auszulegen, der einen Anwendungsvorrang der Richtlinie 


\textsuperscript{982} Im Ergebnis ähnlich \textit{Kühling/Martini et al.}, Die DSGVO und das nationale Recht, S. 21.

\textsuperscript{983} Im Ergebnis ähnlich \textit{Kühling/Martini et al.}, Die DSGVO und das nationale Recht, S. 21.


\textsuperscript{985} \textit{DAV}, Stellungnahme Nr. 8/2013, S. 11.
2002/58/EG vor der EU-DSGVO statuieren will\textsuperscript{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\textsuperscript{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 Erblasserraccount bzw. einer Überlassung der Daten des Erblasserraccounts 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\textsuperscript{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\textsuperscript{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.

\textsuperscript{986} \textit{DAV}, Stellungnahme Nr. 8/2013, S. 11.

\textsuperscript{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.“

\textsuperscript{988} \textit{Steiner/Holzer}, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (264); \textit{Deusch}, Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2 (3), der indes eine Änderung für geboten erachtet.

c. Anspruch auf Herausgabe der Daten bei Beendigung der Vertragsbeziehung


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 rares) Stimmen aus der Literatur.

(1) Prüfungsmaßstab


991 Für die weitere Prüfung wird unterstellt, dass AGB vorliegen, die vom Provider als Verwen- der 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.\textsuperscript{992} Klauseln, die lediglich die einschlägige gesetzliche Regelung wiedergeben („deklaratorische“ Klauseln), sind hingegen kontrollfest.\textsuperscript{993}

Es ist daher zu ermitteln, ob die Rechtsordnung eine dem Regelungsgehalt der zu überprüfenden Klausel entsprechende (inhaltsgleiche) Regelung bereithält.\textsuperscript{994} Zu diesem Zwecke ist festzustellen, welche Normen auf Providerverträge Anwendung finden. Deren rechtliche Einordnung ist im Einzelnen umstritten.\textsuperscript{995} Ange- sichts der Vielgestaltigkeit der Regelungen dürfte sich eine allgemeine rechtliche Zuordnung von vornehherein 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 vornehherein von der Inhaltskontrolle ausgeschlossen.\textsuperscript{996} Für die vorliegende Untersuchung kann daher grundsätzlich davon ausgegangen werden, dass Kündigungs-, Legitimations- und Abwicklungs- klauseln 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\textsuperscript{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

\textsuperscript{992} MüKo/Wurmnest, BGB, § 307 Rn. 1.
\textsuperscript{993} BeckOK/H. Schmidt, BGB, § 307 Rn. 70.
\textsuperscript{994} MüKo/Wurmnest, BGB, § 307 Rn. 6.
\textsuperscript{996} Vgl. MüKo/Wurmnest, BGB, § 307 Rn. 7.
\textsuperscript{997} Vgl. Palandt/Grüneberg, BGB, § 307 Rn. 2.
Weite. Anwendungsbereich und -grundlagen decken sich mit denjenigen des Abs. 1 der Vorschrift. 998


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.

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.


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.


(3) Legitimationsklauseln


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. 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.


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:

„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.

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 Gutgläubensschutzes 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.\footnote{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.\footnote{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.


\footnote{1007} Vgl. im Einzelnen BGH, Urt. v. 8.10.2013 – XI ZR 401/12, NJW 2013, 3716 (3718).
\footnote{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.


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 Palandt/Grüneberg, BGB, § 307 Rn. 37.
1010 Palandt/Grüneberg, BGB, § 307 Rn. 28.

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.


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 vererbblich 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.\textsuperscript{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.\textsuperscript{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.


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

\textsuperscript{1013} Vgl. Palandt/Weidlich, BGB, § 1922 Rn. 36.
\textsuperscript{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 ungerecht fertigt 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 Rechtslage 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.\textsuperscript{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.\textsuperscript{1016} Wenn sie transparent ausgestaltet seien und ein Wahlrecht des Nutzers beinhaltet, 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.\textsuperscript{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.\textsuperscript{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.\textsuperscript{1019} Schließlich verweist sie auf die Möglichkeit der postmortalen Vollmacht, die sie wegen der Gefahr eines Widerrufs durch die Erben

\textsuperscript{1015} Steiner/Holzer, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (266).

\textsuperscript{1016} Kutscher (Diss.), S. 151 f. (mit intensiver Auseinandersetzung mit dem Interactive Account Manager von Google auf S. 153 f., 157 f.).

\textsuperscript{1017} Kutscher (Diss.), S. 157-159.

\textsuperscript{1018} Seidler (Diss.), S. 151 f.

\textsuperscript{1019} Seidler (Diss.), S. 153 f.
allerdings für das weniger geeignete Mittel hält. 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.

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 gehemmt 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 erbrechtlich 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.\textsuperscript{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) verfügte, dass seine unveröffentlichten Manuskripte verbrannt werden sollten.\textsuperscript{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.


\textsuperscript{1023} Vgl. bei Steiner/Holzer, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, 262 (266).

\textsuperscript{1024} Auf dieses Beispiel weist Martini, Der digitale Nachlass und die Herausforderungen postmortaler Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1154), hin.

\textsuperscript{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


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 Legimitationsnachweise von den Erben verlangt werden dürfen (siehe insoweit bereits den Diskussionsstand oben unter I. 2.). Solmecke/Köbrich/Schmitt weisen auf das Problem hin, dass der Erb-

NJW 2013, 3745 (3750 f.) sowie des DAV, Stellungnahme Nr. 34/2013, S. 62-64, wonach der Erbschein als Nachweis verlangt werden kann.


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.


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)


Demgegenüber vertritt eine Mindermeinung, auch die reine Unkenntnis der Überschuldung des Nachlasses stelle einen zur Anfechtung berechtigenden Eigenschaftsirrtum dar. 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.

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.


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.

1041 Staudinger/Otte, § 1954 Rn. 16.
1042 Lange/Kuchinke, S. 218-221.
1048 Schaub, Schwarzgeld im Nachlass: Ratschläge für Erben, ZEV 2011, 624 (625).
(2) Haftungsbeschränkungsmöglichkeiten in Bezug auf „nicht-kaufmännische“ Nachlässe

(a) Haftungsbeschränkungsmöglichkeiten des Alleinerben


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.
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).


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 Dürftigkeitseindeutung gemäß § 1990 Abs. 1 S. 1 BGB zu berufen. Dies hat zur Folge, dass der endgültige Erbe die Nachlassgläubiger auf die Befriedigung aus dem Nachlassverfahren antragsberechtigt und antragspflichtig ist, und dass ihm das Gesetz zur Anordnung einer Nachlassverwaltung oder einer Nachlassinsolvenz den Verwendungszweck zuweist.

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).
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.\textsuperscript{1062}

Ungeachtet dessen muss der gerichtlich wegen Nachlassverbindlichkeiten in Anspruch genommene Erbe, sofern er nicht ohnehin bereits endgültig unbeschränkt haften sollte, die Beschränkung der Erbschaftsverbindlichkeiten 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 Bestreitsfall beweist, dass der Erbe bereits unbeschränkt haftet.\textsuperscript{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.\textsuperscript{1064}

(b) Haftungsbeschränkungsmöglichkeiten von Miterben

Die vorläufige unbeschränkte 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(-beschränkung) 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“\textsuperscript{1065} – nur sehr beschränkte Zugriffsmöglichkeiten haben.\textsuperscript{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,

\textsuperscript{1062} Lettmann, Die Beschränkung der Erbschaftsverbindlichkeiten in der Nachlassaufteilung, RNotZ 2002, 537 (549); Herzog, Haftung des Erben für Miet- und WEG-Schulden, NZM 2013, 175 (177).
\textsuperscript{1063} Klinger, Vorbehalt der beschränkten Erbschaftsverbindlichkeiten als Regressfalle, NJW-Spezial 2005, 541.
\textsuperscript{1064} Klinger, Vorbehalt der beschränkten Erbschaftsverbindlichkeiten als Regressfalle, NJW-Spezial 2005, 541.
\textsuperscript{1065} So wörtlich Kroiß/Ann/Mayer/Kick, BGB, § 2058 Rn. 2.
\textsuperscript{1066} Kroiß/Ann/Mayer/Kick, BGB, § 2058 Rn. 2.

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 Erbschaftsanahme 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 Erbschaftsanahme 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 Erbschaftsanahme 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 Reinerlösverwaltungen, 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 Erbschaftsanahme 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.\textsuperscript{1072} Alternativ kann der Erbe, wenn er das Verfahren der Nachlassverwaltung zunächst vermeiden will, das kostengünstigere Aufgebotverfahren wählen, um vor weiteren Schritten Aufschluss darüber zu erlangen, mit welchen Nachlassverbindlichkeiten er rechnen muss.\textsuperscript{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 Eigentum. 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 unbeschränkt 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.\textsuperscript{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-

\textsuperscript{1072} Lettmann, Die Beschränkung der Erbenhaftung, RNotZ 2002, 537 (545, 557); Herzog, Haftung des Erben für Miet- und WEG-Schulden, NZM 2013, 175 (177).
\textsuperscript{1073} Lettmann, Die Beschränkung der Erbenhaftung, RNotZ 2002, 537 (557); Graf, Möglichkeiten der Haftungsbeschränkung für Nachlaßverbindlichkeiten, ZEV 2000, 125 (131).
\textsuperscript{1074} Mayer, Teilung bricht Gesamthand – Praktische Fälle der Erbauseinandersetzung, Mitt-BayNot 2010, 345 (350).

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. Mit zunehmender Ersetzung der Briefpost durch elektronische Post und zunehmender Verlagerung von Geschäftsaktivitäten auf elektronische „Vertriebskanäle“ wird diese faktische Zugangsmöglichkeit abnehmen. Stellt man sich den Extremfall eines Erblassers vor, der nur oder ganz überwiegend per elektronischer Post kommuniziert und die

---


Dies wird nicht durch die in der kautelarjuristischen Literatur aufgezeigten Vorsorgemöglichkeiten (Stichworte: Vorsorgevollmacht; Auflagen und Vermächtnisse in letztwilligen Verfügungen; Hinterlegung von Passwörtern etc.) 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-

1079 Deusch, Digitales Sterben: Das Erbe im Web 2.0, ZEV 2014, 2 (7 f.).
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. 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 erschien 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 Nachlasssteilung 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 Haftrisiken 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-

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.


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


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/Holzer1083 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 Seidlert 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 typenmischten 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


\(^{1085}\) 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).

\(^{1087}\) Seidlert (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.).

3. **Stellungnahme**


---

1092 Kutscher (Diss.), S. 45/46; zur vertragsrechtlichen Einordnung von „Daten als Entgelt“ siehe Kapitel 3, Abschnitt G.
1093 Klas/Möhrke-Sobolewski, Digitaler Nachlass – Erbschutz 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 – Erbschutz 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.


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.


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 „Splitting“ des Zugrifferechts 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 vererbarlich ist.

2. Diskussionsstand


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.
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 Angehörigen das datenschutzrechtliche Totenfürsorgegut wahrnehmen und die Vererbarkeit der Rechtspositionen ausgeschlossen sei.\footnote{Martini, Der digitale Nachlass und die Herausforderungen postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, 1145 (1153 f.).}

3. Stellungnahme


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 Vererbarkeit 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...


\[1104\] EuGH, Urt. v. 3.7.2012, NJW 2012, 2565 (2568) Rn. 72 (UsedSoft).


Rechtspolitisch wird de lege ferenda zum Teil die Forderung erhoben, das Urheberrecht zu ändern und die Übertragbarkeit unter Lebenden zu gewährleisten. In diesem Zusammenhang wird auf die bereits derzeit bestehenden technischen Schutzmöglichkeiten vor unkontrollierbaren Vervielfältigungen hingewiesen. 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, ohne allerdings auf die Fragestellungen im Hinblick auf den Erschöpfungsgrundsatz einzugehen. Auch Kutscher erörtert die

107 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 des Werkstücks auch bei Online erworbenen Daten möglich ist, wenn die Festplatte des Computers oder das sonstige Speichermedium veräußert wird (Rn. 28).
108 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.
110 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.).
113 Herzog, Der Digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, 3745 (3750).

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 vererbar 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). 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).
Nutzungsrechts auf Lebenszeit im Sinne einer Begrenzung gem. § 31 Abs. 1 S. 2 UrhG bedeuten würde.


3. Überblick über die derzeit vorhandenen AGB-Regelungen

Ein stichprobhafter 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 vererbt 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

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).


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“.


Da die Argumente der Gefahr eines unkontrollierbaren Zweitmarktes und der Gefahr rechtswidriger Mehrfachübertragungen, ohne die erforderliche Lösung 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.


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.).

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. 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.


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).

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 Inhaltskontrolle 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.

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 Er schöpfungsgrundsatzes für digitale Inhalte ausklammert, eher in der Situation des Erben begründet ist. Nur bei ihm stellen sich die aufgezeigten Probleme, dass er


\footnote{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 Nutzungsrecht 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.


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 be-
stimmte Fälle, etwa Verträge mit Verbrauchern) hätte gegenüber der Lösung im
BGB (s. o. b.) den Vorteil, dass sich die diversen aufgezeigten Probleme im Zu-
sammenhang mit den §§ 307 ff. BGB nicht stellen und auch eine Fraktion zwi-
sehen 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\textsuperscript{1138}) sind. Es bliebe das Problem sonstiger zeitlicher Befristun-
gen (s. o.), das aber aus den oben genannten Gründen nicht besonders schwerwie-
gend sein dürfte.

Allerdings stellt sich wieder das Problem einer Fraktion – 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 längst-
mögliche und damit für den Nutzer am wenigsten einschränkende Befristung.
Kürzere Befristungen dürften damit zu Lasten des Nutzers vereinbart werden, ge-
rade die längst mögliche hingegen nicht. Dies würde eine gewisse Fraktion inner-
halb 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 beschrie-
benen Probleme – abzusehen sein. Der Handlungsbedarf ist angesichts des empiri-
rischen Befundes mangels weiter Verbreitung entsprechender, auf den Todesfall
befristender allgemeiner Geschäftsbedingungen jedenfalls nicht drängend. Zu-
dem würden Brüche innerhalb unserer Rechtsordnung vermieden.

e. Vorschlag

Trotz der aufgezeigten Probleme empfiehlt die Arbeitsgruppe vor diesem Hinter-
grund daher, derzeit \textit{keine gesetzliche Regelung} zu treffen. Alle drei aufgezeigten
Regelungsmöglichkeiten unterliegen den jeweils dort aufgeführten nicht unerheb-
lichen 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

\textsuperscript{1138} Vgl. Wandtke/Bullinger/Wandtke/Grunert, UrhG, § 31 Rn. 11.

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.\(^\text{1139}\)

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. Sofort 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

\(^\text{1139}\) Kutscher (Diss.), S. 61 ff (insbes. S. 63).

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


3. Stellungnahme


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.

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 EuErbVO1143, 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.
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. 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. 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


1150 Vgl. Kutscher (Diss.), S. 89.
1151 Vgl. Kutscher (Diss.), S. 89.
1152 DAV, Stellungnahme Nr. 34/2013, S. 6, 8 f.
3. Stellungnahme


C. Ergebnis


<table>
<thead>
<tr>
<th>Autor/in, Hrsg.</th>
<th>Titel</th>
<th>Verlag, Neuausgabe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitkom e.V./Bitkom Research GmbH</td>
<td>Soziale Netzwerke 2013 – Dritte, erweiterte Studie – Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet</td>
<td>Berlin 2013</td>
</tr>
<tr>
<td>Borges, Georg/Meents, Jan Geert (Hrsg.)</td>
<td>Cloud Computing Rechtshandbuch</td>
<td>Saarbrücken/München 2016</td>
</tr>
</tbody>
</table>
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

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.)

Härting, Niko

Herberger, Maximilian/
Martinek, Michael/
Rüßmann, Helmut/
Weth, Stephan (Hrsg.)

Hilber, Marc (Hrsg.)

Hilgendorf, Eric (Hrsg.)

Hoeren, Thomas (Hrsg.)

Hoeren, Thomas/
Sieber, Ulrich/
Holznagel, Bernd (Hrsg.)

Hoffmann, Christian/Luch, Anika/ Schülz, Sönke/
Borchers, Corinna

Hohlfeld, Ralf/
Godulla, Alexander

Hornung, Gerrit/
Müller-Terpitz, Ralf (Hrsg.)

Jauernig

Kayser, Godehard/
Thole, Christoph (Hrsg.),

Keidel, Theodor

Köhler, Helmut

Kreuzer, Till (iRights.Law)

beck-online.GROSSKOMMENTAR zum Bürgerlichen Gesetzbuch, München 2016

Internetrecht, 5. Auflage, Köln 2014

Juris Praxiskommentar zum Bürgerlichen Gesetzbuch, 7. Auflage, Saarbrücken 2014

Handbuch Cloud Computing, Köln 2014

Robotik im Kontext von Recht und Moral, 2014

Big Data und Recht, München 2014

Handbuch Multimedia-Recht - Rechtsfragen des elektronischen Rechtsverkehrs, Münster/Freiburg 2016

Die digitale Dimension der Grundrechte - Das Grundgesetz im digitalen Zeitalter, Baden-Baden 2015


Rechtshandbuch Social Media, 1. Auflage, Berlin/Heidelberg 2015

Bürgerliches Gesetzbuch, Kommentar, 16. Auflage 2015

Insolvenzordnung, Kommentar, 8. Auflage, Heidelberg 2016

BGB Allgemeiner Teil, 40. Auflage 2016

Weiterveräußerungsfähigkeit von digitalen Gütern, Studie, 2015
<table>
<thead>
<tr>
<th>Autor</th>
<th>Titel</th>
<th>Anmerkungen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kroiß, Ludwig/Ann, Christoph, Mayer, Jörg</td>
<td>Kommentar zum Bürgerlichen Gesetzbuch, Band 5: Erbrecht, 4. Auflage 2014</td>
<td></td>
</tr>
<tr>
<td>Kroiß, Ludwig/Horn, Claus-Henrik/Solomon, Dennis</td>
<td>Nachfolgerecht, Kommentar, 1. Auflage 2015</td>
<td></td>
</tr>
<tr>
<td>Kühlung, Jürgen/Buchner, Benedikt</td>
<td>DS-GVO, Kommentar, 1. Auflage 2017</td>
<td></td>
</tr>
<tr>
<td>Kühlung, Jürgen/Martini, Mario et al.</td>
<td>Die DSGVO und das nationale Recht - Erste Überlegungen zum nationalen Regelungsbedarf, 2016</td>
<td></td>
</tr>
<tr>
<td>Kutscher, Antonia</td>
<td>Der digitale Nachlass, Dissertation, Kiel, 2015</td>
<td></td>
</tr>
<tr>
<td>Lange, Heinrich/Kuchinke, Kurt</td>
<td>Erbrecht, Ein Lehrbuch, 5. Auflage 2001</td>
<td></td>
</tr>
<tr>
<td>Leible, Stefan/Lehmann, Matthias/Zech, Herbert (Hrsg.)</td>
<td>Unkörpliche Güter im Zivilrecht, Tübingen 2011</td>
<td></td>
</tr>
<tr>
<td>Maunz, Theodor/Dürig, Günter</td>
<td>Grundgesetz, Kommentar, 78. Auflage 2016</td>
<td></td>
</tr>
<tr>
<td>Müller-Broich, Jan D.</td>
<td>Telemediengesetz, 1. Auflage 2012</td>
<td></td>
</tr>
<tr>
<td>Münchener Kommentar zur Insolvenzordnung</td>
<td>Band 1, 3. Auflage, München 2013</td>
<td></td>
</tr>
<tr>
<td>Münchener Kommentar zur Zivilprozessordnung</td>
<td>Band 2, 4. Auflage, München 2012</td>
<td></td>
</tr>
<tr>
<td>Noerr LLP</td>
<td>Digitalisierte Wirtschaft/Industrie 4.0, Gutachten, 2015</td>
<td></td>
</tr>
<tr>
<td>Autor/innen</td>
<td>Titel</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>Palandt, Otto</td>
<td>Bürgerliches Gesetzbuch, Kommentar, 76. Auflage, München 2017</td>
<td></td>
</tr>
<tr>
<td>Plath, Kai-Uwe (Hrsg.)</td>
<td>BDSG/DSGVO, Kommentar, 2. Auflage, Köln 2016</td>
<td></td>
</tr>
<tr>
<td>Prütting, Hanns/ Gehrlein, Markus</td>
<td>Zivilprozessordnung, Kommentar, 8. Auflage 2016</td>
<td></td>
</tr>
<tr>
<td>Redecker, Helmut</td>
<td>IT-Recht, 5. Auflage 2012</td>
<td></td>
</tr>
<tr>
<td>Rehbinder, Manfred/ Peukert, Alexander</td>
<td>Urheberrecht, 17. Auflage, München 2015</td>
<td></td>
</tr>
<tr>
<td>Säcker, Franz Jürgen</td>
<td>Berliner Kommentar zum TKG, 2. Auflage 2009</td>
<td></td>
</tr>
<tr>
<td>Scheuerle, Klaus-Dieter/ Mayen, Thomas</td>
<td>Telekommunikationsgesetz Kommentar, 2. Auflage, München 2008</td>
<td></td>
</tr>
<tr>
<td>Schmidt, Karsten</td>
<td>Insolvenzordnung, Kommentar, 19. Auflage, München 2016</td>
<td></td>
</tr>
<tr>
<td>Autor(a)</td>
<td>Titel</td>
<td></td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Spindler, Gerald/</td>
<td>Recht der elektronischen Medien, Kommentar, 3. Auflage 2015</td>
<td></td>
</tr>
<tr>
<td>Schuster, Fabian</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thomas, Heinz/</td>
<td>Zivilprozessordnung, Kommentar, 37. Auflage, München 2016</td>
<td></td>
</tr>
<tr>
<td>Putzo, Hans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Titze, Heinrich</td>
<td>Vom sogenannten Motivirrtum, Festschrift für Ernst Heymann (1940), Band 2, S. 70 ff.</td>
<td></td>
</tr>
<tr>
<td>Hirte, Heribert/</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vallender, Heinz (Hrsg.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wolf, Christian</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bullinger, Winfried</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weichert, Thilo</td>
<td>Postmortaler Datenschutz – Auskunftsansprüche von Erben und Angehörigen zu personenbezogenen Internetdaten eines Verstorbenen, Gutachten 2016</td>
<td></td>
</tr>
<tr>
<td>Wolf, Manfred/</td>
<td>AGB-Recht, Kommentar, 5. Auflage, München 2009</td>
<td></td>
</tr>
<tr>
<td>Lindacher, Walter F./</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pfeiffer, Thomas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Neuner, Jörg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zech, Herbert</td>
<td>Information als Schutzgegenstand, Tübingen 2012</td>
<td></td>
</tr>
</tbody>
</table>