

Kapitel 2 – Bestimmung des Erbrechtsobjekts

Den digitalen Nachlass zum Untersuchungsgegenstand zu machen, heißt auch grundsätzlich über datenbasierte Vermögensgegenstände nachzudenken. Der „empirische Realtypus digitaler Nachlass“³² weist Berührungspunkte mit einer großen Bandbreite unterschiedlicher Rechtsobjekte auf.³³ Ausgangspunkt der Frage nach dem „Ob“ und dem „Wie“ der Vererbbarkeit dieser Rechtsobjekte muss es sein, sie als konkrete Bestandteile des (digitalen) Nachlasses zu benennen und sie in ihrer rechtlichen Qualität zu bestimmen. Entsprechend dem Zuschnitt der Arbeit sollen hierzu die Rechtsverhältnisse zwischen dem Anbieter von Informations- und Kommunikationsdiensten und seinem jeweiligen Nutzer untersucht werden: De lege lata ist der zwischen diesen Parteien geschlossene Nutzungsvertrag der Hauptanknüpfungspunkt für die rechtliche Zuordnung der Nutzerkonten³⁴ des Erblassers. Daneben können Immaterialgüter-, insbesondere Urheberrechte, an den Accountinhalten bestehen.³⁵ Der Nutzungsvertrag und die Urheberrechte des Erblassers bilden in ihrer Eigenschaft als Erbrechtsobjekte damit den zentralen Untersuchungsgegenstand dieser Arbeit. Einführend ist daher ein näherer Blick auf diese Rechtspositionen zu werfen (dazu A.). Im Anschluss soll die verwandte Debatte zu möglichen originären Rechtspositionen an Daten dargestellt werden (dazu B.). Dem Nutzer mag eine affektive, umgangssprachliche Einteilung in „eigene“ Daten und andere Daten mitunter möglich sein.³⁶ So ist es etwa denkbar, dass ein Arbeitnehmer die Inhalte und insbesondere die Nachrichten, die er auf

32 *Sorge*, MMR 2018, 372, 372 f.

33 Siehe hierzu bereits die Nachweise in Fn. 5, 6 und 7.

34 Zur rechtlichen Einordnung eines Accounts als solchem vgl. *Kutscher*, Der digitale Nachlass, S. 21 ff.; *Seidler*, Digitaler Nachlass, S. 69 ff. Nach hier vertretener Ansicht kommt ein Recht am Account als solchem allenfalls unter dem Gesichtspunkt eines Rechts an Daten in Betracht, s. zu diesem S. 44 ff.

35 Zu der Unterscheidung zwischen E-Mail und E-Mail-Account als erster *Hoeren*, NJW 2005, 2113, 2114 f.; instruktiv dazu *Bräutigam* in: DAV-Stellungnahme Nr. 34/2013, S. 17 f.; sich *Hoeren* anschließend *Brisch/Müller-ter Jung*, CR 2013, 446, 447; s. auch *Herzog*, NJW 2013, 3745, 3749; *dies./Pruns*, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, S. 66 f.

36 *Richter*, Vorwort, in: Stiftung Datenschutz (Hrsg.), Dateneigentum und Datenhandel, S. 5; kritisch zu diesem Selbstverständnis der Nutzer – vor allem auch in Data-for-Access-Konstellationen – vgl. *Amstutz*, AcP 218 (2018), 439, 439 ff.

seinem (auch) privat genutzten Dienstgerät abgespeichert hat, in private („eigene“) und dienstliche Daten unterteilen könnte.³⁷ Allerdings ist es fraglich, ob und inwieweit diese affektive Beziehung einer Person zu „ihren“ Daten gegenwärtig rechtlich abgebildet wird. Sofern ein originäres, eigentumsähnliches Recht des Nutzers an Daten künftig anerkannt oder vom Gesetzgeber geschaffen wird, könnte sich daraus jedenfalls ein (zusätzliches) Erbrechtsobjekt oder sogar eine Vereinheitlichung der Erbrechtsobjekte im digitalen Nachlass ergeben.

A. Rechtsverhältnisse zwischen Provider und Nutzer

Dauerschuldverhältnisse sind von wesentlicher Bedeutung in der Digitalwirtschaft. Die immer größere Verfügbarkeit von (Online-)Speicherplatz zu immer geringeren Kosten hat zur Folge, dass die Kundenerfahrung des Nutzers an vielen Punkten nicht mehr durch körperliche Gegenstände geprägt ist. Stattdessen wurden die körperlichen Gegenstände durch digitale Versionen ersetzt. Man denke nur an Briefpost, die nunmehr als E-Mail oder Chatnachricht vorliegt, oder körperliche Musik-CDs oder Film-DVDs, die zunehmend durch Streaming-Angebote ersetzt werden.³⁸ Während der Zugriff auf die körperlichen Gegenstände regelmäßig durch das an ihnen bestehende Eigentum bestimmt wird, sind es demgegenüber Nutzungsverträge, die in den meisten Fällen das Recht auf Zugang zu den digitalen Dateien regeln. Das gilt jedenfalls, wenn und soweit die Dateien auf Servern des Providers und nicht auf privaten Endgeräten des Nutzers gespeichert sind. Denn in diesem Fall kommt aus Sicht des Nutzers und seiner Rechtsnachfolger das Sacheigentum am physischen Speichermedium als Erbrechtsobjekt nicht in Betracht. Nutzungsverträge, in deren Rahmen beispielsweise die Mitgliedschaft in sozialen Netzwerken beziehungsweise der Zugang zur digitalen Infrastruktur des Plattformbetreibers vereinbart wird, erhalten dadurch eine Schlüsselfunktion. Im Folgenden sollen die Nutzungsverträge typologisch untersucht werden, wozu das mit

37 Im Falle eines unter Eigentumsvorbehalt erworbenen Endgerätes dürfte ein affektives Zuordnungsverhältnis zu (fast) allen abgespeicherten Daten bestehen, da der Nutzer ein solches Gerät von Anfang an als „sein eigenes“ ansieht und entsprechend unterschiedslos private Daten abspeichert.

38 Zu den Auswirkungen der Digitalisierung auf die Nutzung von urheberrechtlich geschützten Werken s. *Sucker*, Der digitale Werkgenuss im Urheberrecht, S. 69 ff. Zur Behandlung urheberrechtlicher Lizenzen des Erblassers an Werken Dritter im Kontext des digitalen Nachlasses vgl. bereits die Nachweise in Fn. 25.

der Vertragstypenbestimmung in engem Zusammenhang stehende mehrseitige Finanzierungsmodell der Provider darzustellen ist (dazu I.). Im Anschluss sind die Urheber- und Leistungsschutzrechte des Erblässers an einzelnen Inhalten des Accounts sowohl als eigenständige Rechtsposition als auch in ihrem Verhältnis zum Nutzungsvertrag zu beleuchten (dazu II.).

I. Vertragstypologie der Nutzungsverträge

Um eine einzelfallgerechte Typologisierung der Nutzungsverträge vornehmen zu können, sind nach einführenden Bemerkungen zur praktischen Relevanz der Typenbestimmung (dazu 1.), die unterschiedlichen Hauptleistungspflichten des Providers (dazu 2.) und der Umgang mit typengemischten Verträgen (dazu 3.) zu untersuchen. Zur Bestimmung der Parteiinteressen und des Vertragszwecks ist sodann der Fokus auf das mehrseitige Finanzierungsmodell der Provider zu richten (dazu 4.).

1. Praktische Relevanz der Typenbestimmung

Die typologische Einordnung der Verträge zwischen den Diensteanbietern und den Nutzern scheint zunächst von nur untergeordneter praktischer Bedeutung zu sein, da die vertraglichen Rechte und Pflichten der Parteien in den Nutzungsbedingungen der Anbieter regelmäßig ohnehin detailliert ausformuliert werden.³⁹ Allerdings darf nicht übersehen werden, dass dem dispositiven Recht eines Vertragstypus gem. § 307 Abs. 2 Nr. 1 BGB eine Leitbildfunktion bei der Inhaltskontrolle der AGB zukommt.⁴⁰ Insofern gibt die Qualifizierung des Nutzungsvertrags als ein Vertragstyp des BGB den Rahmen der Gestaltungsmöglichkeiten für den Verwender der AGB vor. Darüber hinaus folgt aus der Einordnung, welche Vorschrift dann zur Anwendung kommt, wenn die AGB des Providers ein Nutzungsverhältnis doch einmal nicht ganz umfassend geregelt haben sollten.⁴¹ Für die internationalprivatrechtliche Frage nach dem anwendbaren Recht spielt aus-

39 *Kindl*, Verträge über digitale Inhalte – Vertragsnatur und geschuldete Leistung, in: *Kindl/Arroyo/Gsell* (Hrsg.), Verträge über digitale Inhalte und digitale Dienstleistungen, S. 68.

40 *Kindl* a.a.O. (Fn. 39); *Kutscher*, Der digitale Nachlass, S. 45; *Boehm*, ZEuP 2016, 358, 363.

41 *Boehm*, ZEuP 2016, 358, 363; *Stieper* in: FS Helmut Köhler, S. 730 f.

weislich des Art. 4 Abs. 1 Rom I-Verordnung die Vertragstypologie ebenfalls eine zentrale Rolle.⁴² Vor diesem Hintergrund kann der Typenbestimmung im Einzelfall durchaus eine entscheidende Funktion zukommen.

2. Vielgestaltigkeit der Hauptleistungspflichten

Die Bestimmung eines Vertragstyps erfolgt im Allgemeinen anhand des Vertragsinhalts und genauer anhand der Hauptleistungspflichten der Parteien. Im Bereich der Digitalwirtschaft wird es regelmäßig die Pflicht des Diensteanbieters sein, welche kennzeichnend für die Typenbestimmung ist.⁴³ Der Anbieter stellt dem Nutzer im Rahmen eines nutzungsbeschränkten IT-Systems einen Account zur Verfügung. Je nach vorgesehendem Nutzungszweck dieses Accounts sind die Pflichten der Accountanbieter mitunter sehr unterschiedlich ausgestaltet. Dabei verpflichtet sich der Anbieter zur Eröffnung und Aufrechterhaltung der IT-Infrastruktur, die für die konkreten Dienste notwendig ist und regelmäßig online „Cloud“-Speicherplatz für die Inhalte der Nutzer umfasst. Zu diesen Diensten kann eine Kommunikationsfunktion gehören, die mehreren Nutzern den Austausch untereinander ermöglicht. Dies kann durch Austausch von schriftlichen Nachrichten oder von Bildern, durch Audiodateien als Sprachnachrichten oder mittels internetbasierter (Video-)Telefonie erfolgen. In vielen Fällen wird die Kommunikationsfunktion um eine Möglichkeit der Vernetzung ergänzt, die es den Nutzern ermöglicht, Kontakte zu knüpfen und zu pflegen. In Betracht kommt weiter die Möglichkeit der Nutzer, Inhalte mit der Öffentlichkeit oder einem durch den Nutzer definierten Ausschnitt der Öffentlichkeit zu teilen. Spiegelbildlich ist es den Nutzern in diesen Fällen zumeist möglich, eine Auswahl darüber zu treffen, wessen Inhalte sie abonnieren wollen. Dadurch entsteht eine Plattform mit nut-

42 Sofern keine der in Art. 4 Abs. 1 Rom I-VO genannten Vertragsarten vorliegt, muss auf einen der Auffangtatbestände zurückgegriffen werden, vgl. *Boehm*, ZEuP 2016, 358, 363; *Kutscher*, Der digitale Nachlass, S. 85 ff. Die Begriffe und Vertragstypen der Rom I-VO sind freilich autonom auszulegen und unterscheiden sich ggf. von denen des deutschen Rechts. Ausführlich zum IPR s. S. 70 ff.

43 Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, Mai 2017, S. 197, abrufbar unter https://www.justiz.nrw.de/JM/schwerpunkte/digitaler_neustart/zt_bericht_arbeitsgruppe/bericht_ag_dig_neustart.pdf [17.11.2020]; *Bock*, AcP (217) 2017, 370, 377; *Budzikiewicz*, AcP (218) 2018, 558, 569.

zergenerierten Inhalten.⁴⁴ Überdies existieren zahlreiche Mischformen, bei denen die Kommunikations-, Vernetzungs- und die Publikationsfunktion in unterschiedlichen Verhältnissen den Schwerpunkt des Netzwerks aus Sicht seiner Nutzer bestimmen. Bisweilen werden die Funktionen mit Blick auf ein übergeordnetes Thema ausgerichtet und ausgestaltet. Zu denken ist hier an berufliche Aspekte wie Karriereförderung und professionelle bzw. wissenschaftliche Vernetzung sowie an sonstige thematische Verknüpfung politischer, freizeitleicher, künstlerischer oder verschiedenster anderer Natur.

3. Typengemischte Verträge

Die Darstellung der Funktionen kann naturgemäß nur einen Ausschnitt der großen Vielfalt an Kommunikations- und Informationsdiensten abbilden.⁴⁵ Die entstehende Bandbreite denkbarer Vertragstypen erfordert eine Einzelfallbetrachtung. Eine allgemeingültige Einordnung von Provider-Verträgen ist demgegenüber nicht zielführend.⁴⁶ Das liegt auch an der ständigen Weiterentwicklung des konkreten Erscheinungsbilds der Internetdienste.⁴⁷ Die konkrete Ausgestaltung der Dienste ist vor diesem Hintergrund immer nur eine „Momentaufnahme“,⁴⁸ zu der laufend Funktionen hinzukommen, die einen weiteren Vertragstypus einschlägig erschei-

44 Geläufig ist auch die englische Bezeichnung *User-generated content* (UGC). Siehe zu dem Begriff *Bauer*, User Generated Content, S. 7 ff.; *ders.*, User Generated Content, in: Große Ruse-Khan/Klass/v. Lewinski (Hrsg.), Nutzergenerierte Inhalte als Gegenstand des Privatrechts, S. 3 ff.

45 Anschaulich zur Vielfalt des Angebots formuliert *Martini* in: BeckOK Informations- und Medienrecht, § 1 TMG Rn. 7: „Telemediendienste können in vielfältigen Erscheinungsformen des Wirtschaftslebens und zivilgesellschaftlichen Informationsaustausches auftreten [...]. Das Kaleidoskop ihrer Phänotypen entwickelt sich dynamisch. Der Versuch, einen abschließenden Katalog von Telemedien aufzufächern, wäre zum Scheitern verurteilt.“

46 Vgl. auch die umfassenden Ausführungen bei *Redeker* in: Hoeren/Sieber/Holznaegel (Hrsg.), MMR-HdB, Teil 12, Vertragsrecht für Internetdienste, passim; s. ferner *Härting*, Internetrecht, Kap. D. Verträge über Internetdienstleistungen, S. 203 ff. sowie *Kosmides*, Providing-Verträge, passim.

47 Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 196, abrufbar a.a.O. (Fn. 43).

48 *Hohfeld/Godulla* in: Hornung/Müller-Terpitz (Hrsg.), Rechtshandbuch Social Media, Kap. 2 Rn. 8.

nen lassen können.⁴⁹ Gleichwohl sind gewisse wiederkehrende Punkte erkennbar, denen der Charakter von Leitlinien für die Typologisierung zukommen kann. So handelt es sich bei einer Vielzahl der von den Providern angebotenen Nutzungsverträge um typengemischte Verträge.⁵⁰ In der Literatur wurden dabei primär dienst-, werk- und mietvertragliche Elemente beziehungsweise deren unentgeltliche Entsprechung (i.e. Auftrag und Leihe) herausgearbeitet.⁵¹ Im Umgang mit typengemischten Verträgen ist mittlerweile anerkannt, dass sich die Bestimmung des anzuwendenden Rechts am Sinn und Zweck des Vertrages im Einzelfall zu orientieren hat.⁵² Insofern hat weder die Absorptionsmethode,⁵³ nach welcher auf alle Vertragsklauseln das Recht des im Vordergrund stehenden Vertragstyps anzuwenden ist, noch die Kombinationsmethode,⁵⁴ welche vorsieht, dass auf eine einzelne Klausel die jeweils für sie geltende Norm anzuwenden ist, grundsätzlich Vorrang.⁵⁵ Stattdessen „ist bei der Beurteilung maßgeblich auf die besonderen Umstände des Einzelfalls, auf die Interessenlage der Vertragsparteien sowie auf Sinn und Zweck der vertraglichen Vereinbarungen abzustellen.“⁵⁶ Zur Bestimmung der Parteiinteressen und des Vertragszwecks ist das mehrseitige Finanzierungsmodell der Provider in den Blick zu nehmen, welches in Zusammenhang mit der Frage nach der (Un-)Entgeltlichkeit des Vertragsverhältnisses steht.

49 So etwa bei entstehenden Schnittstellen zu anderen Internetdiensten. Eine solche Schnittstelle kann eine Neubewertung des Nutzungsvertrags erforderlich machen, wenn dadurch Dienste unterschiedlicher Natur und Zielrichtung konvergieren, wie etwa bei Google Accounts, deren Funktionen laufend erweitert werden.

50 Bock, AcP (217) 2017, 370, 376 f.; Wehleit, MMR 2018, 279, 279 f.; Budzikiewicz, AcP (218) 2018, 558, 568 f.; Thiesen, Daten in der Erbmasse, S. 48.

51 Vgl. die Nachweise in Fn. 46; ferner Thiesen, Daten in der Erbmasse, S. 47 ff.; Kutschner, Der digitale Nachlass, S. 45 ff.; Seidler, Der digitale Nachlass, S. 62 ff. und 129 ff.

52 Vgl. nur Emmerich in: MüKo BGB, § 311 Rn. 28 m.w.N.

53 Feldmann in: Staudinger, § 311 BGB Rn. 39; Gehrlein in: BeckOK BGB, § 311 Rn. 21.

54 Feldmann in: Staudinger, § 311 BGB Rn. 40; Gehrlein a.a.O. (Fn. 53).

55 Emmerich in: MüKo BGB, § 311 Rn. 28; Feldmann in: Staudinger, § 311 BGB Rn. 41; Gehrlein a.a.O. (Fn. 53); Stadler in: Jauernig, § 311 BGB Rn. 33.

56 So BGH NJW 2008, 1072 Rn. 19; vgl. ferner bereits die Nachweise in Fn. 55.

4. Mehrseitiges Finanzierungsmodell der Provider

Das denkbare Leistungsspektrum, zu dem sich der Provider im Rahmen des Nutzungsvertrags verpflichtet, wurde soeben skizziert. Nun ist ein Blick auf die nutzerseitigen Pflichten zu werfen. Vereinzelt besteht hier eine ausdrückliche Geldzahlungspflicht. Dies kann eine einmalige Zahlung zum Zeitpunkt der Anmeldung oder des Downloads (etwa der App des Anbieters) oder eine regelmäßig wiederkehrende Zahlung im Rahmen eines Abonnements sein.⁵⁷ Zahlungspflichtige Dienste können die Premium-Versionen eines sonst nicht zahlungspflichtigen Dienstes sein und in dieser Version zusätzliche Funktionen oder zusätzliche Inhalte einschließen.⁵⁸ In anderen Fällen werben kostenpflichtige Dienste damit, eine datenschutz-sensiblere Alternative zu ihren Mitbewerbern zu sein.⁵⁹ Damit verwandt ist das Angebot werbefreier Versionen mancher Dienste gegen Geldzahlung.⁶⁰ Ausgeklammert sei an dieser Stelle die Frage nach In-App-Käufen und ihr Einfluss auf die Einordnung des Rahmenvertrags.⁶¹

Eine große Zahl der Nutzungsverträge wird jedoch geschlossen, ohne eine Geldzahlungspflicht des Nutzers vorzusehen. Mit dem sozialen Netzwerk Facebook und seinen verbundenen Anbietern WhatsApp und Instagram bietet ein Branchenriese⁶² den Nutzern seine Dienste ohne eine Geldzahlungspflicht als Gegenleistung an. Damit steht das Unternehmen exemplarisch für eine große Anzahl anderer Internetdiensteanbieter. Von dieser Tatsache sollte jedoch nicht voreilig auf die Unentgeltlichkeit dieser Vertragsbeziehungen geschlossen werden. Um der Komplexität des Phänomens gerecht zu werden, bedarf es eines Blicks auf das mehrseitige Finanzierungsverhältnis.

57 Zu kostenpflichtigen sozialen Netzwerken s. *Redeker* in: Hoeren/Sieber/Holznaegel (Hrsg.), MMR-HdB, Teil 12 Rn. 420 f.

58 So z.B. Amazon Prime oder Tinder.

59 So z.B. Threema im Vergleich zu WhatsApp.

60 So z.B. Spotify Premium oder YouTube Premium.

61 Eine Analyse der Vertragsbeziehungen bei In-App-Käufen findet sich bei *Kannowski/Till*, NJOZ 2017, 522.

62 Facebook hatte im Dezember 2018 weltweit 1,52 Mrd. täglich und 2,32 Mrd. monatlich aktive Nutzer. In Deutschland waren es 23 Mio. täglich und 32 Mio. monatlich aktive Nutzer, s. PM des BKartA vom 7.02.2019, Bundeskartellamt unter sagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen.

a) Dienste gegen Daten

Die Anbieter finanzieren ihre Dienstleistung, indem sie Dritten anbieten, auf der Nutzeroberfläche des Internetdienstes Werbung zu schalten.⁶³ Grundsätzlich ist es für Werbekunden attraktiv, wenn Werbung zielgruppenspezifisch platziert werden kann.⁶⁴ Werden potenzielle Kunden adressiert, die sich ohnehin bereits für das Produkt des Werbenden interessieren oder zumindest in dessen Zielgruppe fallen, kann eine geringere Anzahl von Personen mit einer höheren Aussicht auf einen Geschäftsabschluss im Einzelfall beworben werden. Die Folge sind Effizienzsteigerungen.⁶⁵ Die Provider können diese Folge für ihre Werbeflächen ermöglichen, weil die Nutzer beim Abschluss des Nutzungsvertrages in die Erhebung und Speicherung ihrer personenbezogenen Daten zu Werbezwecken durch den Diensteanbieter einwilligen. Dies erlaubt den Providern das Anlegen von Nutzerprofilen, anhand derer wiederum die Werbekunden passgenau die Werbeadressaten aussuchen können. Damit wird die datenschutzrechtliche Einwilligung der Nutzer gem. Art. 6 Abs. 1 lit. a) DS-GVO ein Schlüsselement in der Qualitätssicherung des Angebots der Provider gegenüber den Werbekunden. Letztere wiederum hoffen naturgemäß, ihre Werbeausgaben durch Geschäfte mit den adressierten Nutzern zu amortisieren. Dem Nutzungsvertrag liegt damit eine sogenannte Data-for-Access-Konstellation zugrunde.

63 Redeker, IT-Recht, Rn. 1278; ders. in: Hoeren/Sieber/Holznapel (Hrsg.), MMR-HdB, Teil 12 Rn. 424; Schneider in: Redeker (Hrsg.), IT-Verträge, Kap. 3.7. In den Nutzungsbedingungen von Facebook heißt es dazu im zweiten Absatz: Anstelle einer Zahlungspflicht der Nutzer „bezahlen uns Unternehmen und Organisationen dafür, dass wir dir Werbeanzeigen für ihre Produkte und Dienstleistungen zeigen. Durch die Nutzung unserer Produkte erklärst du dich damit einverstanden, dass wir dir Werbeanzeigen zeigen dürfen, die nach unserer Ansicht relevant für dich sind und deinen Interessen entsprechen. Wir verwenden deine personenbezogenen Daten, um festzulegen, welche Werbeanzeigen wir dir zeigen.“, abrufbar unter <https://www.facebook.com/legal/terms/update> [17.11.2020].

64 Mundt in: PM des BKartA vom 7.02.2019, Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen.

65 Dazu und zu weiteren Vorteilen der personalisierten Werbung im Internet siehe Schneider in: Redeker (Hrsg.), IT-Verträge, Kap. 3.7 Rn. 1a; Paal, GRUR 2013, 873, 876 beschreibt diese Konstellation im Kontext von Suchmaschinen.

b) Unentgeltlichkeit des Nutzungsvertrags

Es ist zu klären, ob aus der Tatsache, dass der Nutzer den Provider mit seinen Daten für die Dienstleistung „bezahlt“, die Entgeltlichkeit des Nutzungsvertrags folgt. Dazu müsste die Einwilligung in die Nutzung der personenbezogenen Daten die synallagmatische Gegenleistung für die Nutzungsgewährung des Internetdienstes sein.⁶⁶ Zunächst spricht der Grundsatz der Relativität der Schuldverhältnisse dagegen, die soeben skizzierten Beobachtungen zur Mehrseitigkeit des Social-Media-Marktes in die Beurteilung des spezifischen Vertragsverhältnisses zwischen Provider und Nutzer miteinzubeziehen. Denn grundsätzlich sind die Rechtswirkungen eines Schuldverhältnisses auf die an ihm Beteiligten beschränkt.⁶⁷ Die Rechtsstellung Dritter – im Verhältnis zwischen Provider und Werbekunden also die Rechtsstellung der Nutzer – wird durch das Schuldverhältnis in der Regel nicht berührt.⁶⁸ Gleichwohl kann die Interessenlage der Parteien bei Vertragsschluss durchaus ein Indiz für die Beurteilung des Vertragsverhältnisses sein. Denn es entspräche wohl zumindest dem Interesse des Providers, wenn die nutzerseitige Einwilligung in die Datenverarbeitung vertraglich bindend wäre und sich der Grundsatz *pacta sunt servanda* darauf erstrecken würde.⁶⁹ Das würde für den Provider zu Planungssicherheit bei der Vermarktung der personalisierten Werbeflächen führen. Dagegen spricht jedoch die freie Widerrufbarkeit der datenschutzrechtlichen Einwilligung gem. Art. 7 Abs. 3 DS-GVO, mit welcher der unionale Gesetzgeber der Bedeutung des Grundrechts auf Schutz personenbezogener Daten im Sinne von Art. 8 Abs. 1 und 2 S. 1 GRCh Rechnung trägt.⁷⁰

Dadurch wird die Auseinandersetzung über die Entgeltlichkeit des Nutzungsvertrags eine spezifisch datenschutzrechtliche – und damit spätestens seit Geltung der DS-GVO eine europarechtliche – Frage. Sofern also *Bräu-*

66 So ausdrücklich *Bräutigam*, MMR 2012, 635, 638 f., der darin wahlweise einen Tauschvertrag oder einen Vertrag *sui generis* sieht; s. auch *Webleit*, MMR 2018, 279, 279 f. m.w.N.; a.A. *Hacker*, ZfPW 2019, 148, 172 ff.

67 *Ernst* in: MüKo BGB, Einleitung Schuldrecht, Rn. 18 ff.; *Bachmann* in: MüKo BGB, § 241 Rn. 11; *Mansel* in: Jauernig, BGB, § 241 Rn. 4.

68 Zu den Ausnahmen, die hier allesamt nicht einschlägig sind, s. *Mansel* in: Jauernig, BGB, § 241 Rn. 6 m.w.N.

69 *Bräutigam*, MMR 2012, 635, 636; s. aber *Hacker*, ZfPW 2019, 148, 170 der die Providerinteressen auch bei jederzeitiger Widerrufbarkeit nicht gefährdet sieht.

70 *Frenzel* in: Paal/Pauly (Hrsg.), DS-GVO, Art. 7 Rn. 16. Zum Verhältnis von schuldrechtlicher (Selbst)bindung und freier Widerruflichkeit der Einwilligung siehe auch *Zech*, GRUR 2015, 1151, 1154 f.

tigam dafür argumentiert, dass die datenschutzrechtliche Einwilligung gleichsam unter Anpassung ihrer Rechtsnatur von einer lediglich datenschutzrechtlichen Einwilligung zu einer vertraglichen Verpflichtung jenseits der Anwendbarkeit des Datenschutzrechts umgedeutet werden soll,⁷¹ so ist das mit dem Geltungsanspruch der DS-GVO kaum vereinbar.⁷² Die DS-GVO ist nach Maßgabe ihres Art. 2 DS-GVO auf die Verarbeitung von personenbezogenen Daten durch die Anbieter digitaler Informations- und Kommunikationsdienste anwendbar. Die Rechtmäßigkeit der Verarbeitung wird in der Folge durch Art. 6 DS-GVO bestimmt und kann nicht durch das nationale Recht des BGB überformt werden. Etwas anderes mag allenfalls gelten, wenn einzelne Normen des BGB der Umsetzung europarechtlicher Vorgaben dienen und insofern selbst Ausprägungen von Europarecht sind. Zwar lässt der Widerruf die Zulässigkeit der Datenverarbeitung aufgrund anderer Zulässigkeitsgründe aus Art. 6 Abs. 1 lit. b)-f) DS-GVO unberührt.⁷³ Nähme man jedoch an, dass sich die Zulässigkeit der Datenverarbeitung (auch nach einem Widerruf) sodann aus Art. 6 Abs. 1 lit. b) DS-GVO ergäbe, so liefe die Anordnung „jederzeitiger“ Widerrufbarkeit aus Art. 7 Abs. 3 S. 1 DS-GVO leer. Nach geltendem Recht kommt die Nutzung personenbezogener Daten als Gegenleistung im vertraglichen Synallagma daher nach hier vertretener Ansicht nicht in Betracht.⁷⁴ Demnach handelt es sich bei Nutzungsverträgen *de lege lata* um unentgeltliche Vertragsverhältnisse. Als rechtspolitischer Ausblick sei aber darauf verwiesen, dass der nationale Gesetzgeber die Vorgaben der europäischen Richtli-

71 *Bräutigam*, MMR 2012, 635, 638 ff., allerdings noch zur Rechtslage vor Geltung der DS-GVO; sich dem anschließend *Kutscher*, Der digitale Nachlass, S. 45 f.

72 Entsprechend argumentiert *Klement* in: NK-Datenschutzrecht, Art. 7 DS-GVO Rn. 92 auch spezifisch europarechtlich, wenn er sich *Bräutigam* anschließt. Der Grundsatz der Vertragsfreiheit sei auch europarechtlich anerkannt. Daher sei in dieser Konstellation von einem wirksamen vertraglichen Ausschluss des Widerrufs auszugehen. Es sei treuwidrig, eine Einwilligung zu widerrufen, die wegen einer wirksamen vertraglichen Verpflichtung sofort wieder erteilt werden müsste (*dolo-agit-Einwand*); s. aber *Frenzel* in: Paal/Pauly (Hrsg.), DS-GVO, Art. 6 Rn. 13; wie hier *Hacker*, ZfPW 2019, 148, 169 f.; *Spindler/Dalby* in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, Art. 7 DS-GVO Rn. 12 f.

73 *Frenzel* in: Paal/Pauly (Hrsg.), DS-GVO, Art. 7 Rn. 17a.

74 A.A. *Bock*, AcP (217) 2017, 370, 377; *Specht-Riemenschneider* in: Röhrich/Graf von Westphalen/Haas (Hrsg.), HGB, Plattformnutzungsverträge, Rn. 20 f.; *Spindler/Dalby* in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, Art. 7 DS-GVO Rn. 13 wollen eine Kollision von Schuld- und Datenschutzrecht verhindern, indem der datenschutzrechtliche Widerruf stets zugleich als schuldrechtliche Kündigung aufgefasst wird.

nie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen⁷⁵ wird umsetzen müssen.⁷⁶

5. Zwischenergebnis zur Vertragstypologie von Nutzungsverträgen

Sofern sie die Entgeltlichkeit des Vertragsverhältnisses – wie hier – ablehnen, schlagen einige Stimmen in der Literatur die Annahme eines Auftrags im Sinne von § 662 BGB vor.⁷⁷ Das ist aus mehreren Gründen aber ebenfalls unpassend. Kern des Auftragsverhältnisses ist eine fremdnützige Tätigkeit – nämlich die unentgeltliche Besorgung eines Geschäfts durch den Beauftragten.⁷⁸ Der Betreiber des sozialen Netzwerks wird aber – wie gesehen – gerade in seinem eigenen (ökonomischen) Interesse tätig. Ferner dürften die gesetzlich vorgesehenen Ansprüche des Auftragsrechts den Interessen beider Vertragsparteien zuwiderlaufen. Der Provider wird, als Beauftragter, weder die von ihm erstellten Nutzerprofile noch gar seine Werbeeinnahmen gem. § 667 BGB als das durch die Geschäftsbesorgung Erlangte herausgeben. Der Nutzer wird als Auftraggeber keinen Aufwendungsersatz gem. § 670 BGB für die IT-Infrastruktur des Providers leisten.⁷⁹

Nach alledem einigen sich die Nutzungsvertragsparteien regelmäßig auf einen Vertrag *sui generis*, der für den Nutzer unentgeltlich ist und je nach

75 Im Vergleich zur verabschiedeten Fassung sah die Entwurfsfassung der Richtlinie Daten noch eindeutiger als Gegenleistung im vertraglichen Synallagma vor, vgl. noch Art. 3 Nr. 1 RL-E: „Diese Richtlinie gilt für alle Verträge, auf deren Grundlage ein Anbieter einem Verbraucher digitale Inhalte bereitstellt oder sich hierzu verpflichtet und der Verbraucher als Gegenleistung einen Preis zahlt oder *aktiv eine andere Gegenleistung als Geld in Form personenbezogener oder anderer Daten erbringt.*“ (Hervorhebung nicht im Original) Vgl. dazu *Spindler*, MMR 2016, 147, 147 ff.; s. ferner *Mischau*, ZEuP 2020, 335.

76 Zur Fortentwicklungsperspektive durch den europäischen Gesetzgeber s. *Paal/Hennemann*, NJW 2017, 1697, 1698 m.w.N.; *Metzger*, AcP 216 (2016), 817, passim; zum Ganzen sehr ausführlich und mit rechtspolitischer Handlungsempfehlung an den Gesetzgeber s. Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 199 ff., abrufbar a.a.O. (Fn. 43).

77 *Redeker* in: Hoeren/Sieber/Holznapel (Hrsg.), MMR-HdB, Teil 12 Rn. 422 ff., 428; *Seidler*, Digitaler Nachlass, S. 129 ff.

78 *Schäfer* in: MüKo BGB, § 662 Rn. 1; *D. Fischer* in: BeckOK BGB, § 662 Rn. 1.

79 *Bräutigam*, MMR 2012, 635, 636; das Problem sieht auch *Redeker*, IT-Recht, Rn. 1279, der darüber allerdings hinweggeht und trotzdem von einem Auftrag ausgeht, weil mangels Bestimmtheit „vermutlich keine konkreten Ansprüche bestehen.“

genauer Ausgestaltung des Internetdienstes dienst-, werk- und/oder mietvertragliche Leistungspflichten des Providers vorsieht.⁸⁰

II. Urheber- und Leistungsschutzrechte des Erblassers

Unabhängig von der lediglich nutzungsvertraglichen Rechtsposition an dem gesamten Account und seinen Inhalten können dem Nutzer absolute Rechte nach Maßgabe des UrhG an einzelnen Accountinhalten zustehen:⁸¹ Urheber- bzw. Leistungsschutzrechte an den vom Nutzer selbstgenerierten Inhalten.⁸² Der Wert und die Bedeutung dieser Rechtsposition kann nur im Einzelfall bestimmt werden und variiert nach dem Nutzungsverhalten des Erblassers. Angesichts großer – mitunter sogar unbegrenzter – Speicherkapazitäten, die dem Nutzer vom Provider zur Verfügung gestellt werden, besteht aber jedenfalls das Potenzial einer Vielzahl von urheberrechtlich relevanten Accountinhalten.⁸³

Gem. § 28 Abs. 1 UrhG ist das Urheberrecht vererblich.⁸⁴ Der Übergang dieser Rechtsposition im Erbfall erfolgt grundsätzlich unabhängig vom Schicksal des Nutzungsvertrags. Insbesondere etwaige datenschutz- und telekommunikationsrechtliche Beschränkungen des Erbrechts an der nutzungsvertraglichen Position, die nicht zuletzt dem Schutz der Kommunikationspartner des Erblassers dienen,⁸⁵ spielen mit Blick auf übergehende Urheber- und Leistungsschutzrechte keine Rolle. Dasselbe gilt für einen (formularvertraglichen) Ausschluss der Vererbbarkeit des Accounts,⁸⁶ der sich, seine Wirksamkeit vorausgesetzt, ausschließlich auf die nutzungsvertragliche nicht aber auf die urheberrechtliche Rechtsposition des Erblassers auswirken kann.

80 Siehe dagegen aber *Schäfer* in: MüKo BGB, § 662 Rn. 18 a.E.

81 A.A. *Seidler*, Digitaler Nachlass, S. 73 f.

82 Mit Beispielen *Bullinger* in: Wandtke/Bullinger (Hrsg.), UrhG, § 2 Rn. 156 ff.; *Bauer*, User Generated Content, in: Große Ruse-Khan/Klass/v. Lewinski (Hrsg.), Nutzergenerierte Inhalte als Gegenstand des Privatrechts, S. 6 ff.; *Reinemann/Remmert*, ZUM 2012, 216, 218 ff.

83 Vgl. dazu noch ausführlich auf S. 189 ff.

84 Dasselbe gilt für den Leistungsschutz an Licht- und Laufbildern, s. *Obly* in: Schricker/Loewenheim (Hrsg.), § 28 UrhG Rn. 18, 20; *Nordemann* in: Fromm/Nordemann, § 28 UrhG Rn. 16; *Rehbinder/Peukert*, Urheberrecht, Rn. 991.

85 Vgl. dazu noch ausführlich auf S. 94 ff.

86 Siehe dazu S. 166 ff.

Gleichwohl ist ein enger Zusammenhang zwischen dem Account und seinen Inhalten nicht abzustreiten. Sehen etwa die Nutzungsbedingungen eines Anbieters von Cloud-Speicherplatz im Falle des Todes des Nutzers die Löschung des Accounts mitsamt seinen Inhalten vor,⁸⁷ kann das erhebliche (faktische) Auswirkungen für ein urheberrechtlich geschütztes Werk haben, wenn und soweit keine weiteren Kopien (beispielsweise eines Textmanuskripts oder von Fotografien) außerhalb des Accounts existieren. Ein weiterer Berührungspunkt der vertraglichen und der absoluten Rechtsposition ist die Einräumung von Urheberrechtslizenzen durch den Nutzer, auf welche der Provider angewiesen ist, um die geschützten Inhalte auf einem Server speichern und Dritten, wie den Privatkontakten oder Followern des Nutzers, zugänglich machen zu dürfen.⁸⁸ Im Erbfall ist die Bindung der Rechtsnachfolger an diese Lizenzen im Einzelfall zu prüfen, wobei mit Blick auf den Zweck der Lizenzierung auch das postmortale Schicksal des Nutzungsvertrags zu berücksichtigen ist.⁸⁹

Im weiteren Verlauf der Untersuchung werden die Immaterialgüterrechte des Erblassers als eigenständige Erbrechtsobjekte zu beleuchten sein. Gleichzeitig sind sie auch und gerade in ihren Bezügen zu den Nutzerkonten des Erblassers bei Anbietern von Informations- und Kommunikationsdiensten zu betrachten. Denn aus der gesamten Schnittmenge der Rechtsgebiete „Urheberrecht und Erbrecht“⁹⁰ sind hier diejenigen Aspekte herauszugreifen, die den Lebensbereich eines durchschnittlichen Nutzers sozialer Medien und damit seinen digitalen Nachlass betreffen.

87 So z.B. Apple bezüglich der Apple-ID für iCloud, vgl. Ziff. IV. D. der AGB, abrufbar unter <https://www.apple.com/legal/internet-services/icloud/de/terms.html> [17.11.2020]. Siehe dazu ein Versäumnisurteil des LG Münster ErbR 2019, 455 (mit Anm. von *Pruns*) zulasten von Apple.

88 Betroffen sind mindestens §§ 16, 19a und ggf. 23 S. 1 UrhG, s. *Berberich*, MMR 2010, 736, 737, 739; *Paul* in: Hoeren/Sieber/Holznapel (Hrsg.), MMR-HdB, Teil 7.4 Rn. 140; *Solmecke* ebd., Teil 21.1 Rn. 6; *ders./Dam*, MMR 2012, 71, 72; ferner *König/Stang* in: Münchener Anwaltshandbuch Urheberrecht, § 31 Rn. 14.; zweifelnd aber *Imhof* in: Bisges (Hrsg.), Handbuch Urheberrecht, Kap. 4 Rn. 139.

89 Zum Ganzen s. S. 194 ff.

90 Monografisch dazu insgesamt *Clément*, Urheberrecht und Erbrecht, und *Gloser*, Die Rechtsnachfolge in das Urheberrecht, jeweils passim; überblicksartig zur einschlägigen Rechtsprechung *Gergen*, ZErB 2009, 42, 42 ff.

III. Zwischenergebnis zu A.

Mit der großen Vielfalt der angebotenen Internetdienste korreliert eine Vielgestaltigkeit der Nutzungsverträge. Das betrifft sowohl das Leistungsspektrum des Providers, welches von der technisch-funktionalen Ausgestaltung des Internetdienstes abhängt, als auch die Frage nach einer etwaigen Gegenleistung des Nutzers. Letztere kann in einer Geldleistung oder in der Bereitschaft bestehen, sich durch die Preisgabe persönlicher Daten als „(werbe)vermarktetes Produkt“⁹¹ des Providers gegenüber dessen Werbekunden zur Verfügung zu stellen. Vor diesem Hintergrund bleibt zwar eine einzelfallbezogene Beurteilung unumgänglich. Jedenfalls werden aber eine Vielzahl der Nutzungsverhältnisse als unentgeltliche Verträge eigener Art mit dienst-, werk- und/oder mietvertraglichen Elementen abgeschlossen. In diesem Rahmen hält der Provider einen Account bereit, in welchen der Nutzer unterschiedliche Inhalte einbringen kann. Etwaige an diesen Inhalten bestehende Urheber- und Leistungsschutzrechte sowie die vertragliche Rechtsposition des Nutzers bilden als Erbrechtsobjekte den Gegenstand dieser Untersuchung.

B. Daten als solche – (k)ein Recht an Daten

Die Untersuchung des Erbrechtsobjekts im Rahmen des digitalen Nachlasses berührt eine weitere Debatte, die ebenfalls im Bereich der Schnittstelle zwischen Digitalisierung und (Privat)recht geführt wird: In der rechtswissenschaftlichen Literatur wird über ein sogenanntes Recht an Daten diskutiert.⁹² Dabei stehen zwei verwandte Fragen im Zentrum. Zum einen wird das geltende Recht daraufhin untersucht, ob es ein eigentumsähnliches Ausschließlichkeitsrecht an Daten gibt oder ob ein entsprechendes Recht mittels Analogiebildung konstruiert werden kann.⁹³ Zum anderen wird – in Abhängigkeit von der Beantwortung der ersten Frage – eine rechtspolitische Debatte darüber geführt, ob es sinnvoll und notwendig ist, ein solches Recht neu zu schaffen.⁹⁴ Die Auseinandersetzungen sollen hier (nur)

91 So im Kontext von § 18 Abs. 2a GWB *Paal*, WuW 2016, 453.

92 Grundlegend *Zech*, Information als Schutzgegenstand, passim; *Amstutz*, AcP 218 (2018), 439, 439 ff.; überblicksartig *Boehm*, ZEuP 2016, 358, 381 ff. und *Röttgen* in: *Specht-Riemenschneider/Werry/Werry* (Hrsg.), Datenrecht in der Digitalisierung, S. 373 ff.; vgl. ferner die Nachweise in den folgenden Fußnoten.

93 Hierzu sogleich auf S. 48 ff.

94 Vgl. dazu S. 66 f.

insoweit dargestellt werden, wie sie für die erbrechtliche Untersuchung dieser Arbeit fruchtbar gemacht werden können. Denn wenn und soweit ein entsprechendes Recht an Daten besteht oder eingeführt wird, kann es als Rechtsobjekt in den digitalen Nachlass fallen.⁹⁵ Allerdings begegnet die juristische Konstruktion eines Rechts an Daten technischen wie juristischen Bedenken.

I. Einführung in die Debatte

Ausgangspunkt der Debatte ist die Annahme, Daten seien „der Rohstoff der Zukunft“⁹⁶. Mit diesem Bild geht ein großes Interesse an der Frage nach den Herrschaftsrechten über diesen „Rohstoff“ einher.⁹⁷ Gleichzeitig stellen Daten mit ihren technischen Spezifika – insbesondere der Immaterialität, der einfachen Möglichkeit der Vervielfältigung ohne Qualitätseinbuße sowie rapide wachsenden Speicherkapazitäten – gegenüber sonstigen Gütern eine eigene Kategorie dar.⁹⁸ Es erscheint fraglich, ob und inwieweit die Zuordnung von Daten durch traditionelle Rechtsmaterien erfolgen kann, deren originärer Regelungsgegenstand (wie etwa im Falle des Sachen- oder Immaterialgüterrechts) ein anderer ist.

Vor diesem Hintergrund ist auch der Begriff des „Dateneigentums“, unter dem die Debatte oder einzelne ihrer Aspekte mitunter geführt werden, kritisch zu würdigen.⁹⁹ Die begriffliche Anlehnung an das Sachenrecht

95 *Thiesen*, Daten in der Erbmasse, S. 181 hält es für möglich, dass eine „Materialisierung von Kommunikationsinhalten [...] potenziell die Behandlung des digitalen Nachlasses vereinfachen“ kann; vgl. auch *Stieper*, der fragt, ob neben vertraglichen Abwicklungsansprüchen nicht auch über eine Verdinglichung von Daten im digitalen Nachlass nachgedacht werden müsse, zitiert nach dem Diskussionsbericht von *Bornhauser*, AcP (218) 2018, 594, 597 f.

96 So Bundeskanzlerin *Angela Merkel* zitiert nach *Markendorf*, ZD 2018, 409, 409; *Kühling/Sackmann*, ZD 2020, 24, 24; sowie *Paal/Hennemann*, NJW 2017, 1697, 1697 f., die das Bild „wegen der wettbewerblichen Eigenheiten von Daten [als] etwas schief“ bewerten: Daten sind anders als andere (insbesondere körperliche) Güter im Konsum nicht-rival, sie sind nicht-abnutzbar und idR. nicht-exklusiv. S. dazu auch die Nachweise in Fn. 98 und 115.

97 *Markendorf*, ZD 2018, 409, 409; *Zech*, GRUR 2015, 1151, 1152 sowie *ders.*, CR 2015, 137, 139 m.w.N.

98 *Zech*, CR 2015, 137, 140.

99 *Kühling/Sackmann*, Rechte an Daten, Regulierungsbedarf aus Sicht des Verbraucherschutzes?, 20. November 2018, Rechtsgutachten im Auftrag des Verbraucherzentrale Bundesverband, abrufbar unter <https://www.vzbv.de/pressemitteilung/m-eine-daten-gehoren-dir>, S. 6, 7 f., [17.11.2020].

veranschaulicht, dass unter dem Schlagwort den Möglichkeiten (und Grenzen) eines Zuordnungsregimes für Daten nachgegangen wird.¹⁰⁰ Das ist zwar in funktionaler Hinsicht nicht falsch, insbesondere wenn ein umfassendes Herrschaftsrecht an Daten untersucht bzw. gefordert wird. Dogmatisch hingegen impliziert „Dateneigentum“ fälschlicherweise die Gleichsetzung der Rechtsinstitute von Sacheigentum und einem etwaigen Recht an Daten.¹⁰¹ Das kann durch die Termini „Datenausschließlichkeitsrecht“ oder (eigentumsähnliches) „Recht an Daten“ vermieden werden. Die Bezeichnung Recht an Daten bildet ferner die Breite der geführten Auseinandersetzung besser ab, da neben umfassenden Herrschaftsrechten auch (einfache) Nutzungs- und/oder Zugangsrechte thematisiert werden.¹⁰² Wenn im Folgenden der Begriff „Dateneigentum“ trotzdem gebraucht wird, so geschieht das in dessen Qualität als Schlagwort zur Bezeichnung der gesamten Debatte über einen datenrechtlichen Ordnungsrahmen.

In dieser Debatte lassen sich grob zwei Stoßrichtungen unterscheiden, die zwar verwandt sind und Parallelen aufweisen, aber durch einen jeweils eigenen (rechts)politischen Impetus gekennzeichnet sind und auch teilweise unterschiedliche Anwendungsfelder etwaiger Datenrechte vor Augen haben. Zum einen gibt es die primär aus Sicht des Individuums konzeptionierte Forderung, die Herrschaft einer Privatperson über „ihre eigenen Daten“ zu gewährleisten.¹⁰³ Zum anderen werden Datenrechte im Zusammenhang mit der kommerziellen, maschinengesteuerten Auswertung sehr großer Datenmengen (sog. Big Data) untersucht und hier oft im Zusam-

100 Ebd. Fn. 99.

101 Das Sachenrecht kann aber mangels Körperlichkeit von Daten nicht zur Begründung eines „Dateneigentums“ herangezogen werden. Siehe dazu S. 48 f. So auch die einhellige Meinung, s. die Nachweise in Fn. 113 und 116.

102 Ebd. Fn. 99.

103 In diesem Sinne beispielsweise Fezer, ZD 2017, 99, 99 ff. sowie ders., MMR 2017, 3, passim, der ein „immaterialgüterrechtliches Eigentum an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten“ fordert.

menhang mit Schlagworten wie „Industrie 4.0“¹⁰⁴ und „Smart Cars“ thematisiert.¹⁰⁵

Für den digitalen Nachlass sind jedwede Datenrechte potenziell von Interesse, wenn und soweit sie als Aktiva oder auch als Passiva in den Nachlass fallen (können). Im Kontext sozialer Medien werden dabei vor allem die Rechte an solchen Datensätzen relevant sein, die entweder einen Personenbezug im Sinne des Datenschutzrechts haben oder aus anderen Gründen einen persönlichkeitsrechtlichen Schutz genießen.¹⁰⁶ Als ein Beispiel sei hier die Frage nach Ausschließlichkeitsrechten an Daten im Rahmen von Cloud-Computing im B2C-Bereich genannt.¹⁰⁷

104 Nach *Zech*, GRUR 2015, 1151, 1152 m.w.N. muss im Rahmen der „Industrie 4.0“ zwischen drei Entwicklungen differenziert werden: Erstens werden körperliche Güter mit Datenbezügen ausgestattet (sog. „Smart Products“; bspw. Smartphone, „Smart Cars“). Zweitens werden körperliche Güter durch Daten ersetzt (sog. „e-products“; bspw. E-Books, Streaming). Drittens werden neuartige Güter eigener Art gehandelt – über datengetriebene Wirtschaft hinaus entsteht infolgedessen eine Wirtschaft mit Daten. Daten werden damit zu einem Wirtschaftsgut, das in einer Datenwirtschaft gehandelt wird.; zur wettbewerbsrechtlichen Dimension *Paal/Hennemann*, NJW 2017, 1697, 1698 f.

105 Vgl. *Grützmaier*, CR 2016, 485, 485 ff.; aus ökonomischer Perspektive *Kerber*, GRUR Int. 2016, 989, 990; in diesem Kontext auch thematisiert von *Weidert/Bug* in: *Röhrich/Graf von Westphalen/Haas* (Hrsg.), HGB, Zulieferverträge in der Industrie 4.0, Rn. 24 ff.; *Ensthaler*, NJW 2016, 3473, 3473 ff.; nach *Kübling/Sackmann*, Rechte an Daten, Regulierungsbedarf aus Sicht des Verbraucherschutzes?, abrufbar a.a.O. Fn 99, S. 6, war der Umgang mit Daten aus vernetzten Fahrzeugen sogar der Ausgangspunkt der aktuellen Debatte. Die deutsche Automobilindustrie sei bestrebt, in einer zunehmend datengetriebenen Mobilität weiterhin zentraler Teil der Wertschöpfungskette zu sein und nicht etwa reiner Zulieferer von Digitalkonzernen. In Ansehung der starken deutschen Automobilindustrie bei einer – im Vergleich zu den USA – wenig entwickelten Datenwirtschaft bestehe daran in Deutschland ferner ein industriepolitisches Interesse. So verwundere es nicht, dass eine regulatorische Neuordnung bei Fragen nach der Zuordnung von Daten auch und gerade im Mobilitätsumfeld aufgeworfen werde.

106 Nicht-personenbezogene Daten, auf die das Datenschutzrecht keine Anwendung findet und die auch sonst nicht persönlichkeitsrechtlich relevant sind, werden in Abgrenzung dazu als Rohdaten bezeichnet, s. etwa *Zech*, GRUR 2015, 1151, 1152; *Kerber*, GRUR Int. 2016, 989, 990 f. spricht von „industrial data“; kritisch zu dieser Bezeichnung *Hoeren/Pinelli*, JZ 2020, 879, 879 in Fn. 1.

107 Zu der Frage, ob in diesem Fall Ausschließlichkeitsrechte an den Daten in der Cloud bestehen und, bejahendenfalls, ob diese Rechte dem Cloud-Anbieter bzw. dem Nutzer zustehen, vgl. *Boehm*, ZEuP 2016, 358, 379 ff.

Im Folgenden soll zunächst ein Blick auf die Situation de lege lata geworfen werden (dazu II.), bevor sodann in einem Ausblick die rechtspolitische Diskussion zu beleuchten ist (dazu III.).

II. Konstruktionsvorschläge nach geltendem Recht

Ein explizit (spezial-)gesetzlich geregeltes Ausschließlichkeitsrecht an Daten als solchen besteht im geltenden Recht nicht. Freilich können einzelne immaterialgüterrechtlich geschützte Positionen mit Datenbezug bestehen. Dafür steht exemplarisch der urheberrechtliche Schutz von Software nach §§ 69a ff. UrhG, dessen Grundlage aber der Werkcharakter des Computerprogramms und nicht etwa die Speicherungsform der Software ist.¹⁰⁸ Weder die digitale Form an sich noch der Akt der Datenerzeugung selbst sind im geltenden Recht der (entscheidende) Anknüpfungspunkt für ein Ausschließlichkeitsrecht an Daten. Zur Konstruktion etwaiger Rechte an Daten kommt daher allenfalls die entsprechende Anwendung anderer Regelungen in Betracht.

1. Sachenrecht

Zunächst drängt sich die Untersuchung der Anwendbarkeit sachenrechtlicher Grundsätze auf. Das liegt nicht zuletzt an dem Schlagwort des „Dateneigentums“, unter dem die Debatte vielfach geführt wird. Darüber hinaus liegt für Fragen nach der Güterzuordnung sowie der Zuweisung absoluter Rechtspositionen auch in funktionaler Hinsicht ein Blick in das dritte Buch des BGB nahe. Als Ausgangspunkt der sachenrechtlichen Kategorien von Besitz und Eigentum verweist das Gesetz in den §§ 854 Abs. 1 und 903 S. 1 BGB auf den Begriff der Sache als das maßgebliche Rechtsobjekt. Nach § 90 BGB sind Sachen im Sinne des Gesetzes nur körperliche Gegenstände. Körperlich ist ein Gegenstand, wenn man ihn anfassen oder zumindest sinnlich wahrnehmen und beherrschen kann.¹⁰⁹ In technischer Hinsicht handelt es sich bei gespeicherten Daten um ein bestimmtes Mus-

108 Vgl. § 69a Abs. 3 UrhG, dazu *Dreier* in: *Dreier/Schulze* (Hrsg.), *UrhG*, § 69a Rn. 1 und ferner *Wiebe* in: *Spindler/Schuster* (Hrsg.), *Recht der elektronischen Medien*, § 69a UrhG Rn. 26 ff.

109 *Stresemann* in: *MüKo BGB*, § 90 Rn. 1; *Dörner* in: *HK-BGB*, § 90 BGB Rn. 2 f.; zum Sachbegriff insgesamt auch *Mansel* in: *Jauernig, BGB*, Vor §§ 90 ff. Rn. 2 ff.

ter magnetischer Spannung,¹¹⁰ das nicht ohne Zuhilfenahme technischer Infrastruktur wahrnehmbar ist.¹¹¹ Daten sind – anders als Speichermedien wie etwa Festplatten¹¹² – mangels Körperlichkeit keine Sachen im Sinne des BGB.¹¹³

Außerdem fehlt es Daten regelmäßig¹¹⁴ auch an der für das Sacheigentum charakteristischen Rivalitätsbedingung: Daten können von mehreren Personen simultan genutzt und mit nur geringem Aufwand ohne Verlust vervielfältigt werden.¹¹⁵ An Daten kann folglich weder Sacheigentum noch Besitz im Sinne der §§ 903 S. 1 und 854 Abs. 1 BGB bestehen.¹¹⁶ Umgekehrt ändert sich auch die Eigentumslage an einem Datenträger nicht dadurch, dass auf ihm bestimmte Daten gespeichert werden, solange der Datenträger selbst dabei nicht seine typische Funktion verändert und auf diese Weise zu einer neuen Sache im Sinne von § 950 Abs. 1 S. 2 BGB wird.¹¹⁷ Eine solche Veränderung wird bei praxisnaher Betrachtung regelmäßig nicht gegeben sein.

110 *Wagner* in: MüKo BGB, § 823 Rn. 245. Siehe auch Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 32 f., abrufbar a.a.O. (Fn. 43).

111 *Berberich*, Virtuelles Eigentum, S. 90 f.

112 *Stieper* in: Staudinger, § 90 BGB Rn. 12; *Stresemann* in: MüKo BGB, § 90 Rn. 25; *Wagner* in: MüKo BGB, § 823 Rn. 246.

113 *Boehm*, ZEuP 2016, 358, 381; *Amstutz*, AcP 218 (2018), 439, 544 gegen *Berberich*, Virtuelles Eigentum, S. 92 f.; nach *Stieper* in: Staudinger, § 90 BGB Rn. 18 folge auch bei unterstellter Sachqualität nichts anders, da Daten in diesem Fall wesentliche Bestandteile des Datenträgers darstellten und nach § 93 BGB nicht sonderrechtsfähig wären. A.A. wohl *Mansel* in: Jauernig, BGB, Vor §§ 90 ff. Rn. 3.

114 *Berberich*, Virtuelles Eigentum in: Große Ruse-Khan/Klass/v. Lewinski (Hrsg.), Nutzergenerierte Inhalte als Gegenstand des Privatrechts, S. 181 ff.; rechtspolitisch dazu, wie man mittels Blockchain-Technologie zumindest zu einer (rechtlichen) Erstellungsvermutung gelangen kann, s. *Markendorf*, ZD 2018, 409, 411 ff.

115 *Wagner* in: MüKo BGB, § 823 Rn. 335; *Zech*, Information als Schutzgegenstand, S. 117 ff., 328 f.; *Hoeren/Pinelli*, JZ 2020, 879, 880 sowie Nachweis in Fn. 98.

116 *Stieper* in: Staudinger, § 90 BGB Rn. 17; *Stresemann* in: MüKo BGB, § 90 Rn. 25; *Berberich/Golla*, PinG 2016, 165, 170; zweifelnd *Hoeren*, MMR 2019, 5, 5 ff.

117 *Stieper* in: Staudinger, § 90 BGB Rn. 13; BGH NJW 2016, 317 Rn. 19.

2. Deliktsrechtlicher Schutz von Daten

Unabhängig von ihrer Sachqualität können Daten unter Umständen deliktsrechtlichen Schutz genießen. Denn insbesondere der Schutzbereich des Eigentums an einem Datenträger kann sich auf die darauf abgespeicherten Daten erstrecken. So erfolgt etwa die Löschung oder Änderung gespeicherter Daten im Wege physikalischer Veränderung des Datenträgers und kann so einen Eingriff in das an dem Speichermedium bestehende Eigentum darstellen.¹¹⁸ Allerdings versagt dieser über das Eigentum vermittelte Schutz für Daten in Konstellationen, in denen das Eigentum am Speichermedium und die etwaige „Berechtigung“¹¹⁹ an den Daten auseinander fallen. Ein praktisch bedeutsames Beispiel hierfür ist das Cloud-Computing. Hier steht das Eigentum an dem Server dem Internetdienstleister oder seinem Subunternehmer zu, während die Daten von den einzelnen Nutzern eingebracht werden.¹²⁰

118 *Zech*, CR 2015, 137, 141 f.; *Stieper* in: Staudinger, § 90 BGB Rn. 19; *Wagner* in: MüKo BGB, § 823 Rn. 246, 332.

119 Mit dem hier verwendeten Begriff soll dem Ergebnis dieses Abschnitts, der gerade die Frage nach der Berechtigung an Daten zum Gegenstand hat, nicht vorgegriffen werden. Mit „Berechtigung“ soll lediglich zum Ausdruck kommen, dass beispielsweise der Autor oder der User, der die Speicherung vornimmt, eine Berechtigung an den Daten empfindet („meine Daten“), vgl. dazu bereits Fn. 36 und 37. Wenn die Speicherung aber nicht auf im eigenen Eigentum stehenden Speichermedien erfolgt (s. Cloud-Computing), ergeben sich ggf. (Delikts-)Schutzlücken.

120 *Bock*, AcP (217) 2017, 370, 380 konstatiert eine „immer stärker voranschreitende Entlokalisierung und Zersplitterung der Speicherung.“ Vgl. auch *Boehm*, ZEuP 2016, 358, 385; Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 48 f., abrufbar a.a.O. (Fn. 43). Ähnliche Konsequenzen können sich im herkömmlichen Arbeitsverhältnis ergeben, wenn der Arbeitnehmer (und spätere Erblasser) sein berufliches E-Mail-Postfach auf einem privaten Endgerät nutzt bzw. wenn er vom Arbeitgeber zur Verfügung gestellte Endgeräte (auch) im privaten Kontext nutzt. Ferner ist an unter Eigentumsvorbehalt erworbene oder gemietete Hardware zu denken.

a) Recht am Datenbestand als „Sonstiges Recht“ iSv. § 823 Abs. 1 BGB

Den Schutzlücken,¹²¹ die aus der Entlokalisierung der Speicherung folgen,¹²² wollen einige Stimmen in der Literatur begegnen, indem sie ein Recht am Datenbestand als „sonstiges Recht“ im Rahmen von § 823 Abs. 1 BGB annehmen: Der Schutzzumfang des Deliktsrechts könne nicht davon abhängen, auf welche Weise Daten übermittelt und gespeichert werden. Ansonsten verfehle das Deliktsrecht seine Aufgabe, auch angesichts moderner technischer Phänomene Lösungen auf Grundlage der Wertungen des § 823 Abs. 1 BGB zu finden. In dem Maße, in dem mit Hilfe neuer Technologien Daten losgelöst vom Sacheigentum gespeichert werden, müsse das Privatrecht Schritt halten und den Schutz des „Dateneigentums“ gewährleisten.¹²³

Ausgangspunkt der Anerkennung eines Rechts als „sonstiges Recht“ im Rahmen von § 823 Abs. 1 BGB ist stets, dass es sich um ein eigentumsähnliches Recht handeln muss. So wie die in § 823 Abs. 1 BGB explizit genannten Rechte und Rechtsgüter muss auch jedes „sonstige Recht“ eine absolute, gegenüber jedermann wirkende Rechtsposition sein.¹²⁴ Die ausschließliche Stellung muss gerade aus der Rechtsposition folgen und darf nicht lediglich – etwa technisch bedingt – faktischer Natur sein.¹²⁵ Für das Recht am Datenbestand ist darauf hinzuweisen, dass § 823 Abs. 1 BGB ein bestehendes Recht oder Rechtsgut voraussetzt und dessen Zuweisung gerade nicht selbst vornimmt.¹²⁶ Es darf somit nicht vorschnell von einem

121 *Faust*, Gutachten zum 71. DJT, 2016, S. A 77 f.; *Stieper* in: Staudinger, § 90 BGB Rn. 19; a.A. *Hager* in: Staudinger, § 823 BGB Rn. B 192, der kein „unabdingbares Bedürfnis“ für eine weitere Ausdehnung jenseits des bereits geschützten Eigentums am Datenträger sieht. Instrukтив auch *Herzog/Pruns*, Der digitale Nachlass in der Vorsorge- und Erbrechtspraxis, S. 10 f.

122 Ebd. Fn. 120.

123 *Wagner* in: MüKo BGB, § 823 Rn. 332.

124 *Sprau* in: Palandt, § 823 BGB Rn. 11; *A. Staudinger* in: HK-BGB, § 823 BGB Rn. 28; *Förster* in: BeckOK BGB, § 823 Rn. 143; ferner *Berberich/Golla*, PinG 2016, 165, 172 f.

125 BGH NJW 2012, 2034 Rn. 23 zu Domains. Das gilt sogar, wenn die faktische Position eigentumsfähig im Sinne von Art. 14 Abs. 1 S. 1 GG ist, vgl. a.a.O. Rn. 27 sowie *Sprau* in: Palandt, § 823 BGB Rn. 11. Zu Domains als Rechtsobjekt des digitalen Nachlasses vgl. bereits die Nachweise in Fn. 23. Siehe ferner Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 46 f., abrufbar a.a.O. (Fn. 43).

126 *Thiesen*, Daten in der Erbmasse, S. 164; *Determann*, ZD 2018, 503, 504; *Kühling/Sackmann*, ZD 2020, 24, 26 a.E.

Schutzbedürfnis auf einen bestehenden Schutz *de lege lata* geschlossen werden. Das gilt insbesondere für das Recht an Daten, für welches die Debatte darüber, wem und auf welche Weise das Recht zuzuordnen wäre, noch in vollem Gange ist.¹²⁷ Vor diesem Hintergrund wäre bei der unterstellten Aufnahme des Datenrechts als „sonstiges Recht“ die Frage nach der Aktivberechtigung noch offen, obschon bereits ein geschütztes Rechtsgut ausgemacht wäre. Bezeichnenderweise hat selbst der Gesetzgeber in § 303a StGB – in Abgrenzung zu § 303 StGB – die Fremdheit der Daten gerade nicht zur Voraussetzung für die Strafbarkeit u.a. der Löschung oder Änderung der Daten gemacht.¹²⁸ Zurecht weist *Wagner* insoweit darauf hin, dass die Komplexität der Frage kein Grund ist, mit der notwendigen Konkretisierungsarbeit gar nicht erst anzufangen.¹²⁹ Gleichwohl stellt sich die Frage, ob derart zentrale Fragen wie die Schaffung und Zuordnung von Datenrechten – kurz eines umfassenden „Sachenrechts für Daten“¹³⁰ – nicht dem Gesetzgeber überlassen bleiben müssen.¹³¹

b) Deliktsrechtlicher Schutz von Daten gem. § 823 Abs. 2 BGB

Schon jetzt ist ein deliktsrechtlicher Schutz von Daten auch ohne die Anerkennung eines absoluten Rechts im zuvor dargestellten Sinne möglich. Gem. § 823 Abs. 2 BGB in Verbindung mit § 303a StGB lösen indessen nur vorsätzliche Verletzungshandlungen eine Schadensersatzpflicht aus. Sofern mit Hinweis auf diese Beschränkung die Anerkennung eines absoluten

127 *Faust*, Gutachten zum 71. DJT, 2016, S. A 84 mit instruktiven Beispielen komplexer Zuordnungsfragen; das sieht so auch *Wagner* in: MüKo BGB, § 823 Rn. 336; weitere Beispiele bei Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 42 f., abrufbar a.a.O. (Fn. 43).

128 *Faust*, Gutachten zum 71. DJT, 2016, S. A 84.

129 *Wagner* in: MüKo BGB, § 823 Rn. 336 f. m.w.N. zu entsprechenden Vorschlägen.

130 *Faust*, Gutachten zum 71. DJT, 2016, S. A 84; lediglich für einen Datenbesitz als „Ausschließlichkeitsrecht schwächerer Art“ wirbt *Hoeren*, MMR 2019, 5, 5 ff.

131 *Boehm*, ZEuP 2016, 358, 384 f. etwa warnt vor kollidierenden Rechtspositionen, wenn durch die Anerkennung eines eigenen Rechts am Datenbestand iSv. § 823 Abs. 1 BGB neben nicht personenbezogenen Daten auch personenbezogene Daten, die dann auch durch das Persönlichkeitsrecht geschützt seien, betroffen wären. Siehe aber Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 51 f., abrufbar a.a.O. (Fn. 43).

Rechts an Daten gefordert wird, um eine Haftung für fahrlässige Verletzungshandlungen gem. § 823 Abs. 1 BGB zu konstruieren,¹³² ist der folgenreiche legislative Wille zu betonen. Der Gesetzgeber hat sich bewusst gegen eine deliktsrechtliche Generalklausel entschieden und die Ersatzfähigkeit reiner Vermögensschäden nur unter den restriktiven Voraussetzungen der §§ 823 Abs. 2 und 826 BGB zugelassen.¹³³ Eine Erweiterung der Haftung auch für fahrlässige Verletzungen eines Schutzgesetzes kann mithin richtigerweise ebenfalls nur der Gesetzgeber selbst vornehmen.¹³⁴

c) Rückschlüsse aus dem Deliktsrecht auf den digitalen Nachlass

Es stellt sich die Frage, ob und inwiefern die soeben skizzierte Debatte für die Lösung der Probleme des digitalen Nachlasses fruchtbar gemacht werden kann. Das Deliktsrecht allgemein vermittelt den Schutz des Integritätsinteresses und § 823 Abs. 1 BGB speziell schützt die Integrität der dort genannten Rechtsgüter.¹³⁵ Konkret bedeutet das für das Recht am Datenbestand insbesondere den Schutz vor Löschung und Veränderung der Daten.¹³⁶ Die zentralen Fragen des digitalen Nachlasses sind hingegen im Kern solche der Verkehrsfähigkeit des Erbrechtsobjekts. Insofern die deliktsrechtliche Debatte dem Rechtsverkehr mit Daten den Weg bereitet, liegt darin auch ein Beitrag zur Lösung der Probleme rund um den digitalen Nachlass. Das gilt nicht zuletzt, weil die Rechtsnachfolge im Erbfall ein wichtiger Teilaspekt des Rechtsverkehrs mit Daten ist. Dieser Rechtsverkehr hat indes insbesondere die translative Übertragung von Ausschließlichkeitsrechten und den konstitutiven Erwerb von Tochterrechten

132 So ausdrücklich *Wagner* in: MüKo BGB, § 823 Rn. 338.

133 *Teichmann* in: Jauernig, BGB, Vor §§ 823 ff. Rn. 2; *Förster* in: BeckOK BGB, § 823 Rn. 3; *Faust*, Gutachten zum 71. DJT, 2016, S. A 79 f.; *A. Staudinger* in: HK-BGB, Vorbemerkungen zu §§ 823-853 Rn. 8; *Hager* in: Staudinger, Vor §§ 823 ff. BGB Rn. 19 f. spricht von „kleiner Generalklausel“.

134 *Faust*, Gutachten zum 71. DJT, 2016, S. A 86 f. schlägt eine entsprechende Regelung eines Schutzgesetzes im Rahmen des BSIG vor, um eine Haftung nach § 823 Abs. 2 BGB für fahrlässige Verletzungshandlungen zu ermöglichen. A.A. *Wagner* in: MüKo BGB, § 823 Rn. 339. Zur rechtspolitischen Debatte s. noch S. 66 f.

135 Vgl. nur *Sprau* in: Palandt, Einführung vor § 823 BGB Rn. 1, § 823 BGB Rn. 2.

136 *Zech*, CR 2015, 137, 139 sowie grundlegend *ders.*, Information als Schutzgegenstand, S. 115 ff.; *Berberich/Golla*, PinG 2016, 165, 170; ferner *Determann*, ZD 2018, 503, 504.

zur Grundlage – und erst nachrangig den Integritätsschutz.¹³⁷ Der Integritätsschutz alleine schließt nicht die Zuweisung aller Befugnisse an dem geschützten Recht ein: Die Übertragung eines Rechts oder der Zugang zu einem Gegenstand gehen über den rein abwehrrechtlichen Integritätsschutz hinaus.¹³⁸ Auch das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG ist deliktsrechtlich als Rahmenrecht in § 823 Abs. 1 BGB geschützt, aber weder uneingeschränkt übertragbar noch vollumfänglich vererblich.¹³⁹ Sobald und soweit die fortdauernde Diskussion zum Deliktsrecht die bislang offenen Zuordnungsfragen des Datenrechts klären kann, lassen sich die sodann zugeordneten Datenrechte auch als Erbrechtsobjekte kategorisieren und einer Rechtsnachfolge im Erbfall zuführen. Da aber selbst diejenigen Stimmen, welche die Anerkennung eines Rechts am Datenbestand als „sonstiges Recht“ fordern, einräumen müssen, dass die Zuordnungsfrage (noch) offen ist,¹⁴⁰ hilft die betreffende Debatte dem digitalen Nachlass (noch) nicht weiter.

Allerdings kann der durch § 823 Abs. 1 BGB vermittelte Integritätsschutz vertragliche Ansprüche mitunter ergänzen, sofern das Recht am Datenbestand als „sonstiges Recht“ anerkannt würde: Wenn ein Provider – wie etwa ein Cloud-Anbieter – in seinen AGB (unwirksam) die Unvererbbarkeit der Account-Daten beziehungsweise des zugrundeliegenden Vertragsverhältnisses bestimmt und (in der Annahme der Wirksamkeit seiner AGB) die gespeicherten Daten nach dem Tod des Erblassers löscht.¹⁴¹ In diesem Fall könnte neben die vertraglichen Ansprüche auch ein deliktischer Anspruch treten, der soweit möglich auf Wiederherstellung des Datensatzes, anderenfalls auf Wertersatz, gerichtet ist.¹⁴² Dies gilt freilich mit allen bekannten Schwächen der deliktischen Haftung im Vergleich zur

137 Zech, CR 2015, 137, 139 f.; vgl. auch Grützmacher, CR 2016, 485, 489 f.

138 Thiesen, Daten in der Erbmasse, S. 164; Zech, GRUR 2015, 1151, 1158; ders., CR 2015, 137, 140 und 143; Berberich/Golla, PinG 2016, 165, 170; Determann, ZD 2018, 503, 504.

139 Vgl. nur Hager in: Staudinger, § 823 BGB Rn. C 50b f. und C 34 ff.; zur Vererbbarkeit des allgemeinen Persönlichkeitsrechts s. S. 106 ff.

140 S. die Nachweise in Fn. 129. Die Gegenseite wiederum ist freilich noch strenger und macht die Probleme der Zuordnung zum zentralen Gegenargument gegen die Anerkennung des Rechts am Datenbestand, vgl. hierzu die Nachweise in Fn. 126, 127 und 128.

141 Zu AGB betreffend die Vererbbarkeit von Nutzerkonten vgl. noch auf S. 166 ff.

142 Stieper in: Staudinger, § 90 BGB Rn. 19; Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 46, abrufbar a.a.O. (Fn. 43).

vertraglichen Schadensersatzhaftung.¹⁴³ Die praktische Relevanz dieser Konstellation dürfte zudem insofern abnehmen, als dass die vormals hohen Kosten, die mit der Speicherung der Daten verbunden waren, sinken, während der Wert der Nutzerdaten – möglicherweise auch über den Tod des Nutzers hinaus – an Wert gewinnen. Das Interesse der Provider an einer zügigen Löschung nach dem Erbfall dürfte daher begrenzt sein.¹⁴⁴

d) Zwischenergebnis

Für den Moment sei nach alledem festgehalten, dass selbst wenn man die Geltung eines umfassenden deliktsrechtlichen Integritätsschutzes des Datenbestands vor vorsätzlichen sowie fahrlässigen Verletzungshandlungen bejahte, daraus keine unmittelbaren Rückschlüsse auf Fragen nach der hier vorrangig relevanten Verkehrsfähigkeit des geschützten Rechts folgen.¹⁴⁵ In demselben Maße, in dem der durch § 823 Abs. 1 BGB vermittelte Integritätsschutz zur Begründung des Rechtsverkehrs mit Daten zu kurz greift, greift auch die deliktsrechtliche Debatte als Beitrag zu Fragen des digitalen Nachlasses zu kurz.

3. Urheberrecht

Das Immaterialgüterrecht im Allgemeinen und das Urheberrecht im Besonderen könnten ebenfalls zur Begründung eines Rechts an Daten herangezogen werden. Funktional und begrifflich erscheint das auf den ersten Blick vielversprechend. Nachdem Daten – wie gesehen – mangels Körperlichkeit dem Sachenrecht unzugänglich sind,¹⁴⁶ scheint das Immaterialgüterrecht prädestiniert, da es die rechtliche Zuordnung immaterieller Güter zur Aufgabe hat. Allerdings ist zu beachten, dass das Immaterialgüterrecht nur begrenzt analogiefähig ist.¹⁴⁷ Ungeachtet der umstrittenen Frage, ob

143 Zum Vergleich zwischen Delikt und Vertrag s. nur *Hager* in: Staudinger, Eckpfeiler, T. Rn. 109 m.w.N.

144 Im Gegenteil wegen des Lösungsinteresses der Provider (noch) zur Eile ratend *Bräutigam* in: DAV-Stellungnahme Nr. 34/2013, S. 25 ff.

145 Ähnlich auch *Thiesen*, Daten in der Erbmasse, S. 159 ff.

146 Dazu bereits zuvor auf S. 48 f.

147 *Pierson/Abrens/Fischer*, Recht des geistigen Eigentums, S. 71; *Lettl*, Gewerblicher Rechtsschutz, § 1 Rn. 10 m.w.N.; *Chrocziel*, Einführung in den Gewerblichen Rechtsschutz und das Urheberrecht, Rn. 14 ff.

das geistige Eigentum (sogar) einem strengen Numerus clausus unterliegt,¹⁴⁸ begründet die folgende Überlegung die jedenfalls nur eingeschränkte Flexibilität des Rechtsgebiets. Die Rechtsordnung gewährt durch die Zuteilung eines Ausschließlichkeitsrechts ein Monopol – etwa im Falle des Patenrechts an einer Erfindung, im Falle des Markenrechts an einem Kennzeichen und im Falle des Urheberrechts an einer Schöpfung.¹⁴⁹ Es obliegt primär dem Gesetzgeber, in der Abwägung zwischen der Freiheit von Informationen und sonstigen immateriellen Gütern einerseits und dem Schutz einer Investitions-, Schöpfungs- oder Erfindungsleistung andererseits zu entscheiden, ob und inwiefern ein (neues) Ausschließlichkeitsrecht gerechtfertigt ist.¹⁵⁰

Ein eigenes, explizit geregeltes Immaterialgüterrecht an Daten als solchen besteht nicht. Vor dem soeben dargestellten Hintergrund müsste ein bestehendes Immaterialgüterrecht auf Daten als Schutzobjekt unmittelbar Anwendung finden. Dafür kommt allenfalls das Urheberrecht und dort insbesondere der Urheberrechtsschutz von Datenbankwerken gem. § 4 Abs. 2 UrhG sowie der Leistungsschutz von Datenbanken gem. §§ 87a ff. UrhG in Betracht.¹⁵¹

148 Ausführlich dazu *Obly* in: FS Schricker, S. 105 ff. m.w.N. sowie *Schroeder*, Numerus clausus der Immaterialgüterrechte?, in: Specht/Lauber-Rönsberg/Becker (Hrsg.), Medienrecht im Medienumbruch, Baden-Baden 2017, S. 9 ff. m.w.N.

149 Instrukтив und differenzierend dazu *Bisges* in: Bisges (Hrsg.), Handbuch Urheberrecht, Kap. 1 Rn. 18 ff.; *Schack*, Urheber- und Urhebervertragsrecht, Rn. 14 f., 69.

150 Bejahend etwa *Kleespies*, GRUR 2002, 764, 767; *Berberich*, WRP 2011, 543, 547; *ders.*, Virtuelles Eigentum, S. 216 ff.; differenzierend *Obly* in: FS Schricker, S. 121 der vom „Grundsatz strikter Subsidiarität ergänzender Schutzformen“ spricht. Ungeachtet der genauen Formulierung lehnt auch *Obly* einen sui-generis Schutz von Daten als solchen ab, vgl. a.a.O., S. 105, dort in Fn. 1.

151 Siehe dazu *Specht*, CR 2016, 288, 293 f.; *Dorner*, CR 2014, 617, 621 f.; *Grützma-cher*, CR 2016, 485, 487 f.; *Wandtke*, MMR 2017, 6, 11 f.; *Wiebe*, GRUR 2017, 338, 338 ff.; *Enstbaler*, NJW 2016, 3473, 3474 f.; *Thiesen*, Daten in der Erbmasse, S. 149 ff.; speziell zu Accounts vgl. *Kutscher*, Der digitale Nachlass, S. 29 ff.; Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 57 f., abrufbar a.a.O. (Fn. 43).

a) Urheberrechtsschutz an Sammel- und Datenbankwerken gem.
§ 4 UrhG

Datenbankwerke sind nach § 4 Abs. 2 UrhG solche Sammelwerke (vgl. § 4 Abs. 1 UrhG), deren Elemente systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder auf andere Weise zugänglich sind.¹⁵² Bei Datenbank- und Sammelwerken weist die Auswahl- und Anordnungsentscheidung einen solchen Grad an Individualität auf, dass sie als persönliche geistige Schöpfung urheberrechtlich schutzfähig werden.¹⁵³ An dieser Hürde scheitern sowohl die schlichte Aneinanderreihung von Daten als auch die auf Vollständigkeit angelegte Datenbank, da in keinem der beiden Fälle eine schöpferische Entscheidung zu fällen ist.¹⁵⁴ Ferner scheidet der Schutz ausschließlich automatisch erhobener Datenbanken mangels menschlicher Leistung am Merkmal „persönlich“.¹⁵⁵ Schon allein vor diesem Hintergrund erscheint es fraglich, ob sich durch § 4 UrhG ein geistiges Eigentum an Daten begründen lässt.¹⁵⁶ Denn die Idee des „Dateneigentums“ beruht darauf, ein umfassendes Zuordnungsregime zu begründen. Mit dem Merkmal der persönlichen geistigen Schöpfung wird aber gerade in schützenswerte Datenmengen und andere Datenmengen unterschieden. Diese Prüfung erfolgt anhand des urheberrechtlichen Wertungsmaßstabs, der anders als etwa das Sachenrecht nicht jedem Gegenstand ohne Ansehung seines (schöpferischen) Wertes Schutz zukommen lassen soll. In Ermangelung einer eigenen Regelung wird das Datenrecht durch die behelfsmäßige Anwendung des Urheberrechts dann mit derselben restriktiven Wertung konfrontiert. Ob und inwieweit einem Datensatz Schutz zuteilwird, kann aus urheberrechtlicher Sicht zwar eine ausgewogene Entscheidung darstellen, aus Sicht der Daten-Governance aber zufällig anmuten.

152 *Leistner* in: Schricker/Loewenheim (Hrsg.), § 4 UrhG Rn. 49 ff.; *Schack*, Urheber- und Urhebervertragsrecht, Rn. 154 f.; *Ahlberg* in: BeckOK Urheberrecht, § 4 UrhG Rn. 18 ff.; *Marquardt* in: Wandtke/Bullinger (Hrsg.), UrhG, § 4 Rn. 8.

153 *Leistner* in: Schricker/Loewenheim (Hrsg.), § 4 UrhG Rn. 1.; *Marquardt* in: Wandtke/Bullinger (Hrsg.), UrhG, § 4 Rn. 9 m.w.N.; *Specht*, CR 2016, 288, 293; *Wandtke*, MMR 2017, 6, 11.

154 *Schack*, Urheber- und Urhebervertragsrecht, Rn. 155 f.; *Bisges* in: Bisges (Hrsg.), Handbuch Urheberrecht, Kap. 1 Rn. 143, 146; *Dreier* in: Dreier/Schulze (Hrsg.), UrhG, § 4 Rn. 20.

155 *Specht*, CR 2016, 288, 293; *Dorner*, CR 2014, 617, 621.

156 Zweifelnd auch *Specht*, CR 2016, 288, 293; *Dorner*, CR 2014, 617, 621; Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 57, abrufbar a.a.O. (Fn. 43).

Darüber hinaus ist, auch bei unterstelltem Werkschutz nach § 4 UrhG, der Blick auf den Schutzzumfang zu lenken. Nach dem Gesetzeswortlaut müssen die einzelnen Elemente des Datenbankwerks ihrerseits nicht zwingend Werkcharakter aufweisen.¹⁵⁷ Umgekehrt werden die einzelnen Elemente aber auch nicht selbst zum Schutzobjekt.¹⁵⁸ So ist ein Datenbankwerk gegen die Übernahme der Struktur oder aller bzw. zumindest vieler Elemente geschützt.¹⁵⁹ Dagegen berührt der Zugriff auf einzelne Daten den Schutzbereich nach § 4 Abs. 2 UrhG gerade nicht.¹⁶⁰

Aus § 4 Abs. 1 und 2 UrhG lässt sich nach alledem kein geeignetes Zuordnungsregime für Daten ableiten. Zwar bleibt der Schutz einzelner Datenbanken unbenommen mit der Konsequenz, dass die jeweiligen Datensätze mitunter reflexhaft zum Gegenstand eines Ausschließlichkeitsrechts werden. Gleichwohl werden diese Fälle aber nicht ausreichend praktische Relevanz aufweisen, um die Diskussion zum „Dateneigentum“ entscheidend zu beeinflussen.¹⁶¹

b) Leistungsschutz des Datenbankherstellers gem. §§ 87a ff. UrhG

Datenbanken können auch unter dem Aspekt des Investitionsschutzes durch das UrhG geschützt sein. Die Legaldefinition der Datenbank nach § 87a Abs. 1 S. 1 UrhG unterscheidet sich von der des Datenbankwerks gem. § 4 Abs. 2 UrhG vor allem dadurch, dass statt einer persönlichen geis-

157 § 4 Abs. 1 UrhG („[...] unbeschadet eines an den einzelnen Elementen *gegebenfalls* bestehenden Urheberrechts oder verwandten Schutzrechts [...]“ Hervorhebung nicht im Original) gilt insoweit auch für § 4 Abs. 2 UrhG; vgl. hierzu *Dreier* in: *Dreier/Schulze* (Hrsg.), UrhG, § 4 Rn. 4; *Ahlberg* in: *BeckOK Urheberrecht*, § 4 UrhG Rn. 33; *Wiebe* in: *Spindler/Schuster* (Hrsg.), *Recht der elektronischen Medien*, § 4 UrhG Rn. 5; ausführlich zu den Elementen eines Sammel- bzw. Datenbankwerks *Czychowski* in: *Fromm/Nordemann*, § 4 UrhG Rn. 16 ff.

158 *Dreier* in: *Dreier/Schulze* (Hrsg.), UrhG, § 4 Rn. 4; *Kotthoff* in: *Dreyer/Kotthoff/Meckel/Hentsch* (Hrsg.), *Urheberrecht*, § 4 UrhG Rn. 21.

159 *Wiebe* in: *Spindler/Schuster* (Hrsg.), *Recht der elektronischen Medien*, § 4 UrhG Rn. 17; *Kotthoff* in: *Dreyer/Kotthoff/Meckel/Hentsch* (Hrsg.), *Urheberrecht*, § 4 UrhG Rn. 21.

160 *Leistner* in: *Schricker/Loewenheim* (Hrsg.), § 4 UrhG Rn. 34; *Wiebe* in: *Spindler/Schuster* (Hrsg.), *Recht der elektronischen Medien*, § 4 UrhG Rn. 2; *Czychowski* in: *Fromm/Nordemann*, § 4 UrhG Rn. 40 m.w.N.; *Specht*, CR 2016, 288, 293; *Determann*, ZD 2018, 503, 505.

161 Explizit mit Hinweis auf mangelnde praktische Relevanz auch *Zieger/Smirra*, MMR 2013, 418, 419 und *Dorner*, CR 2014, 617, 621.

tigen Schöpfung eine nach Art oder Umfang wesentliche Investition in den Inhalt der Datenbank vorausgesetzt ist.¹⁶² Die §§ 87a ff. UrhG gewähren ein „Recht der Entnahme“¹⁶³ und schützen damit den Rechtsinhaber davor, dass quantitativ (Datenvolumen) oder qualitativ (Investitionsvolumen) wesentliche Teile der Datenbank von Dritten übernommen werden.¹⁶⁴ Hingegen folgt aus dem Datenbankschutz kein Schutz einzelner Elemente der Datenbank oder gar ein selbstständiges, abtrennbares Recht an den jeweiligen Elementen.¹⁶⁵ Erfasst ist also insbesondere nicht die Möglichkeit, über einzelne Daten zu verfügen oder sie gegen Vervielfältigung oder Kenntnisnahme zu schützen. Auch das Leistungsrecht des Datenbankherstellers vermag daher nicht, einem Recht an Daten den Weg zu bereiten.¹⁶⁶

c) Bezug zum digitalen Nachlass: Rechtsinhaberschaft und Reichweite des Rechts

Es fragt sich, welche Konsequenzen ein urheberrechtlich grundiertes Recht an Daten – seine Geltung ungeachtet der soeben dargestellten Bedenken unterstellt – für den digitalen Nachlass hätte. Die Antwort hierauf hängt primär davon ab, wem das Recht in diesem Fall zustünde.

Wenn das Datenrecht zur Vereinfachung der Rechtsnachfolge als Erbrechtsobjekt dienen soll, müsste der Erblasser daran berechtigt sein. Das

162 *Wandtke*, MMR 2017, 6, 11 f.; ausführlich und differenzierend *Dreier* in: *Dreier/Schulze* (Hrsg.), UrhG, § 87a Rn. 3 ff.; *Schack*, Urheber- und Urhebervertragsrecht, Rn. 291.

163 Vgl. *Vogel* in: *Schricker/Loewenheim* (Hrsg.), § 87b UrhG Rn. 37 zur europarechtskonformen Auslegung der Begriffe „Vervielfältigung“ und „Entnahme“; dazu auch *Wiebe* in: *Spindler/Schuster* (Hrsg.), Recht der elektronischen Medien, § 87b UrhG Rn. 2 ff.

164 *Zech*, GRUR 2015, 1151, 1158; *Hermes* in: *Wandtke/Bullinger* (Hrsg.), UrhG, § 87b Rn. 11 ff.; *Wiebe* in: *Spindler/Schuster* (Hrsg.), Recht der elektronischen Medien, § 87b UrhG Rn. 17 f.

165 *Specht*, CR 2016, 288, 293 f.; *Dorner*, CR 2014, 617, 622; *Wandtke*, MMR 2017, 6, 11; *Thiesen*, Daten in der Erbmasse, S. 151; ausführlich dazu *Zech*, Information als Schutzgegenstand, S. 360 f.; *Determann*, ZD 2018, 503, 505; *Ensthaler*, NJW 2016, 3473, 3474 f.

166 Nach *Dorner*, CR 2014, 617, 622 kommt im Gegenteil sowohl in § 4 UrhG als auch in § 87a UrhG der „klare gesetzgeberische Wille zum Ausdruck, dass Informationen (als Ergebnisse einer Datenaggregation) frei von exklusiven rechtlichen Zuordnungen bleiben sollen.“; s. auch *Ensthaler*, NJW 2016, 3473, 3475.

ist der Fall, wenn der Erblasser originärer Rechtsinhaber oder Lizenznehmer ist. Grundsätzlich kann das nur in Ansehung der konkreten Nutzungshandlung des Erblassers etwa im Rahmen eines bestimmten Internetdienstes beurteilt werden. Trotzdem lassen sich einige abstrakte Überlegungen formulieren. So wird in der Praxis ein Lizenzvertrag zwischen dem Erblasser als Lizenznehmer und einem Datenbank(werk)rechtsinhaber die seltene Ausnahme bilden. Mithin könnte der Erblasser als Nutzer von Internetdiensten allenfalls als originärer Rechtsinhaber in Betracht kommen. Dafür müsste er im Falle des § 4 UrhG die schöpferische Auswahl- oder Anordnungsentscheidung getroffen oder im Falle der §§ 87a ff. UrhG die Investitionsleistung erbracht haben, vgl. § 87a Abs. 2 UrhG.

Auch soweit bei der Nutzung von Internetdiensten systematisch Daten betreffend einen Nutzer erfasst und in einer Datenbank gespeichert und aufbereitet werden, wird die dafür erforderliche Leistung in der Regel durch den Provider erbracht. Dass die Daten die Person des Nutzers betreffen mögen, ist lediglich eine datenschutzrechtliche und nicht eine urheberrechtlich relevante Kategorie. Der Provider entwirft und unterhält eine technische Infrastruktur, die der Erblasser lediglich vorfindet und den Vorgaben entsprechend nutzt. So trifft der Nutzer nur in den seltensten Fällen eine schöpferische Auswahlentscheidung und wohl in keinem Fall tätigt er eine Investition. Sofern und soweit hier Daten(bank)rechte entstehen, stehen sie somit originär dem Provider zu. Es käme folglich nicht zu einer Vereinheitlichung des Erbrechtsobjekts durch ein Datenrecht, wenn dieses aus dem Urheberrecht folgte. Mithin lässt sich der urheberrechtliche Teilbereich der Diskussion um ein „Dateneigentum“ – auch wenn der Ansatz noch weiterentwickelt werden sollte – für den digitalen Nachlass kaum fruchtbar machen.

4. Datenschutzrecht

Auch das *Datenschutzrecht* könnte als Quelle eines Datenrechts in Betracht kommen. Allerdings ist die Funktion des Datenschutzes auch und gerade in der Ausprägung durch die DS-GVO nicht die Güterzuordnung. Vielmehr reguliert das Datenschutzrecht den Umgang mit personenbezogenen Daten und wäre folglich eher Schranke eines etwaigen Datenrechts.¹⁶⁷ Insofern ist auf die zentrale Norm des Art. 6 DS-GVO hinzuweisen, der ein

167 Zech, CR 2015, 137, 141; Paal/Hennemann, NJW 2017, 1697, 1698; differenzierend Kühling/Sackmann, ZD 2020, 24, 27 ff.

präventives Verbot mit Erlaubnisvorbehalt betreffend die Verarbeitung von personenbezogenen Daten statuiert.¹⁶⁸

Ausweislich des Art. 6 Abs. 1 lit. f) DS-GVO ist das Datenschutzrecht ein abwägungsoffenes Recht und ähnelt damit dem Vorbild anderer Persönlichkeitsrechte.¹⁶⁹ Schon im sog. Volkszählungsurteil des BVerfG¹⁷⁰ sowie auch in der daran anknüpfenden Rechtsprechung des BGH, beispielsweise im Spickmich.de-Urteil,¹⁷¹ wird betont, dass eine absolute Herrschaft über die „eigenen Daten“ mit dem Leben in der sozialen Gemeinschaft kollidiere.¹⁷² Zur Wahrnehmung der Informations- und Meinungsfreiheit, müssen personenbezogene Daten (unter gewissen Umständen) auch ohne oder gegen den Willen des Betroffenen genutzt werden können.¹⁷³ Das geltende Datenschutzrecht beabsichtigt, diese ohnehin schon komplexen Interessenkonflikte zu befrieden.¹⁷⁴ Darüber hinaus auch die Zuweisung von Datenrechten in dieser Materie zu verorten, würde eine Kommerzialisierung des Datenschutzes bedeuten und wäre jedenfalls im geltenden Datenschutzrecht systemfremd.¹⁷⁵ Das gilt umso mehr vor dem Hintergrund, dass die DS-GVO auf nicht-personenbezogene Daten gar keine Anwendung findet, vgl. Art. 2 Abs. 1 DS-GVO, und schon deshalb nicht Anknüpfungspunkt für ein hieraus abgeleitetes umfassendes „Dateneigentum“ sein kann.¹⁷⁶ Insofern ist *Zech* zuzustimmen, wenn er zusammenfassend feststellt, dass sich aus dem Datenschutzrecht allenfalls ein rahmenrechtliches

168 *Frenzel* in: Paal/Pauly (Hrsg.), DS-GVO, Art. 6 Rn. 1 f.; *Albrecht* in: NK-Datenschutzrecht, Einführung zu Art. 6 DS-GVO Rn. 1 f.; *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 323; kritisch dazu *Albers/Veit* in: BeckOK Datenschutzrecht, Art. 6 DS-GVO Rn. 2.

169 *Zech*, GRUR 2015, 1151, 1154. Ausführlich zur Abwägung am Maßstab von Art. 6 Abs. 1 lit. f) DS-GVO vgl. auf S. 130 ff.

170 BVerfGE 65, 1, 43 f. = BVerfG NJW 1984, 419, 422.

171 BGHZ 181, 328, 338 = BGH NJW 2009, 2888, 2892.

172 *Taeger*, Datenschutzrecht. Einführung, S. 36 ff., 38; *Zech*, GRUR 2015, 1151, 1154; *Specht*, GRUR Int. 2017, 1040, 1041 f.

173 *Härting*, CR 2016, 646, 648; *ders.*, Internetrecht, Kap. A Rn. 83 ff.; *Thiesen*, Daten in der Erbmasse, S. 147.

174 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, S. 74 f. mit Hinweis auf die Erwägungsgründe 47-49 DS-GVO; *Kühling/Klar/Sackmann*, Datenschutzrecht, Rn. 399; in diesem Sinne, aber zur alten Rechtslage vor Geltung der DS-GVO *Taeger*, Datenschutzrecht. Einführung, S. 36 ff.

175 *Specht*, GRUR Int. 2017, 1040, 1041 f.; *Dorner*, CR 2014, 617, 623 ff.

176 *Paal/Hennemann*, NJW 2017, 1697, 1698 m.w.N.; *Specht*, GRUR Int. 2017, 1040, 1042; *Kühling/Sackmann*, ZD 2020, 24, 29; entsprechend bewertet *Härting*, CR 2016, 646, 648 den Personenbezug als Anknüpfungspunkt für ein Datenrecht auch als ungeeignet.

„Recht an den eigenen persönlichen Daten“ ergibt, hingegen aber kein eigentumsartiges „Recht am eigenen Datum“. ¹⁷⁷

Der datenschutzrechtliche Teil der Debatte zum „Dateneigentum“ und der digitale Nachlass kommen einander am nächsten bei der Frage, ob und inwieweit die subjektiven Rechte, die durch das Datenschutzrecht gewährt werden, vererbbar sind. ¹⁷⁸ Diese Rechte folgen aus Kapitel III der DS-GVO, das die Überschrift „Rechte der betroffenen Person“, trägt, vgl. Art. 12 ff. DS-GVO. Das Ob und das Wie der Vererbbarkeit hängen (auch) davon ab, wie eng datenschutzrechtliche Befugnisse an die Persönlichkeit des Betroffenen gebunden sind oder ob eine gewisse Selbständigkeit und damit letztlich Kommerzialisierung der Befugnisse möglich ist. Die Argumente zum datenschutzrechtlichen „Dateneigentum“ können also auch für die konkrete Frage der Vererbbarkeit fruchtbar gemacht werden. ¹⁷⁹

5. (Lauterkeitsrechtlicher) Leistungs- und Geheimnisschutz

Auch das Lauterkeitsrecht kommt für die Konstruktion eines Datenrechts in Betracht. Insoweit ließe sich zum einen an den lauterkeitsrechtlichen Leistungsschutz, ¹⁸⁰ §§ 3 Abs. 1, 4 Nr. 3 UWG, denken und zum anderen an den Geheimnisschutz, ¹⁸¹ der bislang vor allem in den §§ 17 ff. UWG a.F. geregelt war und sich nunmehr im Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) findet.

177 *Zech*, GRUR 2015, 1151, 1155.

178 Dazu *Solmecke/Köbrich/Schmitt*, MMR 2015, 291, 292 f.; LG Berlin ZEV 2016, 189, 194; dagegen aber KG Berlin ZEV 2017, 386 Rn. 104 jeweils zur Rechtslage vor Geltung der DS-GVO.

179 Zur Eröffnung des Anwendungsbereichs der DS-GVO im Kontext des digitalen Nachlasses s. S. 119 ff.

180 Dazu *Becker*, GRUR 2017, 346, passim; noch zur alten Rechtslage unter § 4 Nr. 9 UWG a.F. *Zech*, Information als Schutzgegenstand, S. 364 f.

181 Zur Rechtslage unter den §§ 17 ff. UWG a.F. vgl. *Zech*, GRUR 2015, 1151, 1155 f.; *Grützmacher*, CR 2016, 485, 488 f.; *Dorner*, CR 2014, 617, 622 f.; *Thiesen*, Daten in der Erbmasse, S. 147 ff. Das neue GeschGehG ändert an den grundlegenden Argumenten, nach denen aus dem Geheimnisschutz nach Maßgabe der §§ 17 ff. UWG a.F. kein Recht an Daten abgeleitet werden kann, wenig.

a) Lauterkeitsrechtlicher Leistungsschutz, §§ 3 Abs. 1, 4 Nr. 3 UWG

Der lauterkeitsrechtliche Leistungsschutz erlaubt keine präzise Nutzungs-
zuweisung, sondern verbietet lediglich die (allzu) direkte – unlautere –
Ausnutzung fremder Leistungen.¹⁸² Eine solche Leistung kann zwar auch
in Form von Daten bestehen; die Daten sind im Falle von § 4 Nr. 3
lit. a), b) UWG dann selbst die Produkte oder Teil eines Angebots sowie
im Falle von § 4 Nr. 3 lit. c) UWG für die Herstellung anderer Produkte
oder Angebote erforderlich.¹⁸³ Da die Kriterien des UWG-Leistungsschut-
zes vor allem zu physischen, sichtbaren Produkten entwickelt wurden und
deshalb an optischen Merkmalen orientiert sind, passt § 4 Nr. 3 UWG aber
nur eingeschränkt auf Daten.¹⁸⁴ Schwerer wiegt noch die Überlegung, dass
die Orientierung und Weiterentwicklung an auf dem Markt bereits vor-
handenen Produkten grundsätzlich ein zulässiger Teil des Wettbewerbs ist.
Außerhalb von Sondergesetzen wie dem PatG und UrhG wird Leistungs-
schutz durch die Generalklausel des § 4 Nr. 3 UWG nur vor unlauterer
Herkunftstäuschung, Rufausbeutung und Industriespionage gewährt.¹⁸⁵
Ein allgemeines Ausschließlichkeitsrecht am Datenbestand, welches einem
Recht an Daten den Weg bereiten könnte, ist damit de lege lata unverein-
bar, da es der gesetzgeberischen Prärogative zur Anerkennung neuer Lei-
stungsschutzrechte vorgreifen würde.

b) Geheimnisschutz, §§ 1 ff. GeschGehG

Die Vorschriften des Nebenstrafrechts zum Schutz von Betriebs- und Ge-
schäftsgeheimnissen in den §§ 17-19 UWG a.F. wurden aufgehoben. An
deren Stelle tritt das GeschGehG, welches unter der nunmehr einheitli-
chen Bezeichnung Geschäftsgeheimnisse im Sinne der Legaldefinition
gem. § 2 Nr. 1 GeschGehG schützt. Mit der Normierung in einem Spezial-

182 *Becker*, GRUR 2017, 346, 346.

183 *Becker*, GRUR 2017, 346, 347 ff. spricht von Daten *als* Erzeugnissen sowie von
Daten *in* Erzeugnissen; dem folgend *Köhler* in: Köhler/Bornkamm/Fedderson
(Hrsg.), § 4 UWG Rn. 3.22.

184 *Becker*, GRUR 2017, 346, 347 f.

185 *Emmerich/Lange*, Unlauterer Wettbewerb, S. 131 f. m.w.N. Auch die Rspr.
nimmt zugunsten der Wettbewerbsfreiheit den Grundsatz der Nachahmungs-
freiheit an, vgl. BGH GRUR 2007, 795 Rn. 51; BGH GRUR 2008, 1115 Rn. 32;
strenger aber etwa *Köhler* in: Köhler/Bornkamm/Fedderson (Hrsg.), § 4 UWG
Rn. 3.3.

gesetz wurde der Schutz von Geschäftsgeheimnissen von seinem Status als Annexmaterie des UWG befreit.¹⁸⁶ Das nunmehr eigene Rechtsgebiet behält zwar die Berührungspunkte zum Lauterkeitsrecht, weist aber in höherem Maße als bislang Wesenszüge des geistigen Eigentums auf.¹⁸⁷ Doch auch unter der Geltung des GeschGehG bleibt es dabei, dass der Geheimnisschutz keine eigenständige rechtliche Zuweisung bewirkt, sondern lediglich eine faktische Ausschließlichkeit verstärkt.¹⁸⁸ Zwar gewähren die §§ 6 ff. GeschGehG dem Rechtsinhaber eine Reihe von Ansprüchen im Falle einer Verletzung des Geheimnisschutzes. Der Schutz besteht aber – neben anderen Voraussetzungen – überhaupt nur dann, wenn die infrage stehende Information nicht allgemein bekannt oder ohne Weiteres zugänglich ist und außerdem den Gegenstand von angemessenen Geheimhaltungsmaßnahmen durch ihren Inhaber bildet, vgl. § 2 Nr. 1 lit. a) und b) GeschGehG.¹⁸⁹ Gibt der Inhaber die Information gegenüber einem Personenkreis preis, der nicht zur Vertraulichkeit verpflichtet ist, scheidet die Information folglich aus dem Schutzbereich des GeschGehG aus. Dass die Information dem Inhaber nicht absolut zugewiesen ist, zeigt sich auch daran, dass es Dritten unbenommen bleibt, sie durch eine eigenhändige Entdeckung bzw. Schöpfung oder (neuerdings) auch im Wege des Reverse Engineering zu erlangen, vgl. § 3 Abs. 1 Nr. 1 und 2 GeschGehG.¹⁹⁰

186 Vgl. das Vorwort in: Harte-Bavendamm/Ohly/Kalbfus (Hrsg.), GeschGehG (Geheimnisschutz lange Zeit als „Stiefkind Aschenputtel“).

187 Ohly, GRUR 2019, 441, 450; Pierson/Abrens/Fischer, Recht des geistigen Eigentums, S. 47 f.; Harte-Bavendamm in: Harte-Bavendamm/Ohly/Kalbfus (Hrsg.), GeschGehG, Einl. A Rn. 127, 129; Berberich/Golla, PinG 2016, 165, 174; einschränkend aber Köhler in: Köhler/Bornkamm/Feddersen (Hrsg.), Vor §§ 17-19 UWG Rn. 12.

188 Pierson/Abrens/Fischer, Recht des geistigen Eigentums, S. 47 f.; Kalbfus in: Harte-Bavendamm/Ohly/Kalbfus (Hrsg.), GeschGehG, Einl. A Rn. 185 zur Abgrenzung vom Ausschließlichkeitsrecht an Patenten; wie hier zum alten Recht bereits Zech, GRUR 2015, 1151, 1156.

189 Zu den Schutzvoraussetzungen nach neuem Recht s. Ohly, GRUR 2019, 441, 442 ff. und Dann/Markgraf, NJW 2019, 1774, 1774 ff. sowie Harte-Bavendamm in: Harte-Bavendamm/Ohly/Kalbfus (Hrsg.), GeschGehG, § 2 Rn. 14 ff.; nach den Gesetzesmaterialien trägt der Geheimnissinhaber die Beweislast für die Etablierung angemessener Geheimhaltungsmaßnahmen, vgl. BT-Drs. 19/4724, S. 24.

190 Dann/Markgraf, NJW 2019, 1774, 1776 bezeichnen § 3 Abs. 1 Nr. 2 GeschGehG als einen Paradigmenwechsel im Geheimnisschutzrecht; dazu Ohly in: Harte-Bavendamm/Ohly/Kalbfus (Hrsg.), GeschGehG, § 3 Rn. 19 ff.

c) Lauterkeitsrecht und digitaler Nachlass

Wiederum stellt sich die Frage, ob die Debatte der Lösung des digitalen Nachlasses zuträglich sein kann. Sowohl der lauterkeitsrechtliche Leistungsschutz als auch der Geschäftsgeheimnisschutz begegnen hier einem ähnlich gelagerten Problem. Um den Erbgang im Kontext des digitalen Nachlasses zu vereinfachen, müsste auch und gerade der Datenbestand des Erblassers in dessen Dimension als Nutzer und Verbraucher erfasst und gegebenenfalls durch ein „Dateneigentum“ vereinheitlicht werden. Das Lauterkeitsrecht als Teil des Wettbewerbsrechts und der Schutz von *Geschäftsgeheimnissen* zielen aber auf die Regulierung und den Schutz gewerblicher Handlungen. Für den Leistungsschutz folgt das bereits aus dem Wortlaut, der bestimmt, dass die Verletzungshandlung gem. § 3 Abs. 1 UWG eine „geschäftliche Handlung“ im Sinne des § 2 Abs. 1 Nr. 1 UWG sein muss und dass die nachgeahmten Waren oder Dienstleistungen gem. § 4 Nr. 3 UWG solche eines „Mitbewerbers“ im Sinne des § 2 Abs. 1 Nr. 3 UWG sein müssen.¹⁹¹ Im Falle des GeschGehG ist ebenfalls eine weitgehende Beschränkung auf Geschäftsgeheimnisse unter Ausschluss von Privatgeheimnissen angebracht. Das folgt aus dem systematischen Zusammenhang und Erwägungsgrund 14 GeschGeh-RL¹⁹², in dem sich der Begriffsdefinition von „Geschäftsgeheimnissen“ ausschließlich über Beispiele aus dem gewerblichen Wettbewerbskontext angenähert wird.¹⁹³

Im Ergebnis ist also festzuhalten, dass de lege lata weder aus dem Lauterkeitsrecht noch aus dem Geschäftsgeheimnisschutz ein „Dateneigentum“ abzuleiten ist. Aber selbst, wenn die oben beschriebenen Ansätze durch die Wissenschaft oder auch durch den Gesetzgeber in Richtung eines Rechts an Daten weiterentwickelt würden, so folgte daraus wohl keine Hilfestellung für den digitalen Nachlass. Dessen bedeutende private und persönlichkeitsrechtssensible Dimension wird durch das Wettbewerbsrecht kaum erfasst.

191 Köhler in: Köhler/Bornkamm/Feddersen (Hrsg.), § 4 UWG Rn. 3.18 f.

192 Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung, (ABl. Nr. L 157 S. 1), Celex-Nr. 3 2016 L 0943.

193 So auch *Ohly*, GRUR 2019, 441, 442, der aber auf Ausnahmefälle hinweist, in denen es Überschneidungen geben könne, wie bei der Vermarktung eigener Persönlichkeitsaspekte durch Prominente oder bei Privatinformationen mit Einfluss auf den Wettbewerb – etwa Gesundheitsdaten leitender Angestellter.

6. Ergebnis: Kein Recht an Daten de lege lata

Nach alledem gilt, dass es de lege lata in Deutschland kein eigentumsähnliches Recht an Daten gibt. Zwar kann angesichts zahlreicher gesetzlicher Regelungen, die (auch) auf Daten oder auf durch sie verkörperte Informationen Anwendung finden, nicht von einer völlig unregulierten Materie ausgegangen werden. Mitunter fallen Datenbestände auch in den Anwendungsbereich eines Regimes, das absolute Rechte an den Daten oder den verkörperten Inhalten gewährt. Als Beispiel sei hier der urheberrechtliche Schutz von Software nach Maßgabe der §§ 69a ff. UrhG genannt. In keinem dieser Fälle liegt die Begründung für den Schutz jedoch in der Eigenschaft der Daten als solchen. Daher kann von diesen Spezialtatbeständen nicht auf ein umfassendes „Dateneigentum“ geschlossen werden.

Aus dieser Feststellung folgt, dass der Schutz und der Handel mit Daten – von Sonderfällen abgesehen – in der Breite nur durch eine Kombination aus vertraglichen Vereinbarungen und dem faktischen Zugang beziehungsweise Ausschluss des Zugangs zu den Daten realisierbar sind.¹⁹⁴ Inwiefern und wem Daten faktisch (un)zugänglich sind, hängt unter anderem (auch) von den Eigentumsverhältnissen an dem Speichermedium ab, auf welchem die Daten abgespeichert sind. Wem das Sacheigentum am Speichermedium zusteht, bestimmt sich indes allein nach klassischen sachenrechtlichen Maßstäben und darf nicht mit der soeben dargestellten Debatte zum „Dateneigentum“ vermengt werden.¹⁹⁵

III. Ausblick: Rechtspolitische Diskussion

Im Anschluss an die Debatte zum geltenden Recht wird derzeit eine lebhaftere rechtspolitische Diskussion darüber geführt, ob und inwieweit es sinnvoll und notwendig ist, der gegenwärtigen Rechtslage mit der Einführung eines eigentumsähnlichen oder in sonstiger Weise spezifischen Datenrechts zu begegnen. Ein wichtiger Teilaspekt dieser Auseinandersetzung ist beispielsweise die Frage des Berechtigten.

194 Diese Einschätzung teilt *Markendorf*, ZD 2018, 409, 410 und nimmt sie zum Anlass, den Einsatz der Blockchain-Technologie als Ausgangspunkt einer Datenrechtsordnung vorzuschlagen.

195 Vgl. dazu *Boehm*, ZEuP 2016, 358, 384 f. Entsprechend sind auch die Frage nach dem Erbrecht an Daten und dem Erbrecht an dem körperlichen Speichermedium zu trennen.

Diese Arbeit bietet nicht den Rahmen, um einen umfassenden Überblick über die rechtspolitische Diskussion zu geben.¹⁹⁶ Es sei lediglich auf die Diskrepanz der Positionen des europäischen und des deutschen Gesetzgebers hingewiesen. Während die Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder momentan im Wesentlichen keinen Reformbedarf sieht,¹⁹⁷ zeigen die europäischen Institutionen mehr Handlungsbereitschaft. So führte die europäische Kommission in ihrer „Strategie für einen digitalen Binnenmarkt in Europa“¹⁹⁸ schon im Jahr 2015 unter Ziff. 4.1 aus, dass sie den Aufbau einer Datenwirtschaft beabsichtige und als Teil dessen auch auf „die neuen Fragen des Eigentums an Daten [...] eingehen“ werde. Im Anschluss daran kündigte die europäische Kommission 2017 in ihrer Mitteilung zum „Aufbau einer europäischen Datenwirtschaft“¹⁹⁹ an, ein Recht des Datenerzeugers an nicht-personenbezogenen Daten erörtern zu wollen. Parallel dazu sehen einige Autoren auch im Richtlinienentwurf über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, der (personenbezogene) Daten als Gegenleistung im vertraglichen Synallagma vorsieht,²⁰⁰ einen potenziellen Anknüpfungspunkt für den Rechtshandel mit (personenbezogenen) Daten.²⁰¹ Schließlich ist hinzuweisen auf die Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten,²⁰² durch welche die Interoperabilität und Portabilität von nicht-personenbezogenen Daten gefördert werden soll. Dem entspricht für personenbezogene Daten der Regelungsgehalt und Telos von Art. 20 DS-

196 Hingewiesen sei aber auf den wirtschaftswissenschaftlichen Beitrag zur Debatte von *Kerber*, GRUR Int. 2016, 989, der „sowohl aus theoretischer als auch empirischer Perspektive“ keine Hinweise sieht, welche die Einführung eines immateriälgüterrechtlichen Datenrechts begründen könnten.

197 Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 97 f. sowie Kapitel 1, passim, S. 29-98, abrufbar a.a.O. (Fn. 43).

198 Mitteilung der Kommission vom 6. Mai 2015, Strategie für einen digitalen Binnenmarkt für Europa, COM [2015] 192 final. Dazu u.a. *Zech*, GRUR 2015, 1151, 1151 ff.

199 Mitteilung der Kommission vom 10. Januar 2017, Aufbau einer europäischen Datenwirtschaft, COM [2017] 9 final, S. 14. Dazu u.a. *Paal/Hennemann*, NJW 2017, 1697, 1698.

200 S. dazu bereits oben die Nachweise in Fn. 75.

201 *Paal/Hennemann*, NJW 2017, 1697, 1698; *Röttgen* in: Specht-Riemenschneider/Werry/Werry (Hrsg.), Datenrecht in der Digitalisierung, S. 390 ff.

202 VO (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union.

GVO.²⁰³ Nicht zuletzt bestimmt Art. 1 DS-GVO als Gegenstand und Ziel der Verordnung neben dem Recht auf Schutz personenbezogener Daten in Art. 1 Abs. 1 und 3 DS-GVO auch den freien Verkehr personenbezogener Daten im europäischen Binnenmarkt.²⁰⁴ Dies kann als Programmsatz verstanden werden, der eine Offenheit für die perspektivische Formierung von Datenrechten signalisiert, die in einem freien Binnenmarkt handelbar wären.

Auch wenn sich hier noch längst kein einheitliches Bild abzeichnet und die Rechtsentwicklung für personenbezogene und nicht-personenbezogene Daten (naturgemäß) nicht identisch verläuft, ist in Brüssel in jedem Fall ein größerer Gestaltungswille zu konstatieren, als ihn der nationale Gesetzgeber in Deutschland bislang zeigt. Die weitere Entwicklung bleibt abzuwarten.

IV. Rückschlüsse aus der Diskussion für den digitalen Nachlass

Aspekte eines möglichen Datenrechts wie etwa die rechtliche Qualität und Fassbarkeit von Daten, ihre Inhaberschaft und die Gewährleistung ihres Schutzes werden vor dem Hintergrund der gesamtgesellschaftlichen Bedeutung der Digitalisierung auf eine große Vielzahl von Rechtsgebieten einwirken. Das zeigt sich exemplarisch am Fall des digitalen Nachlasses. Dessen Ausgangspunkt ist die genaue Bestimmung des Objekts des Erbgangs. In diesem Kontext kann nicht gleichsam inzidenter über die weitreichenden Fragen eines etwaigen Zuordnungsregimes für Daten entschieden werden.²⁰⁵ Aber auch und gerade in Ansehung der Reformbestrebungen auf europäischer Ebene muss die weitere Rechtsentwicklung hier aufmerksam verfolgt werden, da eine (Neu-)Regelung der rechtlichen Qualität oder Zuordnung von Daten auf die Bestimmung des Erbrechtsobjekts zurückwirken dürfte. Für das geltende Recht gilt es nach alledem, zumindest einstweilen eine „Verschuldrechtlichung [statt einer] Verdinglichung

203 Zu Sinn und Zweck von Art. 20 DS-GVO vgl. *Paal* in: *Paal/Pauly* (Hrsg.), *DS-GVO*, Art. 20 Rn. 4-6.

204 *Pötters* in: *Gola* (Hrsg.), *DS-GVO*, Art. 1 Rn. 5 f. bezeichnet die beiden Zielbestimmungen als grds. gleichrangig; zum Grundsatz des freien Datenverkehrs innerhalb der Europäischen Union vgl. *Zerdick* in: *Ehmann/Selmayr* (Hrsg.), *Art. 1 DS-GVO* Rn. 9 ff. m.w.N.

205 *Sorge*, *MMR* 2018, 372, 377.

der Universalsukzession 2.0²⁰⁶ zu konstatieren. Infolgedessen wird der Fokus im Bereich des digitalen Nachlasses darauf liegen müssen, ob und inwieweit vertragliche Rechte und Pflichten des Erblassers vererblich sind.²⁰⁷

C. Zwischenergebnis zu Kapitel 2

Die Rechtsobjekte, die in den digitalen Nachlass fallen, sind disparat. Das gilt zumindest, solange und soweit kein Recht an Daten anerkannt oder vom Gesetzgeber geschaffen wird.²⁰⁸ Die (rechtspolitische) Debatte zum Recht an Daten sowie insbesondere ein entsprechendes legislatives Tätigwerden können indes (auch unbeabsichtigt) Folgen für den Umgang mit dem digitalen Nachlass haben. Das gilt vor allem für die Genese neuer Rechtsobjekte sowie für die Entscheidung darüber, wem und unter welchen Voraussetzungen das etwaige Recht zuzuordnen ist.

Für den weiteren Verlauf der Untersuchung ist auf Grundlage des geltenden Rechts die nutzungsvertragliche Position des Erblassers der entscheidende Anknüpfungspunkt für die Fragen nach der Übergangsfähigkeit und Durchsetzbarkeit des digitalen Erbes. Mit der großen Diversität providerseitiger Informations- und Kommunikationsangebote korrespondierte dabei eine Vielfalt der Nutzungsverträge. Deren jeweilige Spezifika sind einzelfallgerecht bei der folgenden erb-, schuld- und datenschutzrechtlichen Untersuchung zu berücksichtigen. Daneben stehen die Urheber- und Leistungsschutzrechte des Erblassers an selbstgenerierten Accountinhalten als eigenständiges Erbrechtsobjekt.

206 Kritisch so *Sorge*, MMR 2018, 372, 377; s. aber die Studie des Fraunhofer Instituts für Sichere Informationstechnologie, S. 102, abrufbar a.a.O. (Fn. 7).

207 Das gilt trotz der im Schrifttum geäußerten Bedenken gegenüber einem hauptsächlich vertraglich organisiertem Ordnungsregime für Daten: *Faust*, Gutachten zum 71. DJT, 2016, S. A 77 ff. sieht derzeit einen unvollständigen Integritätsschutz von Daten; *Sorge*, MMR 2018, 372, 377 bezeichnet den Ausgangspunkt des digitalen Nachlasses als wenig zukunftssträftig, da schuldrechtliche Ansprüche schon strukturell prekär seien; *Grützmacher*, CR 2016, 485, 492 und 495 weist hin auf die Anfälligkeit vertraglicher Konstruktionen in Fällen von Insolvenz. Zum Ganzen – auch mit Gegenargumenten – vgl. Bericht der Arbeitsgruppe „Digitaler Neustart“ der Konferenz der Justizministerinnen und Justizminister der Länder, S. 29 ff., 90 f., abrufbar a.a.O. (Fn. 43).

208 Anders *Thiesen*, Daten in der Erbmasse, S. 182 nach dem „eine Auseinandersetzung mit möglichen Sonderrechten an Daten nicht die Lücke schließen [kann], die bei einer rein vertragsrechtlichen Herangehensweise entsteht.“