Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet

ARTICLE *in* JURISTENZEITUNG · DECEMBER 2012

DOI: 10.2307/23327860

1 AUTHOR:

Mario Martini

Deutsche Universität für Verwaltungswisse…

12 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Zweitveröffentlichung (iSd § 38 Abs. 4 UrhG) des Beitrags: Der Digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet, Original abgedruckt in der JZ 2012, S. 1145 - 1155

Professor Dr. Mario Martini, Speyer*

Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet

Im digitalen Zeitalter hinterlassen Nutzer im Internet unzählige digitale Fußspuren. Verwaiste Online-Profile oder intime Nachrichten eines E-Mail-Accounts hält der Cyberspace grundsätzlich für die Ewigkeit fest. Welches Schicksal die persönlichen und geschäftlichen Internetdaten nach dem Tod erfahren, darüber macht sich kaum ein Nutzer Gedanken. Nicht nur in der Bevölkerung, auch in der Rechtswissenschaft ist der digitale Nachlass eine Terra incognita. Der Beitrag zeichnet rechtsdogmatische und rechtspolitische Orientierungslinien. Er zeigt auf, warum die Anwendungspraxis zahlreicher Account-Anbieter rechtswidrig ist.

I. Wenn das Online-Profil den Körper überlebt: Die Eigenheiten des digitalen Nachlasses und die Herausforderungen moderner Datenfriedhöfe

Scheidet ein Mensch aus dem Leben, stehen die Angehörigen nicht nur vor einem schweren Abschied und schmerzlichen Verarbeitungsprozessen. Sie sind auch mit der Herausforderung der Nachlassabwicklung konfrontiert. Im digitalen Zeitalter ist diese um eine wichtige Facette reicher geworden: den digitalen Nachlass. Immer häufiger treten Hinterbliebene an die Diensteanbieter mit dem Ansinnen heran, in die Accounts des Verstorbenen Einsicht zu nehmen und die Rechte für Homepage-Auftritte, Blog-Einträge Verstorbener etc., wahrzunehmen. Dürfen aber *Facebook, Google+, Xing, Web.de* & Co. den Erben die Account-Obduktion gestatten? Schafft das eine legitime Chance der Begegnung mit dem Leben des Verstorbenen oder öffnet es eine Büchse der Pandora?

Als digitalem Abziehbild der Person kommt dem digitalen Nachlass nicht nur eine besondere Bedeutung für die –Wahrnehmung der Persönlichkeit des Einzelnen 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 den sonstigen Hinterlassenschaften des Verstorbenen. Das erschwert ihre sachgerechte Behandlung.

1. Besondere Schutzbedürftigkeit und Unvergänglichkeit der digitalen Hinterlassenschaften

Die unablässige Freigabe von Nutzerdaten im Internet legt ein immer feineres digitales 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

---

* *Mario Martini* ist Lehrstuhlinhaber an der Deutschen Universität für Verwaltungswissenschaften Speyer. Der Beitrag gibt die gekürzte Fassung eines Vortrages wieder, den er im Rahmen der Tagung „Facebook, Google & Co. – Chancen und Risiken“ im April 2012 gehalten hat. Die vollständige Fassung des Beitrages ist in dem zugehörigen Tagungsband abgedruckt. Der Autor dankt den Mitarbeitern seines Lehrstuhls für die Unterstützung, allen voran *Clemens Becker*, *Yvonne Schmid* und *Eva Herzog*.

digitalen Identitäten erlauben tiefste Einblicke in die intime Persönlichkeitssphäre, ohne dabei aber den Gesetzen der Vergänglichkeit zu unterliegen: Während in der analogen Welt Vergänglichkeit die Regel ist, verwischt das Internet digitale Fußspuren nicht. Auch deshalb fördert es ein sehr ambivalentes Verhalten seiner Nutzer zutage. Bei den einen beflügelt es die Idee, die Magie des globalen Netzes in einer öffentlichen Inszenierung für eine digitale Unsterblichkeit fruchtbar zu machen. Andere geben ihre Privatheit im virtuellen Leben angesichts ihres Wunsches nach einem möglichst weiten Schutz ihrer persönlichen Daten eher nolens volens auf. Ob die so in Kauf genommene Kontrollmacht der Diensteanbieter über die Daten als „Währung des Internets" nach dem Tod enden bzw. in die Hände der Erben fallen soll, regelt nahezu kein Nutzer explizit. Ihr digitales Vermächtnis nehmen die Verstorbenen gegenwärtig still mit ins Grab.

2. Gemengelage disparater Daten

Anders als die dem räumlichen Zugriff zugänglichen Habseligkeiten des Erblassers (wie etwa das papierene Tagebuch) ist der digitale Nachlass in den Tiefen des Cyberspace vergraben. Er bündelt eine inhomogene Masse unterschiedlichster Daten – von privaten Daten über elektronische Vertragsdokumente bis hin zu Geschäftsdaten. Für die Hinterbliebenen kann dieser im Netz dämmernde Datenschatz nicht nur von hohem ideellen, sondern auch materiellem Wert sein: In der digitalen Grabkammer schlummern immer häufiger Vertragsdokumente des Erblassers, seien es im Internet eingegangene Abonnementverpflichtungen, Online-Rechnungen der Telekom, 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

Den digitalen Datenschatz aufzuspüren, ist nicht nur mühsame Detektivarbeit. Es braucht auch einen digitalen Schlüssel, um ihn zu heben: die korrekten Zugangsdaten des Nutzer-Accounts. Doch wer kennt schon die Benutzernamen und Passwörter zu all den Accounts, die der moderne Nutzer im Laufe seines virtuellen Lebens anlegt? Sofern die Regeln der Datensicherheit (wie Passwortstärke etc.) eingehalten wurden: niemand. Allerdings verfügen die Diensteanbieter in der Regel über die technische Möglichkeit, auf die Account-Daten zuzugreifen oder die Zugangsdaten zugunsten eines berechtigten Dritten zurückzusetzen. Die Betreiber sind verunsichert, ob und ggf. an wen sie die Zugangsdaten herausgeben dürfen oder gar müssen.

Während viele Erben und Angehörige die Autopsie des Accounts als wichtigen Teil der Trauerarbeit begreifen, sollen sie manche Details aus der digitalen Welt des Verstorbenen aber womöglich gerade nicht erfahren – seien es intime Liebesbriefe einer geheimen Romanze, die Aufarbeitung von Ehekrisen in Chats und Foren, der Austausch über Schenkungsabsichten und Vererbungsstrategien oder Opas gut sortierte Pornosammlung.

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

Unter diesen ambivalenten Ausgangsbedingungen gehen die Diensteanbieter mit den Internet-Accounts Verstorbener sehr unterschiedlich um. Während etwa „*Wer-kennt-wen*", *GMX* und *Web.de* den Erben gegen Vorlage des Erbscheins vollen Zugang zu dem hinterlassenen Account verschaffen,[1] lehnen *Yahoo Deutschland* und *Twitter*[2] das kategorisch ab. Aus ihrer Sicht endet das Vertragsverhältnis mit dem Tod. Nach Ablauf einer Karenzfrist hauchen sie dem Account das

---

[1] In den AGB der Anbieter ist diese Praxis nicht verankert. Sie bestätigten die Vorgehensweise aber auf Rückfrage.

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

Lebenslicht aus.[3] Zwischen diesen Extremen finden sich zahlreiche Mischformen. Die VZ-Portale , namentlich *StudiVZ*, *SchuelerVZ* und mein *MeinVZ*, entscheiden im Einzelfall über den Zugang zum Account.[4] 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*,[5] setzen den Status auf „inaktiv", wenn 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 die Zugangsdaten. Mit der Eröffnung der digitalen Grabpflege verändert *Facebook* 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 andeutungsweise in ihren Allgemeinen Geschäftsbedingungen. Die globale Vernetzung 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. Einen spezifischen rechtlichen Ordnungsrahmen hält er, anders als die Legislative anderer Staaten, insbesondere einiger US-Bundesstaaten, für Datenfriedhöfe nicht vor.[6] Den Grabesschatz bzw. – je nach Sichtweise – die Leiche im Keller hat die deutsche Rechtswissenschaft überhaupt noch nicht entdeckt.[7] 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 in Deutschland – statistisch betrachtet – alle zwei Wochen ein *Facebook*-Nutzer.

Die Antwortsuche bewegt sich im Schnittfeld dreier Rechtskreise, nämlich des Erbrechts (unten III. 1), des Datenschutzrechts (unten III. 2. a aa) und des Verfassungsrechts (unten III. 2. a bb).

III. Der digitale Nachlass als Erbschaft?

Aus einer rein zivilrechtlichen Perspektive sind die Fragen vordergründig schnell beantwortet: Mit dem Tode einer Person geht deren Vermögen als Ganzes im Wege der Universalsukzession auf den Erben über. Das Vermögen als Inbegriff aller geldwerten Rechtsbeziehungen umschließt auch Rechte an einer Internetdomain, Credits in Foto-Communitys sowie Guthaben bei Online-Spielen, aber auch im Internet eingegangene Vertragsverpflichtungen. Solche vermögensrechtlichen Positionen sind vererbbar, nicht-vermögensrechtliche hingegen in der Regel nicht.[8]

---

3 *Twitter* ermöglicht eine Sicherungskopie aller öffentlich zugänglichen Daten; einen direkter Zugang zum Account gewährt das Unternehmen aber nicht.

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

5 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."

6 Vgl. etwa Connecticut Public Act No. 05-136; Rhode Island General Laws, Chapter 33-27; Indiana Code 29-1-13; Oklahoma Statutes, Title 58, Section 269.

7 Bislang lediglich *Hoeren*, NJW 2005, 2113 ff.

8 Ein Indiz für die Nichtvererbbarkeit ist die fehlende Übertragungsmöglichkeit unter Lebenden. Der Teufel steckt allerdings im Detail. Es finden sich zahlreiche Ausnahmen. So ist etwa das Urheberrecht nicht übertragbar (§ 29 Abs. 1 UrhG), wohl aber vererblich. Umgekehrt ist die Mitgliedschaft in einem Idealverein personenbezogen, nicht-vermögensrechtlicher Natur und damit grundsätzlich unvererbbar. Die Vereinssatzung kann jedoch nach § 40 BGB eine andere Regelung treffen.

Zwischen vermögensrechtlichen und nicht-vermögensrechtlichen Positionen nehmen die *Immaterialgüterrechte* eine Zwitterstellung ein: Bei ihnen handelt es sich um unkörperliche Gegenstände mit Vermögenswert. Sie gehen regelmäßig kraft gesetzlicher Sonderregelung (sowohl in ihren vermögens- als auch in ihren persönlichkeitsrechtlichen Elementen) auf die Erben über, z.B. das Urheberrecht nach § 28 Abs. 1 UrhG. Urheberrechtsfähige Inhalte der Erblasser etwa auf Videoplattformen, wie *Youtube* oder *FlickR*, berechtigen die Erben daher regelmäßig, die Herausgabe oder Löschung der entsprechenden Aufnahmen zu verlangen. Bis zum Erlöschen des Urheberrechts 70 Jahre nach dem Tod des Urhebers (§ 64 UrhG) stehen den Erben dieselben gesetzlichen Rechte wie diesem zu (§ 30 UrhG). Sie müssen aber (wiewohl das Urheberrecht nach § 29 Abs. 1 UrhG nicht übertragbar ist), eine – bei Internetdiensten nicht unübliche – Einräumung von Nutzungsrechten gegen sich gelten lassen, die der Erblasser zugunsten eines Diensteanbieters vertraglich versprochen hat (§ 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 zum Beispiel einer Homepage (unten 2. b), wirft Fragen auf. Sie sachgerecht zu beantworten, bereitet Kopfzerbrechen, lassen sich diese Daten doch nicht ohne Weiteres in das binäre Schema vermögensrechtlicher und nicht-vermögensrechtlicher Positionen pressen (dazu sogleich 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.[9]

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.[10]

Nicht jedes schuldrechtliche Rechtsverhältnis geht aber im Wege der Universalsukzession auf die Erben über. Die Übertragbarkeit von Vertragspflichten macht der Gesetzgeber regelmäßig davon abhängig, ob der jeweilige Gegenüber gegen einen Gläubigerwechsel und die damit verbundene Inhaltsänderung geschützt werden muss (Rechtsgedanke des § 399 Alt. 1 BGB). Dergestalt schutzbedürftig sind die Diensteanbieter in der Regel nicht: Sie schließen Verträge über Internet-Accounts regelmäßig ohne Rücksicht auf die Person des Nutzers, meist auch ohne nähere Prüfung der Personenidentität. Die Nutzer nehmen bei ihnen kein persönliches Vertrauen in Anspruch. Der Erbfall ändert das Wesen der zugrunde liegenden schuldrechtlichen Ansprüche 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. Den Erben erwächst daraus dann als Haupt- oder Nebenrecht aus dem Vertrag ein Zugriffsrecht auf die in Internet-Accounts gespeicherten Daten der Erblasser, insbesondere ein Recht auf Auskunft und Herausgabe der Zugangsinformationen.[11]

2. Auswirkungen des Persönlichkeitsschutzes auf die Vererbbarkeit von Account-Daten

Eine alleinige Betrachtung des digitalen Nachlasses durch die rein zivilrechtliche Brille greift jedoch zu kurz. Sie trägt der Bedeutung der Daten für die Persönlichkeitsentfaltung des Einzelnen

---

9 Wenn diese Dateien aber mithilfe eines Passworts gegen den Zugriff durch Dritte gesichert sind, stellt sich wie bei Daten eines Internet-Accounts die Frage, ob die Überwindung einer solchen Zugangssicherung das postmortale Persönlichkeitsrecht des Verstorbenen verletzen kann. Dazu im Einzelnen unten III. 2 a.

10 Vgl. *Leipold*, in: MüKo BGB, 5. Aufl. 2010, § 1922 Rn. 20; *Müller-Christmann*, in: Bamberger/Roth (Hrsg.), Beck´scher Online-Kommentar BGB, Ed. 21, Nov. 2011, § 1922 Rn. 31.

11 Für E-Mails vgl. *Hoeren*, NJW 2005, 2113 (2114).

nicht angemessen Rechnung. Aus den einfachgesetzlichen Vorschriften des Datenschutzrechts und/oder aus dem verfassungsrechtlichen postmortalen Persönlichkeitsschutz kann sich namentlich eine Unzulässigkeit der Passwortweitergabe ergeben.

Das Datenschutzrecht hat als Ausprägung des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) den Auftrag, den Einzelnen vor Beeinträchtigungen des Persönlichkeitsrechts durch den Umgang mit personenbezogenen Daten zu schützen (§ 1 Abs. 1 BDSG). Es reagiert insbesondere auf den Befund, dass (gerade mithilfe moderner Informationstechnologien) in der Synthese aller über eine Person verfügbaren Daten ein umfassendes Persönlichkeitsprofil erschlossen werden kann, das einem erhöhten Gefährdungspotenzial ausgesetzt ist.[12]

Als Schutzinstrument hat der Gesetzgeber für die Daten eines Internet-Accounts nicht nur die allgemeinen Datenschutzgesetze,[13] sondern vor allem die bereichsspezifischen Regelungen des TMG für Telemediendienste auf den Posten gestellt. Soziale Netzwerke im Internet, E-Mail-Accounts und Online-Spiele im Allgemeinen, sind Telemediendienste i.S.d. § 1 Abs. 1 S. 1 TMG.[14] Die bei der Erstellung und Nutzung solcher Accounts anfallenden Daten sind demnach in erster Linie den §§ 11 ff. TMG unterworfen; subsidiär kommen – vorbehaltlich des territorialen und sachlichen Anwendungsbereichs des TMG – über den Verweis des § 12 Abs. 3 TMG auch die allgemeinen datenschutzrechtlichen Regelungen zur Anwendung. Das Fernmeldegeheimnis des § 88 TKG ist demgegenüber nicht berührt: Seine Verpflichtungen zur Geheimhaltung bestehen zwar auch nach dem Ende der Telekommunikationsverbindung fort (§ 88 Abs. 2 Satz 2, Abs. 3 Sätze 2 u. 3 TKG). Das einfachgesetzliche Fernmeldegeheimnis adressiert aber ausschließlich Telekommunikationsanbieter, also diejenigen, die die fraglichen Inhalte übertragen, nicht aber die Inhalteanbieter (wie etwa Facebook) selbst (§ 88 Abs. 2 Satz 1 i.V. mit § 3 Nr. 6 und § 3 Nr. 24 TKG).[15]

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[16] und § 37 Abs. 1 BbgBestG)[17] 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, die der Erblasser über sich angelegt hat (unten b).

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

Nach überkommener Auffassung endet der Datenschutz grundsätzlich mit dem Tod. Ab diesem Zeitpunkt ist dann nach dieser Lesart der Weg frei für den Zugriff der Erben auf den Nutzer-Account, soweit der Erblasser selbst keine expliziten Verfügungen getroffen hat.

---

12 BVerfGE 65, 1 (45).

13 Für den privaten Sektor gilt in erster Linie das BDSG, für öffentliche Stellen zusätzlich die verschiedenen Landesdatenschutzgesetze.

14 Vgl. *Heckmann,* in: ders. (Hrsg.), Internetrecht, 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.

15 Aus den gleichen Gründen ist auch § 206 StGB nicht einschlägig.

16 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«.

17 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.

Das scheint aus dem Grundgedanken des Datenschutzrechts bruchfrei ableitbar: Die datenschutzrechtlichen Regelungen knüpfen an *personenbezogene Daten* an (§ 3 Abs. 1 BDSG i.V. mit § 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 um Informationen über einen *lebenden* Menschen handeln muss.[18] So versteht die Rechtsordnung den Begriff auch regelmäßig in anderen Vorschriften, etwa in § 61 Nr. 1 VwGO.

Eine Stütze findet diese Sichtweise auch in dem Schutzzweck des BDSG. Sein Ziel ist es, die freie Entfaltung der Persönlichkeit zu wahren, indem es eine aktive Teilnahme am Verarbeitungsprozess erhobener Daten gewährleistet.[19] Eine solche ist naturgemäß nur einem lebenden Menschen möglich. Träger des Grundrechts auf freie Entfaltung der Persönlichkeit ist nur die lebende Person.[20] Denn das Grundrecht des Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG als Keimzelle des Datenschutzrechts setzt die Fähigkeit zur Entfaltung einer Persönlichkeit voraus. Diese erlischt aber mit dem Tode.[21]

Die Schutzwirkungen des Persönlichkeitsrechts sind insoweit vor und nach dem Tod verschieden.[22] Entsprechend ist das Allgemeine Persönlichkeitsrecht als höchstpersönliches Nicht-Vermögensrecht auch nicht vererbbar. Die Literatur liest daher in der datenschutzrechtlichen Begriffsbestimmung „personenbezogene Daten“ das Wort „lebend“ als ungeschriebene Voraussetzung mit.

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 bildet sich die Verpflichtung heraus, die Daten Verstorbener den Erben im Zweifel nicht zugänglich zu machen (unten bb).

aa) (Einfachgesetzlicher) Postmortaler Datenschutz?

(1) Argumente für die Anwendbarkeit der Vorschriften des Datenschutzrechts auf Daten Verstorbener

Bei genauerem Hinsehen setzen die datenschutzrechtlichen Wendungen „personenbezogene Daten“ und „natürliche Person“ nur die Beziehung 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.[23] 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 Verstorbene keine Möglichkeit der aktiven Teilnahme am Verarbeitungsprozess mehr hat, rechtfertigt es nicht, ihm den besonderen Persönlichkeitsschutz vorzuenthalten, den sensible personenbezogene Daten verdienen.

Wiewohl das Datenschutzrecht vorrangig die lebende Person und deren Persönlichkeits*entfaltung* im Blick hat, löscht der Tod umgekehrt die bereits gereifte Persönlichkeit nicht rückwirkend aus. Das Persönlichkeitsbild lebt weiter und bleibt verletzbar. Die Daten Verstorbener würden zum Plünderungsobjekt der Nachwelt, hätten sie nicht mehr am Schutz des Datenschutzrechts teil. Ihnen den postmortalen Datenschutz zu versagen, bliebe überdies nicht ohne

---

18 In diesem Sinne *Buchner*, in: Taeger/Gabel (Hrsg.), BDSG, 2010, § 3 BDSG Rn. 8; *Dammann*, in: Simitis (Hrsg), BDSG 7. Aufl. 2011, § 3 BDSG Rn. 17; *Kühling/Seidel/Sividris*, Datenschutzrecht, 2. Aufl. 2011, S. 79.

19 *Dammann*, in: *Simitis* (Fn. 18), § 3 BDSG Rn. 17.

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

21 Zum postmortalen Persönlichkeitsrecht vgl. aber unten III. 2. a bb.

22 Der BGH zeigt sich dabei für das als sonstiges Recht im Sinne des § 823 Abs. 1 BGB entwickelte, einfachgesetzliche Persönlichkeitsrecht weitaus schutzoffener als das *BVerfG* für das verfassungsrechtliche postmortale Persönlichkeitsrecht. Zum bereits früh gewährten Anspruch auf Unterlassung bzw. Widerruf ehrverletzender Äußerungen vgl. nur BGHZ 50, 133 (137).

23 In diesem Sinne etwa auch § 5 Abs. 2 S. 1 BArchG und § 7 Abs. 1 Satz 3 ArchG NRW.

Auswirkung auf das Verhalten und die Persönlichkeitsentfaltung zu Lebzeiten.[24] Denn auf die Vertraulichkeit und Integrität ihrer Daten könnten die Lebenden nicht mehr vertrauen.

Ohne einen solchen Schutz wäre nicht zuletzt rechtlich nur schwer konstruierbar, warum (allgemein für möglich gehaltene) testamentarische Verfügungen oder postmortale Vollmachten über den Umgang mit den eigenen Daten, insbesondere die Ausübung von Löschungsrechten, für die Zeit nach dem Tod bindend sein können.[25] Denn solche Verfügungen auf den Todesfall setzen sachlogisch voraus, dass die auszuübenden Rechte, auf die sich die Vollmacht bezieht, nach dem Tod des Account-Inhabers fortbestehen können.

Auch andere einfachgesetzliche Regelungen, wie § 35 Abs. 5 SGB I für die Sozialdaten eines Verstorbenen oder die Regelungen in § 22 S. 3 KunstUrhG 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 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. Die Vorschriften tragen in sachgerechter Weise dem Umstand Rechnung, dass die fortschreitende Gefährdung personenbezogener Daten, die mit der Durchdringung des Alltags durch das Internet und seine vielfältigen digitalen Angebote einhergeht, vor den Daten eines Verstorbenen nicht haltmacht.

Bezieht man die Daten eines Verstorbenen in den Kreis der personenbezogenen Daten ein, ist der rechtliche Rahmen gesteckt, um einem Missbrauch der Daten nach dem Tod entgegenzuwirken. Diese Auslegung der einfachgesetzlichen Regelungen entspricht auch der Zielvorstellung der Datensparsamkeit und dem „engen Gebot der Zweckbindung“[26], von dem das Datenschutzrecht der Telemediendienste durchdrungen ist: Den Diensteanbietern sollen die Informationen über Personen zeitlich grundsätzlich nur solange zukommen, wie dies zur Bereitstellung von Telemedien erforderlich ist (vgl. § 12 Abs. 2 TMG). Mit dem Gedanken der Datensparsamkeit korrespondiert in dem Umfang ein Recht auf Vergessenwerden, das insoweit dem deutschen Datenschutzrecht bereits eingeschrieben ist.

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

Gewähren die datenschutzrechtlichen Bestimmungen des BDSG und des TMG demnach auch einen postmortalen Schutz personenbezogener Daten,[27] ist damit freilich die entscheidende Frage noch nicht beantwortet, ob sie auch die Freigabe der Accountdaten gegenüber den Erben untersagen. Dafür bedürfte es einer datenschutzrechtlichen Geheimhaltungspflicht des Diensteanbieters im Binnenverhältnis 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 wird diese Regelungslücke nicht füllen. Es begrenzt ausschließlich die Befugnis zur Datenverarbeitung im Verhältnis zwischen Nutzer und Diensteanbieter. Eine Norm, 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 Geheimhaltung gegenüber dem Erben freilich durchaus: namentlich für die Einsichtnahme in die Krankenpapiere eines Verstorbenen[28], das anwaltliche und notarielle Beratungsgeheimnis (§ 43a Abs. 2 Satz 1 BRAO, § 18 Abs. 1, Abs. 2 Halbsatz 2 BNotO) und das Archivgeheimnis (§ 5 Abs. 2 S. 1 BArchG). Die

---

[24] Dazu im Einzelnen unten III. 2. a. bb. (1) β, S. 10

[25] Vgl. *Meents,* in: Taeger/Gabel (Fn. 18), § 6 BDSG Rn. 3; *Wedde*, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 4.4 Rn. 87.

[26] *Roßnagel*, NZV 2006, 281 (285); *Spindler/Nink* (Fn. 14), § 12 TMG Rn. 7 m.w.N.

[27] So auch *Bergmann/Möhrle/Herb*, BDSG, Losebl. (Stand: Sept. 2011), § 3 Rn. 7.

[28] Dazu etwa BGH, NJW 1983, 2627; BSG, NJW 1986, 3105; BAG, NJW 2010, 1222; *Bender*, Das postmortale Einsichtsrecht in Krankenunterlagen, 1998, S. 23 ff.

Verletzung von Privatgeheimnissen sanktioniert der Gesetzgeber – auch nach dem Tod des Betroffenen – mit dem scharfen Schwert des Strafrechts: Die Verschwiegenheitspflicht besteht ausweislich des Normbefehls des § 203 Abs. 4 StGB für den Arzt und andere berufliche Geheimnisträger, wie Steuerberater und Berufspsychologen, auch nach dem Tod unverändert fort.[29] Dem liegt die gesetzgeberische Vorstellung zugrunde, dass das bipolare Vertrauensverhältnis zwischen dem Geheimnisträger und dem Patienten gegen das Eindringen Dritter besonders schutzbedürftig ist. Soll es seine Funktion sachgerecht erfüllen, bedingt das die Fortwirkung der Schweigepflicht über den Tod hinaus.[30] Einsicht nehmen darf der Erbe in die Krankenunterlagen nur, soweit eine tatsächliche oder mutmaßliche[31] Einwilligung des Verstorbenen vorliegt oder vermögensrechtliche Ansprüche im Raum stehen, z.B. Ersatzansprüche wegen Kunstfehlern.[32]

Die Entbindung von der Schweigepflicht teilt die höchstpersönliche Natur des Persönlichkeitsrechts, das es schützen soll.[33] Es handelt sich um eine höchstpersönliche Aufgabe des Patienten. Daran ändert auch der Übergang des Strafantragsrechts auf die Angehörigen nach § 77 Abs. 2 i.V. mit § 205 Abs. 2 Satz 2 StGB nichts.[34] Denn das Strafantragsrecht und der Strafgrund sind unterschiedlichen Zielen verschrieben: Das Strafantragsrecht soll die Offenbarung eines Geheimnisses ahnden, nicht aber die Durchbrechung der Schweigepflicht ermöglichen. Auch die unterschiedlichen Adressatenkreise der Normen weisen in diese Richtung: Im einen Fall sind dies die Erben, im anderen Fall die Angehörigen.

Die Einsichtnahme in die Krankenakte und in den Internet-Account liegen wertungsmäßig auf gleicher Stufe: Der Zugriff auf die geheimhaltungsbedürftigen Informationen ist in beiden Fällen jeweils nur unter Vermittlung eines Geheimnisträgers als „Gatekeeper“ möglich. Der Arzt und der Telemediendienstanbieter dringen typischerweise tief in die Privatsphäre ihrer Vertragspartner ein. Das Geheimhaltungsvertrauen ist integrale Voraussetzung der Vertragsbeziehung. Müsste der Patient bzw. Kunde damit rechnen, dass seine Daten nach dem Tod Dritten offenbart werden, würde er manche Informationen seinem Arzt womöglich gar nicht er anvertrauen bzw. nicht in dem Account eines Telemediendiensteanbieters hinterlegen.

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. Spiegelbildlich dazu fehlt ihm auch ein Zeugnisverweigerungsrecht im Strafverfahren.[35] Das TMG lässt seine vergleichbare Schutzintention aber normativ anklingen: Es begründet eine Geheimhaltungsverpflichtung. Das TMG verpflichtet die Diensteanbieter namentlich in § 13 Abs. 4 Nr. 3 TMG sicherzustellen, dass die Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen können. Das impliziert auch die Pflicht, Dritten keinen Zugang zu eröffnen. Dem Diensteanbieter ist es verwehrt, sich darüber aus eigener Machtvollkommenheit hinwegzusetzen. Die Pflicht zur Geheimhaltung ist eine vertragliche Hauptpflicht, die die unbefangene Inanspruchnahme der Dienstleistungen und die Vertraulichkeit der dort hinterlegten

---

29 Ähnlich auch § 9 Abs. 1 S. 1 und 2 Deutsche Ärztinnen und Ärzte-(Muster-)Berufsordnung (MBO); für einen abnehmenden sachlichen Gehalt der postmortalen Schweigepflicht immerhin aber OLG Düsseldorf, NJW 1959, 823; damit sympathisierend auch BGHZ 91, 393 (398); dagegen aber die wohl ü.M.; vgl. *Bender* (Fn. 28), S. 303 m.w.N.

30 Vgl. dazu auch *Bender* (Fn. 28), S. 303 f.

31 Vgl. BGHZ 91, 392 (399)*; BayObLG,* NJW 1987, 1492 (1493); *Bender* (Fn. 28), S. 319, 403 ff.; *Müller-Christmann*, in: *Bamberger/Roth* (Fn. 10)*,* § 1922 Rn. 43; (ablehnend) *Solbach*, DRiZ 1978, 204 (205).

32 Vgl. *BGH,* NJW 1983, 2627 (2628); *OLG München,* VersR 2009, 982; ausführlich zum Ganzen *Hess*, ZEV 2006, 479 ff.

33 Vgl. bereits RGSt 71, 21 (22); *Bender* (Fn. 28), S. 352 (mit Fn. 1 ff.) u. S. 384.

34 BGH, NJW 1983, 2627 (2629), a.A. *Solbach*, DRiZ 1978, 204 f.; zur Problematik auch *Bender* (Fn. 28), S. 310 m.w.N.

35 Nicht immer sind auch die in Online-Accounts hinterlegten Informationen so sensibel wie manche 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.

Informationen sichert. Dass dieser Schutz auch nach dem Tod fortbesteht, sagt die Vorschrift nicht in aller Deutlichkeit, entspricht aber ihrer ratio.[36]

bb) Verfassungsrechtlicher postmortaler Persönlichkeitsschutz

Ein solcher postmortaler Schutz kann jedenfalls Ausdruck eines nachwirkenden verfassungsrechtlichen Persönlichkeitsschutzes sein: Auch wenn das Persönlichkeits*recht* mit dem Tode erlischt, gewährt das GG einen postmortalen *Schutz* der Persönlichkeit.[37] Dieser erweist sich nicht als ein Aliud, sondern als ein wesensgleiches Minus zum verfassungsrechtlichen Persönlichkeitsschutz für die Lebenden.[38] Seine Grundlage findet er 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 der Toten kann insoweit auch nicht weiter gehen als der Schutz der Lebenden. Das schließt einen verfassungsrechtlichen Schutz des Ergebnisses der lebenslangen Persönlichkeitsentfaltung 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.[39] Dass der Verstorbene seine Rechte nicht mehr selbst verteidigen kann, heißt mithin nicht, dass der Diensteanbieter den höchstpersönlichen Informationen des Verstorbenen nach dem Tod keinen Schutz mehr angedeihen lassen müsste.

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.[40]

Um das Risiko einer Verletzung des allgemeinen Achtungsanspruchs durch Veröffentlichung entwürdigender Darstellungen – den typischen Fall postmortaler Persönlichkeitsverletzungen – geht es im Falle des digitalen Nachlasses des durchschnittlichen Internetnutzers regelmäßig nicht. Denn ausschließlich der innerste Kreis der Angehörigen erhält Zugang zu den sensiblen Daten und revidiert auf dieser Grundlage gegebenenfalls sein bisheriges Bild vom Verstorbenen.

Das Lebensbild eines Menschen kann aber auch dadurch beeinträchtigt werden, dass Dritte Einblick in intime Details der eigenen Persönlichkeit erhalten. Zum postmortalen Persönlichkeitsschutz gehört, dass der Einzelne auch nach seinem Tod gegen die Ausforschung seiner Persönlichkeit durch unbefugte Dritte geschützt bleibt. Unbefugte „Dritte“ in diesem Sinne können auch Erben oder eigene Angehörige sein. Denn diese sind nicht unbedingt legitime Treuhänder der Persönlichkeitsrechte des Verstorbenen. Der Schutz des postmortalen Persönlichkeitsrechts besteht schließlich nicht um der Nachfahren, sondern um des Verstorbenen willen.[41]

---

36 Entscheidend ist, dass die Geheimhaltungspflicht nicht ausdrücklich aufgehoben ist. Entsprechend versteht auch die strafrechtliche Literatur § 203 StGB überwiegend als lediglich deklaratorischen Ausdruck eines verfassungsrechtlichen Gebots postmortalen Persönlichkeitsschutzes. *Lenckner/Eisele*, in: Schönke/Schröder (Hrsg.), StGB, 28. Aufl. 2010, § 203 Rn. 70.

37 Vgl. etwa *Höfling*, in: *Sachs* (Hrsg.), GG, 5. Aufl. 2009, Art. 1 Rn. 39; ablehnend etwa *Hoch*, Fortwirken zivilrechtlichen Persönlichkeitsschutzes nach dem Tode, 1975, S. 40 ff.; ebenso etwa *Claus,* Postmortaler Persönlichkeitsschutz im Zeichen allgemeiner Kommerzialisierung, 2004, S. 66 ff., 96 ff.

38 *Bender* (Fn. 28), S. 306 und 447.

39 Siehe nur BVerfGE 30, 173 (194); BGHZ 15, 249 (259).

40 Vgl. BVerfG, NJW 2001, 591 (594); BVerfG, NJW 2001, 2957 (2958); ferner BVerfGE 93, 266 (293).

41 Anders aber die sog. Andenkensschutzlehre; zu ihr etwa *Claus* (Fn. 37), S. 66 ff., 96 ff. *Lehmann*, Postmortaler Persönlichkeitsschutz, 1973, S. 120 ff.

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* Nutzung von Daten Ausstrahlungen auf die *heutige* Offenbarung dieser Daten hat. Sonst sehen sich die Nutzer im Gefolge des Fehlens eines dauerhaften Schutzes ihrer Daten in der freien Entfaltung ihrer Persönlichkeit schon zu Lebzeiten gehindert. Wenn „die Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“[42], hat das unmittelbar Auswirkungen auf die Persönlichkeitsentfaltung im Hier und Jetzt. Dieser nachwirkende Persönlichkeitsschutz entpuppt sich insoweit als Garant der vollen Persönlichkeitsentfaltung zu Lebzeiten – gleichsam als eine Vervollkommnung des lebenszeitigen Schutzes.[43] Ein sachgerechter Persönlichkeitsschutz muss auch verfassungsrechtlich bereits auf der Stufe der *Persönlichkeitsgefährdung* beginnen.[44] Nur dann lässt sich den Gefahrenlagen[45] angemessen Rechnung tragen, die sich mit dem besonders intensiven Eindringen in die Persönlichkeitssphäre von Nutzern im Internet verbinden: 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.[46] Hinzu treten die bestechende Leichtigkeit, mit dem die personenbezogenen Daten im Internet generiert werden, ebenso wie der Detaillierungsgrad, den die Nutzerinformationen erreichen können.

Der Persönlichkeitsschutz in der digitalen Kommunikation kann bei konsequenter Fortschreibung der Rechtsprechung des *BVerfG* sogar Ausfluss einer verfassungsrechtlichen Schutzpflicht aus Art. 10 Abs. 1 GG sein. Das Telekommunikationsgeheimnis erstreckt sich zwar nur auf Telekommunikationsvorgänge, nicht aber auf nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherte Inhalte und Umstände der Kommunikation. Kommunikationsvorgänge eines E-Mail-Accounts sieht das BVerfG aber solange als nicht beendet an, wie die Nachrichten noch beim Provider gespeichert sind.[47] Nicht nur bei IMAP-E-Mail-Accounts, auch bei der Nachrichtenzustellung über den Vermittlungskanal sozialer Netzwerke, wie z. B. Facebook, verbleiben die sensiblen Informationen grundsätzlich weiter im Herrschaftsbereich des Providers. Solange besteht 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 vorgenommen wurden. Während der Speicherung der Daten auf eigenen Servern kann der Diensteanbieter insbesondere unbemerkt auf die Kommunikationsvorgänge zugreifen. Der verfassungsrechtliche Auftrag des Schutzes drittvermittelter Privatheit auf Distanz (Art. 10 Abs. 1 GG) als Ausformung des besonderen würdegeprägten Persönlichkeitsschutzes ist dann betroffen. Lücken füllend tritt das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme hinzu.[48]

So wie das *BVerfG* schon in seinem Volkszählungsurteil konstatierte, dass es im Informationszeitalter kein an sich „belangloses“ Datum mehr geben könne,[49] muss dies grundsätzlich auch in *zeitlicher* Hinsicht gelten, soll den realen Gefährdungen der Persönlichkeit im Cyberspace

---

42 *BVerfGE* 65, 1 (43).

43 Vgl. auch *Schack,* JZ 1989, 609 (614).

44 *BVerfG*E 118, 168 (184 f.).

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

46 Anders als dort sind sie aber (regelmäßig bewusst) in einer über den Tod hinaus wirkenden Weise durch eine Zugangssperre digital gegen den unbefugten Zugriff Dritter gesichert. Vgl. zu den Unterschieden auch unten (3).

47 *BVerfG* MMR 2009, 673 (674 f.)

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

49 BVerfGE 65, 1 (43).

hinreichend begegnet werden. Fehlende Transparenz und dem Nutzer in ihrer Reichweite unbekannt bleibende Risiken – wie die Möglichkeit einer umfangreichen Profilbildung oder die Unvergänglichkeit über das Internet verbreiteter Informationen – können sich sonst erheblich auf das Kommunikationsverhalten und auf die Hinterlegung von Daten für die Zukunft auswirken. Diese Auswirkungen bereits heute zu berücksichtigen, ist ein Gebot vorsorgenden bzw. nachwirkenden Grundrechtsschutzes.

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.“[50] 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 leiten lässt. Postmortaler Persönlichkeitsschutz ist insoweit insbesondere Vertrauensschutz für die Lebenden, namentlich Teil einer objektivrechtlichen staatlichen Schutzpflicht, (auch nicht-vermögensrechtliche[51]) 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 konstruiert: Die erforderliche Vertrauensbasis zwischen Arzt und Patient kann nicht entstehen, wenn der schutzbedürftige Vertragspartner nicht auch für die Zeit nach dem Tod auf die Verschwiegenheit des Geheimnisträgers zählen kann.

(2) Bedeutung des verfassungsrechtlichen postmortalen Persönlichkeitsschutzes im digitalen Zeitalter

Werden vertrauliche Informationen nach dem Tod denjenigen zugespielt, denen der Erblasser sie zu Lebzeiten vorenthalten wollte, kann gerade davon der Einschüchterungseffekt ausgehen, vor dem das Telekommunikationsgeheimnis und das informationelle Selbstbestimmungsrecht schützen sollen. 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, etwa einer heimlichen 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, verletzen.

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 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 zur Verfügung stehen. Vertrauliche Mitteilungen, für die die Accounts gedacht sind, würde er sonst dort im Zweifel nicht hinterlegen. Dies durch entsprechende Schutzvorkehrungen abzusichern, verbürgt § 13 Abs. 4 Nr. 3 TMG dem Nutzer der entsprechenden Telemediendienste auch ausdrücklich. Entsprechend ist er mit der Weitergabe seiner Zugangsdaten grundsätzlich solange nicht einverstanden, wie er diese nicht ausdrücklich Dritten mitgeteilt hat.

---

[50] BGHZ 50, 133 (139); Hervorhebungen d. Verf.; zustimmend etwa *Schack*, JZ 1989, 609 (610); skeptisch BVerfGE 30, 173 (194).

[51] 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.

(3) Schlussfolgerungen

Die Kunden sind das Kapital der Diensteanbieter. Dessen Grundstock ist das Vertrauen in die Geheimhaltung. Dieses unausgesprochene Vertrauen, das dem Vertrag als Geschäftsgrundlage inhärent ist, würde durch die Freigabe des Zugangs für Dritte *post mortem* zerstört.

Das postmortale Persönlichkeitsrecht verleiht diesem Geheimhaltungsvertrauen seinen normativen Flankenschutz. An ihm findet das Auskunfts- und Nutzungsinteresse der Hinterbliebenen seine Grenze.

Ein solcher besonderer Schutz von Account-Daten erscheint selbst angesichts des Umstandes gerechtfertigt, dass das papierene Tagebuch dem Zugriff der Erben offensteht.[52] Denn während jenes dem räumlichen Einwirkungsbereich der Erben ausgesetzt ist, ist der im Zweifel ungleich detailreichere Wissensschatz eines Online-Kontos schon zu Lebzeiten nur durch Einbeziehung eines Geheimhaltungsverpflichteten hebbar.

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 solange geschützt, wie er nicht ausdrücklich oder stillschweigend gegenüber dem Diensteanbieter oder Dritten die Freigabe verfügt. Die Rechte auf Geheimhaltung seiner Nutzeraccount-Daten verwandeln sich nach 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 wirken insoweit als Teil der staatlichen Schutzpflicht auch mittelbar in die Auslegung vertragsrechtlicher Rechtsbeziehungen hinein.[53] 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 Grundmodell (§ 307 Abs. 1, 2 Nr. 1 BGB).

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

Der digitale Nachlass hat vielfältige Facetten. Zu ihm gehören höchstpersönliche Daten, aber auch vermögensrechtliche Positionen, wie etwa das Urheberrecht an digital gespeicherten Bildern – schließlich auch geschäftliche Nachrichten, womöglich Geschäftsgeheimnisse, die in die Verfügungsgewalt des Arbeitgebers gehören.

Diese können jeweils ein unterschiedliches rechtliches Schicksal fristen. Sie sind aber in dem Nutzer-Account regelmäßig miteinander verwoben. Aus dem multifunktionellen Nebeneinander folgt eine Gemengelage. Die *personenbezogenen* Elemente stehen dem Zugriff der Erben nicht offen, sehr wohl aber der *vermögensrechtliche* Teil. Um diesen geltend machen zu können, muss der Erbe wiederum auf den Account zugreifen können, soll das Erbrecht nicht zur leeren Hülle degenerieren.

Zur Auflösung dieses Dilemmas erweist sich eine Differenzierung zwischen geschäftlichen und privaten Accounts als Entscheidungsraster 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; auch das *eine* Geständnis eines Ehebruchs im überwiegend geschäftlichen Account kann ein Lebensbild verändern.

Bei solchen gemischten Nutzungen ist es – entsprechend dem Vorbild des § 100a Abs. 4 S. 2 StPO – sachgerecht, nach der Art des betroffenen Gegenstandes zu scheiden. Zu trennen ist danach zwischen ganz oder überwiegend die Vermögenssphäre betreffenden und ganz oder überwiegend höchstpersönliche Sachverhalte betreffenden Daten.[54]

---

52 Vgl. etwa BVerfGE 80, 367; BGH, GRUR 1955, 201 (203); LG Koblenz, NJW 2012, 2227; *Claus* (Fn. 37), S. 98; siehe aber auch BGHZ 13, 334 ff.

53 Vgl. auch *BGHZ* 13, 334; 24, 200; 26, 349; 30, 7; 31, 308.

54 Vgl. zum Zugriffsrecht des Arbeitgebers zu Lebzeiten auf den (zulässigerweise) auch privat genutzten dienstlichen Account LAG Berl.-Bbg, NZA-RR 2011, 342; *Fübier/Splittgerber* NJW 2012, 1995 (1996 ff.).

Auch hier bleiben Grenzfälle multifunktioneller Verwendungszusammenhänge, die nicht bruchfrei voneinander tranchierbar sind, sondern einer Ermessensentscheidung bedürfen. Das Dilemma lässt sich daher – ähnlich wie im Falle der Einsichtnahme in die Krankenunterlagen, bei der die Entscheidung in die Hände des Arztes gelegt ist[55] – wohl nicht anders auflösen als durch die treuhänderische Einschaltung eines neutralen Dritten, sei es eines Testamentsvollstreckers, sei es des Diensteanbieters. Letzterer verfügt über die technischen Möglichkeiten einer Trennung und sollte der Pflicht unterliegen, den Erben Zugang (nur) zu den vermögensrechtlichen Teilen des digitalen Nachlasses zu verschaffen. Bei der Sezierung der vermögensrechtlichen und höchstpersönlichen Account-Daten hat er den tatsächlichen bzw. mutmaßlichen[56] Willen des Erblassers umzusetzen. Das wird den Account-Betreibern einigen Aufwand abverlangen[57] (den diese in ihr Geschäftsmodell einpreisen [müssen]) und bei der Vielzahl sowie Mischstruktur der in einem Account versammelten Nachrichten zugleich nicht ohne eine Toleranzschwelle der Pauschalierung zumutbar und realisierbar sein.

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, kann für die im Internet für jedermann einsehbaren Daten des Verstorbenen, insbesondere Webseiten, die zur Gänze frei zugänglich sind, wie etwa Internet-Blogs oder persönliche Homepages, Anderes 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 nach § 13 Abs. 7 sowie § 12 Abs. 3 TMG i.V.m. §§ 19, 20, 35 BDSG die Rechte auf Auskunft, Berichtigung, Löschung oder Sperrung zu. Diese Rechte können – der Effektivität des Datenschutzes wegen – durch Rechtsgeschäft weder ausgeschlossen noch beschränkt werden (§ 6 Abs. 1 BDSG i.V. mit § 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 für nicht übertragbar und damit auch für nicht vererbbar.[58] Das überzeugt 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 Betroffenen von den Wahrnehmungsberechtigten ausgeübt werden, ohne dass die geschützte Persönlichkeit selbst sich weiter zu entfalten in der Lage wäre.[59] Fände der Schutz personenbezogener Daten mit dem Tod sein Ende, würde das Grundanliegen des Persönlichkeitsschutzes im Datenschutzrecht geradezu pervertiert. Denn die Daten stünden dann den Diensteanbietern unbegrenzt als Verfügungsmasse offen. Anliegen des Datenschutzrechts ist es, den Achtungswert der Persönlichkeit in allen ihren Facetten gegen eine Beeinträchtigung zu schützen. Das bedingt eine Aufrechterhaltung von

---

55 BGH, JZ 1984, 279 (284 f.).

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

57 Reduzieren können die Betreiber diesen Aufwand in legitimer Weise durch Lenkung des Nutzungsverhaltens: So können sie etwa Unterpostfächer für private und geschäftliche Nachrichten vorsehen oder ihre Accounts gezielt auf private oder geschäftliche Nachrichten ausrichten.

58 *Bergmann/Möhrle/Herb* (Fn. 27), § 6 Rn. 12; *Gola/Schomerus*, in: dies. (Hrsg.), BDSG, 10. Aufl. 2010, § 6 BDSG Rn. 3; *Schaffland/Wiltfang*, BDSG, 2011, § 6 Rn. 2.

59 Vgl. zur Vererblichkeit von Immaterialgüterrechten auch *Lehmann* (Fn. 41), S. 45 ff.; zur konstruktiven Herleitung der Wahrnehmungsbefugnis *Claus* (Fn. 37), S. 60 ff.

Schutzpositionen des Datenschutzes, soweit sich in der weiteren Verwendung der Daten eine Persönlichkeitsverletzung realisieren kann.

Da dem Erblasser bei öffentlich zugänglichen Profildaten – anders als bei höchstpersönlichen, nicht öffentlich zugänglichen Informationen – kein Geheimhaltungsinteresse gegenüber den eigenen Erben eigen ist, fehlt es zwar an derjenigen Interessenkollision, die den Erben bzw. Angehörigen die legitime treuhänderische Wahrnehmung der postmortalen Persönlichkeitsrechte des Erblassers versagt. Es mangelt aber an gesetzlichen Regelungen, die die Person der Wahrnehmungsberechtigten als Wächter der Schutzrechte des Verstorbenen benennen.

Sachgerecht erscheint eine Anleihe bei § 22 S. 3 KunstUrhG bzw. § 60 Abs. 1 UrhG. Diese Normen sprechen den Angehörigen das Wahrnehmungsrecht für die Verbreitung von Bildnissen des Verstorbenen zu. Die Interessenlagen beider Schutzmaterien sind vergleichbar[60], eine Schließung der Gesetzeslücke im Wege der analogen Anwendung der Vorschriften erscheint insoweit angezeigt. Zur Klarstellung sollte der Gesetzgeber eine solche Regelung 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 solange, wie von einer gesteigerten Schutzbedürftigkeit des besonderen Ansehens und der Selbstdarstellung der Persönlichkeit gesprochen werden kann. Das Schutzbedürfnis – und entsprechend die Schutzverpflichtung – schwinden in dem Maße, in dem die Erinnerung an den Verstorbenen verblasst.[61] Wann diese kritische Schwelle überschritten ist, lässt sich nur im Wege einer politischen Dezision bestimmen.[62] Maßstab für die Festsetzung der Schutzfrist sollte die Verletzbarkeit der Persönlichkeitsrechte des Verstorbenen durch den Diensteanbieter und die Öffentlichkeit sein. Jedenfalls nach 30 Jahren besteht eine besondere Neugierde der Nachwelt gegenüber den öffentlich verfügbaren Internetdaten Verstorbener regelmäßig nicht mehr.[63] Trotz der Schnelllebigkeit, aber angesichts der Unvergänglichkeit und der Sensibilität der im Internet hinterlegten Daten entspricht ein solcher Zeitraum einer sachgerechten Abwägung der widerstreitenden Interessen.

3. Zwischenfazit

Die Zugangsinformationen eines Internet-Accounts sind grundsätzlich[64] höchstpersönlich.[65] Die Pflichten des Diensteanbieters zur Geheimhaltung der Nutzer-Account-Daten gehen entsprechend nicht mit dem Tod unter, sondern leben fort. Auch wenn die Erben in die vermögensrechtliche Nutzerstellung des Erblassers eintreten, ist es ihnen aus Gründen des postmortalen Persönlichkeitsschutzes versagt, auf Accounts zuzugreifen, die den Schutz privater Vertraulichkeit

---

60 Ein Unterschied besteht darin, dass der Erblasser die Internetdaten bereits zu Lebzeiten 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 bestehenden Daten in die Verfügungsgewalt der Angehörigen zu legen.

61 Dazu etwa *Claus* (Fn. 37), S. 105 ff. m.w.N.

62 St. Rspr. des BGH; vgl. BGHZ 50, 133 (140 f.); 107, 384 (392); *Bergmann/Möhrle/Herb* (Fn. 27), § 3 Rn. 6.

63 Vgl. auch die unterschiedlichen Fristenregelungen in § 22 S. 3 KunstUrhG (10 Jahre), § 64 UrhG (grundsätzlich 70 Jahre) bzw. §§ 82, 76 UrhG (50 Jahre für den ausübenden Künstler) und § 5 Abs. 2 S. 1 BArchG (30 Jahre).

64 Dagegen erschöpft sich grundsätzlich ein Online-Banking-Account in einer vermögensrechtlichen Position, die im normalen Erbgang übergeht.

65 So auch *Hoeren*, NJW 2005, 2113 (2114); *Müller-Christmann*, in: *Bamberger/Roth* (Fn. 10) § 1922 Rn. 24; *Schlüter*, in: Ermann (Hrsg.), BGB, 12. Aufl. 2008, § 1922 Rn. 8.

genießen und damit Einblick in die intimste Persönlichkeitssphäre des Verstorbenen erlauben. Etwas anderes gilt nur, soweit ein anderer 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, wie z.B. ein „Phishing" voraus, durch die die Daten gegenüber Dritten besonders geschützt sind.[66] Daran fehlt es im Falle einer Herausgabe der Daten durch den Diensteanbieter selbst. Nicht ausgeschlossen 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.

Die Pflicht zur Geheimhaltung höchstpersönlicher Zugangsdaten entbindet die Diensteanbieter nicht von der Pflicht, die Informationen zu den *vermögensrechtlichen Positionen* an die Erben herauszugeben. Diese gehen im normalen Erbgang über, soweit nicht ausnahmsweise der Nutzungsvertrag selbst die Vererbbarkeit der Rechtspositionen wirksam ausschließt.

Für die *öffentlich verfügbaren* personenbezogenen Informationen über den Verstorbenen, z.B. die Daten einer eigenen Homepage oder eines Internet-Blogs, nehmen die Angehörigen das datenschutzrechtliche Totenfürsorgerecht wahr. Die insoweit bestehenden 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.

IV. Rechtspolitische Desiderate

Der digitale Nachlass ist für den Unbedarften Grund zur Ratlosigkeit, für den kundigen Thebaner dagegen ein Anlass zum Handeln. Jeder tut gut daran, noch zu Lebzeiten zu verfügen, 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 verfügte er, dass seine unveröffentlichten Manuskripte nach seinem Tod verbrannt werden sollen, worüber sich sein Freund und Nachlassverwalter *Max Brod* aber glücklicherweise hinwegsetzte. So bedeutsam wie das Wirken *Kafkas* 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.

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

Der junge Amerikaner *Jeremy Toemans* machte aus der Not eine Tugend: Als seine Familie nach dem Tod seiner Großmutter vor der Frage stand, wie denn die vielen digitalen Identitäten der technikbegeisterten Dame ermittelt werden sollten, brachte ihn das auf eine Geschäftsidee. Er gründete ein Internet-Unternehmen, das sich der Verwaltung von Passwörtern zu Internet-Accounts aller Couleur verschreibt. Im Todesfall gibt es die hinterlegten Zugangsdaten an die zuvor dekretierten Vertrauenspersonen heraus. *Legacy Locker* gilt heute als Marktführer unter den digitalen Nachlassverwaltern. Diese schießen gegenwärtig wie Pilze aus dem Boden. Die Existenz

---

[66] *Lenckner/Eisele*, in: Schönke/Schröder (Fn. 36), § 202a Rn. 10a; zu § 206 StGB siehe oben Fn.15.

derartiger Passwort-Tresore ist ein Beleg für den bislang unbefriedigten Bedarf nach einer praktikablen Verwaltung des digitalen Vermächtnisses im Kampf gegen das digitale Chaos.

Ob sie eine sachgerechte Antwort darauf bilden, steht auf einem anderen Blatt. Regelmäßig ist die Herausgabe der Account-Zugangsdaten an den digitalen Testamentsvollstrecker Voraussetzung für die Inanspruchnahme seiner Dienste. Dies widerspricht aber allen Prinzipien der Geheimhaltung von Passwörtern. In der Regel erhalten die Kunden weder Einblick in die Sicherheitsmechanismen noch haben sich bislang Gütesiegel, Qualitätskontrollen oder gar eine wirksame staatliche Aufsicht etabliert.

Ob der Erblasser sein Leben eher aushaucht als der digitale Totengräber, ist auch nicht besiegelt. Erste Anbieter, wie *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 ist nur bedingt eine zufriedenstellende Regelung digitaler Nachlasssorge. Denn es gehört zu den unumgänglichen Verhaltensregeln, sichere Passwörter nicht nur zu erstellen, sondern auch regelmäßig zu ändern. Das Prozedere bei Einschaltung eines klassischen Testamentsvollstreckers erweist sich 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. Sofern die Vertragspartner dies nicht im Wege einer privatautonomen Regelung individualvertraglich gestalten, ist der Gesetzgeber im Interesse eines umfassenden Schutzes der Persönlichkeitaufgerufen, die damit verbundene Unsicherheit zu beseitigen. Er sollte die Diensteanbieter darauf verpflichten, den Nutzern schon beim Anlegen eines neuen Accounts explizite (später jederzeit änderbare) Gestaltungsvorgaben für den Todesfall zu eröffnen. § 13 Abs. 4 TMG sollte um eine Nr. 3a ergänzt werden, der den Diensteanbieter abringt sicherzustellen, dass „die Nutzer die Möglichkeit haben, Regelungen für die Verwendung ihrer personenbezogenen Daten nach dem Tod zu treffen."

Den ambivalenten Wünschen der Account-Inhaber lässt sich so durch eine präferenzorientierte Eröffnung von Handlungsoptionen, sei es die Umschaltung in den Kondolenzmodus, die Löschung eines Accounts oder die Weitergabe der Account-Daten, angemessen gerecht werden. So wird dem Dateninhaber entsprechend dem Grundgedanken des informationellen Selbstbestimmungsrechts die Möglichkeit zuteil, darüber zu verfügen, wer in welchem Umfang auf seine Daten nach seinem Tod zugreifen darf.

Die technische Verpflichtung der Diensteanbieter auf ein Datennachlassmanagement sollte von einer Aktivierungsfunktion flankiert werden: „Sofern die Nutzer keine Vorgaben für den Todesfall getroffen haben, fordern die Diensteanbieter die Nutzer in regelmäßigen Abständen zu einer entsprechenden Erklärung auf, soweit der Nutzer dem nicht widerspricht" (§ 13 Abs. 4 Nr. 3a Satz 2 TMG-E). Treffen die Nutzer gleichwohl keine Verfügung, kommt die verfassungsrechtliche Wertung zum Tragen, nach welcher die Personenbezogenheit der in den Accounts hinterlegten Daten den

Erben eine Account-Autopsie verschließt,[67] den Angehörigen aber die Wahrnehmung der datenschutzrechtlichen Rechte im Hinblick auf die in Internet *öffentlich verfügbaren personenbezogenen* Informationen anvertraut ist.[68] Das trägt der Aufgabe des postmortalen Persönlichkeitsschutzes Rechnung, 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.

aa) Erklärungsmanagement als „Nudge"

Ein solches Regelungskonzept entspricht in der Sache dem (durchaus nicht unumstrittenen[69]) rechtsphilosophischen Regelungskonzept eines liberalen Paternalismus.[70] Sein Bestreben ist es, staatliche Regelungsziele, die sich auf der Grundlage privatautonomer Gestaltung der Vertragspartner bisher nicht in einer hinreichenden bzw. staatlich erwünschten Weise einstellen, durch Induzierung selbstregulativer Wahlhandlungen zu erreichen. Die Bürger sollen individuelle Präferenzentscheidungen, die sie infolge von Unwissenheit, Nachlässigkeit oder zeitlichen Inkonsistenzen etc. bisweilen unterlassen, ohne staatlichen Zwang, aber auf Veranlassung eines staatlichen „*Nudge*" (also eines „Schubsers") treffen und so zur Erreichung von Gemeinwohlzielen und sachgerechten Regelungsergebnissen beitragen.

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 schließt auch die (negative) Freiheit ein, 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 Verfügungserklärung, erweist sich insofern gegenüber einer Erklärungspflicht als grundrechtsschonender. Sieht der Gesetzgeber für den Fall einer fehlenden individuellen Erklärung des Erblassers eine gesetzliche Ausfallregelung (sachgerechterweise die Nichtweitergabe der Account-Daten) und einen Hinweis des Diensteanbieters auf die Folgen einer Nicht-Erklärung vor, führt er die Rechtsfragen des digitalen Nachlasses einer grundrechtsschonenden und effektiven Regelung zu.

b) Aktivierungsregeln

Ein Problem beseitigt das Einwilligungsmanagement freilich nicht: Es verfügt zwar, was im Todesfall mit den Daten passiert. Es stellt aber nicht sicher, dass der Anbieter von dem Tod erfährt. In der Regel ist den Erben gerade unklar, welche Accounts überhaupt zu den digitalen Hinterlassenschaften gehören. Meist gibt es kaum 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, oder durch die vorsorgende Benachrichtigung der Vertrauenspersonen über ihre Einsetzung als digitaler Testamentsvollstrecker.

---

67 Vgl. dazu oben III. 2. a. bb.

68 Vgl. dazu oben III. 2. b.

69 Vgl. zur Kritik etwa *Eidenmüller*, JZ 2011, 814 (819 f.); mit dem Modell hingegen sympathisierend *Smeddinck*, Die Verwaltung 2011 (44), 375 ff. Differenzierend: *Kirste,* JZ 2011, 805 ff.

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

V. 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 oder es stehen ausschließlich vermögensrechtliche Bestandteile des digitalen Nachlasses im Raum. Die Entfaltung der Persönlichkeit im Informationszeitalter wäre nämlich erheblich gehemmt, könnten sich die Nutzer nicht darauf verlassen, dass ihre Daten auch nach ihrem Tode nur denjenigen zugänglich gemacht werden, denen sie diese zugänglich machen wollten.

De lege ferenda ist die gesetzliche Verpflichtung der Diensteanbieter zu einem Einwilligungsmanagement und zu Profileinstellungen für das digitale Vermächtnis angezeigt, welche die Ausübung der Verfügungsmacht für die Zeit nach dem Tod sichert. Sie beseitigt die bestehende Unsicherheit der Ermittlung des mutmaßlichen Willens ebenso präferenzkompatibel wie effektiv und schonend. Entsprechend dem letzten Willen des Verstorbenen wird der digitale Nachlass dann entweder zum gesicherten Sarkophag, dessen Geheimnisse im Verborgenen bleiben, oder zu einem wertvollen Instrument der Trauerarbeit, der Begegnung und der Erinnerung. Trotz aller wachsenden Bedeutung des digitalen Leichenbegängnisses bleibt eines dabei freilich unverändert. *Vinzenz Erath* hat es auf den Punkt gebracht: „Das kostbarste Vermächtnis eines Menschen ist immer noch die Spur, die seine Liebe in unseren Herzen zurückgelassen hat.”