Typoskript im Sinne des § 38 Abs. 2 UrhG aus: Hill/Martini/Wagner, Facebook, Google und Co. – Gefahren und Chancen, Nomos Verlag 2013, S. 77 ff.

„Wenn ich einmal soll scheiden…": Der digitale Nachlass und seine unbewältigte rechtliche Abwicklung

Mario Martini[1]

Im digitalen Zeitalter hinterlassen Nutzer im Internet unzählige digitale Fußspuren. Kaum ein Nutzer macht sich darüber Gedanken, welches Schicksal diese Unmengen an persönlichen und geschäftlichen Daten nach dem Tod erfahren. Das Internet verwischt die Spuren jedenfalls nicht. Verwaiste Online-Profile, womöglich das digitale Abbild eines erfüllten Lebens auf der Timeline, oder intime Nachrichten eines E-Mail-Accounts hält der Cyberspace grundsätzlich für die Ewigkeit fest. Wie die Rechtsordnung auf die Herausforderungen reagieren soll, die mit einem Nachlass verbunden sind, der an einem von Raum und Zeit entrückten Ort der Unvergänglichkeit begraben ist, ist noch weitgehend ungeklärt. Der Beitrag entwickelt rechtsdogmatische und rechtspolitische Antworten.

Justin Ellsworth gehörte zu den unauffälligen Marinesoldaten, die für die USA im Irakkrieg ihren Dienst versahen. Erst *posthum* wurde sein Name einer breiten Öffentlichkeit bekannt: Den 20-Jährigen traf eine in *Fallujah* detonierte Bombe tödlich. Als Soldat hatte er zwar vorsorglich alle üblichen testamentarischen Verfügungen getroffen. Seinen digitalen Nachlass hat er aber nicht geregelt. Als seine Eltern *Yahoo* aufforderten, ihnen die Zugangsdaten zu seinem E-Mail-Account mitzuteilen,[2] verweigerte sich das Unternehmen diesem Ansinnen. In den USA sorgte der Fall für Aufsehen. Er beschwor eine Diskussion über den richtigen Umgang mit den digitalen Hinterlassenschaften der Internetnutzer herauf. In Deutschland steht die Debatte noch am Anfang.

Scheidet ein Mensch aus dem Leben, stehen die Angehörigen und Erben nicht nur vor einem schweren Abschied und schmerzlichen Verarbeitungsprozessen. Sie sind auch mit der Herausforderung der Nachlassabwicklung konfrontiert. Im

1 *Mario Martini* ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer. Sein Dank gilt den Mitarbeitern seines Lehrstuhls für die Mitarbeit, allen voran *Clemens Becker*, *Yvonne Schmid* und *Quirin Weinzierl*. Eine Kurzfassung des Beitrags ist abgedruckt in der JZ 2012, 1145 ff.

2 Oakland Co. Mich. Prob. Ct. In the Matter of Justin M. Ellsworth, Deceased, No. 2005-296, 651-DE. Dazu etwa *Darrow/Ferrera*, Who own´s a Decendent´s E-Mails?, NYU Journal of Legislation & Public Plicy 10 (2007), 281 ff.; *Herbst*, Death in Cyberspace, RES GESTAE 2009, 16 (21).

digitalen Zeitalter ist diese um eine wichtige Facette reicher geworden: den digitalen Nachlass. Gegenwärtig bleiben die Hinterbliebenen regelmäßig ratlos mit der Frage zurück, was mit den zahllosen digitalen Fußspuren des Verstorbenen, z.B. einem *Facebook*-Profil oder dem E-Mail-Account, zu geschehen hat. Immer häufiger treten Erben und Angehörige mit dem nachvollziehbaren Ansinnen an die Diensteanbieter heran, in die Accounts des Verstorbenen Einsicht zu nehmen und seine Rechte für Homepage-Auftritte, Blog-Einträge etc. wahrzunehmen. Dürfen aber *Facebook, Google+, Xing, Web.de* & Co. den Erben die Account-Obduktion gestatten – und sollen sie es dürfen? Bietet das eine legitime Chance der Trauerarbeit und der Begegnung mit dem Leben des Verstorbenen oder öffnet es die Büchse der Pandora, die für den Persönlichkeitsschutz Unheilvolles verheißt?

Um diesen Fragen auf den Grund zu gehen, arbeitet der Beitrag nach einem Blick auf die wachsende Bedeutung der Problemlage (unten I.) die Eigenheiten des digitalen Nachlasses heraus (unten II.), um sie gegen die unterschiedlichen Reaktionsmuster der Diensteanbieter auf die damit verbundenen Herausforderungen zu spiegeln (unten III.). Die rechtliche Analyse fördert die Erkenntnis zutage, dass die bisherige Anwendungspraxis der Anbieter ebenso wie die bisher zum digitalen Nachlass vertretenen Auffassungen überwiegend nicht dem geltenden Recht entsprechen (unten IV.). Die Überlegungen münden in rechtspolitische Gestaltungsvorschläge für eine sachgerechte Behandlung des digitalen Nachlasses (unten V.).

I. Wenn das Online-Profil den Körper überlebt: Der digitale Nachlass und die Herausforderungen moderner Datenfriedhöfe

In einer Zeit, in der das Internet aus unserem Alltag nicht mehr wegzudenken ist, machen die digitalen Hinterlassenschaften einen substanziellen Teil des Nachlasses eines Menschen aus. Nicht nur die *Digital Natives* bloggen, mailen, posten, skypen und twittern: Mehr als 50 Millionen Deutsche nutzen das Internet; in der Gruppe der 14- bis 19-Jährigen sind es 95 % eines Jahrgangs. Die durchschnittliche aktive Nutzungsdauer beträgt mehr als zwei Stunden am Tag.[3] Weite Teile der Bevölkerung sind damit im Web 2.0 angekommen und partizipieren an den Diensten sozialer Netzwerke, sind Kunden im Online-Banking, bei *PayPal*, *Amazon* oder Auktionshäusern, speichern Urlaubs- und Partyfotos in der digitalen Wolke oder bewerten Produkte, Dienstleistungen und Orte. Die meisten die-

3 Vgl. *BITKOM*, Presseinformationen vom 12. und 13. April 2011, http://www.bitkom.org/67675_67667.aspx (20.5.2012).

ser Dienste setzen eine Anmeldung bzw. Registrierung des Nutzers voraus: Nur über den eigenen Nutzer-Account und die zugehörigen Log-in-Daten erhält der Interessent Zugang zu dem vollständigen Angebot der Diensteanbieter und zu dem hinterlegten, dadurch gegen unbefugten Zugriff gesicherten Datenschatz – seien es Kontaktdaten von Freunden und Bekannten, seien es persönliche oder geschäftliche Nachrichten, Informationen, Lieblingsprodukte, politische Einstellungen oder Meinungen.

Das unablässige Freigeben von Daten legt ein immer feineres Raster über unsere Person. Es entsteht ein digitaler Schattenriss, der immer häufiger zum *pars pro toto* der Persönlichkeit wird. Online-Profile lassen sich zu Collagen unseres Lebens zusammenfügen. Die so entstehenden digitalen Identitäten überdauern den Tod des Nutzers. Sie erlauben tiefste Einblicke in die intime Persönlichkeitssphäre ihrer Urheber, ohne dabei aber den Gesetzen der Vergänglichkeit zu unterliegen.

II. Eigenheiten des digitalen Nachlasses

Als digitalem Abziehbild der Person kommt dem digitalen Nachlass nicht nur eine besondere Bedeutung für die Wahrnehmung der Persönlichkeit des Verstorbenen in der Nachwelt zu (unten 1.). Auch die konzentrierte Bündelung disparater, mitunter hochsensibler Daten an einem Ort (unten 2.) und die zur Öffnung des digitalen Grabschatzes zu überwindenden Zugangshürden (unten 3.) unterscheiden die digitalen von sonstigen Hinterlassenschaften des Verstorbenen. Das erschwert ihre sachgerechte Behandlung.

1. Besondere Schutzbedürftigkeit und Unvergänglichkeit der digitalen Hinterlassenschaften

Während in der analogen Welt die Vergänglichkeit die Regel ist, vergisst das Internet nichts.[4] In seiner Entgrenzung von Raum und Zeit fördert es ein bemerkenswertes Verhalten seiner Nutzer zutage: Wiewohl der Wunsch nach einem umfassenden Schutz persönlicher Daten in der Bevölkerung sehr verbreitet ist, geben viele Nutzer ihre Privatheit in weiten Bereichen des virtuellen Lebens be-

4 Die außerordentlich niedrigen Speicherkosten der digitalen Welt und die nahezu nicht bestehenden Verfallswerte machen das möglich. Die Kosten-Nutzen-Relation zwischen den Aufbewahrungskosten und dem Aufbewahrungswert verschiebt sich dadurch: Das Internet ist ein Ort des Sammelns und Hortens von Informationen.

reitwillig auf. Die Diensteanbieter erlangen dadurch regelmäßig eine dauerhafte Kontrollmacht über sensible personengebundene Informationen, die als Währung des Internets gleichsam die Schatzkammer ihrer Unternehmen bilden. Nutzer zahlen im Internet lieber mit persönlichen Daten, als kostenpflichtige Dienste in Anspruch zu nehmen.

Dieser Öffnung der Privatsphäre liegen disparate Motive zugrunde. Teilweise ist das Verhalten von dem Wunsch getragen, die Magie des globalen Netzes für eine digitale Unsterblichkeit fruchtbar zu machen.[5] Für diese Nutzer ist das digitale Leben Teil einer öffentlichen Inszenierung. Sie wollen mit ihrer digitalen Identität auch über den Tod hinaus in Erinnerung bleiben. Für andere sind die Internetmedien nur ein Mittel der Spontankommunikation, deren Nutzenfunktion sich im Zweck effizienter Informationsübermittlung und der Kommunikation im Hier und Jetzt erschöpft. Entsprechend wollen sie den Zugriff auf ihre digitale Identität auf ihre Lebzeit beschränken und keine digitale Fußspur über den Tod hinaus hinterlassen – nicht selten getragen von der Sorge vor einer posthumen Entstellung des Persönlichkeitsbildes in der Öffentlichkeit oder im Bekanntenkreis.

In testamentarischen Verfügungen finden diese Überlegungen nur selten ihren expliziten Niederschlag. Der größte Teil der Nutzer macht sich über die Verwendung der eigenen Daten nach dem Tod keinerlei Gedanken.

2. Gemengelage disparater Daten

Anders als die in der Wohnung befindlichen oder dem sonstigen räumlichen Zugriff zugänglichen Habseligkeiten des Verstorbenen (wie etwa das mit der Online-Welt vielleicht am ehesten vergleichbare papierene Tagebuch) ist der digitale Nachlass für die Erben nicht körperlich greifbar, sondern in den Tiefen des Cyberspace vergraben. Er bündelt eine inhomogene Masse unterschiedlichster Daten – von persönlichen Daten über elektronische Vertragsdokumente bis hin zu Geschäftsdaten.[6] Für die Hinterbliebenen kann dieser Datenschatz nicht nur von hohem ideellen, sondern auch materiellem Wert sein. In der digitalen Grabkammer schlummern immer mehr Belege vertraglicher Rechte und Pflichten des Erblassers, seien es im Internet eingegangene Abonnementverpflichtungen, On-

5 Vgl. etwa den Fall „öffentlichen Sterbens" der 12-jährigen Bloggerin *Jessica Joy Rees*, der in den USA für Aufsehen sorgte, dazu www.spiegel.de/schul-spiegel/0,1518,807755,00.html (9.10.2012).

6 Zu den sich damit verbindenden rechtlichen Herausforderungen siehe unten IV. 2. a. cc, S. 110.

line-Rechnungen der Telekom oder der Stadtwerke, seien es Rechte an einer Domain, ein Hosting-Vertrag, ein Guthaben bei *PayPal*, Credits in Foto-Communitys oder virtuelle Grundstücke in der Online-Welt von „*Second Life*".

3. Zugangshürden zur Erschließung des digitalen Nachlasses

Diesen digitalen Datenschatz aufzuspüren, ist nicht nur mühsame Detektivarbeit. Es braucht auch einen digitalen Schlüssel, um ihn zu heben. Ohne ihn sind die digitalen Identitäten wertlos. Gehoben werden kann der Datenschatz aber grundsätzlich unkompliziert: unter Verwendung der korrekten Zugangsdaten des Nutzer-Accounts. Doch wer kennt schon die Benutzernamen und vor allem die Passwörter zu all den Accounts, die *Justin Ellsworth* oder *Max Mustermann* im Laufe ihres Lebens angelegt haben? Sofern die zahlreichen Regeln der Datensicherheit, wie Passwortstärke und Geheimhaltung, penibel eingehalten wurden: niemand.[7] Allerdings ist es dem Betreiber der Plattform in der Regel technisch möglich, auf die Account-Daten zuzugreifen oder zumindest die Zugangsdaten zugunsten eines berechtigten Dritten zurückzusetzen. Die Betreiber sind verunsichert, ob und gegebenenfalls an wen sie die entsprechenden Zugangsdaten herausgeben dürfen oder gar müssen.

Während viele Erben die Autopsie des Accounts als wichtigen Teil der Trauerarbeit begreifen, insbesondere den Verstorbenen auf diese Weise in Erinnerung behalten wollen, soll manchen Details aus der digitalen Welt des Verstorbenen diese letzte Ehre aber gerade nicht zuteilwerden – seien es intime Liebesbriefe einer geheimen Romanze, die Aufarbeitung von Ehekrisen in Chats und Foren, sei es der Austausch über Schenkungsabsichten und Vererbungsstrategien oder Opas gut sortierte Pornosammlung.

III. (Uneinheitliche) Reaktionsmuster der Anbieter auf die Herausforderungen des digitalen Nachlasses

Unter diesen ambivalenten Ausgangsvoraussetzungen gehen die Diensteanbieter mit den Internet-Accounts Verstorbener sehr unterschiedlich um. Während etwa

7 Sofern die gängigen Standards eingehalten werden, speichert der Plattformbetreiber die Zugangsdaten mithilfe einer Einwegverschlüsselung. Nicht einmal der Betreiber kennt dann das Passwort. Um den Zugriff Berechtigter, z.B. im Falle des Vergessens von Passwörtern, sicherzustellen, ist der Diensteanbieter aber regelmäßig in der Lage, auf die Nutzerdatenbank als Administrator zuzugreifen und ein neues Passwort zu generieren.

„*Wer-kennt-wen*“, *GMX* und *Web.de* den Erben gegen Vorlage des Erbscheins vollen Zugang zu dem hinterlassenen Account verschaffen,[8] gewähren *Yahoo Deutschland* und *Twitter*[9] keinen Einblick in das Nutzerkonto. Aus ihrer Sicht endet das Vertragsverhältnis mit dem Tod. Nach Ablauf einer Karenzfrist hauchen sie dementsprechend dem Account mitsamt aller hinterlegten Daten kurzerhand das Lebenslicht aus.[10]

Zwischen diesen Extremen finden sich vielfältige Mischformen. Die VZ-Portale, namentlich *StudiVZ*, *SchuelerVZ* und *MeinVZ*, entscheiden im Einzelfall über den Zugang zum Account.[11] Andere Diensteanbieter verwehren den Angehörigen zwar die direkte Nutzung des Accounts, geben aber etwa gespeicherte Fotos als Rohdaten an die Berechtigten heraus. Wieder andere, wie *Xing*,[12] setzen den Status auf „inaktiv“, sobald eine Todesmeldung eingeht, und löschen den Account nach geraumer Zeit, wenn der Inhaber sich auf E-Mail-Anfragen nicht rührt. Auch eine Umwidmung des Accounts in einen Gedenkstatus kommt zusehends in Mode. *Facebook* handhabt das so: Auf Anfrage der Angehörigen versetzt das Unternehmen das Nutzer-Profil in einen Kondolenz-Modus. Bestätigte Freunde können dann Trauerbekundungen auf der zum virtuellen Kondolenzbuch umfunktionierten Pinnwand hinterlassen. Alle anderen Funktionen werden deaktiviert, das Profil wird gleichsam plastiniert; die Erben und Angehörigen erhalten insbesondere keinen Zugriff auf nicht-öffentliche Daten. Indem *Facebook* der digitalen Grabpflege den Weg ebnet, verändert es gleichzeitig das Verständnis für das Nachleben. Es schafft eine neue Form der Trauerarbeit.

Die Diensteanbieter bewegen sich mit ihren unterschiedlichen Praktiken in einer rechtlichen Grauzone. Sie verankern diese meist erst gar nicht oder nur an-

8 In den AGB der Anbieter ist diese Praxis nicht verankert (vgl. etwa die AGB von *GMX*, www.gmx.net/dienst/4436588.html [17.07.2012]); sie bestätigten diese aber auf Rückfrage. Den digitalen Nachlass halten sie für einen Teil der (vermögensrechtlichen) Erbmasse.

9 Vgl. AGB Nr. 5.4 von *Yahoo Deutschland*, http://info.yahoo.com/legal/de/yahoo/tos.html (20.5.2012); AGB Nr. 6, 10 der *Twitter*-Datenschutzrichtlinie, http://twitter.com/tos (20.5.2012).

10 *Twitter* bietet aber an, zuvor eine Sicherungskopie aller öffentlich zugänglichen Daten anzufertigen; einen direkten Zugang zum Account gewährt das Unternehmen nicht. Es gibt auch keine öffentlich zugänglichen Informationen weiter, die in Zusammenhang mit dem Account des Verstorbenen stehen.

11 Eine Regelung zum Umgang mit dem digitalen Nachlass findet sich in deren Allgemeinen Geschäftsbedingungen nicht. Vgl. statt aller die AGB von *StudiVZ*, http://www.studivz.net/l/terms (4.6.2012).

12 Vgl. Nr. 3.1 der *Xing*-Datenschutzbestimmungen: „XING wird diese Daten [s.c. Benutzername und Passwort] in keinem Fall an Dritte weitergeben und/oder diese Dritten sonst wie zur Kenntnis geben.“ (https://www.xing.com/privacy [6.9.2012]).

deutungsweise in ihren Allgemeinen Geschäftsbedingungen.[13] Die globale Verbreitung des Internets und die damit einhergehende Unsicherheit der Nutzer, wo welche Daten verarbeitet und gespeichert werden, erhöht die Unübersichtlichkeit der Rechtslage weiter.

Der deutsche Gesetzgeber schweigt sich zum digitalen Nachlass aus. Eine klare gesetzliche Regelung fehlt – anders als in anderen Staaten, etwa in Teilen der USA. *Connecticut* hat bereits im Jahr 2005[14], *Rhode Island* im Jahr 2007[15] eine Regelung getroffen. Diese US-Bundesstaaten verpflichten die Anbieter, den Angehörigen unter bestimmten Voraussetzungen eine Abschrift der E-Mails des verstorbenen Bundesstaatsangehörigen auszuhändigen. *Indiana* geht mit seiner ebenfalls im Jahr 2007[16] getroffenen Regelung darüber hinaus. Es verleiht den Angehörigen das Recht, die Herausgabe aller elektronisch gespeicherten Informationen des Verstorbenen zu verlangen. *Oklahoma*[17] und *Idaho*[18] haben in den Jahren 2010 und 2011 noch spezifischere Regelungen erlassen. Sie erlauben die Überwachung, Weiterführung oder Auflösung aller Accounts des Verstorbenen in sozialen Netzwerken, Microblogging-Websites (z.B. *Twitter*) oder bei E-Mail-Diensteanbietern. Allen genannten Regelungen ist die Verbürgung des Rechts der Angehörigen bzw. Erben gemeinsam, den Zugang zu dem Account (zuletzt in dem Bundesstaat lebender) Verstorbener von dem Diensteanbieter verlangen und ihm gegenüber gegebenenfalls rechtlich durchsetzen zu können, es sei denn, der Verstorbene hat selbst explizite Regelungen, sei es testamentarischer Art, sei es im Rahmen des Nutzungsvertrages, mit dem Diensteanbieter getroffen.[19]

Angesichts des unklaren nationalen rechtlichen Ordnungsrahmens tut sich die Rechtswissenschaft diesseits des Atlantiks mit einer Antwort auf die Frage nach dem digitalen Nachlass schwer. Genauer müsste man wohl sagen: Sie hat den Grabesschatz bzw. – je nach Sichtweise – die Leiche im Keller überhaupt noch

13 Vgl. oben Fn. 8 ff.

14 Connecticut Public Act No. 05-136, http://www.cga.ct.gov/2005/act/Pa/2005PA-00136-R00SB-00262-PA.htm (18.07.2012).

15 Rhode Island General Laws, Chapter 33-27, http://www.rilin.state.ri.us/Statutes/TITLE33/33-27/INDEX.HTM (18.07.2012).

16 Indiana Code 29-1-13, http://www.in.gov/legislative/ic/code/title29/ar1/ch13.html (18.07.2012).

17 Oklahoma Statutes, Title 58, Section 269, http://www.oklegislature.gov/osStatuesTitle.aspx (17.07.2012). Eine ähnliche Regelung plant der Bundesstaat Nebraska (vgl. http://nebraskalegislature.gov/FloorDocs/Current/PDF/Intro/LB783.pdf (16.7.2012).

18 Idaho Code, Section 15-3-715, http://legislature.idaho.gov/idstat/Title15/T15CH3SECT15-3-715.htm (18.07.2012).

19 Vgl. dazu http://webserver1.lsb.state.ok.us/cf/2009-10%20ENR/hB/HB2800%20ENR.-DOC (16.7.2012); http://www.digitalestateresource.com/law/ (18.7.2012).

nicht entdeckt. Rechtsprechung gibt es noch nicht. Aufsätze sind Mangelware.[20] Bis die Obergerichte die juristische Leichenstarre überwunden haben, wird noch manche Totenmesse gelesen werden. Doch die aufgeworfenen Fragen stellen sich mit wachsender Dringlichkeit. Immerhin stirbt – statistisch betrachtet – alle zwei Minuten ein *Facebook*-Nutzer.[21]

IV. Der digitale Nachlass als Erbschaft?

Aus einer rein zivilrechtlichen Perspektive sind die Fragen nach der sachgerechten Behandlung des digitalen Nachlasses vordergründig schnell beantwortet: Zwar werden „die Bande der Liebe" – wie *Thomas Mann* formulierte – „nicht mit dem Tod durchschnitten", wohl aber die vermögensrechtlichen Beziehungen des Verstorbenen selbst zu seinen Schuldnern und Gläubigern. Die Erben treten an seine Stelle. Das Vermögen des Erblassers geht nach der Zentralnorm des Erbrechts als Ganzes im Wege der Universalsukzession auf den Erben über (§ 1922 Abs. 1 BGB).[22] Als Inbegriff aller geldwerten Rechtsbeziehungen[23] umschließt es Kontoguthaben, Rechte an einer Internetdomain, aber auch Credits in Foto-Communitys oder Web-Clubs sowie Guthaben bei Online-Spielen und im Internet eingegangene Vertragsverpflichtungen. Solche vermögensrechtlichen Positionen sind vererbbar, nicht-vermögensrechtliche hingegen in der Regel nicht.[24]

20 Bislang lediglich *Hoeren*, NJW 2005, 2113 ff. (beschränkt auf den E-Mail-Account und die private Homepage).

21 Unter Zugrundelegung einer jährlichen Sterberate von 10, 92 je tausend Einwohnern (s.c. 893.736 Toten jährlich; vgl. www.indexmundi.com/g/g.aspx?c=gm&v=26&l=de [6.9.2012]) ergäbe sich bei 24,87 Millionen deutschen *Facebook*-Nutzern (vgl. de.statista.com/statistik/daten/studie/70189/umfrage/nutzer-von-facebook-in-deutschland-seit-2009/ [9.10.2012]) für den (hypothetischen) Fall einer gleichmäßigen Generationenverteilung innerhalb der *Facebook*-Gemeinde namentlich eine Zahl von 271.588 Sterbefällen im Jahr.

22 Das Gesetz verwendet hin und wieder den Begriff des Nachlasses (z.B. in §§ 1960, 1975 BGB). Ein inhaltlicher Unterschied ist damit nicht verbunden, vgl. *Müller-Christmann*, in: Bamberger/Roth (Hrsg.), BeckOK BGB, 21. Ed., Nov. 2011, § 1922 Rn. 11.

23 *Leipold*, in: Münchner Kommentar zum BGB, 5. Aufl. 2010, § 1922 Rn. 2.

24 Ein Indiz für die Nichtvererbbarkeit ist dabei die fehlende Übertragungsmöglichkeit unter Lebenden. Der Teufel steckt dabei allerdings im Detail. Es finden sich zahlreiche (im Zweifel durch Auslegung auf der Grundlage der jeweiligen Interessenlagen zu ermittelnde) Ausnahmen. So ist etwa der Nießbrauch eine vermögensrechtliche Position, aber nach § 1061 S. 1 BGB gleichwohl nicht vererbbar. Das Urheberrecht ist nicht übertragbar (§ 29 Abs. 1 UrhG), wohl aber vererblich. Umgekehrt ist etwa die Mitgliedschaft in einem Idealverein zwar personenbezogen, nichtvermögensrechtlicher Natur und damit grundsätzlich unvererbbar. Die Vereinssatzung kann jedoch nach § 40 BGB eine andere

Zwischen vermögensrechtlichen und nicht-vermögensrechtlichen Positionen nehmen die *Immaterialgüterrechte* eine Zwitterstellung ein: Bei ihnen handelt es sich um unkörperliche Gegenstände mit Vermögenswert. Für ihren Rechtsübergang hat der Gesetzgeber Sonderregelungen getroffen. Immaterialgüterrechte gehen regelmäßig (sowohl in ihrem vermögens- als auch in ihren persönlichkeitsrechtlichen Elementen) auf die Erben über.[25] Das gilt namentlich für das Urheberrecht (§ 28 Abs. 1 UrhG), das Patentrecht (§ 15 Abs. 1 S. 1 PatG), Gebrauchsmuster (§ 22 Abs. 1 S. 1 GebrMG), Geschmacksmuster (§ 29 Abs. 1 GeschmMG) und die geschützte Marke (§ 27 Abs. 1 MarkenG). Urheberrechtsfähige Inhalte des Erblassers auf Videoplattformen, wie *Youtube* oder *FlickR*, berechtigen die Erben daher regelmäßig, die Herausgabe oder Löschung der entsprechenden Foto- bzw. Videoaufnahmen zu verlangen. Den Erben stehen bis zum Erlöschen des Urheberrechts 70 Jahre nach dem Tod des Urhebers (§ 64 UrhG) dieselben gesetzlichen Rechte wie diesem zu (§ 30 UrhG). Sie müssen jedoch (wiewohl das Urheberrecht nicht übertragbar ist [§ 29 Abs. 1 UrhG]), eine – bei Internetdiensten nicht unübliche – Einräumung von Nutzungsrechten, die der Erblasser zugunsten eines Diensteanbieters vertraglich versprochen hat, gegen sich gelten lassen (§ 31 Abs. 1 S. 1 UrhG).

Welches Schicksal aber die große Masse der persönlichen Daten des Erblassers fristet, seien es passwortgesicherte Daten eines Internet-Accounts (unten 2. a.), seien es öffentlich verfügbare Internetdaten, z.B. einer Homepage (unten 2. b.), hinterlässt offene Fragen. Sie sachgerecht zu beantworten, bereitet einiges Kopfzerbrechen, lassen sich diese Daten doch nicht ohne Weiteres in das binäre Schema vermögensrechtlicher und nicht-vermögensrechtlicher Positionen pressen (unten 1.).

1. Der Internet-Account als vererbbares Vermögen?

Soweit Daten eines Verstorbenen, z.B. heruntergeladene E-Mails *auf einem lokalen Datenträger*, insbesondere einer Festplatte oder einem USB-Stick, *verkörpert* sind, geht das Eigentum an dem Datenträger grundsätzlich im normalen Erbgang auf die Erben über. Die gespeicherten Daten teilen grundsätzlich deren rechtliches Schicksal.[26]

Regelung treffen. Vgl. dazu auch *Müller-Christmann*, in: BeckOK BGB (Fn. 22), § 1922 Rn. 24; *Schlüter*, in: *Ermann*, BGB, 11. Aufl. 2004, § 1922 Rn. 8; *Leipold*, in: MüKo BGB (Fn. 23), § 1922 Rn. 19.

25 *Leipold*, in: MüKo BGB (Fn. 23), § 1922 Rn. 94.

26 Wenn diese Dateien aber mithilfe eines Passworts gegen den Zugriff durch Dritte gesichert sind, stellen sich ähnliche Fragen wie bei Daten eines Internet-Accounts – die Frage

Internet-Accountdaten sind jedoch regelmäßig nicht lokal, sondern auf den Datenserverfestplatten der Anbieter gespeichert. An den Servern erwirbt der Nutzer kein Eigentum. Die Erben können allenfalls in das bestehende vermögensrechtliche Vertragsverhältnis mit dem Diensteanbieter eintreten.[27] Im Falle eines Vertragsübergangs erwüchse aus dem Nutzungsvertrag als Haupt- oder Nebenrecht ein Anspruch der Erben auf Zugangsgewährung zum Account des Erblassers.

Nicht jedes schuldrechtliche Rechtsverhältnis geht aber im Wege der Universalsukzession auf die Erben über. Sowohl der Nutzungsvertrag[28] als auch das Gesetz können einen Vertragsübergang ausschließen.[29] Die Übertragbarkeit von Vertragspflichten macht der Gesetzgeber regelmäßig davon abhängig, ob der jeweilige Gegenüber gegen den mit dem Austausch des Vertragspartners verbundenen Gläubigerwechsel geschützt werden muss (Rechtsgedanke des § 399 Alt. 1 BGB).[30] Dies ist insbesondere dann der Fall, wenn sich die vertragliche Bindung auf die Person des Berechtigten beschränken sollte. So erlöschen beispielsweise das Vorkaufsrecht und das schenkweise gegebene Rentenversprechen kraft gesetzlicher Regelung im Allgemeinen mit dem Tod des Berechtigten (§ 473 S. 1 BGB) bzw. des Schenkers (§ 520 BGB) und sind daher nicht vererbbar.[31]

Ein solches besonderes persönliches Band ist zwischen Internetdiensteanbieter und Nutzer nicht geknüpft: Sie schließen Verträge über Internet-Accounts regelmäßig ohne Rücksicht auf die Person des Nutzers, häufig auch ohne nähere Prüfung der Personenidentität. Die Nutzer nehmen bei ihnen kein persönliches Vertrauen in Anspruch. Den Diensteanbietern kommt ein schutzwürdiges Inte-

nämlich, ob die Überwindung einer solchen Zugangssicherung das postmortale Persönlichkeitsrecht des Verstorbenen verletzen kann. Dazu im Einzelnen unten unter IV. 2., S. 87 ff.

27 Vgl. *Leipold*, in: MüKo BGB (Fn. 23), § 1922 Rn. 20; *Müller-Christmann*, in: BeckOK BGB (Fn. 22), § 1922 Rn. 31.

28 In diesem Sinne etwa die Nutzungsbedingungen des Plattformbetreibers „*wimdu*" (eines Portals, über das Wohnungen in aller Welt zur Miete bzw. Übernachtung angeboten bzw. gefunden werden können), Nr. 4.1 der Nutzungsbedingungen (http://www.wimdu.de/terms [17.7.2012]); ebenso Nr. 2. 4 der Nutzungsbedingungen von „*glamour.de*" (http://www.glamour.de/nutzungsbedingungen [17.7.2012]) sowie Nr. 2.4. der Nutzungsbedingungen von "*myvideo.de*" (http://www.myvideo.de/AGB [16.7.2012]).

29 Die Vertragsfreiheit gestattet es, die Vererbbarkeit vertraglicher Positionen auszuschließen, vgl. BGH, WM 1989, 1813; *Leipold*, in: MüKo BGB (Fn. 23), § 1922 Rn. 20.

30 Der Gesetzgeber lässt sich dabei von der Wertung leiten, wie sehr das jeweilige Vertragsverhältnis und die jeweiligen vertragstypischen Erfüllungsrisiken auf die individuellen Personen zugeschnitten sind und damit auch nur zwischen diesen Personen Geltung beanspruchen kann.

31 Weitere Beispiele bei *Leipold*, in: MüKo BGB (Fn. 23), § 1922 Rn. 23.

resse daher grundsätzlich nicht zu. Der Erbfall ändert das Wesen der zugrunde liegenden schuldrechtlichen Ansprüche mithin nicht.

All das spricht dafür, dass die Erben schuldrechtlich in das Vertragsverhältnis mit den Anbietern von Internetdiensten eintreten – erweitert um ein außerordentliches Kündigungsrecht der Erben.[32] Dann steht den Erben möglicherweise der Zugriff auf die in Internet-Accounts gespeicherten Daten der Erblasser, insbesondere ein Recht auf Auskunft und Herausgabe der Zugangsinformationen, offen.[33] So sieht etwa der Bundesdatenschutzbeauftragte die Rechtslage.[34]

2. In memoriam postmortaler Persönlichkeitsschutz: Auswirkungen des Persönlichkeitsschutzes auf die Vererbbarkeit von Account-Daten

Die alleinige Betrachtung des digitalen Nachlasses durch die zivilrechtliche Brille verfängt jedoch nicht. Sie trägt namentlich der Bedeutung der Daten für die Persönlichkeitsentfaltung des Einzelnen nicht angemessen Rechnung. Der digitale Nachlass erweist sich längst nicht alleine als eine Frage des Erbrechts, das sich ausschließlich mit den vermögensrechtlichen Folgen des Ablebens eines Menschen auseinandersetzt. Aus den einfachgesetzlichen Vorschriften des Datenschutzrechts und/oder dem verfassungsrechtlichen postmortalen Persönlichkeitsschutz kann sich das Verbot ergeben, Dritten Zugang zu dem Inhalt des Accounts zu verschaffen, insbesondere das Passwort weiterzugeben.

Das Datenschutzrecht hat als Ausprägung des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)[35] den Auftrag, die

32 Vgl. §§ 564, 580, 581 Abs. 2, 605 Nr. 3 BGB; dazu auch *Müller-Christmann*, in: BeckOK BGB (Fn. 22), § 1922 Rn. 39 f.: Die Frage nach der Vererbbarkeit bzw. Auflösbarkeit bei Dauerschuldverhältnissen beurteilt sich grundsätzlich nach den Umständen des Einzelfalls.

33 Für E-Mails vgl. *Hoeren*, NJW 2005, 2113 (2114). Er differenziert dabei zwischen geschäftlichen und ungewollten (vererbbaren) E-Mails einerseits, sowie privaten (nicht vererbbaren) E-Mails andererseits. Dazu auch unten S. 111.

34 Stellungnahme der Pressestelle des Bundesdatenschutzbeauftragten vom 21.4.2010.

35 Einige Bundesländer haben das Recht auf informationelle Selbstbestimmung bzw. das Recht auf Datenschutz ausdrücklich in ihren Landesverfassungen verankert (zum Beispiel Art. 33 Verf. Bln; Art. 11 Verf. Bbg; Art. 6 Abs. 1 Verf. M-V; Art. 4 Abs. 2 Verf. NRW; Art. 33 sächs. Verf.; Art. 6 Abs. 1 Verf. LSA; Art. 2 Sätze 2 und 3 saarl. Verf.; Art. 6 Abs. 2 thür. Verf.). Das Recht auf informationelle Selbstbestimmung versteht sich als interpretatorische Fortschreibung des Allgemeinen Persönlichkeitsrechts (vgl. dazu etwa *Simitis,* NJW 1984, 398 [399]; *Martini*, JA 2009, S. 839 ff.). Ihm liegt insbesondere die verfassungsrechtliche Überlegung zugrunde, dass (gerade mithilfe moderner Informationstechnologie) in der Synthese aller über eine Person verfügbaren Daten ein umfassendes Persönlichkeitsprofil erschlossen werden kann. „Insoweit gibt es unter den Bedin-

personenbezogenen Daten eines Menschen gegen Missbrauch und unbefugte Kenntnisnahme zu schützen. Aus ihm fließen wichtige Vorgaben für die Pflichten der Diensteanbieter und für die Rechte der Angehörigen.[36] Maßgeblich sind insoweit nicht nur die allgemeinen Datenschutzgesetze,[37] sondern vor allem die bereichsspezifischen Regelungen des TMG: Soziale Netzwerke im Internet, Accountdienstleister wie *Web.de* oder *Gmx.net*, Online-Auktionshäuser und Online-Spiele im Allgemeinen bieten Telemediendienste i.S.d. § 1 Abs. 1 S. 1 TMG an.[38] Die bei der Erstellung und Nutzung solcher Accounts anfallenden Interaktionen zwischen Nutzer und Diensteanbieter sind folglich in erster Linie den §§ 11 ff. TMG unterworfen; subsidiär kommen – vorbehaltlich des territorialen[39] und sachlichen[40] Anwendungsbereichs des TMG – über den Verweis des § 12

gungen der automatischen Datenverarbeitung kein »belangloses« Datum mehr." (BVerfGE 65, 1 [45]).

36 Die Reichweite der datenschutzrechtlichen Regelungen ist dabei in jedem Fall begrenzt. Die Rechte der Angehörigen können nicht über die Rechte des ursprünglich Betroffenen hinausgehen; zu den datenschutzbezogenen Rechten siehe unten IV. 2. a. aa., S. 92 ff. und IV. 2. b., S. 112 ff.

37 Dazu zählen für den privaten Sektor in erster Linie das BDSG und für den öffentlichen Sektor zusätzlich die verschiedenen Landesdatenschutzgesetze.

38 Vgl. *Heckmann,* in: ders. (Hrsg.), jurisPraxis-Kommentar Internetrecht, Telemediengesetz, E-Commerce, E-Government, 2. Aufl. 2009, Kap. 1.14 Rn. 5; *Jotzo*, MMR 2009, 232 (234); *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 2. Aufl. 2011, § 14 TMG Rn. 5.

39 Moderne Datenverarbeitung beschränkt sich längst nicht mehr auf den nationalen Handlungskontext. Die globalisierte, vernetzte Welt bringt eine grenzüberschreitende internationale Datenspeicherung und -verarbeitung mit sich. Für Stellen, die aus dem EU-Ausland heraus in Deutschland operieren, ist bei EU-grenzüberschreitendem Datenverkehr nach dem in § 1 Abs. 5 S. 1 BDSG verankerten Sitzprinzip grundsätzlich das nationale Recht des Sitzlandes, d.h. des Landes, in dem die für die Verarbeitung verantwortliche Stelle ihre Niederlassung hat, anwendbar. Sonstige Anbieter, die von außerhalb der EU operieren, unterfallen nach der in § 1 Abs. 5 S. 2 BDSG verankerten Grundregel des Territorialprinzips deutschem Datenschutzrecht, wenn sie im Inland personenbezogene Daten erheben, verarbeiten oder nutzen. Eine Ausnahme gilt dabei für den Einsatz von Datenträgern ausschließlich zum Zwecke des Transits durch das Inland (§ 1 Abs. 5 S. 4 BDSG).

40 Die Anwendung des Datenschutzrechts auf Telemedienanbieter ist nicht durch § 27 Abs. 1 S. 2 BDSG sachlich eingeschränkt. Dieser Ausnahmetatbestand greift zum einen nur im unmittelbaren Anwendungsbereich des TMG und zum anderen nur, wenn die personenbezogenen Daten „ausschließlich für persönliche oder familiäre Tätigkeiten" erhoben, verarbeitet oder genutzt werden. Der Datenumgang muss also mit allen seinen Bestandteilen der privaten Lebensführung einer natürlichen Person dienen. (In ähnlichem Sinne nahezu wortgleich Art. 2 Nr. 2 lit. d des Entwurfs einer Europäischen Datenschutzverordnung). Für die Erben mag diese Voraussetzung zutreffen, nicht aber für die Diensteanbieter. Auf Letztere kommt es aber an. Sowohl der Dienstvertrag selbst als auch die Intention des Diensteanbieters, durch das Sammeln der Daten Werbeeinnahmen zu erzielen, dienen nämlich nicht mit allen ihren Bestandteilen der privaten Lebensführung einer

Abs. 3 TMG auch die allgemeinen datenschutzrechtlichen Regelungen zur Anwendung.[41]

Das Fernmeldegeheimnis des § 88 TKG als Ausdruck einer Schutzpflicht des Staates für die Integrität von Telekommunikationsprozessen ist demgegenüber nicht berührt: Seine Verpflichtungen zur Geheimhaltung bestehen zwar auch nach dem Ende der Telekommunikationsverbindung fort (§ 88 Abs. 2 S. 2, Abs. 3 S. 2 u. 3 TKG). Es adressiert aber ausschließlich Telekommunikationsanbieter, also diejenigen, welche die Übertragung von Signalen über Telekommunikationsnetze übernehmen (§ 88 Abs. 2 Satz 1 i.V.m. § 3 Nr. 6 und § 3 Nr. 24 TKG), nicht aber diejenigen, welche als Telemedienanbieter die Inhalte für die zu transportierenden Signale bereitstellen (sog. Inhalteanbieter – Content-Provider), wie z. B. *Facebook*.[42]

Wie mit den Accounts Verstorbener umzugehen ist, regeln die datenschutzrechtlichen Vorschriften nicht ausdrücklich. Weder das TMG noch das BDSG enthalten (anders als etwa § 4 Abs. 1 S. 2 BlnDSG[43] und § 37 Abs. 1 BbgBestG)[44] eine Rechtsvorschrift, die ihren Anwendungsbereich ausdrücklich auf Verstorbene ausdehnt. Aus ihrem Sinn bzw. ihrem verfassungsrechtlichen Hintergrund lassen sich aber Rückschlüsse ziehen, aus denen sich eine Einschränkung des zulässigen Umgangs mit den Daten Verstorbener herleiten lässt.

Zu unterscheiden ist insoweit zwischen dem Zugang zu höchstpersönlichen, nicht-öffentlichen Daten von Internet-Accounts Verstorbener, insbesondere E-Mail-Konten (unten a), sowie jedermann zugänglichen Internetinformationen,

natürlichen Person. Für den Diensteanbieter, der in der Regel schon keine natürliche Person ist, greift die Ausnahme des § 27 Abs. 1 S. 2 BDSG mithin nicht. Andernfalls könnte man von jeder Daten haltenden Stelle die Daten Dritter erfragen, solange man sie nur zu persönlichen oder familiären Zwecken verwenden will. Das entspricht jedoch nicht dem Sinn des Gesetzes. A.A. *Hoeren*, NJW 2005, 2113 (2115).

41 Zusätzliche Erlaubnistatbestände, die das allgemeine Datenschutzrecht nicht vorsieht, entstehen dadurch nicht; insoweit ist das TMG abschließend, vgl. *Spindler/Nink*, in: Spindler/Schuster (Fn. 38), § 12 TMG Rn. 11.

42 Aus den gleichen Gründen ist auch § 206 StGB nicht einschlägig. Er verpflichtet ausschließlich Inhaber oder Beschäftigte von Unternehmen, die geschäftsmäßig Post- und Telekommunikationsdienste erbringen. Vgl. auch etwa *Lünenbürger,* in: Scheuerle/Mayen (Hrsg.), TKG, 2. Aufl. 2008, § 3 Rn. 58. Anders verhält es sich mit dem verfassungsrechtlichen Schutz des Art. 10 Abs. 1 GG. Dazu siehe unten S. 103.

43 Die Vorschrift erklärt „für Daten über Verstorbene" die Regelungen über personenbezogene Daten für entsprechend anwendbar, „es sei denn, daß schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können".

44 Angesichts des unterschiedlichen Anwendungsbereichs der Vorschriften und der verschiedenen Kompetenzzuordnungen rechtfertigt das noch keinen Umkehrschluss. Zwar ergibt sich aus diesen landesrechtlichen Vorschriften, dass die betroffenen Länder die Daten Verstorbener nicht als personenbezogene Daten einstufen. Der Bund ist an – gegebenenfalls deklaratorische – Begriffsverwendungen der Länder aber nicht gebunden.

die der Erblasser über sich angelegt hat (unten b). Sie sind von jeweils verschiedener Sensibilität und fristen daher ein unterschiedliches rechtliches Schicksal.

a) Nicht-öffentlich verfügbare Daten, z.B. eines E-Mail-Accounts

Dass der Diensteanbieter den Erben oder sonstigen Dritten den Zugang zu dem Account und den darin verfügbaren nicht-öffentlich zugänglichen Informationen des Erblassers *zu Lebzeiten* des Erblassers nicht eröffnen dürfte, versteht sich.

Mit dem *Tod des Nutzers* endet nach überkommener Auffassung aber der Datenschutz grundsätzlich.[45] Dieses Datum markiert dann nach dieser Lesart auch das Ende des Schutzes von Daten gegenüber den Erben. Es macht den Weg frei für deren Zugriff auf den Account, soweit der Erblasser selbst keine expliziten anderweitigen Verfügungen getroffen hat.

Das scheint prima facie aus dem Gegenstand des Datenschutzrechts bruchfrei ableitbar: Die datenschutzrechtlichen Regelungen knüpfen an *personenbezogene Daten*[46] an (§ 3 Abs. 1 BDSG i.V.m. § 12 Abs. 1 und Abs. 3 TMG). Personenbezogene Daten müssen sich auf eine *natürliche Person* beziehen (§ 3 Abs. 1 BDSG bzw. § 11 Abs. 2 TMG). Das legt den Schluss nahe, dass es sich bei ihnen

45 Vgl. etwa *Kühling/Seidel/Sividris*, Datenschutzrecht, 2. Aufl. 2011, S. 79; ebenso die überwiegende Rechtsauffassung in den USA, dazu etwa *Darrow/Ferrera* (Fn. 2), 281 (313).

46 Die in sozialen Netzwerken hinterlegten Informationen über den eigenen Werdegang, Lieblingsbeschäftigungen, das Aussehen, politische Ansichten und Interessen sind der Prototyp solcher Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person: Die Accounts sind geradezu mit Informationen über den Account-Inhaber, Fotos, Freundeslisten, Kontaktdaten usw. gespickt. Die Sensibilität einer solchen Information ist dabei für die Einordnung als personenbezogenes Datum unerheblich, da es im modernen Informationszeitalter kein „belangloses Datum“ mehr gibt (BVerfGE 65, 1 [45]). Erfasst werden nicht nur objektive Informationen über eine Person, sondern auch Werturteile, wie etwa die Einordnung als ehrlich und zuverlässig oder Aussagen über die Kreditwürdigkeit einer Person; vgl. *Buchner*, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG und einschlägigen Vorschriften des TMG und TKG, 2010, § 3 BDSG Rn. 4 f.; *Dammann*, in: Simitis (Hrsg.), BDSG, 7. Aufl. 2011, § 3 BDSG Rn. 5, 7. Den Schutz des Gesetzes genießen die hinterlegten Daten aber nur dann, wenn der Account-Inhaber entweder bestimmt oder zumindest bestimmbar, also identifizierbar, ist. Dies ist der Fall, wenn die Anmeldung eines Accounts die Angabe des Klarnamens erfordert oder sonstige Informationen, wie beispielsweise eine E-Mail-Adresse, Telefonnummer, Kfz-Kennzeichen, (Steuer-)Identifikationsnummer oder eine Kombination verschiedener Angaben, wie etwa Geburtsdatum und Anschrift, im konkreten Kontext eine Wiedererkennung des Account-Inhabers ermöglichen. Selbst durch ein nicht verfremdetes Bild im Internet kann der Betroffene hinreichend bestimmbar sein, wenn davon auszugehen ist, dass ein Betrachter die Identität der Person erkennen kann, *Caspar*, DÖV 2009, 965 (967).

um Informationen über einen *lebenden* Menschen handeln muss.[47] So versteht die Rechtsordnung den Begriff auch regelmäßig in anderen Vorschriften, so etwa in § 61 Nr. 1 VwGO.[48]

Eine Stütze findet diese Sichtweise auch in dem Schutzzweck des BDSG. Dieses soll im Grundsatz den Einzelnen davor schützen, durch den Umgang mit personenbezogenen Daten in seinem Persönlichkeitsrecht verletzt zu werden (§ 1 Abs. 1 BDSG). Sein Ziel ist es, die freie Entfaltung der Persönlichkeit zu wahren, indem es eine aktive Teilnahme am Verarbeitungsprozess erhobener Daten gewährleistet.[49] Eine solche ist naturgemäß nur einem lebenden Menschen möglich. So ist Träger des Grundrechts auf freie Entfaltung der Persönlichkeit, der Keimzelle des Datenschutzrechts, auch nur die lebende Person.[50] Denn das Grundrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG setzt die Fähigkeit zur Entfaltung einer Persönlichkeit voraus. Diese erlischt aber mit dem Tode.[51]

Die Schutzwirkungen des Persönlichkeitsrechts sind insoweit vor und nach dem Tod verschieden.[52] Entsprechend ist das Allgemeine Persönlichkeitsrecht

47 In diesem Sinne *Buchner*, in: Taeger/Gabel (Fn. 46), § 3 BDSG Rn. 8; *Dammann*, in: Simitis (Fn. 46), § 3 BDSG Rn. 17; *Kühling/Seidel/Sividris* (Fn. 45), S. 79.

48 Vgl. *Redeker/von Oertzen*, VwGO, 15. Aufl. 2010, § 61 Rn. 1; *Martini,* VerwProzR, 5. Aufl. 2011, S. 33; siehe auch § 50 Abs. 1 ZPO. Zu unterscheiden ist davon die Frage der Wahrnehmung prozessualer Rechte für eine bereits von dem (inzwischen) Verstorbenen erhobene Klage im Anschluss an den Tod eines Klägers. Für diesen Fall sieht etwa die ZPO Regelungen zur Unterbrechung des Verfahrens bis zu dessen Aufnahme durch die Rechtsnachfolger vor (§ 239 Abs. 1 ZPO). Sie geht mithin davon aus, dass das Verfahren sich nicht durch den Tod gleichsam automatisch erledigt. Vgl. dazu auch OVG NRW, KStZ 1978, 16. Dieser Rechtsgedanke lässt sich durchaus für die Geltendmachung von Rechten bzw. die Verteidigung der Rechtsstellung im Hinblick auf Daten fruchtbar machen, die der Verstorbene zu Lebzeiten angelegt hat.

49 *Dammann*, in: Simitis (Fn. 46), § 3 BDSG Rn. 17.

50 BVerfGE 30, 173 (194); BVerfG, NJW 2001, 2957 (2958).

51 Der Schutz des Ansehens Verstorbener läuft dadurch aber nicht leer. Die Würde wirkt nach dem Tod fort (sog. postmortales Persönlichkeitsrecht; siehe dazu im Einzelnen unten S. 100 ff.). Die Wertentscheidung des Grundgesetzes für die Unantastbarkeit der menschlichen Würde entfaltet (etwa durch den strafrechtlichen Schutz des Andenkens Verstorbener in § 189 StGB und durch den Pietätsschutz des § 168 StGB und das Verbot der Post-mortem-Befruchtung nach § 4 Abs. 1 Nr. 3 ESchG) auch über den Tod hinaus seine Wirkung. Entsprechend endet das an den Staat gerichtete Gebot, den Einzelnen vor Angriffen auf seine Menschenwürde zu schützen, als tragendes Konstitutionsprinzip der Verfassung nicht mit dem Tode, auch wenn die Person selbst diese Rechte nicht mehr verteidigen kann. So schon BVerfGE 30, 173 (194). Skeptisch insoweit *Schönberger*, Postmortaler Persönlichkeitsschutz, 2011, S. 74 ff.

52 Der BGH zeigt sich dabei für das als sonstiges Recht im Sinne des § 823 Abs. 1 BGB entwickelte einfachgesetzliche Persönlichkeitsrecht im Grundsatz weitaus schutzoffener als das BVerfG für das verfassungsrechtliche postmortale Persönlichkeitsrecht. Zum Anspruch auf Unterlassung bzw. Widerruf ehrverletzender Äußerungen bei fortwirkender Beeinträchtigung des Persönlichkeitsrechts eines Verstorbenen: BGHZ 50, 133 (137) –

als höchstpersönliches Nichtvermögensrecht aufgrund seines besonderen Personenbezugs auch nicht vererbbar. Die Höchstpersönlichkeit der datenschutzrechtlichen Positionen steht bei dieser Lesart einer Fortwirkung des Persönlichkeitsrechts über den Tod hinaus entgegen. In die datenschutzrechtliche Begriffsbestimmung „personenbezogene Daten" liest die Literatur[53] das Wort „lebend" mithin als ungeschriebene Voraussetzung hinein.

Ob diese Prämisse bei sachgerechter Auslegung der einfachgesetzlichen Bestimmungen zutrifft, ist aber zu bezweifeln (unten aa). Jedenfalls im Zusammenspiel mit dem Schutzgedanken des verfassungsrechtlichen postmortalen Persönlichkeitsrechts ergibt sich die Verpflichtung, die Account-Daten eines Erblassers im Zweifel nicht dem Zugriff der Erben zu öffnen (unten bb).

aa) (Einfachgesetzlicher) Postmortaler Datenschutz?

(1) Anwendbarkeit der Vorschriften des Datenschutzrechts auf Daten Verstorbener

Bei genauerem Hinsehen setzen die datenschutzrechtlichen Wendungen „personenbezogene Daten" und „natürliche Person" in der Sache zunächst nur die Be-

Mephisto; vgl. auch BGHZ 107, 384 – Emil Nolde; OLG Hamburg NJW 1990, 1995 (1996) – Heinz Erhardt; OLG Köln NJW 1999, 1969 – Konrad Adenauer; BGH, GRUR 2007, 168 (169); *Seifert,* NJW 1999, 1889 (1893 ff.); kritisch *Westermann,* FamRZ 1969, 561 ff.; *Stein,* FamRZ 1986, 7 (8 f.). Dieser postmortale Persönlichkeitsschutz ermöglicht es den Berechtigten, die Wahrung des Ansehens des Verstorbenen (über die *ultima ratio* des Strafrechts hinaus) durchzusetzen. Vor allem ein *argumentum e contrario* kommt dabei zum Tragen: Aus der Sicht des BGH lässt sich nämlich nicht schlüssig begründen, warum der persönlichkeitsrechtliche Unterlassungsanspruch in dem Augenblick völlig erlöschen sollte, in dem sich der Betroffene nicht mehr selbst verteidigen kann. Das überzeugt: Selbst wenn das Lebensbild, gegen dessen Entstellung der Unterlassungsanspruch schützen solle, zu Ende gemalt ist, besteht dessen Glanz als verletzbares und schutzwürdiges Gut fort. Das Persönlichkeitsrecht erfährt aber auch aus Sicht des BGH mit dem Tode der Person eine „einschneidende Einschränkung", da mit diesem Zeitpunkt „alle diejenigen Ausstrahlungen enden, welche die Existenz einer aktiv handelnden Person bedingen" (BGHZ 50, 133 [136] – Mephisto). Bei Verstorbenen muss daher auch aus der Sicht des BGH ein anderer Wertungsmaßstab zur Anwendung kommen als bei Lebenden. Als Wahrnehmungsberechtigte sieht der BGH in erster Linie die vom Verstorbenen zu Lebzeiten dazu Berufenen an, erweitert diesen Kreis jedoch in Analogie zu § 22 S. 3 KunstUrhG, § 60 Abs. 1 S. 1 a.E. UrhG, § 77 Abs. 2 StGB um die nahen Angehörigen des Verstorbenen. Auf die Erbenstellung kommt es demgegenüber richtigerweise nicht an; vgl. BGHZ 15, 249 (259); BGHZ 50, 133 (140); a.A. *Stein,* FamRZ 1986, 7 (16), die die Erben als wahrnehmungsberechtigt ansieht, wenn der Erblasser keine abweichende Bestimmung getroffen hat.

53 Siehe die Nachweise in Fn. 47.

ziehung zwischen den geschützten Daten und einem *zum Zeitpunkt der Entstehung der Daten* lebenden Menschen voraus – in Abgrenzung zu solchen Daten, die sich entweder auf eine juristische Person beziehen oder einen Personenbezug gänzlich vermissen lassen. Auf eine natürliche Person (also personen-)bezogen bleiben die Daten auch nach dem Tod.[54] Sie adressieren nämlich weiterhin einen konkreten Menschen als Betroffenen. „Personenbezogene Daten" und „natürliche Person" bedingen mithin begrifflich nicht notwendigerweise einen heute *lebenden* Menschen. Dass der Begriff der natürlichen Person gemeinhin mit demjenigen der lebenden Person gleichgesetzt wird, erklärt sich aus dem besonderen Schutzzweck der Vorschriften, eine handlungsfähige Person zu adressieren. So können nach den Grundvorstellungen des Verfahrensrechts nur lebende Personen Prozesse führen. Im Datenschutzrecht kann diese Wertung im Hinblick auf die Nachwirkungen des Persönlichkeitsschutzes aber anders ausfallen. Dass der Verstorbene keine Möglichkeit der aktiven Teilnahme am Verarbeitungsprozess mehr hat, rechtfertigt es noch nicht, ihm den besonderen Persönlichkeitsschutz vorzuenthalten, den sensible personenbezogene Daten verdienen.[55]

54 In diesem Sinne etwa auch § 5 Abs. 2 S. 1 BArchG („Archivgut […], das sich auf natürliche Personen bezieht, darf erst 30 Jahre nach dem Tode des Betroffenen [...]) und § 7 Abs. 1 S. 3 ArchG NRW („Für Archivgut, das sich nach seiner Zweckbestimmung oder nach seinem wesentlichen Inhalt auf eine oder mehrere natürliche Personen bezieht [personenbezogenes Archivgut] endet die Schutzfrist jedoch nicht vor Ablauf von zehn Jahren nach dem Tod der betroffenen Person […]").

55 Diesen Gedanken scheint vordergründig eine Parallele zu dem Nasciturus und Geschäftsunfähigen zu stützen. Denn das, was für die Zeit vor der Geburt gilt, muss grundsätzlich in ähnlicher Weise auch für die Zeit nach dem Tod gelten: Es entspricht einer weitverbreiteten Überzeugung, dass vom Begriff der personenbezogenen Daten, gleichsam einem vorwirkenden Schutzbereich, auch solche Informationen erfasst sind, die einen Nasciturus betreffen. Die Ausweitung dieses Schutzes gründet sich vor allem auf die sich im Gefolge einer zunehmenden Verfeinerung der medizinischen Untersuchungstechniken, wie der Präimplantationsdiagnostik, verändernde Gefährdungslage (vgl. dazu das Gesetz zur Regelung der Präimplantationsdiagnostik vom 21.11.2011, das einen neuen § 3a in das Embryonenschutzgesetz einfügt).
Erst recht sind die Daten eines Geschäftsunfähigen oder eines Minderjährigen schützenswert, selbst wenn diese nicht in der Lage sind, die Verwendung ihrer Daten aktiv mitzugestalten. Die Rechtsordnung stuft diese sogar als besonders schutzwürdig ein. Insoweit kommt es nicht auf die konkrete Möglichkeit einer aktiven Mitwirkung im fraglichen Zeitpunkt an. Entscheidend für die Schutzwürdigkeit ist vielmehr, ob die Verwendung der Daten Auswirkungen auf eine (lebende) natürliche Person haben kann. So werden dann in den genannten Fällen die gesetzlichen Vertreter für berufen gehalten, die Interessen der Betroffenen wahrzunehmen. Die Tatsache, dass eine Person nicht selbst aktiv am Verarbeitungsprozess teilnehmen kann, reicht allein also nicht aus, um eine entsprechende Einschränkung des Schutzbereichs vorzunehmen, solange die Daten grundsätzlich personenbezogen und damit schutzwürdig sind und eine berechtigte Person die Interessen des Verstorbenen in dessen Namen wahrnehmen kann.
Wenn der Gesetzgeber den besonderen Schutz der Daten Minderjähriger sowie die Vor-

Wiewohl das Datenschutzrecht vorrangig die lebende Person sowie deren Persönlichkeits*entfaltung* im Blick hat[56] und nach dem Tod eine Persönlichkeitsveränderung ausgeschlossen ist, löscht der Tod die bereits gereifte Persönlichkeit nicht mit Rückwirkung aus. Das Persönlichkeitsbild lebt weiter und bleibt verletzbar. Die Daten Verstorbener degenerierten zum Plünderungsobjekt der Nachwelt, hätten sie nicht mehr die Rückendeckung des Datenschutzrechts. Das bliebe auch nicht ohne Auswirkung auf das Verhalten und die Persönlichkeitsentfaltung der Lebenden.[57] Denn auf die Vertraulichkeit und Integrität ihrer Daten könnten die Lebenden nicht mehr vertrauen.

Endete der Datenschutz kategorisch mit dem Tod, wäre auch rechtlich nur schwer konstruierbar, warum Personen (allgemein für möglich gehaltene) bindende testamentarische Verfügungen oder postmortale Vollmachten über den Umgang mit den eigenen Daten, insbesondere die Ausübung von Löschungsrechten, für die Zeit nach ihrem Tod treffen können.[58] Denn derartige Verfügungen auf den Todesfall setzen sachlogisch voraus, dass die auszuübenden Rechte, auf die sich die Vollmacht bezieht, nach dem Tod des Account-Inhabers fortbestehen. Soweit die persönlichkeitsbezogenen Daten weiterwirken, gilt das grundsätzlich auch für das an ihnen bestehende Recht. Verlören die betreffenden Daten vom Zeitpunkt des Todes ihren Personenbezug, wäre ein solches Fortwirken aber gerade ausgeschlossen: Mangels personenbezogener Daten gingen die entsprechenden Rechte den Weg allen Fleisches.[59]

Auch andere einfachgesetzliche Regelungen, wie § 35 Abs. 5 SGB I für die Sozialdaten eines Verstorbenen oder die Regelungen in § 22 S. 3 KunstUrhG

verlagerung des Schutzes für den Nasciturus gerade im Hinblick auf die Vorwirkungen einer Datenverwendung für das spätere Leben hochhält, spricht insoweit prima facie manches dafür, diese Erkenntnisse auf die neue Gefährdungslage zu übertragen, die sich durch die Verlagerung zahlreicher alltäglicher Handlungen in die digitale Welt des Internets – in gleichsam umgekehrter Richtung – stetig verändert. Allerdings lässt sich dieser Vorwirkungsgedanke auf die Daten Verstorbener nicht ohne Weiteres bruchfrei übertragen, geht es hier doch nicht um eine Fortwirkung, sondern Nachwirkung – nicht um Genese, sondern Autolyse. Beides ist wesensmäßig verschieden.

56 Es kommt dabei jedoch in diesem Kontext nicht darauf an, ob das Allgemeine Persönlichkeitsrecht in seiner Ausprägung als Grundrecht auf Datenschutz (auch) postmortal geschützt wird, sondern ob das einfachgesetzliche Datenschutzrecht diesen Schutz selbst erfassen will.

57 Dazu im Einzelnen unten IV. 2. a. bb. (1) β, S. 102.

58 Vgl. *Meents,* in: Taeger/Gabel (Fn. 46), § 6 BDSG Rn. 3; *Wedde*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 4.4 Rn. 87.

59 Denkbar ist dann allenfalls ein Rekurs auf individualvertragliche Rechte im Verhältnis zwischen dem Nutzer und dem Diensteanbieter. Solche Rechte verankern die Nutzungsverträge der meisten Diensteanbieter allerdings nicht ausdrücklich. Die Wahrnehmungsberechtigten sind dann auf eine entsprechende erweiternde Auslegung der Verträge oder den *good will* der Diensteanbieter angewiesen.

zum Recht am eigenen Bild, verdeutlichen, dass der Gesetzgeber dem Schutz von Daten auch nach dem Tod einen Stellenwert einräumen will. Indem insbesondere § 35 Abs. 5 S. 1 SGB I die sozialrechtliche Verarbeitungsbefugnis auf Daten Verstorbener erweitert, geht die Vorschrift implizit davon aus, dass die Sozialdaten Verstorbener weiter unter das Sozialgeheimnis fallen und grundsätzlich einen besonderen Geheimhaltungsschutz genießen. So wie diese Regelungen der postmortalen Gefährdung von Daten Verstorbener in bestimmten Lebensbereichen Rechnung tragen, muss die Rechtsordnung auch in ihre datenschutzrechtlichen Wertüberlegungen einstellen, dass die fortschreitende Gefährdung personenbezogener Daten, die mit der Durchdringung des Alltags durch das Internet und den vielfältigen digitalen Angeboten einhergeht, vor den Daten eines Verstorbenen nicht haltmacht.

Bezieht man auch die Daten eines Verstorbenen in den Kreis der personenbezogenen Daten ein,[60] ist der rechtliche Rahmen gesteckt, um einem Missbrauch des Datenbestandes nach dem Tod entgegenzuwirken. Selbst wenn die verfassungsrechtlichen Vorgaben einen solchen Schutz nicht zwingend gebieten sollten,[61] ist jedenfalls eine entsprechende Auslegung der einfachgesetzlichen Regelungen angezeigt. Das entspricht auch der Zielvorstellung der Datensparsamkeit und dem „engen Gebot der Zweckbindung“, [62] von dem das Datenschutzrecht der Telemediendienste durchdrungen ist: Den Inhabern von Daten sollen die Informationen über Personen zeitlich grundsätzlich nur so lange zukommen dürfen, wie diese Vorhaltung zur Bereitstellung von Telemedien erforderlich ist (vgl. § 12 Abs. 2 TMG). Die Bestands- und Nutzungsdaten sind insbesondere zu löschen, wenn diese für das zugrunde liegende Vertragsverhältnis nicht mehr benötigt werden und keine sonstige Erlaubnisnorm einschlägig ist.[63] Mit dem Gedanken der Datensparsamkeit korrespondiert in dem Umfang ein Recht auf Verges-

60 Auch der BGH geht in seinem Beschluss vom 30.7.1990, NJW 1991, 568, vom Schutz des Namens und Geburtsdatums von Erblassern aus.

61 Dazu aber unten IV 2. a. bb., S. 100 ff.

62 *Spindler/Nink*, in: Spindler/Schuster (Fn. 38), § 12 TMG Rn. 7 m.w.N.; *Roßnagel*, NZV 2006, 281 (285).

63 Diese Rechte muss der Betroffene gem. § 12 Abs. 3 TMG über § 35 Abs. 2 S. 2 Nr. 1 bzw. Nr. 3 BDSG geltend machen; vgl. OLG Bamberg, MMR 2006, 481 (482); *Spindler/Nink*, in: Spindler/Schuster (Fn. 38), § 14 TMG Rn. 5. Für (kostenlose) Suchmaschinen bspw. bedeutet dies, dass eine Speicherung über den jeweiligen Suchvorgang hinaus mangels Erforderlichkeit nicht durch § 15 Abs. 1 TMG gedeckt ist, vgl. *Ott*, MMR 2009, 453. Abrechnungsdaten hingegen könnten gem. § 15 Abs. 4 TMG weiterhin verwendet werden; im Falle einer Aufbewahrungspflicht sind die Daten zu sperren, statt zu löschen. Zu geplanten, weitergehenden Löschungspflichten der Diensteanbieter siehe den Gesetzesentwurf des Bundesrates zur Änderung des Telemediengesetzes vom 3.8.2011, BT-Drucks. 17/6765, S. 1 ff.

senwerden, das insoweit dem deutschen Datenschutzrecht bereits eingeschrieben ist.

Einer Einbeziehung von Daten Verstorbener in den datenschutzrechtlichen Schutzgegenstand widerstreitet auch die Europäische Datenschutzrichtlinie nicht.[64] Sie benennt den Schutz von Verstorbenen zwar nicht ausdrücklich. Die Mitgliedstaaten sind aber grundsätzlich nicht gehindert, den Schutzbereich auszudehnen, soweit dabei das Unionsrecht im Übrigen Beachtung findet.[65] Die datenschutzrechtlichen Bestimmungen des BDSG und des TMG versagen dem digitalen Nachlass mithin nicht seine postmortalen Schutzwirkungen, sondern gewähren einen postmortalen Schutz personenbezogener Daten.[66]

(2) Schlussfolgerungen – Vergleichsfälle aus der „analogen Welt"

Bringt man die Daten Verstorbener unter den Begriff der personenbezogenen Daten, ist damit freilich die entscheidende Frage noch nicht beantwortet, ob die dann anwendbaren Vorschriften des Datenschutzrechts die Freigabe der Accountdaten *gegenüber den Erben* untersagen. Dafür bedürfte es einer datenschutzrechtlichen Geheimhaltungspflicht des Diensteanbieters sub specie des Binnenverhältnisses zwischen Erbe und Erblasser. Gesetzliche Antragsrechte und Löschungsansprüche Lebender, z.B. nach §§ 19, 20, 34 und 35 BDSG i.V.m. § 12 Abs. 3 TMG, reichen insoweit nicht hin. Sie beziehen sich nicht auf die Herausgabe von Zugangsinformationen gegenüber den Erben. Auch das neue Recht auf Vergessenwerden im Internet des Art. 17 der geplanten Europäischen Datenschutzgrundverordnung[67] wird diese Regelungslücke nicht füllen. Es regelt

64 Ebenso der Entwurf der Europäischen Datenschutzgrundverordnung (vom 25.2.2012, COM [2012] 11 endg.): Den Begriff „betroffene Person" beschreibt die Verordnung offen (Art. 4 Abs. 1). Sie versteht darunter jede identifizierbare natürliche Person, namentlich „eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche oder jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind". Unter diesen Begriff kann auch der Verstorbene fallen, muss es aber nicht. Die Verordnung lässt insoweit – ebenso wie die Datenschutzrichtlinie – Interpretationsspielraum.

65 Vgl. EuGH, Rs. C-101/01 (Lindquist), Slg 2003, I-12992 (13027, Rn. 98 f.); *Dammann/Simitis*, EG-Datenschutzrichtlinie, 1997, Art. 2 Erl. 1; *Dammann*, in: Simitis (Fn. 46), § 3 BDSG Rn. 18.

66 So auch *Bergmann/Möhrle/Herb*, BDSG, Losebl. (Stand: Sept. 2001), § 3 Rn. 7.

67 Vgl. zu ihr Fn. 64.

ausschließlich die Befugnis zur Datenverarbeitung im Verhältnis zwischen Nutzer und Diensteanbieter. Eine Norm aber, die den Internetnutzer datenschutzrechtlich ausdrücklich gegen den Zugriff seiner Erben auf den eigenen Account abschirmt, fehlt.

Für vergleichbare Fälle aus der analogen Welt finden sich solche Vorschriften zur Geheimhaltungspflicht gegenüber dem Erben durchaus: namentlich für die Einsichtnahme in die Krankenpapiere eines Verstorbenen[68] oder andere Privatgeheimnisse der Offline-Welt, etwa das anwaltliche und notarielle Beratungsgeheimnis (§ 43a Abs. 2 S. 1 BRAO, § 18 Abs. 1, Abs. 2 Hs. 2 BNotO) und das Archivgeheimnis (§ 5 Abs. 2 S. 1 BArchG). Die Verletzung von Privatgeheimnissen sanktioniert der Gesetzgeber mit dem scharfen Schwert des Strafrechts – und dies ausdrücklich auch für den Fall der Offenbarung von Geheimnissen nach dem Tod des Betroffenen: Die Verschwiegenheitspflicht besteht nach dem Normbefehl des § 203 Abs. 4 StGB für den Arzt und andere berufliche Geheimnisträger,[69] wie Steuerberater und Berufspsychologen, unverändert als Kontinuum fort.[70] Der Tod zerschneidet das persönliche Band des Vertrauens zwischen Arzt und Patient mithin nicht.

Einsicht nehmen darf der Erbe in die Krankenunterlagen nur, soweit der Verstorbene ausdrücklich eingewilligt hat bzw. mutmaßlich[71] eingewilligt hätte oder

68 Vgl. auch BGH, NJW 1983, 2627; BSG, NJW 1986, 3105; BAG, NJW 2010, 1222 (1222); OLG München, ZEV 2009, 40; *Bender*, Das postmortale Einsichtsrecht in Krankenunterlagen, 1998, S. 23 ff.; zur Frage, ob einem Erben entsprechende Auskunftsrechte gegenüber dem Krankenversicherer bzw. gegenüber dem früheren Arbeitgeber zustehen: LAG Berlin, RDV 1990, 266; *Gola/Schomerus*, in: dies. (Hrsg.), BDSG, 10. Aufl. 2010, § 6 BDSG Rn. 3.

69 Für manche Geheimhaltungspflichten bestehen strafrechtliche Sondernormen als Leges speciales, etwa nach § 355 StGB.

70 Die Schweigepflicht von Ärzten geht bereits in die Antike zurück; der Eid des *Hippokrates* verpflichtete zum Stillschweigen über die persönlichen Angelegenheiten des Patienten. Ähnlich auch heute § 9 Abs. 1 S. 1 und 2 Deutsche Ärztinnen und Ärzte-(Muster-) Berufsordnung (MBO). Dort heißt es: „Ärztinnen und Ärzte haben über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist – auch über den Tod der Patientin oder des Patienten hinaus – zu schweigen. Dazu gehören auch schriftliche Mitteilungen der Patientin oder des Patienten, Aufzeichnungen über Patientinnen und Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde." Die MBO bildet die Folie für die Berufsordnungen der Landesärztekammern, die die standesrechtlichen Berufspflichten der Ärzte festschreiben. Für einen abnehmenden sachlichen Gehalt der postmortalen Schweigepflicht immerhin aber OLG Düsseldorf, NJW 1959, 823; damit (für den Fall, dass das Geheimhaltungsinteresse durch die geänderte Sachlage aufgrund des Todes überholt ist) sympathisierend auch BGHZ 91, 393 (398); dagegen aber die wohl überwiegende Meinung; vgl. *Bender* (Fn. 68), S. 303 m.w.N.

71 Eine solche mutmaßliche Einwilligung des Erblassers als Erklärungssurrogat kommt beispielsweise in Betracht, wenn der behandelnde Arzt als Zeuge vernommen werden soll, um Zweifel an der Geschäfts- und Testierfähigkeit des Erblassers auszuräumen; BGHZ

vermögensrechtliche Ansprüche im Raum stehen, z.B. Ersatzansprüche wegen Kunstfehlern.[72] Dem liegt die gesetzgeberische Vorstellung zugrunde, dass das bipolare Vertrauensverhältnis zwischen dem Geheimnisträger und dem Patienten eines besonderen Schutzes gegen das Eindringen Dritter bedarf. Denn nur auf dem Fundament der ärztlichen Schweigepflicht kann das für die Behandlung erforderliche Vertrauen zwischen Arzt und Patient gedeihen.[73] Soll der Geheimnisschutz seine Funktion sachgerecht erfüllen, bedingt das auch die Fortwirkung der Schweigepflicht über den Tod hinaus.[74]

Die Entbindung von der Schweigepflicht teilt damit die höchstpersönliche Natur des Persönlichkeitsrechts, das es schützen soll.[75] Es handelt sich um eine dem Patienten vorbehaltene Aufgabe, die als nichtvermögensrechtliches Recht nicht im normalen Erbgang auf Dritte übergeht. Daran ändert auch der Übergang des Strafantragsrechts auf die Angehörigen nach § 77 Abs. 2 i.V.m. § 205 Abs. 2 S. 2 StGB nichts.[76] Denn das Straf*antragsrecht* und der Straf*grund* verfolgen unterschiedliche Ziele: Das Strafantragsrecht soll die Offenbarung eines Geheimnisses ahnden, nicht aber die Durchbrechung der Schweigepflicht ermögli-

91, 392 (399); BayObLG, NJW 1987, 1492 (1493); BayObLG, NJW-RR 1991, 1287; *Müller-Christmann*, in: BeckOK BGB (Fn. 22), § 1922 Rn. 43; *Bender* (Fn. 68), S. 319, 403 ff. Zum Schutz des postmortalen Persönlichkeitsrechts des Erblassers ist dabei entscheidend auf das soziale Interaktionsverhalten des Verstorbenen, nicht auf das Durchschnittsverhalten von Menschen abzustellen. Ob der mutmaßliche Wille den Einblick in die Krankenunterlagen überhaupt rechtfertigen kann, wird allerdings unterschiedlich beantwortet. Vgl. dazu (zustimmend) *Kuchinke*, Ärztliche Schweigepflicht, Zeugniszwang und Verpflichtung zur Auskunft nach dem Tod des Patienten, in: Gedächtnisschrift für Küchenhoff, 1987, 371 (378); (ablehnend) *Solbach*, DRiZ 1978, 204 (205); *Schönberger* (Fn. 51), S. 211 ff. (sie schlägt eine Abwägung zwischen den individuellen Belangen der Angehörigen mit dem Allgemeininteresse an der Wahrung der postmortalen Verschwiegenheit vor).

72 Vgl. BGH, NJW 1983, 2627 (2628): Dem Einsichtnahmeanspruch, der ursprünglich dem Patienten als Nebenanspruch aus dem Behandlungsvertrag zusteht, ist insoweit ein vermögensrechtlicher Gehalt eigen. In diesem Umfang kann der Anspruch gem. § 1922 Abs. 1 BGB auf die Erben übergehen, soweit nicht sein Wesen aus besonderen Gründen einem Gläubigerwechsel entgegensteht. Vgl. auch die Anmerkungen von *Giesen*, JZ 1984, 279 und *Bosch*, FamRZ 1983, 109; *Schönberger* (Fn. 51), S. 208 ff.; OLG München, VersR 2009, 982; für eine einheitliche Rechtsnatur der Entbindungsbefugnis demgegenüber *Bender* (Fn. 68), S. 381; ausführlich zum Ganzen *Hess*, ZEV 2006, 479 ff.

73 Vgl. BVerfG, NJW 1972, 1123 (1124); BGH, NJW 1992, 763 (765).

74 Vgl. dazu auch *Bender* (Fn. 68), S. 303 f.

75 Vgl. dazu etwa bereits RGSt 71, 21 (22); OLG Celle, NJW 1965, 362 sowie die Nachweise bei *Bender* (Fn. 68), S. 352 mit Fn. 1 ff. u. S. 384; *Schönberger* (Fn. 51), S. 208.

76 So aber *Solbach*, DRiZ 1978, 204 f.; zur Problematik auch *Bender* (Fn. 68), S. 310 m.w.N.

chen.[77] Auch die unterschiedlichen Adressatenkreise der Normen weisen in diese Richtung: Im einen Fall sind dies die Erben, im anderen Fall die Angehörigen.

Die Einsichtnahmen in die Krankenakte und den Internet-Account liegen wertungsmäßig auf gleicher Stufe: Der Zugriff auf die geheimhaltungsbedürftigen Informationen ist in beiden Fällen jeweils nur unter Vermittlung eines Geheimnisträgers möglich. Der Arzt und der Telemediendiensteanbieter sind gleichsam „Gatekeeper". Beide Berufsgruppen kommen typischerweise mit Privatgeheimnissen ihrer Vertragspartner in Berührung und dringen tief in deren Privatsphäre ein. In beiden Fällen bedingen sich der Einblick in höchstpersönliche Daten des Erblassers und der Schutz des dem jeweiligen Dienstleister entgegengebrachten Geheimhaltungsvertrauens. Denn Letzteres ist integrale Voraussetzung für die gedeihliche Entwicklung der mit tiefen Einblicken in die Persönlichkeitssphäre verbundenen Vertragsbeziehung. Müsste der jeweilige Vertragspartner damit rechnen, dass seine Daten nach dem Tod Dritten offenbart werden, würde er manche Informationen seinem Vertragspartner womöglich nicht anvertrauen. Der Patient wie der Account-Nutzer müssen sich darauf verlassen können, dass ihre Vertragspartner über alle sensiblen Daten, auf die sie im Rahmen ihrer Tätigkeit Zugriff erlangen, Stillschweigen wahren, die Informationen insbesondere nicht Dritten zugänglich machen.

Einen „Schönheitsfehler" hat der Vergleich allerdings: Der Internetdiensteanbieter ist kein strafrechtlicher Geheimnisträger im Sinne des § 203 StGB. Für ihn fehlt eine dem § 203 Abs. 4 StGB entsprechende klare Regelung.[78] Spiegelbildlich dazu fehlt ihm auch ein Zeugnisverweigerungsrecht im Strafverfahren.[79] Nicht immer sind auch die in Online-Accounts hinterlegten Informationen so sensibel wie die Berichte einer Patientenakte, zum Teil sind sie umgekehrt aber sensibler. Man denke etwa an einen im Cyberspace ausgetragenen Dialog über Vererbungsstrategien oder den Online-Flirt.

77 BGH, NJW 1983, 2627 (2629); zur Wahrnehmungsberechtigung für zivilrechtliche Ansprüche bei Verletzung der ärztlichen Schweigepflicht etwa *Schönberger* (Fn. 51), S. 205 f.

78 § 203 Abs. 4 StGB erfasst entsprechend dem fragmentarischen Charakter des Strafrechts allerdings nur die strafrechtliche Verantwortung des Geheimnisträgers, nicht aber dessen regelmäßig weitergehende zivilrechtliche und berufsordnungsrechtliche Pflichtenstellung. Rechtspolitisch ist die Einbeziehung des Anbieters von Telemediendiensten in die Strafnorm des § 203 StGB erwägenswert.

79 Für den Arzt und andere berufliche Geheimnisträger etabliert der Gesetzgeber ein Zeugnisverweigerungsrecht in § 53 Abs. 1 Nr. 3 StPO bzw. § 383 Abs. 1 Nr. 6 ZPO. Aufgrund der gesetzlichen Verpflichtung der Telemediendiensteanbieter nach § 13 Abs. 4 Nr. 3 TMG trifft auch diese eine gesetzliche Verpflichtung zur Geheimhaltung von Tatsachen, die ihnen kraft ihres Berufes anvertraut sind. Ihnen ist daher *im Zivilprozess* ein Zeugnisverweigerungsrecht zuzugestehen (§ 383 Abs. 1 Nr. 6 ZPO).

Das TMG und die strafrechtlichen Schutznormen verfolgen immerhin eine ähnliche Schutzrichtung. Sie begründen beide eine Geheimhaltungsverpflichtung: Das TMG verpflichtet die Diensteanbieter namentlich in seinem § 13 Abs. 4 Nr. 3 sicherzustellen, dass die Nutzer Telemedien gegen die Kenntnisnahme Dritter geschützt in Anspruch nehmen können. Das impliziert auch die Pflicht, Dritten keinen Zugang zu dem Account zu eröffnen.[80] Dem Diensteanbieter ist es verwehrt, sich darüber aus eigener Machtvollkommenheit hinwegzusetzen. Die Pflicht zur Geheimhaltung ist insoweit eine vertragliche Hauptpflicht, die die unbefangene Inanspruchnahme der Dienstleistungen und die Vertraulichkeit der dort hinterlegten Informationen sichert.[81] Dass dieser Schutz nach dem Tod fortbesteht, sagt die Vorschrift nicht ausdrücklich.[82] Das entspricht aber ihrer ratio.

bb) Verfassungsrechtlicher postmortaler Persönlichkeitsschutz

Ein solcher postmortaler Schutz kann auch Ausdruck und Folge eines nachwirkenden verfassungsrechtlichen Persönlichkeitsschutzes sein: Das Grundgesetz gewährt einen postmortalen Schutz der Persönlichkeit des Verstorbenen, wenngleich das Persönlichkeits*recht* mit dem Tode erlischt.[83] Dieser erweist sich nicht

80 Der Telemedienanbieter gleicht dem Vermieter eines Tresors, der – je nach technischer Ausgestaltung des Dienstes – über den verwahrten Inhalt nicht unbedingt Kenntnis haben muss, aber den Schlüssel für den Zugang zum Inhalt in den Händen hält.

81 Zu einer möglichen Strafbarkeit wegen § 202a bzw. § 202c StGB siehe unten S. 116.

82 Entscheidend ist aber nicht, dass eine ausdrückliche gesetzliche Anordnung der Geheimhaltungspflicht über den Tod hinaus fehlt, sondern dass die Geheimhaltungspflicht nicht ausdrücklich aufgehoben ist. Entsprechend versteht auch die strafrechtliche Literatur die Vorschrift des § 203 StGB insoweit überwiegend als lediglich deklaratorisch, nicht aber als konstitutiv. Denn sie ist Ausdruck eines verfassungsrechtlichen Gebots postmortalen Persönlichkeitsschutzes. *Lenckner/Eisele*, in: Schönke/Schröder (Hrsg.), StGB, 28. Aufl. 2010, § 203 Rn. 70.

83 Vgl. etwa *Höfling*, in: Sachs (Hrsg.), GG, 5. Aufl. 2009, Art. 1 Rn. 39. Er sieht bereits bei einer auch nur drohenden Verletzung der Menschenwürde durch einen Privaten den Staat dazu verpflichtet, die Gefahr effektiv abzuwehren; einen verfassungsrechtlichen Persönlichkeitsschutz des Verstorbenen demgegenüber ablehnend etwa *Hoch*, Fortwirken zivilrechtlichen Persönlichkeitsschutzes nach dem Tode, 1975, S. 40 ff., der nur ein „Recht der Hinterbliebenen zur Wahrung des Andenkens an den Verstorbenen" (a.a.O., S. 176 ff.) anerkennen will; ähnlich *Lehmann*, Postmortaler Persönlichkeitsschutz, 1973, S. 120 ff., die – wie zahlreiche andere in der zivilrechtlichen Literatur – nur einen mittelbaren Persönlichkeitsschutz der Verstorbenen über den gleichsam verlängerten Arm der Persönlichkeitsrechte der Hinterbliebenen konstruiert (sog. *Andenkensschutzlehre*); ebenso etwa *Claus,* Postmortaler Persönlichkeitsschutz im Zeichen allgemeiner Kommerzialisierung, 2004, S. 66 ff., 96 ff.; *Schönberger* (Fn. 51), S. 45 ff.; zu Recht kritisch *Luther*,

als ein Aliud, sondern als ein wesensgleiches Minus zum verfassungsrechtlichen Persönlichkeitsschutz für die Lebenden.[84] Seine Grundlage findet der postmortale Schutz in dem Achtungsanspruch, der von der Menschenwürde des Art. 1 Abs. 1 GG ausgeht.

(1) Inhalt des verfassungsrechtlichen postmortalen Persönlichkeitsschutzes

Art. 1 Abs. 1 GG umhegt zwar nur den Kernbereich der menschlichen Existenz gegen schwere Beeinträchtigungen. Sein Schutz für die Toten kann insoweit auch nicht weiter gehen als der Schutz der Lebenden. Das schließt einen verfassungsrechtlichen Schutz des die Person überdauernden Ergebnisses der lebenslangen Persönlichkeitsentfaltung und der mit ihm verbundenen Achtungserwartung vor postmortalen Verfälschungen aber nicht aus. Die als Teile der Menschenwürde geschützten Werte der Persönlichkeit überdauern als personaler Eigenwert die durch den Tod begrenzte Rechtsfähigkeit ihres Trägers.[85] Dass der Verstorbene seine Rechte nicht mehr selbst verteidigen kann,[86] heißt mithin nicht, dass der Diensteanbieter den höchstpersönlichen Informationen des Verstorbenen nach dem Tod keinen Schutz mehr angedeihen lassen müsste.

Postmortaler Persönlichkeitsschutz nichtvermögenswerter Persönlichkeitsrechte, 2009, S. 88 ff.

84 *Bender* (Fn. 68), S. 306 und 447, a.A. *Luther* (Fn. 83), S. 112.

85 Siehe nur BVerfGE 30, 173 (194). Bereits im Kontext der Frage, wem die Befugnis zur Veröffentlichung von Tagebüchern eines Verstorbenen zusteht, hat der BGH die Fortwirkung des Urheberpersönlichkeitsrechts über den Tod des ursprünglichen Rechtsträgers anerkannt, BGHZ 15, 249 (259) – Cosima Wagner; vgl. auch LG München, UFITA 20, 230 ff. – von Witzleben; ***Koebel,*** NJW 1958, 936 (937); *Hubmann,* Das Persönlichkeitsrecht, 1953, S. 340 ff.; *Nipperdey,* UFITA 30, 1 (20 f.); *von Gamm,* NJW 1955, 1826.

86 Das Privatrecht tut sich mit dieser Rechtskonstruktion schwer. Denn in seiner relationalen anspruchsbasierten Schutzrichtung bedarf es zur Begründung von Rechten einer rechtsfähigen Person. Das Privatrecht vermag daher nicht zufriedenstellend zu beantworten, welchem Subjekt die aus dem postmortalen Persönlichkeitsrecht erwachsenden Rechte zugeordnet werden sollen. Vgl. zur Diskussion um „subjektlose Rechte“ etwa *Claus* (Fn. 83), S. 54 ff.; *Lehmann* (Fn. 83), S. 105 ff.; *Heldrich*, Der Persönlichkeitsschutz Verstorbener, in: Festschrift für Heinrich Lange, 1970, 163 (168); *Schönberger* (Fn. 51), S. 14 f., 74 ff.; *Luther* (Fn. 83), S. 64 ff. Aufgrund der hieraus folgenden Wehrlosigkeit des Toten im Kampf der Meinungen fordert *Pabst*, NJW 2002, 999 (1004) differenzierte Kriterien für die Verletzung des Menschenwürdetatbestandes, die über den Schutz gegenüber diffamierender Schmähkritik hinausgehen.

(α) Postmortaler Persönlichkeitsschutz als Ausdruck der Achtung der Würde des Verstorbenen

Postmortal sind verfassungsrechtlich zweierlei Ausprägungen des Menschseins geschützt: der „allgemeine Achtungsanspruch" als autonomes Wesen mit personalem Eigenwert, der den Verstorbenen davor bewahrt, herabgewürdigt oder erniedrigt zu werden, und der „sittliche, personale und soziale Geltungswert", der durch die eigene Lebensleistung erworben wurde.[87] Mit dem Fortdauern der Menschenwürde geht also eine Verpflichtung des Staates einher, Verstorbene auch postmortal vor Ausforschung der engeren persönlichen Lebenssphäre, Erniedrigung oder Ächtung zu schützen und zu verhindern, dass sie in einer herabwürdigenden Weise verächtlich gemacht oder verspottet werden.

Um das Risiko einer Verletzung des allgemeinen Achtungsanspruchs oder personalen Geltungswerts durch Veröffentlichung entwürdigender Darstellungen – den typischen Fall postmortaler Persönlichkeitsverletzungen – geht es im Falle des digitalen Nachlasses des durchschnittlichen Internetnutzers regelmäßig nicht. Denn mit der Herausgabe der Account-Schlüssel erhält nur der engste Kreis der Angehörigen Zugang zu den sensiblen Daten und revidiert auf dieser Grundlage gegebenenfalls sein bisheriges Bild vom Verstorbenen (eventuell auch zum Positiven).

Das Lebensbild eines Menschen kann aber nicht nur durch den fortwirkenden Schutz des Lebensbildes missachtende Ehrverletzungen in Presseveröffentlichungen oder in der öffentlichen Meinung beeinträchtigt werden,[88] sondern auch dadurch, dass Dritte Einblick in intime Details der eigenen Persönlichkeit erhalten, die ihnen nicht zuteilwerden sollen. Zum postmortalen Persönlichkeitsschutz gehört es im Interesse eines umfassenden Persönlichkeitsschutzes im digitalen Zeitalter namentlich, dass der Einzelne auch nach seinem Tod gegen die Ausforschung seiner Persönlichkeit durch unbefugte Dritte geschützt bleibt. „Dritte" in diesem Sinne können auch Erben oder eigene Angehörige sein. Denn diese sind nicht unbedingt legitime Treuhänder der Persönlichkeitsrechte des Verstorbe-

87 Dieser Schutz ist absolut und einer Güterabwägung nicht zugänglich, da er sich aus der unantastbaren Menschenwürde ableitet; vgl. auch BVerfG, NJW 2001, 591 (594); BVerfG, NJW 2001, 2957 (2958); ferner BVerfGE 93, 266 (293).

88 Kritisch gegenüber einer Beschränkung des postmortalen Persönlichkeitsschutzes auf den Würdeschutz: *Herdegen,* in: Maunz/Dürig (Hrsg.), GG, 55. Lfg., Mai 2009, Art. 1 Rn. 57; *Starck* in: v. Mangoldt/Klein/Starck, GG, 5. Aufl. 2005, Art. 1 Rn. 211; *Stern*, Staatsrecht III/1, 1988, S. 1052 f.

nen.[89] Schließlich besteht der Schutz des postmortalen Persönlichkeitsrechts nicht um der Nachfahren und ihrer Willfährigkeit, sondern um des Verstorbenen willen.[90]

(β) Postmortaler Geheimnisschutz im Interesse der Lebenden: Postmortaler Persönlichkeitsschutz als Schutz des Geheimhaltungsvertrauens der Lebenden

Ein solcher nachwirkender Persönlichkeitsschutz kann insbesondere dann verfassungsrechtlich geboten sein, wenn die *künftige, postmortale* Nutzung von Daten Ausstrahlungen auf die *heutige* Offenbarung dieser Daten hat. Sonst sehen sich die Nutzer durch das Fehlen eines dauerhaften Schutzes ihrer Daten schon zu Lebzeiten in der freien Entfaltung ihrer Persönlichkeit behindert. Wenn „die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“[91], hat das unmittelbar Auswirkungen auf die Persönlichkeitsentfaltung im Hier und Jetzt. Der nachwirkende Persönlichkeitsschutz entpuppt sich insoweit als Garant der vollen Persönlichkeitsentfaltung zu Lebzeiten – gleichsam als eine Vervollkommnung des lebenszeitigen Schutzes. An der Art, wie eine Rechtsordnung mit den Toten umgeht, lässt sich namentlich ablesen, wie sie es mit den Lebenden hält. Ein sachgerechter Persönlichkeitsschutz muss daher auch verfassungsrechtlich bereits auf der Stufe der *Persönlichkeitsgefährdung* der Lebenden beginnen.[92] Nur dann lässt sich den Gefahrenlagen[93] angemessen Rechnung tragen, die sich mit dem besonders intensiven Eindringen in die Persönlichkeitssphäre von Nutzern im Internet verbinden:[94]

89 Das spricht insbesondere gegen die vielfach vertretene Andenkensschutzlehre, die als Träger des postmortalen Persönlichkeitsrechts nicht die Verstorbenen, sondern deren Angehörige versteht (vgl. zu ihr bereits oben Fn. 83).

90 In diesem Sinne bereits *Hubmann*, Das Persönlichkeitsrecht, 1953, S. 245 f.; vgl. auch *Luther* (Fn. 83), S. 92.

91 BVerfGE 65, 1 (43).

92 BVerfGE 118, 168 (184 f.) – Kontostammdaten.

93 Siehe dazu ausführlich *Trute*, JZ 1998, 822 (823) m.w.N.; *Roßnagel*, ZRP 1997, 26 (27 f.).

94 Dieses erhebliche Schutzbedürfnis wird nicht zuletzt an der Entscheidung des BVerfG zu Online-Durchsuchungen vom 27.2.2008 sichtbar: Die Allgegenwärtigkeit informationstechnischer Systeme und die zentrale Bedeutung ihrer Nutzung für die private Lebensgestaltung nahezu aller Bürger bringen eine neue Bedrohungslage mit sich, welche die anderen Grundrechte und bisherigen Ausprägungen des Allgemeinen Persönlichkeitsrechts nicht in ausreichendem Maße zu erfassen vermögen. Unter Rückgriff auf diesen Grundgedanken ist das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als weitere Ausprägung des Allgemeinen Persönlichkeits-

Der Bedeutungszuwachs von Internetplattformen bringt es mit sich, dass personenbezogene Daten der Nutzer über ihre Accounts in bislang nie da gewesener Weise gebündelt werden und somit einen tiefen Einblick in das Online-Verhalten der Account-Inhaber gewähren. An sich wenig bedeutsame Daten können durch ihre elektronische Verknüpfung und Auswertung einen neuen sensiblen Informationsgehalt generieren, der die Persönlichkeitsstruktur eines Menschen bis in seine letzten Winkel auszuleuchten vermag. Die Profile in sozialen Netzwerken machen mitunter Bereiche der Intimsphäre zugänglich, die bislang allenfalls in einem Tagebuch offen gelegt wurden.[95] Hinzu treten die bestechende Leichtigkeit, mit der die personenbezogenen Daten im Internet generiert werden, und der Detaillierungsgrad, den die Nutzerinformationen erreichen können, sowie die in Zeit und Raum entgrenzte Öffentlichkeit, die sie herstellen können.

Soweit Kommunikationsvorgänge zwischen Personen betroffen sind, kann der Persönlichkeitsschutz in der digitalen Kommunikation bei konsequenter Fortschreibung der Rechtsprechung des BVerfG Ausfluss einer verfassungsrechtlichen Schutzpflicht aus Art. 10 Abs. 1 GG sein. Das Telekommunikationsgeheimnis hat zwar einen zeitlich begrenzten Schutzradius. Es erstreckt seinen Schutz nur auf Telekommunikationsvorgänge, nicht aber auf nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherte Inhalte und Umstände der Kommunikation. Darin spiegelt sich der spezifische Schutzzweck des Art. 10 Abs. 1 GG: Er soll die Vertraulichkeit einer drittvermittelten Kommunikation (unabhängig vom jeweiligen Inhalt und von der verwendeten Form der unkörperlichen Nachrichtenübermittlung) vor staatlichem Zugriff schützen. Seine Gewährleistung der „Privatheit auf Distanz" will die Teilnehmer des Austauschvorganges so stellen, wie sie ohne Inanspruchnahme der Telekommunikationstechnologie, also bei unmittelbarer Kommunikation in beiderseitiger Gegenwart, stünden.[96] Wenn die Daten den Herrschaftsbereich des zur Nachrichtenübertragung eingeschalteten Dritten in einer Weise ver-

rechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entstanden (BVerfGE 120, 274 [302 ff.]; *Hoffmann-Riem*, JZ 2008, 1009 ff.; vgl. zum Ganzen auch *Roggan* [Hrsg.], Online-Durchsuchungen, 2008); zur Kritik vgl. bei *Britz*, DÖV 2008, 411 (412); *Kühling/Seidel/Sividris* (Fn. 45), S. 69.

95 Anders als dort sind sie aber (regelmäßig bewusst) in einer über den Tod hinauswirkenden Weise durch eine Zugangssperre digital gegen den unbefugten Zugriff Dritter gesichert. Vgl. zu den Unterschieden auch unten S. 107.

96 BVerfGE 100, 313 (366); BVerfG, MMR 2006, 217 (220). Die technikspezifischen Risiken der unbemerkten Kenntnisnahme der Inhalte oder der näheren Umstände eines Telekommunikationsvorgangs sollen dadurch ausgeglichen werden. Den Diensteanbietern ist es daher zu diesem Zweck untersagt, sich oder anderen über das erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen.

lassen haben, die dem Empfänger das Löschen der Kommunikationsinhalte und -verkehrsdaten am eigenen Rechner ermöglicht, endet dieser Schutz daher.[97] Kommunikationsvorgänge eines E-Mail-Accounts stehen aber, auch wenn sie als solche abgeschlossen sind, [98] umgekehrt so lange unter dem Schutz des Art. 10 Abs. 1 GG, wie die Nachrichten noch beim Provider gespeichert sind. Für die Daten eines IMAP-E-Mail-Accounts hat das BVerfG das ausdrücklich entschieden.[99] Denkt man die Rechtsprechung des BVerfG zu IMAP-E-Mail-Accounts konsequent weiter, geht mit ihr eine Perpetuierung des Schutzes von Kommunikationsvorgängen einher. Nicht nur bei diesen, sondern auch bei der Nachrichtenzustellung über den Vermittlungskanal sozialer Netzwerke, wie z.B. *Facebook* oder *Xing*, verbleiben die sensiblen Informationen grundsätzlich weiter im Herrschaftsbereich des Providers. Solange besteht dann auch die spezifische Gefährdungslage, vor der Art. 10 Abs. 1 GG schützen soll: der technisch bedingte Mangel an Beherrschbarkeit und die Gefahr, dass Dritte Einblick in Kommunikationsvorgänge nehmen, die unter Einschaltung eines Kommunikationsmittlers stattgefunden haben. Erfasst ist dann vom Schutz des Art. 10 Abs. 1 GG nicht nur die unmittelbare Signalübertragung, für die das Telekommunikationsgeheimnis ursprünglich konzipiert war,[100] sondern auch der ruhende Kommunikationsvorgang.

Dieser Ausweitung des Schutzbereichs ist grundrechtsdogmatische Sensibilität eigen.[101] Denn die sich in der Kommunikation manifestierende Persönlichkeitsentfaltung mittels Telekommunikationsanlagen verlässt dann ihren ursprünglichen Schutzkern der Integritätsgewährleistung für laufende Telekommunikationsvorgänge. Sie ist aber konsequent. Sie setzt den Art. 10 Abs. 1 GG innewohnenden Auftrag des Schutzes drittvermittelter Privatheit konsequent auf neue Kommunikationsmedien und ihre Gefährdungslagen um. Noch auf Servern

97 BVerfG, MMR 2006, 217 ff.; BVerfG, MMR 2009, 673 (674 f.); *Eckhardt*, DuD 2006, 365 ff.; *Hanebeck/Neunhoeffer*, K&R 2006, 112 (113 f.)

98 Art. 10 Abs. 1 GG schützt die Übertragung von Daten zwischen Computern über Standleitungen genauso wie z.B. den E-Mail-Verkehr, unabhängig davon, ob die Übertragung „in Echtzeit" erfolgt oder ob die Informationen auf Servern zwischengespeichert werden. Vgl. zu § 88 TKG bereits oben S. 89.

99 BVerfG MMR 2009, 673 (674 f.). Dazu auch *Gaede*, StV 2009, 96 ff.; *Härting*, CR 2009, 581 (582 f.); *Klein*, NJW 2009, 2996 ff.

100 Insofern unterscheidet sich das einfachrechtliche Fernmeldegeheimnis bei dieser Sichtweise von dem verfassungsrechtlichen. Statische Prozesse des Speicherns von Nachrichten auf dem Account erfasst jenes nicht, sondern es knüpft an Telekommunikationsvorgänge an und adressiert ausschließlich Telekommunikationsanbieter. Unter einem Telekommunikationsvorgang versteht das TKG dabei den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen (§ 3 Nr. 22 TKG).

101 Kritisch etwa *Krüger*, MMR 2009, 680 (682).

des Diensteanbieters gespeicherte individuelle Kommunikationsvorgänge zwischen Personen bewegen sich nämlich in einer von keinem der Kommunikationsteilnehmer beherrschbaren Sphäre. So kann der Diensteanbieter während der Speicherung der Daten auf eigenen Servern unbemerkt auf die Kommunikationsvorgänge zugreifen. Dass kein laufender Telekommunikationsvorgang mehr stattfindet und der Nutzer Nachrichten schon zur Kenntnis genommen hat, ändert daran nichts. In der Sphäre Dritter gespeicherte Kommunikationsvorgänge berühren damit das Telekommunikationsgeheimnis als Ausformung des besonderen würdegeprägten Persönlichkeitsschutzes.

Art. 10 Abs. 1 GG ist zwar ferner an den Staat, nicht aber unmittelbar an Private gerichtet. Für ihre Tätigkeiten wird aber eine Schutzpflicht des Staates wirksam. Denn betroffen ist dann der Schutzgehalt der unkörperlichen Übermittlung von Informationen an individuelle Empfänger mithilfe des Telekommunikationsverkehrs.[102]

Ergänzend erfasst auch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG mit seinem Allgemeinen Persönlichkeitsrecht, insbesondere dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme,[103] diese Formen der Persönlichkeitsentfaltung grundrechtlich. Gemeinsam formieren sie das postmortale Persönlichkeitsrecht.

So wie das Bundesverfassungsgericht schon in seinem Volkszählungsurteil den sachlichen Schutzbereich des Rechts auf informationelle Selbstbestimmung bewusst weit fasste und konstatierte, dass es im Informationszeitalter kein an sich „belangloses“ Datum mehr geben könne,[104] muss dies auch in *zeitlicher* Hinsicht gelten, soll den realen Gefährdungen der Persönlichkeit im Cyberspace hinreichend begegnet werden: Es genügt den Anforderungen im digitalen Zeitalter dann nicht mehr, die schier unendlichen Mengen an personenbezogenen Daten nur zu Lebzeiten der betroffenen Person umfassend zu schützen. Fehlende Transparenz und dem Nutzer in ihrer Reichweite unbekannt bleibende Risiken – wie die Möglichkeit einer umfangreichen Profilbildung, die Unvergänglichkeit online verbreiteter Informationen und die Leichtigkeit der Offenbarung geheim geglaubter sensibler Informationen wider Willen – können sich sonst erheblich auf das Kommunikationsverhalten der Menschen und auf die Hinterlegung von Daten für die Zukunft auswirken. Diese Auswirkungen bereits heute zu berücksichtigen, ist ein Gebot vorsorgenden bzw. nachwirkenden Grundrechtsschutzes.

102 BVerfGE 67, 157 (172); 106, 28 (35 f.).

103 BVerfGE, 120, 274 ff., kritisch zu dessen Mehrwert etwa *Gurlit*, NJW 2010, 1035 (1037) m.w.N.

104 BVerfGE 65, 1 (43); *Kühling/Seidel/Sividris* (Fn. 45), S. 52 bezeichnen diese Entscheidung im „Lochkarten-Zeitalter“ zu Recht als „visionär“.

Denn nur demjenigen, der auf den Schutz der Integrität seiner sensiblen digitalen Daten durch die Hinterbliebenen vertrauen kann, eröffnet sich zu Lebzeiten die volle digitale Handlungsfreiheit.[105]

So verlieh denn auch der BGH in seiner *Mephisto*-Entscheidung seiner Überzeugung Ausdruck, dass „die Menschenwürde und [die] *freie Entfaltung zu Lebzeiten* nur dann zureichend gewährleistet sind, wenn der Mensch auf einen Schutz seines Lebensbildes *wenigstens* gegen grobe ehrverletzende Entstellungen nach dem Tode vertrauen und in dieser Erwartung leben kann".[106] Darin offenbart sich ein Grundgedanke, der für die Bewältigung des postmortalen Datenschutzes von herausragender Bedeutung ist. Es ist die Erkenntnis, dass sich der Mensch bei all seinem Handeln auch und gerade von zukünftigen Entwicklungen und den auf die Zeit nach dem eigenen Tod projizierten Erwartungen an die Rechtsordnung leiten lässt. Die sittliche Autonomie des Lebenden wäre gefährdet, wenn er befürchten müsste, dass seine Lebensleistung nach seinem Tod verzerrt oder seine Intim- oder Privatsphäre beliebig durchleuchtet werden dürfte und damit dem Zugriff Dritter ungeschützt ausgesetzt wäre.[107] Postmortaler Persönlichkeitsschutz ist insoweit insbesondere Vertrauensschutz für die Lebenden, namentlich Teil einer objektivrechtlichen[108] staatlichen Schutzpflicht, (auch nichtvermögensrechtliche[109]) ausdrückliche oder durch entsprechende Sicherungen zum Ausdruck gebrachte Verhaltenserwartungen an den Umgang mit Geheimnissen zu respektieren, die das Individuum als Ausfluss seiner personalen Selbstbestimmung für die Zeit nach seinem Tod gehegt hat.

Ähnlich ist auch das Prinzip der postmortalen Geheimhaltungspflicht beruflicher Geheimnisträger in seiner Schutzrichtung konstruiert: Die erforderliche Vertrauensbasis zwischen Arzt und Patient, Rechtsanwalt und Klient oder Be-

105 In diesem Sinne etwa auch *Schack*, JZ 1989, 609 (614); *Schönberger* (Fn. 51), S. 84 ff.

106 BGHZ 50, 133 (139) – Mephisto; Hervorhebungen des Verf.; zustimmend etwa *Schack*, JZ 1989, 609 (610); dogmatisch skeptisch bzw. ablehnend zu diesem Gedanken BVerfGE 30, 173 (194) – Mephisto; *Claus* (Fn. 83), S. 97 f.; mit Blick auf das zivilrechtliche postmortale Persönlichkeitsschutz: *Luther* (Fn. 83), S. 102 (anders aber *ders.*, a.a.O., S. 118 ff. im Hinblick auf eine staatliche Schutzpflicht).

107 In diesem Sinne etwa auch *Luther* (Fn. 83), S. 118; *Maurer*, DÖV 1983, 7 (9); *Hager*, JURA 2000, 186 (190).

108 Die Konstruktionsprobleme eines subjektlosen Rechts, die die zivilrechtliche Diskussion prägen und ihr Kopfzerbrechen bereiten (vgl. insbesondere Fn. 86), stellen sich insoweit bei diesem Verständnis nicht in gleichem Maße. In diesem Sinne auch für eine öffentlichrechtliche Ausgestaltung und Normierung des postmortalen Persönlichkeitsschutzes plädierend *Luther* (Fn. 83), S. 147 ff.

109 Für vermögensrechtliche Positionen ergibt sich die Pflicht der Rechtsordnung zur Beachtung der letztwilligen Verfügungen aus der durch Art. 14 Abs. 1 GG garantierten Testierfreiheit. Vgl. *Gleichauf*, Das postmortale Persönlichkeitsrecht im internationalen Privatrecht, 1999, S. 99 f.; *Schönberger* (Fn. 51), S. 76 f.

rufspsychologen und zu Beratendem kann nicht entstehen, wenn der schutzbedürftige Vertragspartner nicht auch für die Zeit nach dem Tod auf die Verschwiegenheit des Geheimnisträgers zählen kann.[110]

(2) Funktionen und Spezifika des verfassungsrechtlichen postmortalen Persönlichkeitsschutzes im digitalen Zeitalter

Werden vertrauliche Informationen nach dem Tod denjenigen zugespielt, denen der Erblasser sie zu Lebzeiten immer vorenthalten wollte, kann gerade davon der (in der angloamerikanischen Rechtsprechung als „*chilling effect*" bezeichnete) Einschüchterungseffekt ausgehen, vor dem das Telekommunikationsgeheimnis und das informationelle Selbstbestimmungsrecht schützen sollen.[111] Sie wollen gegen die Weitergabe und fremde Kenntnisnahme von Informationen schützen, die der Urheber der Nachricht Dritten nicht zugänglich machen möchte. Das gilt nicht nur für vertrauliche Nachrichten des Verstorbenen an Dritte, sondern auch für die Offenbarung vertraulicher Nachrichten, die der Verstorbene von noch lebenden Dritten, z.B. seiner Geliebten, im Vertrauen auf die Geheimhaltung des Inhalts der Nachricht über den Kanal eines sozialen Netzwerks erhalten hat. Die Herausgabe der Account-Informationen des Verstorbenen und die damit verbundene Offenbarung der Nachrichten lebender Dritter kann auch deren Persönlichkeitsrechte, insbesondere deren besondere Ausformung in Art. 10 Abs. 1 GG,[112] verletzen.

Warum dem Internet-Account im Verhältnis zum papierenen Tagebuch insoweit ein gesteigerter Schutz zukommen soll, leuchtet auf den ersten Blick nicht ohne Weiteres ein. Denn das Tagebuch unterfällt nach überkommener Auffassung immerhin dem normalen Erbgang und steht grundsätzlich dem Zugriff der Erben offen.[113] Zwischen beiden Formen der Entfaltung von Höchstpersönlichkeit lassen sich aber reale Unterschiede von rechtlicher Relevanz festmachen: Nicht nur wird ein Papiertagebuch nur selten so umfassend geführt, dass ein ähnlich präzises Persönlichkeitsprofil und eine derart detaillierte Chronik wie diejenige gezeichnet werden können, die Online-Accounts – insbesondere in ihrer Zu-

110 *Bender* (Fn. 68), S. 301.

111 BVerfGE 115, 166 (188).

112 Das gilt nach Einschätzung des BVerfG jedenfalls dann, wenn die E-Mail-Nachrichten auf dem Server des Telemedienanbieters noch zwischengespeichert sind. Vgl. Fn. 99.

113 Vgl. dazu etwa BGH, GRUR 1955, 201 (203) – Cosima Wagner; zur Verwertung von Tagebuchaufzeichnungen im Strafverfahren BVerfGE 80, 367 ff.; LG Koblenz, NJW 2012, 2227; *Claus* (Fn. 83), S. 98; siehe aber auch zur Unzulässigkeit der Veröffentlichung eines nicht freigegebenen Briefes BGHZ 13, 334 ff. – Leserbrief.

sammenschau – hervorzubringen vermögen. Vor allem ist ein Tagebuch – anders als ein Internet-Account – schon zu Lebzeiten gegen die bewusste oder unbewusste Kenntnisnahme durch Dritte nur soweit geschützt, wie es dem räumlichen Einwirkungsbereich Dritter entzogen ist. Für den Online-Account besteht dieser Schutz bei ordnungsgemäßer Verwahrung der Zugangsdaten aufgrund seiner Passwortsicherung uneingeschränkt. Sein Wissensschatz ist nur durch Einbeziehung eines Geheimhaltungsverpflichteten hebbar. Wer einen Internet-Account nutzt, kann davon ausgehen, dass außer ihm und dem Diensteanbieter niemandem Zugriff auf die Daten möglich ist. Die Besonderheit des passwortgesicherten Teils des digitalen Nachlasses liegt somit darin begründet, dass nach dem Tod Informationen von außergewöhnlichem Umfang, großer Detailliertheit und Informationsdichte sowie höchster Sensibilität bekannt werden können, die nie für andere Augen bestimmt waren, vielmehr durch Zugangshürden hiergegen gesichert wurden.

Auch wer seine digitale Identität bewusst in der Öffentlichkeit und für die digitale Ewigkeit auslebt, will die Verfügungsgewalt über seinen digitalen Schattenriss regelmäßig nicht ohne Weiteres unbegrenzt Dritten anvertrauen. Vielmehr vertraut er grundsätzlich darauf und darf darauf vertrauen, dass der volle Zugriff auf seine Daten mithilfe des digitalen Schlüssels nur ihm und dem Diensteanbieter, nicht aber Dritten, sei es auch den Angehörigen, offen steht. Dies durch entsprechende Schutzvorkehrungen sicherzustellen, verbürgt § 13 Abs. 4 Nr. 3 TMG den Nutzern der entsprechenden Telemediendienste auch ausdrücklich. Jeder, der Diensteanbietern Informationen über sich zur Verfügung stellt, tut dies dann grundsätzlich auf der Grundlage des Vertrauens, dass die Zugangsinformationen nur demjenigen zukommen, dem er diese bewusst verschafft hat. Vertrauliche Mitteilungen, für die die Accounts gedacht sind, würde der Nutzer sonst dort im Zweifel nicht hinterlegen. Zu diesem Zweck sind die digitalen Schlüssel gegen den Zugriff Dritter angelegt und gesetzlich vorgesehen. Entsprechend ist der Nutzer mit der Weitergabe seiner Zugangsdaten grundsätzlich so lange nicht einverstanden, wie er diese nicht ausdrücklich Dritten mitgeteilt hat. Er muss mit einer solchen Weitergabe auch nicht rechnen.

(3) Schlussfolgerungen

Die Kunden sind das Kapital der Diensteanbieter. Dessen Grundstock ist das Vertrauen in die Geheimhaltung. Dieses unausgesprochene Vertrauen als Geschäftsgrundlage des Vertrages würde zerstört, gäben die Diensteanbieter den Zugang zu dem Account *posthum* frei.

Das postmortale Persönlichkeitsrecht verleiht diesem Geheimhaltungsvertrauen seinen normativen Flankenschutz. An ihm findet das Auskunfts- und Nutzungsinteresse der Hinterbliebenen seine Grenze. Der Nutzer ist gegen die Weitergabe seiner Zugangsdaten daher nicht erst dann geschützt, wenn er das ausdrücklich durch letztwillige Verfügung bestimmt hat. Es verhält sich vielmehr umgekehrt: Er ist so lange geschützt, wie er nicht ausdrücklich oder stillschweigend gegenüber dem Diensteanbieter oder Dritten die Freigabe verfügt. Sonst würde die Freiheitsvermutung zugunsten des Persönlichkeitsschutzes der Lebenden in ihr Gegenteil verkehrt. Denn dieser verbürgt dem Nutzer gerade, selbst zu bestimmen, ob und innerhalb welcher Grenzen er sensible Lebenssachverhalte einem Dritten offenbart. Die entsprechende Geheimhaltungsverpflichtung des Telemediendiensteanbieters endet daher – ähnlich wie bei dem beruflichen Geheimnisträger – nicht einfach mit dem Tod. Die Rechte auf Geheimhaltung seiner Nutzeraccount-Daten bestehen vielmehr fort.[114] Sie verwandeln sich mit dem Tod in ein Recht auf Respektierung des Persönlichkeitsbildes des Verstorbenen, das sich in einem Verbot der Weitergabe von Account-Zugangsdaten äußert.

Die als Abwehrrechte des Einzelnen gegenüber dem Staat konzipierten Grundrechte, namentlich das Allgemeine Persönlichkeitsrecht und der Achtungsanspruch der Menschenwürde, wirken insoweit als Teil der staatlichen Schutzpflicht auch mittelbar in die Auslegung vertraglicher Rechtsbeziehungen hinein. Sie schützen nicht nur vor direkten staatlichen Eingriffen, sondern strahlen auf die Auslegung und Anwendung einfachgesetzlicher Vorschriften aus.[115]

Entsprechend darf der Diensteanbieter sich auch nicht in Allgemeinen Geschäftsbedingungen das Recht vorbehalten, Erben den Zugriff auf den Account zu eröffnen. Denn darin läge eine unzulässige Abweichung vom gesetzlichen

114 Davon zu trennen ist die Frage, wer diese Rechte im Falle der Verletzung durch den Diensteanbieter geltend machen kann. Da der Inhaber des Rechts nicht mehr zur Ausübung in der Lage ist, droht das Recht als „inhaberloses Recht“ verteidigungslos zu bleiben. Denkbar ist es, das Wahrnehmungsrecht in Analogie zu den Vorschriften des § 22 S. 3 KunstUrhG und des § 205 Abs. 2 S. 3 StGB den Angehörigen des Verstorbenen als treuhänderisches Recht anzuvertrauen (in diesem Sinne für das Recht auf Einsichtnahme in Krankenunterlagen etwa *Bender* [Fn. 68], S. 386 ff.). Allerdings fällt seine Verteidigung dann in die Hände derjenigen, gegen deren Neugierde das Geheimhaltungsrecht gerade vorrangig schützen soll. Sachgerechter erscheint es daher, Verstöße gegen die Geheimhaltungspflicht den jeweiligen Aufsichtsbehörden der Diensteanbieter als Kontrollbefugnis anzuvertrauen. Zur Wahrnehmungsbefugnis für die datenschutzrechtlichen Rechte im Hinblick auf öffentlich einsehbare Daten des Verstorbenen vgl. unten IV. 2. b., S. 112.

115 Sie beeinflussen damit auch die Auslegung des Allgemeinen Persönlichkeitsrechts als eines sonstigen Rechts i.S.d. § 823 Abs. 1 BGB; vgl. BGHZ 13, 334 – Leserbriefe; BGHZ 24, 200 – Spätheimkehrer; BGHZ 26, 349 – Herrenreiter; BGHZ 30, 7 – Caterina Valente; BGHZ 31, 308 – Burschenschaft.

Grundmodell (§ 307 Abs. 1, 2 Nr. 1 BGB). Der Anbieter darf den Erben vielmehr nur dann den Zugriff eröffnen, wenn der Erblasser dem ausdrücklich zugestimmt hat oder mutmaßlich erkennbar zugestimmt hätte.

cc) Auflösung der Gemengelage zwischen vermögensrechtlichen und nichtvermögensrechtlichen Positionen eines digitalen Nachlasses

Der digitale Nachlass ist keine uniforme Masse. Er hat vielfältige Facetten und Bestandteile. Zu ihm gehören nicht nur höchstpersönliche Daten, die dem Zugriff der Erben grundsätzlich nicht zugänglich sein sollen. Vielmehr umfasst er auch vermögensrechtliche Positionen, nicht zuletzt vermögensrechtliche Bestandteile des Persönlichkeitsrechts,[116] Immaterialgüterrechte, beispielsweise das Urheberrecht an digital gespeicherten Bildern, die nicht dem Bereich höchstpersönlichen Schutzes unterfallen – schließlich auch geschäftliche Nachrichten, womöglich Geschäftsgeheimnisse, die in die Verfügungsgewalt des Arbeitgebers gehören. Diese können ein unterschiedliches rechtliches Schicksal fristen.

Sie sind aber in dem Nutzer-Account regelmäßig an einem Ort miteinander verwoben. Aus dem multifunktionellen Nebeneinander folgt eine Gemengelage: Die *personenbezogenen* Elemente stehen dem Zugriff der Erben nicht offen, sehr

116 In der Persönlichkeit kann ein bedeutender wirtschaftlicher Wert stecken. Deutlich wird das etwa an der Vermarktung des Lebens und Todes prominenter Persönlichkeiten, wie etwa *Lady Diana*, *Uwe Barschel* oder *Marlene Dietrich* etc. Nach Auffassung der zivilrechtlichen Rechtsprechung steht dem persönlichkeitsrechtlichen Abwehranspruch unabhängig vom verfassungsrechtlichen Schutzumfang auch ein vermögensrechtlicher Anspruch zur Seite (vgl. BGHZ 143, 214 [218]; BGH, NJW 2000, 2201; BGH, Urt. v. 31.5.2012, I ZR 234/10 – Gunter Sachs; dazu *Beuthien*, NJW 2003, 1220; *Claus* [Fn. 83], S. 23 ff.; *Frommeier,* JuS 2002, 13 [16]; *Götting*, NJW 2001, 585; *ders.*, GRUR 2004, 801; *Gregoritza*, Die Kommerzialisierung von Persönlichkeitsrechten Verstorbener, 2003, S. 108 f.; *Klingelhöffer,* ZEV 2000, 327; *ders*. ZEV 2002, 75; *T. Müller,* GRUR 2003, 31; *Ullmann,* WRP 2000, 1049 [1053]; *Wortmann*, Die Vererblichkeit vermögensrechtlicher Bestandteile des Persönlichkeitsrechts, 2005, S. 293 ff. – *Schack,* JZ 2000, 1060 [1061] dagegen lehnt die Vererbbarkeit vermögensrechtlicher Bestandteile ab). Die Verfassung steht einer solchen Ausweitung des einfachgesetzlichen Schutzes auf vermögensrechtliche Positionen keineswegs entgegen (vgl. BVerfG, NJW 2006, 3409). Im Gegenteil entspricht er durchaus dem Anliegen des Persönlichkeitsschutzes: Er ermöglicht den Erben als Inhabern der vermögenswerten Bestandteile des Persönlichkeitsrechts, gegen eine Beeinträchtigung des Lebensbildes des Verstorbenen durch eine unbefugte Nutzung vorzugehen. Er trägt auch dem Umstand Rechnung, dass die Vielfalt, das Ausmaß und die Intensität der Vermarktung der Persönlichkeit durch die verbesserten technischen Mittel und die wachsende Bedeutung der Medien zugenommen haben. Bei der Geltendmachung der vermögensrechtlichen Aspekte des Persönlichkeitsschutzes sind die Erben aber an den mutmaßlichen Willen des verstorbenen Trägers des Persönlichkeitsrechts gebunden; vgl. dazu z.B. *Ahrens,* ZEV 2006, 237 (238).

wohl aber der *vermögensrechtliche* Teil. Um diesen geltend machen zu können, muss der Erbe freilich auf den Account zugreifen können. Sonst wird das Erbrecht am vermögensrechtlichen Teil zur leeren Hülle.

Zur Auflösung dieses Dilemmas mag es prima vista angängig erscheinen, an den Adressaten der Nachricht sowie die Schutzrichtung der Geheimhaltungspflicht anzuknüpfen, also zwischen überwiegend geschäftlichen sowie privaten Accounts zu unterscheiden. Bei Ersteren gingen dann die Rechte auf die Erben des Verstorbenen (vorbehaltlich der Rechte Dritter) über; bei Letzteren nicht.[117] Eine Stütze findet diese Differenzierung in der Struktur der jeweils zugrunde liegenden Vertrauensbeziehung: In dem einen Fall ist sie tendenziell weniger, in dem anderen Fall in besonderer Weise auf die Geheimhaltung höchstpersönlicher sensibler Daten richtet.

Ein solches Entscheidungsraster erweist sich jedoch regelmäßig als zu grobmaschig: Soll der Erbe keinen Zugriff auf die höchstpersönlichen Informationen erhalten, dann muss das grundsätzlich für alle Daten aus dem Kernbereich höchstpersönlicher Lebensgestaltung gelten. E-Mail-Accounts werden heute regelmäßig gemischt genutzt.[118] Und auch das *eine* Geständnis eines Ehebruchs im überwiegend geschäftlichen Account kann ein Lebensbild verändern.

Bei solchen gemischten Nutzungen sollte – entsprechend dem Grundgedanken des § 100a Abs. 4 S. 2 StPO – unmittelbar nach der Art des betroffenen Gegenstandes, also der Art der betroffenen Tatsache, unterschieden werden. Zu trennen ist danach zwischen ganz oder überwiegend die Vermögenssphäre betreffenden und ganz oder überwiegend höchstpersönliche Sachverhalte betreffenden Daten und Nachrichten.[119]

Auch hier bleiben Grenzfälle multifunktioneller Verwendungszusammenhänge, die nicht bruchfrei voneinander scheidbar sind, sondern einer Ermessensentscheidung bedürfen. Das Dilemma lässt sich daher womöglich – ähnlich wie im Falle der Einsichtnahme in die Krankenunterlagen, bei der die Entscheidung in die Hände des Arztes gelegt ist[120] – nicht anders sauber auflösen als durch die

117 In diese Richtung *Hoeren*, NJW 2005, 2113 (2114).

118 Der Arbeitgeber darf allerdings die private Nutzung von E-Mail-Accounts verbieten. Vgl. dazu und zu den Rechtsfolgen § 11 Abs. 1 Nr. 1 TMG; *Fülbier/Splittgerber*, NJW 2012, 1995 (1995); kritisch *Holzner*, ZPR 2011, 12 (13), der ein absolutes Verbot der Privatnutzung von geschäftlichen E-Mail-Accounts für kaum noch begründbar hält.

119 Vgl. zum lebzeitigen Zugriffsrecht des Arbeitgebers auf den (zulässigerweise) auch privat genutzten dienstlichen Account, insbesondere zur Eigenschaft des Arbeitgebers als Diensteanbieter i.S.d. § 3 Nr. 6 TMG: LAG Berlin-Brandenburg, NZA-RR 2011, 342; *Fülbier/Splittgerber* (Fn. 118), 1996 ff.

120 Der BGH gesteht dem Arzt dabei einen nicht justiziablen Spielraum zu. Der in Anspruch genommene Arzt sei „gewissermaßen selbst die letzte Instanz“ BGH, JZ 1984, 279 (284 f.). Zu Recht kritisch mit Blick auf die Gefahr, dass der „Gott in Weiß” sich ange-

treuhänderische Einschaltung eines neutralen Dritten, sei es eines Testamentsvollstreckers, sei es des Diensteanbieters. Der digitale Nachlass mag für den Nutzer technisch unteilbar erscheinen, für den Diensteanbieter ist er es aber nicht zwingend. Dieser verfügt über die technischen Möglichkeiten einer Trennung und könnte de lege ferenda (subsidiär, falls kein anderer unbefangener digitaler Totengräber bestellt ist oder in Betracht kommt) der Pflicht unterliegen, den Erben Zugang (nur) zu den vermögensrechtlichen Teilen des digitalen Nachlasses zu verschaffen. Er muss dann Vermögensrechtliches und Höchstpersönliches des Accounts sezieren. Bei der Entscheidung hat er den tatsächlichen bzw. mutmaßlichen[121] Willen des Erblassers umzusetzen. Das würde den Account-Betreibern einigen Aufwand abverlangen[122] (den diese in ihr Geschäftsmodell einpreisen [müssten]) und zugleich bei der Vielzahl sowie Mischstruktur der in vielen Accounts versammelten Nachrichten nicht ohne eine Toleranzschwelle der Pauschalierung zumutbar und realisierbar sein. Wahrscheinlich ist es aber realistischer und daher de lege ferenda vorzugswürdig, nach dem Typus des Accounts zu unterscheiden: In allen Fällen, in denen hinter einem Account legitimerweise vermögensrechtliche Positionen vermutet werden dürfen, darf der Erbe den Zugriff verlangen. Verbergen sich demgegenüber hinter einem Account typischerweise ausschließlich nicht-vermögensrechtliche, sondern persönliche Inhalte, etwa im Falle eines Accounts bei den anonymen Alkoholikern, überwiegt das Persönlichkeitsinteresse des Verstorbenen und sollte Erben oder Angehörigen ein Zugriff (vorbehaltlich entgegenstehenden ausdrücklichen oder erkennbaren mutmaßlichen Willens des Verstorbenen) nicht eröffnet sein.

sichts häufiger eigener Interessenkollisionen zum Richter in eigener Angelegenheit aufschwingt, *Bender* (Fn. 68), S. 390 ff., 414 ff.

121 Vgl. auch die ähnliche, wenngleich ethisch weitaus brisantere Wertung des Gesetzgebers in § 4 Abs. 1 S. 4 TPG.

122 Reduzieren können die Betreiber diesen Aufwand dadurch in legitimer Weise, dass sie das Nutzungsverhalten ihrer Kunden entsprechend lenken: So können sie etwa Unterpostfächer für private und geschäftliche Nachrichten vorsehen oder ihre Accounts gezielt auf private oder geschäftliche Nachrichten ausrichten, die dann durch gemeinsame Verwaltungsoptionen unkompliziert zusammengeführt, aber auch je nach Tageszeit (berufspolitisch wünschenswert) bewusst getrennt werden können. Oder sie können sich für den ihnen entstehenden Aufwand die Erhebung von Gebühren (insbesondere von den Erben) vorbehalten.

b) Öffentlich verfügbare Internetinformationen über den Verstorbenen, z. B. eines Internet-Blogs oder einer Website, und Wahrnehmung darauf bezogener datenschutzrechtlicher Rechte nach dem Tod

Wiewohl der Diensteanbieter den Erben nicht den vollständigen Zugriff auf den Account des Verstorbenen eröffnen darf, muss für die im Internet verfügbaren, für jedermann einsehbaren (Profil-)Daten des Verstorbenen, wie etwa Internet-Blogs oder persönliche Homepages, nicht das Gleiche gelten. Denn ihnen kommt aufgrund der bereits durch den Erblasser veranlassten Veröffentlichung kein besonderer Geheimhaltungsschutz zu.

aa) Wahrnehmungsberechtigung der Angehörigen

Zu Lebzeiten stehen dem Betroffenen für seine personenbezogenen Daten die Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung zu (§ 13 Abs. 7 sowie § 12 Abs. 3 TMG i.V.m. §§ 19, 20, 35 BDSG).[123] Diese Rechte können – der Effektivität des Datenschutzes wegen – durch Rechtsgeschäft weder ausgeschlossen noch beschränkt werden (§ 6 Abs. 1 BDSG i.V.m. § 12 Abs. 3 TMG).

Post mortem könnten die Erben in die Rolle des Erblassers schlüpfen und dessen Rechte aus dem BDSG wahrnehmen. Da diese Rechte ihrem Wesen nach eng mit der Person des Betroffenen verknüpft sind, halten manche diese allerdings wegen ihres höchstpersönlichen Charakters für nicht übertragbar und damit auch für nicht vererbbar.[124]

Das verfängt nicht. Auch andere Ausprägungen des Persönlichkeitsrechts, wie beispielsweise das Recht am eigenen Bild oder das vermögensrechtliche postmortale Persönlichkeitsrecht, sind vererbbar bzw. können nach dem Tod des Be-

123 Vgl. die nicht abschließende Aufzählung in § 6 BDSG. Insbesondere dem Auskunftsrecht kommt dabei eine besondere Bedeutung zu, da die Kenntnis des Betroffenen von über ihn gespeicherten Daten erforderlich ist, um überhaupt die anderen Rechte ausüben zu können. Vgl. AG Hamburg Altona, DuD 2005, 170 (171): „entscheidungsvorbereitendes Wissen". Siehe dazu auch § 13 Abs. 7 TMG, wonach der Anbieter eines Telemediendienstes zur ggf. elektronischen Auskunft gegenüber dem Nutzer verpflichtet ist; *Spindler/Nink*, in: Spindler/Schuster (Fn. 38), § 13 TMG Rn. 16. Hinzu kommen z.B. mögliche Schadensersatzansprüche aus §§ 7, 8 BDSG.

124 *Bergmann/Möhrle/Herb* (Fn. 66), BDSG, § 6 Rn. 12; *Gola/Schomerus*, in: dies. (Hrsg.) (Fn. 68), § 6 BDSG Rn. 3; *Schaffland/Wiltfang*, BDSG, 2011, § 6 Rn. 2.

troffenen von den Wahrnehmungsberechtigten ausgeübt werden, ohne dass die geschützte Persönlichkeit selbst sich weiter zu entfalten in der Lage wäre.[125]

Den Schutz personenbezogener Daten mit dem Tod still zu Grabe zu tragen,[126] hieße, das Grundanliegen des Persönlichkeitsschutzes im Datenschutzrecht geradezu zu pervertieren. Denn die Daten stünden dann den Diensteanbietern unbegrenzt als Verfügungsmasse zu Gebote. Anliegen des Datenschutzrechts ist es, den Achtungswert der Persönlichkeit in ihren relevanten Facetten gegen eine Beeinträchtigung zu schützen. Das bedingt eine Aufrechterhaltung von Schutzpositionen des Datenschutzes auch nach dem Tod, soweit sich in der weiteren Verwendung der Daten eine Persönlichkeitsverletzung realisieren kann. Ähnlich wie beim Schutz der Daten von Ungeborenen und Minderjährigen[127] lässt sich rechtspolitisch weniger darüber streiten, *ob* es eines solchen Schutzes bedarf, als darüber, *wer* diesen Schutz nach dem Tod wahrzunehmen berechtigt ist.

Da dem Erblasser bei öffentlich zugänglichen Profildaten – anders als bei höchstpersönlichen, nicht öffentlich zugänglichen Informationen – kein Geheimhaltungsinteresse gegenüber seinen Erben eigen ist, fehlt es in dieser Konstellation an einer Interessenkollision, die den Erben bzw. Angehörigen die legitime treuhänderische Wahrnehmung der postmortalen Persönlichkeitsrechte des Erblassers versagt.

Den sozialen Achtungswert des Verstorbenen und die Verfügungsgewalt über seine öffentlichen Daten können regelmäßig die Angehörigen am ehesten verteidigen, standen sie doch dem Toten besonders nahe. Es mangelt freilich (jenseits der Möglichkeit einer Vollmacht auf den Todesfall[128]) an gesetzlichen Regelungen, die die Person der Wahrnehmungsberechtigten als Wächter der Schutzrechte des Verstorbenen auf den Posten stellen. Sachgerecht erscheint insoweit eine Anleihe bei § 22 S. 3 KunstUrhG bzw. § 60 Abs. 1 UrhG. Diese sprechen den Angehörigen das Wahrnehmungsrecht[129] für die Verbreitung von Bildnissen des Verstorbenen zu. Die Interessenlagen beider Schutzmaterien sind vergleich-

125 Vgl. zur Vererblichkeit von Immaterialgüterrechten auch *Lehmann* (Fn. 83), S. 45 ff.; zur konstruktiven Herleitung der Wahrnehmungsbefugnis in ihren dogmatischen Begründungsansätzen *Claus* (Fn. 83), S. 60 ff.

126 Vgl. zu dieser Frage im Einzelnen oben S. 92.

127 Vgl. dazu bereits oben Fn. 55.

128 Diesen Rechten liegt der Gedanke zugrunde, dass die Rechtsordnung Gebote und Verbote für das Verhalten der Rechtsgenossen zum Schutz verletzungsfähiger Rechtsgüter auch unabhängig vom Vorhandensein eines lebenden Rechtssubjekts vorsehen und Unterlassungsansprüche durch jemanden wahrnehmen lassen kann, der nicht selbst Subjekt eines entsprechenden Rechts ist.

129 Es handelt sich dabei nicht um einen Vererbungstatbestand. Die Berechtigung bleibt dementsprechend von einer Ausschlagung der Erbschaft unberührt. Die Schutzansprüche fallen auch dann nicht in den Nachlass, wenn die Schutzberechtigten zugleich Erben sind.

bar.[130] Eine Schließung der Gesetzeslücke im Wege der analogen Anwendung der Vorschrift erscheint insoweit angezeigt. Eine solche Regelung sollte der Gesetzgeber auch ausdrücklich im TMG verankern. § 12 Abs. 3 TMG sollte daher um folgende Sätze 2 und 3 erweitert werden: „Datenschutzrechtliche Rechte nehmen nach dem Tod des Nutzers dessen Angehörige wahr. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Nutzers und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Nutzers."

bb) Zeitliche Dauer der Wahrnehmungsberechtigung

Der besondere Schutz einer Wahrnehmungsberechtigung besteht zeitlich nicht grenzenlos – vielmehr nur so lange, wie von einer gesteigerten Schutzbedürftigkeit des besonderen Ansehens und der Selbstdarstellung der Persönlichkeit ausgegangen werden kann. Das Schutzbedürfnis – und entsprechend die Schutzverpflichtung – schwinden in dem Maße, in dem die Erinnerung an den Verstorbenen verblasst und die Neugierde gegenüber seinen Privatgeheimnissen nachlässt.[131]

Wann diese Schwelle überschritten ist, lässt sich grundsätzlich nur im Wege einer politischen Dezision bestimmen.[132] Eine äußerste Grenze zieht nur das auf die staatliche Schutzpflicht gegründete verfassungsrechtliche Untermaßverbot sowie das die (mit dem postmortalen Persönlichkeitsrecht ggf. kollidierenden) Grundrechte Dritter schützende Übermaßverbot. Innerhalb dieses politischen Gestaltungskorridors kommt dem Staat eine Einschätzungsprärogative zu. Maßstab für die Festsetzung der Schutzfrist sollte dabei die Verletzbarkeit des postmortalen Persönlichkeitsrechts des Verstorbenen durch den Diensteanbieter und die Öffentlichkeit sein.

Einen analogiefähigen Anhaltspunkt kann die gesetzliche Regelung des § 22 S. 3 KunstUrhG bilden. Sie schützt Bildnisse des Verstorbenen für einen Zeit-

130 Ein Unterschied besteht jedoch darin, dass der Erblasser die Internetdaten zu Lebzeiten bereits für diesen Zweck vorgehalten hat, während die Abbildung im Sinne des § 22 KunstUrhG erst nach dem Tod der Öffentlichkeit zur Verfügung gestellt wird. Gemeinsam ist beiden Materien aber das Schutzziel, die öffentliche Darstellung einer Person und die Verfügungsberechtigung über die insoweit bestehenden Daten nicht in die Verfügungsgewalt des Dateninhabers, sondern der Angehörigen zu legen.

131 Dazu etwa *Claus* (Fn. 83), S. 105 ff.; *Schönberger* (Fn. 51), S. 27 ff. jeweils m.w.N.

132 St. Rspr. des BGH; vgl. BGHZ 50, 133 (140 f.); 107, 384 (392); *Bergmann/Möhrle/Herb* (Fn. 66), § 3 Rn. 6. Zu unterschiedlichen Lösungsmodellen vgl. etwa *K. Müller*, Postmortaler Rechtsschutz – Überlegungen zur Rechtssubjektivität Verstorbener, 1996, S. 68 ff.; *Luther* (Fn. 83), S. 171 ff.

raum von zehn Jahren. Das allgemeine Urheberrecht wiederum befristet den Schutz sowohl für den originär urheberrechtlichen als auch den persönlichkeitsrechtlichen Aspekt auf einen Zeitraum von 70 bzw. 50 Jahren (§ 64 UrhG für den quivis ex populo bzw. §§ 82, 76 UrhG für den ausübenden Künstler).[133] Diese Regelung ist allerdings von einem anderen Schutzgedanken getragen: nämlich der Gewährleistung einer hinreichenden Schutzfrist für die wirtschaftliche Verwertung der geschützten Rechte.

Tauglichster Orientierungspunkt einer Fristenregelung ist der Zeitraum einer Generationenfolge, also nach überkommener Auffassung 30 Jahre.[134] Vorbild kann insoweit insbesondere § 5 Abs. 2 S. 1 BArchG sein.[135] Die Vorschrift verfolgt einen ähnlichen Schutzgedanken wie das Datenschutzrecht der digitalen Hinterlassenschaften: 30 Jahre nach dem Tod besteht eine Gefahr besonderer Neugierde der Nachwelt gegenüber behördlichem Archivgut, das sich auf natürliche Personen bezieht, ebenso wie gegenüber den öffentlich verfügbaren Internetdaten Verstorbener regelmäßig nicht mehr. Gewöhnlich ist das engere soziale Umfeld der Freunde und Bekannten des Verstorbenen, die mit dessen Namen etwas verbinden können, häufig auch seine Kinder, dann den Weg alles Irdischen gegangen. Trotz der Schnelllebigkeit, aber angesichts der Unvergänglichkeit und der Sensibilität der im Internet hinterlegten Daten entspricht ein Zeitraum von 30 Jahren einer sachgerechten Abwägung der widerstreitenden Interessen.

3. Zwischenfazit

Auch wenn die Erben grundsätzlich in die vermögensrechtliche Nutzerstellung des Erblassers einrücken, ist es ihnen aus Gründen des postmortalen Persönlichkeitsschutzes versagt, auf Accounts zuzugreifen, die den Schutz privater Vertraulichkeit genießen und damit Einblick in die intimste Persönlichkeitssphäre des Verstorbenen erlauben. Die Zugangsinformationen eines Internet-Accounts sind grundsätzlich[136] höchstpersönlich. Die Rechte des Betroffenen bzw. die korres-

133 BGHZ 50, 133 (140).

134 Anders aufgrund eines auf den Schutz der Persönlichkeitsrechte der Angehörigen bezogenen Ansatzes *Bizer*, NVwZ 1993, 653 (655 ff.).

135 Die Archivgesetze der Bundesländer weichen davon teilweise ab. Vgl. z.B. § 7 Abs. 1 LArchG NRW, das nicht auf den Tod des Betroffenen, sondern auf den Zeitpunkt der Entstehung der Unterlagen abstellt.

136 Etwas anderes gilt etwa für den Zugang zu einem Online-Banking-Account. Dieser erschöpft sich grundsätzlich in einer vermögensrechtlichen Position, die im normalen Erbgang übergeht. Mittelbar ergeben sich zwar auch aus derartigen Transaktionen möglicherweise Einblicke in höchstpersönliche Lebensbereiche des Verstorbenen, z.B. ver-

pondierenden Pflichten des Diensteanbieters auf Geheimhaltung seiner Nutzer-Account-Daten gehen entsprechend nicht mit dessen Tod unter, sondern bestehen fort. Daten aus der höchstpersönlichen Lebenssphäre und solche, die aus anderen Gründen mit der Person des Erblassers eng verbunden sind, unterfallen daher nicht dem normalen Erbgang.[137] Etwas anderes gilt nur, soweit ein abweichender tatsächlicher oder mutmaßlicher Wille des Erblassers zweifelsfrei erkennbar ist.

Gibt der Diensteanbieter die Zugangsinformationen an die Erben heraus, ohne dass dies dem ausdrücklichen oder mutmaßlichen Willen des Verstorbenen entspricht, macht er sich aber nicht nach § 202a StGB eines Ausspähens von Daten strafbar. Denn dieser Straftatbestand setzt die „Überwindung" von Sicherungen voraus, durch welche die Daten besonders geschützt sind.[138] Die Überwindung impliziert nach der Vorstellung des Gesetzgebers einen „nicht unerheblichen zeitlichen oder technischen Aufwand", in dem sich die „strafwürdige kriminelle Energie" des Täters manifestiert.[139] Der Täter muss namentlich zu einer Zugangsart gezwungen sein, die der Verfügungsberechtigte erkennbar verhindern wollte und bestehende Sicherungen umgeht (Hacking).[140] Daran mangelt es im Falle der freiwilligen Herausgabe des Passworts durch den Berechtigten selbst[141] ebenso wie im Falle einer Herausgabe der Daten durch den Diensteanbieter. Der Diensteanbieter macht sich auch nicht nach § 202c Nr. 1 StGB strafbar. Er macht dem Erben zwar Passwörter zugänglich, die den Zugang zu geschützten Daten ermöglichen. Seine Tathandlung dient aber nicht der Vorbereitung einer Straftat des Hacking, die der Gesetzgeber mit dem Tatbestand selbstständig mit Strafe bedrohen will.[142] Der Diensteanbieter nimmt nämlich nicht eine eigene oder fremde Computerstraftat *i.S.d. § 202a StGB* in Aussicht.[143] Nicht ausgeschlossen

schwiegene Unterhaltspflichten. Die vermögensrechtlichen Positionen sind jedoch ohne diese personenbezogenen Einblicke nicht wahrnehmbar und damit nicht trennbar.

137 So auch *Hoeren*, NJW 2005, 2113 (2114); *Müller-Christmann*, in: BeckOK BGB (Fn. 22), § 1922 Rn. 24; *Schlüter*, in: Ermann (Hrsg.), BGB (Fn. 24), § 1922 Rn. 8.

138 *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 82), § 202a Rn. 10a; *Weidemann*, in: BeckOK StGB, 20. Ed. 2012, § 202a Rn. 13; zu § 206 StGB siehe oben S. 89 mit Fn. 42.

139 Vgl. die Begründung der Bundesregierung zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität, BT-Drucks. 16/3656, S. 10.

140 Vgl. BT-Drucks. 16/3656, S. 10.

141 BT-Drucks. 16/3656, S. 18.

142 BT-Drucks. 16/3656, S. 11.

143 Vgl. zum Erfordernis des Vorbereitens BT-Drucks. 16/3656 S. 19; *Eisele*, in: Schönke/Schröder (Fn. 82), § 202c Rn. 7.

ist aber die Verwirklichung eines Bußgeldtatbestandes im Sinne des § 16 Abs. 2 Nr. 3 TMG bzw. des § 43 Abs. 2 Nr. 3 BDSG i.V.m. § 12 Abs. 3 TMG.[144]

Die Pflicht zur Geheimhaltung höchstpersönlicher Zugangsdaten entbindet die Diensteanbieter nicht von der Pflicht, die Informationen zu den *vermögensrechtlichen Positionen,* auch vermögensrechtlichen Bestandteilen persönlichkeitsrechtlicher Positionen, an die Erben herauszugeben. Im Nutzungsvertrag vereinbarte Ausschlüsse der Vererbbarkeit der Rechtspositionen gehen aber vor.

Für die *öffentlich verfügbaren* personenbezogenen Informationen über den Verstorbenen, z.B. die Daten einer eigenen Homepage oder eines Internet-Blogs, nehmen die Angehörigen die datenschutzrechtlichen Löschungsrechte[145] wahr. Die insoweit ursprünglich dem Verstorbenen zustehenden Rechte erlöschen nicht mit dem Tod. Denn dem Grundgedanken des Datenschutzrechts entspricht es, den Schutz persönlicher Daten nicht auf die Lebenszeit des Betroffenen zu begrenzen, sie insbesondere nicht *post mortem* zur freien Verfügungsmasse mutieren zu lassen.

V. Rechtspolitische Desiderate

Der digitale Nachlass ist für den Unbedarften Grund zur Ratlosigkeit, für den Kundigen demgegenüber Anlass zum Handeln. Jeder tut gut daran, noch zu Lebzeiten Bestimmungen darüber zu treffen, was mit seinem digitalen Nachlass geschehen soll. Bislang machen die Menschen davon kaum Gebrauch – geschweige denn, dass sie sich darüber Gedanken machen, was mit ihren Datenfriedhöfen nach dem Tod geschehen soll. Sie halten es vielmehr mit *Epikur*: „Mit dem Tod habe ich nichts zu schaffen. Bin ich, ist er nicht. Ist er, bin ich nicht."

Franz Kafka war da vorausschauender. In seinem Testament hatte er verfügt, dass seine unveröffentlichten Manuskripte nach seinem Tod verbrannt werden sollen. Dass sich sein Freund und Nachlassverwalter *Max Brod* über diesen letzten Willen hinwegsetzte, entpuppte sich als Glücksfall der Kulturgeschichte. Wichtige Teile des Schaffens von *Kafka* wären uns sonst verborgen geblieben.

144 Der Rekurs auf das BDSG erweist sich dabei als nicht unproblematisch, handelt es sich doch um einen Bußgeldtatbestand, der besonderen Anforderungen an die Normenklarheit unterworfen ist.

145 Dazu oben S. 113.

1. Wenn das Passwort aus dem Jenseits kommt…: Digitale Testamentsvollstrecker als (kritikwürdige) Antwort des Marktes auf die Herausforderungen digitaler Datenfriedhöfe

So bedeutsam wie das Oeuvre von *Kafka* ist der digitale Nachlass des durchschnittlichen Internetnutzers nicht. So gut geordnet wie der Nachlass zu *Kafkas* Zeit sind unsere diversen digitalen Identitäten im Zweifel auch nicht. Bei der Unzahl digitaler Fußspuren, die die Menschen im Internet hinterlassen, wächst es sich für die Erben in der Folge zu einer immer größeren Herausforderung aus, einen Überblick über die digitalen Identitäten zu behalten bzw. zu gewinnen.

Der junge Amerikaner *Jeremy Toemans* machte aus dieser Not eine Tugend:[146] Als sich seine Familie nach dem Tod seiner 94-jährigen Großmutter mit der Frage konfrontiert sah, wie denn die vielen digitalen Identitäten der technikbegeisterten alten Dame ermittelt werden sollten, brachte ihn das auf eine Geschäftsidee. Er gründete ein Internetunternehmen, das sich der Verwaltung von Passwörtern zu Internet-Accounts aller Couleur verschreibt und die hinterlegten Zugangsdaten im Todesfall an die zuvor dekretierten Vertrauenspersonen herausgibt. Anwender können in diesem Online-Datentresor Passwörter und Zugangsdaten zu sozialen Netzwerken, E-Mail-Konten und zum Online-Banking hinterlegen. *Legacy Locker*.com gilt heute als Marktführer unter den digitalen Nachlassverwaltern. Immer neue digitale Testamentsvollstrecker, wie z.B. *www.datainherit.com*, *www.deathswitch.com*, *netarius.com*, strömen auf den Markt und bieten im Kampf gegen das private digitale Chaos ihre Dienste feil. Üblicherweise ist dort eine Vertrauensperson zu benennen, an welche die Daten herausgegeben werden sollen. Die Existenz solcher Passwort-Tresore ist ein Beleg für den bislang unbefriedigten Bedarf an einer praktikablen Verwaltung des digitalen Nachlasses.

Ob sie eine sachgerechte Antwort darauf bilden, steht auf einem anderen Blatt. Denn die Dienste bergen massive Risiken. Regelmäßig ist die Herausgabe der Account-Zugangsdaten an den digitalen Testamentsvollstrecker Voraussetzung für die Inanspruchnahme seiner Dienste. Die Herausgabe von Account-Zugangsdaten widerspricht aber allen Prinzipien der Geheimhaltung von Passwörtern. Sie setzt ein schier grenzenloses Gottvertrauen voraus, das zahlreiche ausländische Anbieter mit niedrigen Sicherheitsstandards nicht verdienen. In der Regel erhalten die Kunden auch weder Einblick in die Sicherheitsmechanismen noch haben sich bislang Gütesiegel, Qualitätskontrollen oder gar eine wirksame

146 *Carolin Neumann*, Spiegel Online, Was nach dem Tod mit dem Facebook-Profil passiert, vom 17.03.2009, abrufbar unter:http://www.spiegel.de/netzwelt/web/0,1518,613708,00.-html (9.10.2012).

staatliche Aufsicht etabliert, die vertrauensbildende Orientierungsmarken setzen könnten.

Ob der Erblasser sein Leben eher aushaucht als der digitale Totengräber, ist auch nicht besiegelt. Erste Anbieter, wie *Ivedo* und *mywebwill*, haben bereits das Zeitliche gesegnet. Im Falle der Insolvenz des digitalen Bestatters ist weder die Funktionsfähigkeit des Dienstes noch in jedem Falle die Sicherheit der hinterlegten Daten gewährleistet. Nicht zuletzt stellt ein solcher Daten-Sarkophag, in dem massenhaft Kennwörter gespeichert sind, ein vorzügliches Angriffsziel für neuzeitliche digitale Grabräuber in Gestalt krimineller Hacker dar.

Auch ein Notar als klassischer Testamentsvollstrecker bietet nur bedingt eine zufriedenstellende Regelung digitaler Nachlasssorge. Denn es gehört zu den unumgänglichen Verhaltensregeln, sichere Passwörter nicht nur einmalig zu erstellen, sondern auch regelmäßig zu ändern. Unabhängig davon, ob man schon die Hinterlegung bei einem Notar als Sicherheitsrisiko einstufen will, erweist sich das Prozedere bei Einschaltung eines klassischen Testamentsvollstreckers daher zumindest als ausgesprochen unpraktisch.

2. Datennachlassmanagement, Profileinstellungen und Aktivierungsregeln als sachgerechte Mechanismen einer digitalen Testierfreiheit

Die Schwierigkeiten der Verwaltung des digitalen Nachlasses lassen sich zielgenauer und praktikabler auf anderem Wege bewältigen: durch Inpflichtnahme der Diensteanbieter für ein Einwilligungsmanagement und die digitale Testierfreiheit sichernde Profileinstellungen. Solche Verpflichtungen sollte der Gesetzgeber *de lege ferenda* etablieren.

a) Erklärungsmanagement

Bislang können die Nutzer in den Menüs sozialer Netzwerke nahezu alles regeln – nur eines regelmäßig nicht: den Umgang mit den persönlichen Daten nach dem Tod. Angesichts der damit verbundenen Vorwirkungen ist es integraler Bestandteil sachgerechten Persönlichkeitsschutzes, eine verlässliche Lösung auch für diese Zeit zu entwickeln. Wer nicht weiß, was mit seinen Daten nach seinem Tode passieren wird, sieht sich einer Unsicherheit in der Ausübung seines informationellen Selbstbestimmungsrechts ausgesetzt. Sofern die Vertragspartner dies nicht im Wege einer privatautonomen Regelung individualvertraglich gestalten, ist der Gesetzgeber im Interesse eines umfassenden Schutzes der Persönlichkeit legitimiert und aufgerufen, die Unsicherheit der Nachlasssorge zu beseitigen.

Aus den Überlegungen zum postmortalen Persönlichkeitsschutz ergeben sich insoweit wesentliche Anforderungen an eine sinnvolle rechtspolitische Ausgestaltung:

Der Gesetzgeber sollte den Diensteanbietern abringen, den Nutzern schon beim Anlegen eines neuen Accounts die Möglichkeit zu eröffnen, explizite (zu jedem späteren Zeitpunkt änderbare) Vorgaben hinterlegen zu können, was mit den gespeicherten Daten im Todesfall geschehen soll. § 13 Abs. 4 TMG sollte um eine Nr. 3a ergänzt werden, der die Diensteanbieter verpflichtet sicherzustellen, dass „die Nutzer die Möglichkeit haben, Regelungen für die Verwendung ihrer personenbezogenen Daten nach dem Tod zu treffen“. Ein Nutzer kann dann wählen zwischen der Weitergabe der Account-Daten an bestimmte Personen, der unverzüglichen Löschung des Accounts mitsamt aller hinterlegten Daten oder der Sperrung und Umschaltung in einen Kondolenzmodus.[147] Letzterer erweist sich insbesondere für soziale Netzwerke als eine sachgerechte Gestaltungsoption. Denn lebenden wie verstorbenen Nutzern kann daran gelegen sein, die Bekanntschaften zu Personen, mit denen sie zu Lebzeiten verbunden waren, weiterhin in dem Netzwerk abzubilden. Ein Kondolenzmodus ermöglicht es, die digitale Erinnerung an den Verstorbenen wach zu halten und gleichzeitig die Daten des Betroffenen nach seinem Tod weiterhin verwendbar zu belassen, ohne den Eltern oder sonstigen nahen Angehörigen Zugang zu sensiblen personenbezogenen Daten des Verstorbenen zu eröffnen.

Den ambivalenten Wünschen der Account-Inhaber, die je nach Art und Inhalt der mit den Zugängen verknüpften Daten unterschiedlich ausfallen und vollkommen gegensätzlich sein können, lässt sich so durch eine präferenzorientierte Eröffnung von Handlungsoptionen angemessen gerecht werden. Das trägt der Grundintention des postmortalen Persönlichkeitsschutzes in besonderer Weise Rechnung. Dessen Aufgabe besteht darin, das Geheimhaltungsvertrauen der Lebenden gegen eine Gefährdung ihrer Persönlichkeitsentfaltung bei der Bewegung in der „digitalen Welt" durch die ungewollte postmortale Offenbarung von Telemediendienstgeheimnissen zu immunisieren. Dem ist schon vorgebeugt, wenn sichergestellt ist, dass der Einzelne zur Erklärung darüber aufgefordert wird, welche Teile des digitalen Lebens nach dem Tode offen gelegt werden und welche nicht – und darüber hinaus eine sachgerechte persönlichkeitsschützende Grundentscheidung als Reserveregelung für den Fall getroffen wird, dass der

147 Diese Lösung ist auch passgenauer und präferenzkompatibler als die pauschale Löschungspflicht, die der Bundesrat in § 13 Abs. 4 S. 1 Nr. 4 TMG seines Entwurfs zur Änderung des Telemediengesetzes – allerdings auch ohne unmittelbaren Bezug zum Ableben eines Nutzers – vorgesehen hat; BT-Drucks. 17/6765, S. 5 und 9.

Bürger sein lebzeitiges Selbstbestimmungsrecht ungenutzt lässt.[148] Der Bereich, in dem der Einzelne sich gegebenenfalls einer Selbstzensur unterwirft, wird dadurch berechen- und handhabbar.

Die technische Verpflichtung auf ein Datennachlassmanagement sollte eine Aktivierungsfunktion der Diensteanbieter flankieren: „(…) Sofern der Nutzer keine Erklärung über die Verwendung seiner personenbezogenen Daten nach dem Tod getroffen hat, fordert der Diensteanbieter ihn in regelmäßigen Abständen zu einer entsprechenden Erklärung auf, soweit dieser dem nicht widerspricht" (§ 13 Abs. 4 Nr. 3a S. 2 TMG-E). Dem Diensteanbieter obliegt es dann, den Account als digitaler Totengräber in den postmortalen Zustand zu versetzen. Treffen die Nutzer gleichwohl keine Verfügung, sollte die verfassungsrechtliche Wertung zum Tragen kommen, nach welcher die Personenbezogenheit der in den Accounts hinterlegten Daten den Erben eine Account-Autopsie im Zweifel verschließt,[149] den Angehörigen aber die Wahrnehmung der datenschutzrechtlichen Rechte im Hinblick auf die im Internet öffentlich verfügbaren personenbezogenen Informationen anvertraut ist.[150]

aa) Erklärungsmanagement als „Nudge"

Eine solche Lösung entspricht in der Sache dem (durchaus nicht unumstrittenen[151]) rechtsphilosophischen Regelungskonzept des liberalen Paternalismus.[152]

148 Zur Rechtslage im Falle fehlender Erklärung des Verstorbenen hinsichtlich der Bestattungsart, einer Organentnahme bzw. einer Sektion vgl. etwa *Schönberger* (Fn. 51), S. 92 ff., 163 ff., 187 ff.; *Müller*, Postmortaler Rechtsschutz – Überlegungen zur Rechtssubjektivität Verstorbener, 1996, S. 121 ff.; BSG, NZS 2006, 43 (46 f.).

149 Vgl. dazu oben IV. 2. a. bb., S. 100.

150 Vgl. dazu oben IV. 2. b., S. 112.

151 Berechtigt ist durchaus die Kritik, dass der liberale Paternalismus tatsächlich weniger liberal ist, als er sich gibt. Denn er unterstellt den Menschen, dass Präferenzentscheidungen, die für sie langfristig negative Folgerungen zeitigen können, kurzfristig aber einen Genuss oder Gewinn versprechen, z.B. das Rauchen, der Verzicht auf frühzeitige Altersvorsorge, nicht den tatsächlichen Präferenzen der Menschen entsprechen. Dafür fehlt es aber an validen und objektivierbaren Indikatoren. Begreift man den liberalen Paternalismus demgegenüber als ein staatliches Regulierungskonzept, das auf die Erreichung guter gesamtgesellschaftlicher Ergebnisse auf der Grundlage von „abgenötigten" Präferenzentscheidungen mithilfe sanften staatlichen Drucks hinwirkt, präsentiert er sich im Verhältnis zu anderen Rationalisierungskonzepten, insbesondere staatlichen Wahlentscheidungen, durchaus, je nach Regelungskontext, als attraktive und grundrechtsschonende Governance-Alternative; vgl. zur Kritik am Modell des liberalen Paternalismus auch *Eidenmüller*, JZ 2011, 814 (819 f.); mit dem Modell hingegen sympathisierend *Smeddinck*, Die Verwaltung 2011 (44), 375 ff. *Kirste* (JZ 2011, 805 ff.) schlägt eine Differenzierung zwischen einem harten und einem weichen Paternalismus vor.

Sein Bestreben ist es, staatliche Regelungsziele, die sich auf der Grundlage privatautonomer Gestaltung der Vertragspartner bisher nicht in einer hinreichenden bzw. erwünschten Weise einstellen, durch staatliche Induzierung selbstregulativer Wahlhandlungen zu erreichen. Die Bürger sollen individuelle Präferenzentscheidungen, die sie infolge von Unwissenheit, Nachlässigkeit oder zeitlichen Inkonsistenzen schädigender Verhaltensweisen etc. häufig unterlassen, ohne staatlichen Zwang, aber auf der Grundlage eines staatlichen „Nudge" (also eines „Schubsers") treffen und damit zur Erreichung von Gemeinwohlzielen und sachgerechten Regelungsergebnissen beitragen.

Einer Aufforderung zur Offenbarung der Präferenzen hinsichtlich des Umgangs mit den eigenen digitalen Hinterlassenschaften kann insoweit eine geeignete Anschubfunktion zukommen. Dem gleichen Grundgedanken ist die jüngst gesetzlich etablierte Entscheidungs- bzw. Erklärungslösung zur Organentnahme verschrieben.[153] Sie soll mitmilfe eines solchen „Schubsers" die bislang noch klaffende Lücke zwischen der grundsätzlich vorhandenen hohen Spendenbereitschaft und der tatsächlichen Spendentätigkeit schließen bzw. verkleinern.

bb) Erklärungsmanagement versus Erklärungspflicht vor dem Spiegel der Verfassung

Erklärungspflichten gehen mit Eingriffen in die Grundrechte der Bürger einher. Sie berühren namentlich die durch Art. 2 Abs. 1 GG verfassungsrechtlich geschützte Privatautonomie. Diese verbürgt auch die (negative) Freiheit, keine Verfügungen für den Fall des Todes zu treffen oder sich mit den damit verbundenen Folgen gar nicht auseinanderzusetzen. Gesetzlich begründete Erklärungspflichten sind daher rechtfertigungsbedürftig, insbesondere Verhältnismäßigkeitsanforderungen unterworfen. Die verpflichtende Einräumung der *Möglichkeit*, letztwillige Verfügungen über den digitalen Nachlass zu treffen (in Verbindung mit der Aufforderung zur Abgabe einer Nachlasserklärung und einer gesetzlichen „Reserveregelung" für den Fall des Ausbleibens einer Erklärung), erweist

152 Vgl. dazu *Sunstein/Thaler*, Nudge, 2009.

153 Sie besteht darin, potenzielle Organspender in regelmäßigen Abständen mit der Frage zu konfrontieren, ob sie im Falle ihres Todes ihre Organe zu spenden bereit sind. Jeder Bürgerin und jedem Bürger bleibt es aber weiterhin freigestellt, eine Erklärung zur Organ- und Gewebespende abzugeben. Das Gesetz betont diese Entscheidungsautonomie ausdrücklich (§ 2 Abs. 2a Transplantationsgesetz). Die Regelung ist von dem Gedanken des Respekts vor der individuellen Entscheidung getragen, sich nicht erklären zu wollen (vgl. Entwurf eines Gesetzes zur Regelung der Entscheidungslösung in Transplantationsgesetz, BT-Drucks. 17/9030, S. 17).

sich insofern gegenüber einer Erklärungspflicht als grundrechtsschonender. Sieht der Gesetzgeber für den Fall einer fehlenden individuellen Erklärung des Erblassers eine gesetzliche Ausfallregelung (namentlich sachgerechterweise die Nichtweitergabe der Account-Daten an die Nachfahren) und einen obligatorischen Hinweis des Diensteanbieters auf die Folgen einer Nicht-Erklärung vor, führt er die Rechtsfragen des digitalen Nachlasses einer ebenso grundrechtsadäquaten wie effektiven Regelung zu.

b) Aktivierungsregeln

Ein Problem beseitigt das Einwilligungsmanagement freilich nicht: Es verfügt zwar, was im Todesfall mit den Daten geschieht. Es sichert aber nicht, dass der Anbieter von dem Tod erfährt. In der Regel ist den Erben gerade unklar, welche Accounts überhaupt zu den digitalen Hinterlassenschaften gehören. Anders als für den Großteil der Vermögensgegenstände der Offline-Welt existieren hinsichtlich der Accounts meist keine Aufzeichnungen – allenfalls E-Mails mit Anmeldebestätigungen oder Ähnliches, die die Adressaten nicht selten wieder löschen. Um den digitalen Nachlass vollständig zu erfassen, bedürfte es eines „Account-Inventars". Statt durch Dienste wie *legacylocker.com* lässt sich dieses Ziel aber auch durch Aktivierungsregeln der Anbieter sicherstellen, die bei längerer Inaktivität des Nutzers Nachfragen an den Account-Inhaber bzw. benannte Vertrauenspersonen richten, bzw. durch die vorsorgende Benachrichtigung der Vertrauenspersonen über ihre Einsetzung als digitaler Testamentsvollstrecker und die damit verbundene Bitte, im Todesfall Kontakt mit dem Diensteanbieter aufzunehmen.

VI. Fazit

Unsere Schritte werden verstummen, unsere digitalen Fußspuren aber bleiben. Das Recht, sie verwischen zu dürfen, ist im digitalen Zeitalter wichtiger Bestandteil des Persönlichkeitsschutzes. Die Diensteanbieter dürfen den Erben den Schlüssel zum digitalen Postfach des Erblassers daher grundsätzlich nicht aushändigen, es sei denn, die Herausgabe entspricht dessen ausdrücklichem oder mutmaßlichem Willen.

Die Gerichte in den USA haben im Falle des Soldaten *Justin Ellsworth*[154] anders entschieden. Sie verurteilten *Yahoo*, den Eltern des Soldaten den Zugang zu

154 Vgl. dazu bereits oben Fn. 2.

dessen Account vollständig einzuräumen. Deutsche Gerichte sollten dem Geheimhaltungsvertrauen Verstorbener entsprechend dem Stellenwert des Persönlichkeitsschutzes in unserer Verfassung ein höheres Gewicht einräumen. Sie sollten den Angehörigen den Zugang zum Account grundsätzlich verwehren, soweit nicht lediglich vermögensrechtliche Rechtspositionen im Raum stehen. Deren Durchsetzung müssen die Diensteanbieter als „Tresorverwalter" den Erben ermöglichen.

Die Idee des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und Privatheit auf Distanz (Art. 10 Abs. 1 GG) würde wie eine Seifenblase zerplatzen, wenn sich die Nutzer nicht darauf verlassen könnten, dass ihre Daten auch nach ihrem Tode nur denjenigen zugänglich gemacht werden, denen sie diese zugänglich machen wollten. Die Entfaltung der Persönlichkeit im Informationszeitalter wäre namentlich erheblich gehemmt, müssten Nutzer befürchten, ihre personenbezogenen Daten würden nach ihrem Tode zum Spielball der Nachwelt.

Um Zweifelsfälle und Unsicherheiten bei der Behandlung des digitalen Nachlasses ebenso schonend wie präferenzkompatibel *de lege ferenda* auszuschließen bzw. zu minimieren, sollte der Gesetzgeber die Diensteanbieter zu einem Einwilligungsmanagement und zu Profileinstellungen für das digitale Vermächtnis verpflichten, welche die Ausübung der Verfügungsmacht für die Zeit nach dem Tod sichern. § 13 Abs. 4 TMG sollte um eine Nr. 3a ergänzt werden, welche die Nutzer Regelungen für die Verwendung ihrer personenbezogenen Daten nach dem Tod zu treffen befähigt, und die Diensteanbieter verpflichtet, die Nutzer in regelmäßigen Abständen zur Abgabe einer ggf. noch ausstehenden Erklärung über die Verwendung ihrer Daten nach dem Tod aufzufordern. § 13 Abs. 4 Nr. 3 TMG sollte dann ergänzend klarstellen, dass die Diensteanbieter „Erben den Zugang zu persönlichen Nachrichten nur verschaffen dürfen, wenn der Erblasser das ausdrücklich verfügt hat".[155]

Was für die durch ein Passwort als Geheimhaltungsschutz gesicherten Account-Daten eines Verstorbenen gilt, hat nicht in gleicher Weise für die im Internet *öffentlich einsehbaren Daten*, z.B. einer privaten Homepage, Gültigkeit. Für sie und die auf sie bezogenen datenschutzrechtlichen Rechte kommt den Angehörigen ein zeitlich (sinnvollerweise auf 30 Jahre) befristetes Wahrnehmungsrecht zu.

155 Ein (grundsätzlich denkbarer und *de lege lata* durchaus rechtlich erforderlicher) Rekurs auf den mutmaßlichen Willen des Erblassers ist im Falle des hier vorgeschlagenen Einwilligungsmanagements regelmäßig nicht mehr erforderlich. Der Wille ergibt sich dann nämlich aus den ausdrücklichen, im Profil hinterlegten postmortalen Verfügungen des Nutzers. Entsprechend entfällt auch die häufig bestehende Unsicherheit in der Ermittlung des mutmaßlichen Willens.

VII. Ausblick – Online-Communitys für Tote?

Der digitale Nachlass ist nicht nur weitgehend juristisches Neuland. Er ist auch, wie an dem Boom digitaler Testamentsvollstrecker deutlich wird, ein sich etablierender Markt. Was in der Offline-Welt nicht funktioniert – unsterblich zu werden –, wird im Cyberspace Realität. Dass mancherorts bereits Grabsteinen Quick Responce-Codes (QR-Codes) eingraviert werden, die Links zu einer Online-Präsenz des Verstorbenen, etwa einer eigens für den Verstorbenen eingerichteten Trauerseite oder einem Wikipedia-Eintrag o.ä., preisgeben, gibt nur einen ersten Vorgeschmack auf den Friedhof sowie das Requiem der Zukunft. Auch Plattformen für die digitale Unsterblichkeit wie *Stayalive.com* schießen gegenwärtig wie Pilze aus dem Boden: Menschen können sich dort zu Lebzeiten ein virtuelles Mausoleum errichten; Angehörige können Fotoalben und Kondolenzbücher anlegen und Beileidbekundungen auf den Weg bringen. Bei *DeadSoci.al* können Lebende für die Zeit nach ihrem eigenen Tod Videos, Audio- oder Textnachrichten „aus dem Jenseits" zur Versendung über soziale Netzwerke vorbereiten. Diese Form der Digitalisierung ist weniger ein Sargnagel der Pietät als eine Erscheinungsform einer Exterritorialisierung der Erinnerungs- und Bestattungskultur. Die Trauerkultur erfährt einen grundlegenden Wandel: Das digitale Leichenbegängnis trägt dazu bei, die räumliche Verbannung von Tod und Trauer aus dem gesellschaftlichen Alltag abzuschwächen. Das Internet wird zur Gedenkstätte. Die Trauer des digitalen Zeitalters hat ein anderes Gesicht und neue Ausdrucksformen. Es entsteht eine entgrenzte, virtuelle Zone der Verarbeitung, des Trostes und der Erinnerung. An einem ändert die virtuelle Grabpflege freilich nichts. Die schönste Gedenktafel, die ein Mensch bekommen kann, wird auch weiterhin nicht im Internet zu finden sein. Sie „steht in den Herzen der Mitmenschen" (*Albert Schweitzer*).