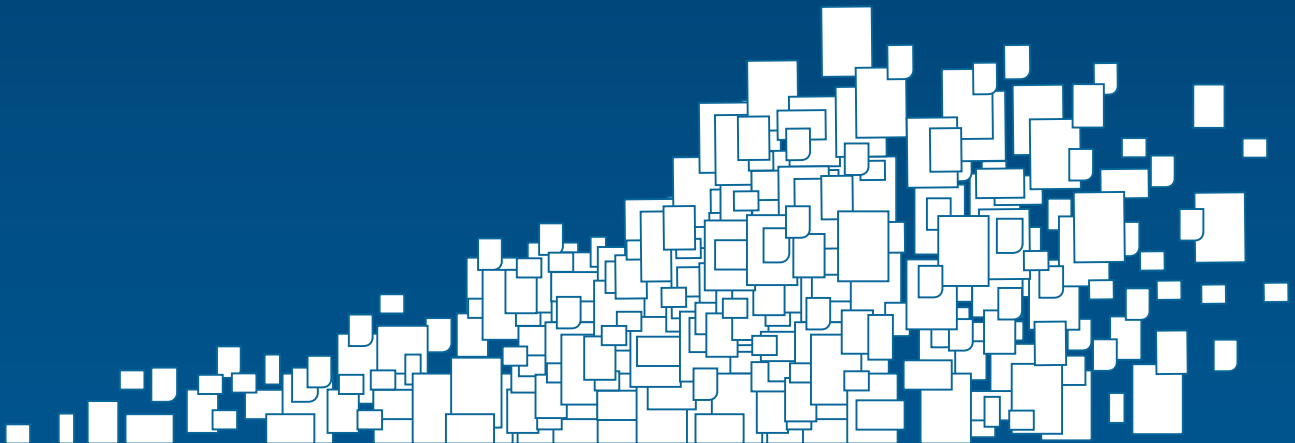




School of
Management and Law

**Sterben und Erben
in der digitalen Welt**

**Von der Tabuisierung zur Sensibilisierung.
Crossing Borders.**



Ergebnisse eines interdisziplinären Forschungsprojekts von
Elke Brucker-Kley, Thomas Keller, Lukas Kurtz, Kurt Pärli, Matthias Schweizer, Melanie Studer

F&E-Projektförderung



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Kommission für Technologie und Innovation KTI

Herausgeber

ZHAW School of Management and Law
Stadthausstrasse 14
Postfach
8401 Winterthur
Schweiz

Abteilung General Management
Institut für Wirtschaftsinformatik
www.zwi.zhaw.ch

Abteilung Business Law
Zentrum für Sozialrecht
www.zsr.zhaw.ch

Kontakt

sterben-erben-digital.zwi.iwr@zhaw.ch

Projektleitung

Elke Brucker-Kley
Institut für Wirtschaftsinformatik
Tel. +41 58 934 66 85
elke.brucker-kley@zhaw.ch

Projektinformationen im Internet

<http://zwi.zhaw.ch/digitalessterben>

Zwecks besserer Lesbarkeit wird in dieser Publikation überwiegend die männliche Form verwendet. Die weibliche Form ist selbstverständlich immer mit eingeschlossen.

Copyright © 2012 ZHAW School of Management and Law, Zürcher Hochschule für Angewandte Wissenschaften

Alle Rechte für den Nachdruck und die Vervielfältigung dieser Arbeit liegen bei der ZHAW School of Management and Law. Die Weitergabe an Dritte bleibt ausgeschlossen.

Abstract

Immer mehr Menschen verfügen über Social-Media-Profile und hinterlassen immer mehr Daten (Bilder, Videos, Nachrichten etc.) und Spuren im Internet. Doch was passiert im Todesfall? Profile zu löschen oder Zugriff auf Daten zu erlangen, ist für Angehörige kompliziert oder unmöglich. Der Umgang mit dem digitalen Nachlass wirft zudem erb- und persönlichkeitsrechtliche Fragestellungen auf.

Ziel dieses interdisziplinären Forschungsprojekts war es, diese Fragen für den Schweizer Kontext zu klären und eine solide Basis für die Weiterentwicklung bestehender

Lösungsmodelle sowie die Entwicklung potentieller neuer Lösungsmodelle zu schaffen. Die Analysen ergaben ein differenzierteres Bild der grundlegenden Problematik, der unterschiedlichen Interessensgruppen und Spannungsfelder sowie der rechtlichen und administrativen Rahmenbedingungen. Auf dieser Grundlage wurde ein erweiterter Lösungsraum für den digitalen Nachlass entwickelt, der nicht nur das Pionierfeld digitale Nachlassplanung und Willensvollstreckung präzisiert, sondern auch die Sicherstellung der Datenherrschaft zu Lebzeiten, das «Recht auf Vergessen» sowie den Bedarf an Beratung und Sensibilisierung der Internetnutzerschaft und der Plattformbetreiber einbezieht.

4 Inhalt

7 1. Hintergrund und Ziele des Forschungsprojekts

- 1.1 Ausgangssituation und Zielsetzung
- 1.2 Projektrahmen und Forschungsfragen

11 2. Der digitale Nachlass: Relevanz und Eigenschaften

- 2.1 Vom E-Mail Konto zur digitalen Identität: Was wird zum digitalen Nachlass?
- 2.2 Der digitale Nachlass: Eigenschaften und Problematiken

16 3. Vom Datenspeicher zum Datenfriedhof: Wird der digitale Nachlass bedeutender?

- 3.1 Internet ist Teil des täglichen Lebens geworden
- 3.2 Durch die zunehmend aktive Internetnutzung hinterlassen wir immer mehr persönliche Daten
- 3.3 Die Onlinebevölkerung in der Schweiz altert
- 3.4 Mehr als 3 000 verstorbene Facebook-User jährlich in der Schweiz

27 4. Szenarien für den digitalen Nachlass

- 4.1 Die Grundsatzentscheidung: Digitale Nachlassplanung ja oder nein
- 4.2 Welche Szenarien gilt es durch die digitale Nachlassplanung zu vermeiden?

34 5. Praktiken der Plattformanbieter

38 6. Rechtliche Rahmenbedingungen

- 6.1 Die erbrechtliche Komponente des digitalen Todes
- 6.2 Die persönlichkeitsrechtliche Komponente des digitalen Todes
- 6.3 Datenschutz und digitales Sterben
- 6.4 Durchsetzung des digitalen letzten Willens

66 7. Anknüpfungspunkte bei der Administration von Todesfällen

70 8. Lösungsansätze für den digitalen Nachlass

- 8.1 Der erweiterte Lösungsraum
- 8.2 Digitale Vererbungsdienste
- 8.3 Bewahren – Digitale Andenkendienste
- 8.4 Löschen – Lösungsmöglichkeiten für ein Recht auf Vergessen
- 8.5 Entscheiden – Beratung bei der digitalen Nachlassplanung und Willensvollstreckung

87 9. Fazit

90 Literaturverzeichnis

96 Autoren der Studie

98 Beteiligte Experten

100 Anhang: Praktiken und Regelungen der Plattformanbieter zum Vorgehen im Todesfall



1. Hintergrund und Ziele des Forschungsprojekts

1.1 AUSGANGSSITUATION UND ZIELSETZUNG

In der Schweiz sind 2011 schätzungsweise mehr als 3000 Facebook-Mitglieder verstorben. Es ist davon auszugehen, dass diese Zahl in den nächsten Jahren weiter zunehmen wird, zumal die Social-Media-Aktivitäten der Altersgruppen über 50 Jahren höhere Wachstumsraten aufweisen, als die der bereits stark vertretenen Altersgruppe zwischen 20 und 49 Jahren. Facebook ist nur ein Beispiel in einer Reihe von Plattformen, mit deren Hilfe im Laufe eines Lebens grosse Informationsmengen in Form von Dokumenten, Fotos, Videos, Kontakten und vielem mehr angesammelt werden. Darüber hinaus existieren in zunehmendem Masse wichtige Informationen wie Finanzdokumente oder Behördenkorrespondenz nur noch in digitalisierter Form. Persönliche Informationen werden bewusst und unbewusst im Rahmen der alltäglichen Internetnutzung offengelegt und gestreut. Was passiert mit der Vielzahl an Informationen in Social Media und anderen Internet-Plattformen nach dem Tod eines Menschen?

Bereits zu Lebzeiten ist es kaum mehr möglich, Kontrolle über die Speicherung und Weiterverarbeitung persönlicher Daten im Internet zu bewahren. Wie und weshalb sollte man daher versuchen, über deren Fortbestand im Todesfall zu verfügen? Die Angehörigen haben in der Regel keine Kenntnis über die Gesamtheit der Online-Aktivitäten und keinen Zugriff, um Profile zu deaktivieren oder Informationen zu löschen oder zu verschieben. Dem gegenüber stehen unterschiedlichste Praktiken und Nutzungsbedingungen der Plattformanbieter.

Ziel des interdisziplinären Forschungsprojektes

«Sterben und Erben in der digitalen Welt» ist es, die offenen Fragen in Zusammenhang mit dieser Problematik für den Schweizer Kontext zu klären und eine solide Ausgangsbasis für die Weiterentwicklung bestehender Lösungsmodelle sowie die Entwicklung potentieller neuer Lösungsmodelle zu schaffen. Angesichts des geringen Reifegrades der digitalen Nachlassplanung gilt es:

- Ein klares Bild der Interessen, Rechte, Pflichten und Möglichkeiten der Anspruchsgruppen in der Schweiz zu zeichnen.
- Die rechtlichen Rahmenbedingungen für die digitale Nachlassplanung und Willensvollstreckung in der Schweiz herauszuarbeiten.
- Die zunehmende Relevanz des digitalen Nachlasses aufzuzeigen und die Anspruchsgruppen, insbesondere die Internetnutzenden, für die Thematik zu sensibilisieren.

1.2 PROJEKTRAHMEN UND FORSCHUNGSFRAGEN

Um den verschiedenen Facetten der Thematik gerecht zu werden, ist ein interdisziplinärer Ansatz gefordert.

Zusammensetzung des Projektteams

Die systemischen, wirtschaftlichen und rechtlichen Aspekte werden durch das Institut für Wirtschaftsinformatik und die Abteilung Business Law an der ZHAW School of Management and Law abgedeckt. Das Institut für Wirtschaftsinformatik ist die anwendungsorientierte Plattform für Betriebswirtschaft und Informatik der ZHAW School of Management and Law mit einer schwerpunktmässigen Ausrichtung auf Prozess- und Informationsmanagement. Die Abteilung Business Law bringt Forschungs- und Be-

ratungskompetenz im nationalen und internationalen Wirtschaftsrecht sowie Europarecht, Arbeits- und Sozialrecht ein. Ein Forschungsschwerpunkt des Zentrums für Sozialrecht der Abteilung Business Law liegt im Bereich Schweizerisches und Europäisches Datenschutzrecht, das für die Thematik des digitalen Sterbens und Erbens von wesentlicher Bedeutung ist. Die Expertinnen und Experten innerhalb und ausserhalb der ZHAW, die ihr Fachwissen und ihre Perspektiven auf die Thematik mit dem Projektteam geteilt haben, sind im Anhang zu diesem Forschungsbericht aufgeführt.

Vorgehen und Methodik

Die Projektergebnisse werden in den zwei Phasen Analyse und Lösungsentwurf erarbeitet. Die in diesem Rahmen adressierten Forschungsfragen sind in Tabelle 1 dargestellt.

Tabelle 1

FORSCHUNGSFRAGEN, METHODIK UND ARBEITSERGEBNISSE

Forschungsfragen

Vorgehen und Resultat

Der digitale Nachlass: Eigenschaften und Problematik (Kapitel 2)

Was umfasst ein digitaler Nachlass? Welche Umstände erschweren den Umgang mit den verteilt im Internet gespeicherten Daten und Konten von Verstorbenen?

Schaffung der Arbeitsgrundlagen:
 – Nutzungsabhängige Ausprägung des digitalen Nachlasses und dessen rechtlicher Relevanz
 – Kenntnis, Zugriff, Eigentum und Kontrolle, Archivierungswürdigkeit, Lösbarkeit und Vergessen als zentrale Faktoren im Umgang mit dem digitalen Nachlass

Vom Datenspeicher zum Datenfriedhof (Kapitel 3)

Welche Faktoren beeinflussen Grösse und Relevanz des digitalen Nachlasses?

Auswertung bestehender soziodemographischer Analysen zur Internetnutzung in der Schweiz:
 – Entwicklung der Internetnutzung in der Schweiz (quantitativ und qualitativ)
 – Altersstruktur und Sterbeziffern der Schweizer Social-Media-Nutzerschaft (Beispiel Facebook, Xing)

Szenarien für den digitalen Nachlass (Kapitel 4)

Was passiert mit dem digitalen Nachlass im Todesfall mit und ohne digitale Nachlassplanung?
 Welche proaktiven und reaktiven «Anwendungsfälle» im Umgang mit digitalen Werten im Todesfall sind grundsätzlich denkbar?

Entwicklung und Bewertung von proaktiven und reaktiven Anwendungsfällen im Umgang mit dem digitalen Nachlass:
 – Optionen und Szenarien mit und ohne digitale Nachlassplanung und Willensvollstreckung
 – Szenarien, die durch digitale Nachlassplanung vermieden werden können

Die Praktiken der Plattformanbieter (Kapitel 5)

Wie gehen Plattformanbieter momentan mit Todesfällen von Mitgliedern um?

Analyse der Nutzungsbedingungen, Datenverwendungsrichtlinien und Kundenhilfen von 7 Internetplattformen, die ein breites Nutzungsspektrum abdecken:

- Vergleichende Darstellung des Vorgehens im Todesfall von Mitgliedern bei Facebook, Xing, Google (Gmail, YouTube), Yahoo! (Flickr), Twitter und PayPal

Rechtliche Rahmenbedingungen (Kapitel 6)

Wie sehen die rechtlichen Rahmenbedingungen für die digitale Nachlassplanung und Willensvollstreckung in der Schweiz aus? Welche offenen Fragen gibt es?

– Welche **erbrechtlichen Möglichkeiten** und Grenzen gibt es, über den digitalen Nachlass zu verfügen und den Willen zu vollstrecken?

Bewertung der Handlungsmöglichkeiten des Erblassers:

- Vererbbarkeit von Daten
- Einsetzbarkeit der konventionellen und digitalen Nachlassplanungsinstrumente

– Welche **persönlichkeitsrechtlichen Aspekte** hat der digitale Nachlass und welche Grenzen und Möglichkeiten der Durchsetzbarkeit von Rechtsansprüchen gibt es für Angehörige nach dem Tod?

Analyse der persönlichkeitsrechtlichen Komponenten des digitalen Nachlasses:

- Grenzen des postmortalen Persönlichkeitsschutzes und des Andenkensschutzes

– Welche **datenschutzrechtlichen Fragestellungen** wirft der digitale Nachlass auf? Gibt es ein «**Recht auf Vergessen**» im Internet?

Analyse der datenschutzrechtlichen Handlungsmöglichkeiten:

- Grundsätze zum Umgang mit Daten von Verstorbenen
- Möglichkeit von Auskunftsgesuchen (Beispiel E-Mail)
- Problematik und technische Umsetzbarkeit eines «Rechts auf Vergessen im Internet» inkl. EU-Rechtsvergleich

– Welche Möglichkeiten und Grenzen gibt es bei der Durchsetzbarkeit von hinterlegten Wünschen des Verstorbenen oder Ansprüchen der Angehörigen gegenüber Plattformanbietern? Welches Recht und welcher Gerichtsstand sind anwendbar?

Betrachtung der Durchsetzbarkeit von Ansprüchen aus Persönlichkeits- und Datenschutzverletzungen im Internet:

- Auswirkungen der mehrheitlich fehlenden erbrechtlichen Relevanz der Daten und des eingeschränkten postmortalen Persönlichkeitsschutz auf die Durchsetzbarkeit
- Auswirkungen der grenzüberschreitenden Datenhaltung

Anknüpfungspunkte bei der Administration von Todesfällen (Kapitel 7)

Wie werden Todesfälle in der Schweiz administriert? Gibt es Anknüpfungspunkte für die digitale Nachlassplanung und Willensvollstreckung?

Analyse der Prozesse und Rechtsgrundlagen bei Registrierung, Meldung und Beurkundung von Todesfällen (am Beispiel des Bevölkerungsamtes der Stadt Zürich):

- Systemische Infrastruktur des eidgenössischen Zivilstands- und Meldewesens (Infostar, Einwohnerregisterharmonisierung)
- Anknüpfungspunkte für die digitale Nachlassplanung und fehlende Rechtsgrundlagen

Lösungsansätze für den digitalen Nachlass (Kapitel 8)

Welche Möglichkeiten und Angebote existieren bereits für die digitale Nachlassplanung und Willensvollstreckung?

Bewertung der momentan verfügbaren Wege und Instrumente zur digitalen Nachlassplanung und Willensvollstreckung:

- Vergleich in Bezug auf deren Praktikabilität, Sicherheit sowie Durchsetzbarkeit aus rechtlicher Sicht
- Typisierung, Funktionalitäten und Erfolgsfaktoren von digitalen Vererbungsdiensten

Welche Ansatzpunkte bestehen für praktikable und den rechtlichen Rahmenbedingungen in der Schweiz angepasste Lösungen?

Entwurf eines erweiterten Lösungsraums unter Einbezug von:

- Datenherrschaft und -selektion zu Lebzeiten
 - Recht auf Vergessen
 - Verantwortlichkeiten der Plattformanbieter
 - Beratung bei der digitalen Nachlassplanung sowie der Angehörigen im Todesfall
-

Präzisierung des Forschungsgegenstandes

Der Fokus der Analyse- und Entwurfsarbeiten im Rahmen des Projekts liegt auf dem digitalen Nachlass als Ergebnis der privaten Internetnutzung. Die Tatsache, dass die Grenzen zwischen privater und beruflicher Nutzung von Internet und Endgeräten zunehmend verschwimmen, wird den Umgang mit dem digitalen Nachlass verkomplizieren. Auch die rechtlichen Fragestellungen wären im Kontext der beruflichen und kommerziellen Internetnutzung zu erweitern.

Zudem wird der Forschungsgegenstand auf den digitalen Nachlass in Form von im Internet gespeicherten Daten eingeschränkt. Die auf physischen Datenträgern (PC, Tablet, Mobiltelefon, DVD etc.) lokal gespeicherten Daten sind Teil des digitalen Nachlasses, werden jedoch nicht näher betrachtet, da diese sowohl für die Angehörigen als auch aus erbrechtlicher Perspektive vergleichsweise unproblematisch sind. Auf die Möglichkeit Endgeräte beziehungsweise physische Datenträger als Anhaltspunkt zu nutzen, um die Online Aktivitäten und darüber den virtuellen digitalen Nachlass von Verstorbenen zu identifizieren, wird im Lösungsentwurf eingegangen.

Finanzierung

Das Forschungsprojekt wird durch Forschungsgelder der ZHAW School of Management and Law und der Kommission für Technologie und Innovation des Eidgenössischen Volkswirtschaftsdepartements (KTI¹) ermöglicht.

¹ Das Projekt wurde als Vorprojekt ohne Wirtschaftspartner von der KTI mitfinanziert.

2. Der digitale Nachlass: Relevanz und Eigenschaften

2.1 VOM E-MAIL KONTO ZUR DIGITALEN IDENTITÄT: WAS WIRD ZUM DIGITALEN NACHLASS?

Welche «digitalen Werte» und «Spuren im Internet» sammeln sich im Laufe eines Lebens an? Handelt es sich um Vermögenswerte, emotionale Werte, Aspekte einer digitalen Identität oder überwiegend doch nur um belanglose digitale Habseligkeiten oder gar Datenmüll?

Es ist kaum möglich, die Ausprägung eines typischen digitalen Nachlasses zu erfassen oder Aussagen zu dessen Umfang oder gar Relevanz zu machen. Das Spektrum reicht vom Datenspeicher in der Cloud, über ein Social-Media-Profil bis hin zum Avatar, der persönliche Eigenschaften wie Stimme, Aussehen oder Vorlieben speichert. Die Inhalte können alles und nichts, bedeutungslos, vertraulich, urheberrechtlich geschützt oder strafrechtlich relevant sein. Zu individuell sind die Verhaltensmuster der verschiedenen Internetgenerationen und einzelnen Nutzer und zu dynamisch sind die Geschäftsmodelle im Internet, die permanent neue Angebote, aber auch Wege der Sammlung, Streuung und Auswertung von Daten eröffnen. Die Häufigkeit, mit der das Wallstreet Journal im Online-Thema «What they know»² (WSJ Online, o.J.) über neue Tracking-Mechanismen im Internet berichtet, lässt ahnen, welche Reichweite und Aussagekraft unsere Spuren im Internet mittlerweile erreicht haben. Es geht beim digitalen Nachlass

längst nicht nur um die eigentlichen **Inhalte** (z.B. Foto-dateien), sondern um die **Gefäße**, – und dies sind in zunehmendem Masse Internet-Plattformen – in denen wir diese aufbewahren aber auch teilen, die **Konten** inklusive persönliche Profilinformationen, an die sie gebunden sind, sowie die auswertbaren **Spuren**, die wir ausgehend davon im Rahmen unserer Internetaktivitäten hinterlassen. Um angesichts dieser dynamischen und «schwammigen» Masse an Daten eine Arbeitsdefinition des «digitalen Nachlasses» für das Forschungsprojekt zu schaffen, wurden zwei Arbeitsgrundlagen erstellt:

- Eine Beschreibung der speziellen Eigenschaften des digitalen Nachlasses und der daraus resultierenden Problematiken (siehe Kapitel 2.2.)
- Eine nutzungsabhängige Klassifikation, die mögliche Komponenten eines digitalen Nachlasses und deren Relevanz aus rechtlicher Sicht abbildet (siehe Tabelle 2). Diese kann nur eine unvollständige Momentaufnahme sein, deren konkrete Ausprägung und Relevanz vom individuellen Nutzungsverhalten abhängt. Eingeflossen sind Klassifikationen der (OECD, 2007) für nutzergenerierte Inhalte und des Bundesamts für Statistik für Internetaktivitäten (Bundesamt für Statistik, 2011b) sowie Social-Media-Taxonomien (z.B. Social Media Prisma (Ethority, o.J.)

² <http://online.wsj.com/public/page/what-they-know-digital-privacy.html>

Tabelle 2

NUTZUNGSABHÄNGIGE AUSPRÄGUNG EINES DIGITALEN NACHLASSES

NUTZUNGSABHÄNGIGE KLASSIFIKATION EINES DIGITALEN NACHLASSES (BEISPIELHAFTE AUSPRÄGUNG / PRIVATE INTERNETNUTZUNG)		RECHTLICHE RELEVANZ		
		Persönlichkeitsrecht	Urheberrecht	Vermögens- / Vertragsrecht
SOCIAL MEDIA UND NUTZERGENERIERTE INHALTE		●	◐	○
Teilen und kommentieren		◐	◐	○
Dokumente, Präsentationen, E-Books	Scribd, slideshare, Google docs	◐	◐	○
Fotos, Bilder	Flickr, Picasa	◐	◐	○
Videos	YouTube, dailymotion, vimeo	◐	◐	○
Musik	Soundcloud, muziboo	◐	◐	◐
Software, Apps	appexchange	○	◐	◐
Allgemeines Filesharing	rapidshare	◐	◐	○
Publizieren		◐	◐	◐
Persönliche oder kommerzielle Websites (Verträge mit Hosting-Anbietern, Domain-Name, Seiteninhalte)	Hostpoint, Genotec, Swisscom, Sunrise etc.	◐	◐	●
Wikis (Bibliotheken, Einträge)	Wikipedia	◐	○	○
Microblogs (Tweets, Listen)	Twitter	◐	○	○
Blogs (Eigener Blog, Blogbeiträge, Kommentare)	overblog	◐	◐	○
Diskussionsforen (Konto, Postings)	themenabhängig	◐	○	○
Literarische Werke (Texte, Gedichte) und Kritiken/Feedback	Fanfiction.net	◐	◐	○
Journalistische Beiträge (Bürger-Journalismus)	GlobalVoices	◐	◐	○
Social Networking		◐	◐	○
Profile, Kontakte, Posts, Nachrichten, Fotos, Videos, Links etc. in sozialen Netzwerken, Guthaben/virtuelle Währung	Facebook, myspace, hi5, studivz	◐	◐	◐
Profile, Kontakte, Nachrichten Beiträge in professionellen/interessenbasierten Netzwerken	Xing, LinkedIn	◐	◐	○
Dateiablagen (online Speicher)		◐	◐	○
Konten, Dateien in der Cloud (ohne Kenntnis des Speicherorts)	Amazon S3, Dropbox, W	◐	◐	○

Konten, Online gespeicherte Dateien (mit Kenntnis des Speicherorts onshore oder near/offshore)	Swisscom, mydrive.ch			
KOMMUNIKATION				
E-Mail-Konten, E-Mails, Anhänge, Kontakte	GoogleMail, Cablecom, Swisscom			
Internet-Telephonie: Konten, Kontakte	Skype			
Chat, Instant Messaging etc.: Konten, Kontakte	Google Talk, Windows Live Messenger			
TRANSAKTION (E-COMMERCE, E-GOVERNMENT)				
E-Finance				
E-banking: Konten, Depots, Korrespondenz etc.	Plattformen der Banken			
E-insurance: Policen, Korrespondenz etc.	Plattformen der Anbieter			
E-payment: Konten, Guthaben, Kreditkarten-Daten etc.	PayPal			
EBPP (Electronic Bill Payment and Presentment): Konten, Rechnungen, Korrespondenz etc.	PostFinance (e-Rechnung), PayNet von Telekurs			
Online Shopping, Auktionen, Online Booking (Reisen, Tickets etc.)				
Benutzerkonten, (offene) Transaktionen	Amazon, ebay, Ricardo.ch			
E-Government				
Transaktionen/Zahlungen, Formulare, Korrespondenz etc.	ZHprivateTax			
UNTERHALTUNG, ONLINE GAMING UND VIRTUELLE REALITÄTEN				
Konten, Spielstände, Guthaben	World of Warcraft, Battle.net			
Konten, Avatare, virtuelle Güter, virtuelle Währung	Second Life			
INFORMATION (KONSUM NICHT PRODUKTION)				
Online Zeitungen, Magazine etc. Konten/Online Abonnemente, Kommentare	nzz.ch			

Erbrechtlich relevant

Rechtliche Relevanzeinstufung, generalisiert (abhängig von der individuellen Nutzung und den konkreten Inhalten):

keine
 gering
 teilweise
 hoch
 sehr hoch

2.2 DER DIGITALE NACHLASS: EIGENSCHAFTEN UND PROBLEMATIKEN

Im Unterschied zu physischen Dokumenten, Aktenordnern, Adressbüchern oder Fotoalben sind digitale Werte per Definition kaum greifbar. Zu Lebzeiten ist dies eine normale Begleiterscheinung der zu-

nehmenden Digitalisierung und Virtualisierung des täglichen Lebens. Im Todesfall wirft diese Immaterialität jedoch Problematiken auf, die den Umgang mit dem digitalen Nachlass eines Verstorbenen für die Hinterbliebenen komplizieren:

Kenntnis:

Der digitale Nachlass ist in zunehmendem Mass nicht lokal auf Endgeräten der Verstorbenen, sondern verteilt in diversen Internetplattformen gespeichert. Die Angehörigen haben in der Regel keine Kenntnis aller Internet-Konten und Social-Media-Aktivitäten einer verstorbenen Person. Internet-Reputationsdienste können helfen, finden jedoch nicht zwingend alle Spuren, insbesondere dann, wenn der Verstorbene die Möglichkeiten zum Schutz der Privatsphäre im Internet ausgenutzt hat. Hinzukommt, dass die digitale Identität nicht unbedingt der realen Identität entspricht, wenn der Verstorbene unter einem oder mehreren Pseudonymen (Avatar, Nickname, Künstlernamen, Firmenname) online aktiv war. Ob diese «digitalen Identitäten» ohne Kenntnis der Angehörigen unerkannt fortbestehen, ist nicht nur eine Frage der Pietät, sondern kann auch handfeste finanzielle Konsequenzen haben, dann nämlich, wenn sich beispielsweise ein Vertrag mit einem kommerziellen Website Hosting Anbieter automatisch verlängert, urheberrechtlich relevante Werke existieren oder ein Guthaben auf einem PayPal-Account besteht. Zusätzlich erschwert wird der Umgang mit dem digitalen Nachlass, wenn den Angehörigen das Internet-Know-How fehlt, d.h. die Kenntnis über das Spektrum an Möglichkeiten von Social Media bis E-Commerce.

Zugriff:

Internet-Konten und Social-Media-Profile sind zugriffsgeschützt. Sofern der Verstorbene diese Zugriffsdaten nicht hinterlegt und zugänglich gemacht hat, haben die Angehörigen keinen Zugriff und sind abhängig von den Praktiken und AGB der Plattformanbieter. Nur wenige Internet-

dienste verfügen über eine explizit kommunizierte Regelung für den Umgang mit Daten und Accounts im Todesfall, wie dies z.B. bei Facebook der Fall ist. Einige Internetdienste erteilen Zugriff bzw. erstellen Datenkopien nach Vorlage einer Todesurkunde. Andere wiederum haben sehr strikte Regelungen, die den Zugriff für Dritte auch im Todesfall nicht zulassen, wie z.B. Yahoo! in den Allgemeinen Geschäftsbedingungen (Stand: April 2012):

«Ein Account ist nicht übertragbar und alle Rechte an dem Account und den gespeicherten Inhalten erlöschen mit dem Tod des Nutzers.»

Yahoo! Deutschland, 2012

Eigentum und Kontrolle:

Die Frage des Zugriffs ist eng verknüpft mit der Frage des Eigentums. Eine Reihe von Internetplattformen haben Aussagen zum Eigentum in ihre AGB aufgenommen (z.B. Facebook Nutzungsbedingungen (Facebook, 2012) (Stand: Juni 2012) «Du bist Eigentümer aller Inhalte und Informationen, die du auf Facebook postest. ... Du gibst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit

Facebook postest (IP-Lizenz). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst, ausser deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht.» Der ausschliessliche Nutzungsanspruch wird somit – nicht nur bei Facebook – bereits zu Lebzeiten abgetreten, sei es durch Anerkennen der Anbieter-AGB oder durch das für die moderne Internetnutzung typische Teilen von Informationen. **Der Kontrollverlust wird sozusagen zur Nutzungsvoraussetzung.** Unabhängig von der Frage, ob der User zu Lebzeiten Eigentümer (=rechtliche Verfügungsgewalt) oder Besitzer (=tatsächliche Herrschaftsgewalt) seiner digitalen Inhalte ist, hat diese Frage auch erbrechtliche Relevanz (siehe Kapitel 6.1). In der Schweiz gilt gem. Art. 560 Abs. 1 ZGB das Prinzip der Universalsukzession. Das bedeutet, dass die Erben die Erbschaft eines Verstorbenen als Ganzes erwerben. Ob die Daten, als Immaterialgüter, Teil dieser Erbmasse sind, hängt vom konkreten Inhalt ab. Nur urheberrechtlich geschützte Inhalte sind vererblich (Art. 16 Abs. 1 URG), während der Grossteil der Daten wohl unter die Persönlichkeitsrechte fallen, die mit dem Tod enden und nicht vererbbar sind (Art. 31 Abs. 1 ZGB). Einen Anspruch auf Daten geltend zu machen oder deren Löschung zu verlangen, ist für die Erben oder sonstigen Hinterbliebenen im Konfliktfall somit kaum durchsetzbar (siehe Kapitel 6.2 bis 6.4.).

Archivierungswürdigkeit und Format:

Sterben ist eng mit Andenken verbunden. Wie und wodurch möchte ich in Erinnerung bleiben? Welche Hinterlassenschaften könnten meinem Andenken schaden? Wenn Fotos, Familienrezepte und Korrespondenz nur noch digital existieren, liegt es nahe, zumindest einen Teil dieses «digitalen Nachlasses» für die Nachwelt zu bewahren und langfristig zugänglich zu machen. Eine finale Lösung für die «unendliche» Archivierung in entsprechenden Formaten und Speichermedien existiert noch nicht, so dass die fortlaufende Konvertierung wertvoller digitaler Erinnerungsstücke Voraussetzung für deren Erhaltung ist. Nicht erst im Todesfall relevant ist die

Frage des Aussortierens. Dienste wie LifeNaut oder die Facebook-Chronik ermöglichen es, bereits zu Lebzeiten wichtige Lebensstationen mit digitalen Erinnerungsstücken zu dokumentieren (siehe Kapitel 8.3). Ob die Lebenszeit dieser Dienste jedoch ausreichen wird, um ein digitales Erbe für künftige Generationen zu bewahren, ist nicht zu garantieren.

Löschbarkeit und Vergessen:

Bereits zu Lebzeiten ist es nahezu unmöglich, Spuren der Internetnutzung endgültig und vollständig zu löschen. Technologische Fortschritte wie die Indexierung und Analyse von Internetinhalten, Multisite-Postings oder Austauschformate erleichtern die Suche und das Teilen von Informationen, erschweren aber auch das «Recht auf Vergessen» im Internet. Ein Bild oder Profil kann auf einer Plattform gelöscht werden, aber im Cache der Internetsuchmaschinen und Webarchiven weiterbestehen. Das «Ausmerzen» dieser gestreuten Spuren ist aufwendig und erfordert unter anderem, dass bei einzelnen Suchmaschinen die Löschung aus dem Cache beantragt wird³. Für ein Verfallsdatum für Daten wie es Viktor (Mayer-Schönberger, 2010) als eine Möglichkeit des «digitalen Vergessens» propagiert, gibt es bereits technische Lösungen (siehe Kapitel 8.4). Ob und wie sich diese durchsetzen können, ist jedoch fraglich. In der Schweiz wurde im März 2012 ein Postulat an den Nationalrat eingereicht und angenommen, das den Bundesrat beauftragt, die Aufnahme des «Rechts auf Vergessen im Internet» in die Gesetzgebung zu prüfen (Schwaab, 2012). In einer Stellungnahme zur Annahme des Postulats vom 9.5.2012 wird auf den Bericht zur Evaluation des Bundesgesetzes über den Datenschutz verwiesen. Zu den darin skizzierten Zielsetzungen der Revisionsarbeiten zähle auch eine Verbesserung der Datenkontrolle und -herrschaft. In diesem Sinne solle auch eine Präzisierung des «Rechts auf Vergessen» geprüft werden (siehe Kapitel 6.3.5).

³ siehe z.B. Google Webmaster Tools «Inhalte aus Google entfernen» (Google, o.J.). URL: <http://support.google.com/webmasters/bin/answer.py?hl=de&answer=164734>

3. Vom Datenspeicher zum Datenfriedhof: Wird der digitale Nachlass bedeutender?

Zahlenspiele wie «Jede Minute sterben weltweit drei Facebook-Mitglieder» oder «Jährlich 3000 Facebook-Tote in der Schweiz» sind hilfreich, um die Thematik ins Bewusstsein zu rücken (siehe Kapitel 3.4). Die Relevanz des digitalen Nachlasses allein an den Altersgruppenstatistiken und Mortalitätsraten der Schweizer Onlinebevölkerung festzumachen, wäre jedoch eindimensional. Dass in zunehmendem Masse von einer immer breiteren Bevölkerungsmasse Spuren und Daten auf dem Internet hinterlassen werden, ist unbestritten. Verändert hat sich jedoch nicht nur die Quantität, sondern auch die Art der Nutzung.

Alle Facetten der Internetnutzung und deren Auswirkung auf die digitale Identität und den digitalen Nachlass zu beschreiben, ist unmöglich. Nachfolgend werden daher drei wesentliche Faktoren, die den digitalen Nachlass zunehmend relevanter werden lassen, mit Blick auf die Schweiz, beleuchtet:

1. Das Internet ist Teil des täglichen Lebens geworden und hat alle Altersgruppen und sozialen Schichten erreicht. Immer mehr Personen nutzen häufiger und länger das Internet. Getrieben wird diese Entwicklung von technologischen, wirtschaftlichen und sozialen Faktoren. Sinkende Kosten und wachsende Verbreitung von Hochleistungsinternetzugängen, mobile Nutzung sowie einfache Werkzeuge für die Bereitstellung von Inhalten sind die Wegbereiter einer Entwicklung, die zum gesellschaftlichen Phänomen – global und so auch in der Schweiz – geworden ist.

2. Wesentliche Treiber der zunehmenden Internetnutzung sind die permanent wachsenden Nutzungsmöglichkeiten, die immer mehr Lebensbereiche durchdringen. **Die Art der Internetnutzung hat sich seit dem Durchbruch des World Wide Web Mitte der 90er Jahre grundlegend verändert.** Stand zu Beginn die Beschaffung von Informationen und die E-Mail-Kommunikation im Vordergrund, so hat der Konsum von Produkten und Dienstleistungen sowie in jüngerer Zeit die einfache Interaktion und Publikation via Social Media zunehmend an Bedeutung gewonnen. Konsequenz dieser **aktiven Nutzung des Internet** sind mehr oder weniger sichtbare Spuren, die Teil unserer digitalen Identität und letztendlich des digitalen Nachlasses sind.

3. Alter ist immer noch das wesentlichste soziodemographische Unterscheidungsmerkmal bei der Internetnutzung in der Schweiz (Bundesamt für Statistik, 2012). Aber auch dieser «digitale Graben» wird kontinuierlich schmaler. **Die Schweizer Onlinebevölkerung altert**, und mit zunehmendem Alter steigt zwangsläufig die Mortalitätsrate der Internetnutzerschaft.

3.1 INTERNET IST TEIL DES TÄGLICHEN LEBENS GEWORDEN

Das Bundesamt für Statistik publiziert seit Ende der 90er Jahre die Indikatoren zur Mediennutzung und zur Informationsgesellschaft in der Schweiz (Bundesamt für Statistik, 2010a). Die Zeitreihenstatistiken zu verschiedenen Themenbereichen, wie Internetnutzung oder IKT-Ausstattung in privaten Haushalten dokumentieren die zunehmende wirtschaftliche und soziale Bedeutung der Informations- und Kommunikationstechnologie in der Schweiz und im internationalen Vergleich. Die Zahlen aus den Jahren 2004 und 2010 machen deutlich, wie massiv sich das Internet im Alltag der Schweizer Bevölkerung verbreitet hat:

«77% aller Schweizer Haushalte verfügen über einen Internetanschluss. Davon sind 91% Hochgeschwindigkeitsanschlüsse und 65% dieser Haushalte nutzen das Internet über mehr als ein Medium.»

Bundesamt für Statistik (Stand 2010)

Tabelle 3

INTERNETNUTZUNG IN DER SCHWEIZ VON 2004 BIS 2010

in %

Indikatoren der Internetnutzung in Schweizer Haushalten	2004	2010
Haushalte mit Internetzugang (in % aller Haushalte)	61	77
Internetnutzung mehrmals wöchentlich (in % der Bevölkerung ab 14 Jahren)	54	75
Wöchentliche individuelle Internetnutzung mehr als 6 Stunden (in % der Internetnutzer)	33	43
Internetnutzung zu Hause (in % der regelmässigen Internetnutzer ab 14 Jahren)	47	76
Internetzugang über mehr als ein Medium (in % aller Haushalte mit Internetanschluss)	10	65
Hochgeschwindigkeits-Internetanschlüsse (in % aller Haushalte mit Internetanschluss)	–	91
Hochgeschwindigkeits-Internetanschlüsse (in % der Einwohner mit Hochgeschwindigkeits-Abonnement)	17	37
Internetzugang über Mobiltelefon (in % aller Haushalte mit Internetanschluss)	1	39
Breitbandzugriff auf Mobilnetz (% der Einwohner mit Vertrag für Breitbandinternetzugriff)	–	49

Datenquellen: BFS-Bundesamt für Statistik (2011b). Indikatoren Informationsgesellschaft – Internetnutzung. URL: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html (6.3.2012)

BFS-Bundesamt für Statistik (2012). Internet in den Schweizer Haushalten: Ergebnisse der Erhebung Omnibus IKT 2010. URL: <http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/22/publ.html?publicationID=4742> (6.3.2012)

3.2 DURCH DIE ZUNEHMEND AKTIVE INTERNET-NUTZUNG HINTERLASSEN WIR IMMER MEHR PERSÖNLICHE DATEN

Die Indikatoren zur Internetnutzung in der Schweiz liefern nicht nur Daten zum Umfang der Internetnutzung, sondern auch zur Art der Onlineaktivitäten (Bundesamt für Statistik, 2011b).

E-Mail-Kommunikation ist ungebrochen der wichtigste Grund der Internetnutzung, auch wenn die Generation der unter 25-Jährigen (93%) weniger über E-Mail kommuniziert als die Generation der 25- bis 34-Jährigen (97%). SMS und Social Media scheinen also einen Einfluss auf die E-Mail-Kommunikation zu haben, ohne diese bereits ernsthaft zu verdrängen (Bundesamt für Statistik, 2012, p.25). E-Mail-Konten sind essentieller Teil der Privatsphäre. Darüber hinaus dient die E-Mail-Adresse bei vielen Internet-

Diensten als Benutzername und/oder als Erkennungsmerkmal für das Anfordern oder Erneuern von Login-Daten. Der Zugriff zum E-Mail-Konto ist somit «Generalschlüssel» zu einem grossen Teil der Internet-Konten – und somit auch zum digitalen Nachlass – einer Person⁴.

⁴ Siehe auch Kapitel 6.3.4 (Auskunftsgesuch am Beispiel E-Mail Account)

«Im Februar 2012 haben sich in der Schweiz stündlich 141 neue Facebook-Mitglieder angemeldet.»

[Social Media Schweiz](#)

Tabelle 4

ONLINE AKTIVITÄTEN FÜR PRIVATE ZWECKE IN SCHWEIZER HAUSHALTEN

in %

Indikatoren der Internetnutzung in Schweizer Haushalten (in % der Internetnutzer, in den letzten 3 Monaten)	2004	2010
E-Mails senden und empfangen	90	93
Suche nach Informationen über Produkte und Dienstleistungen	73	73
Nachrichten, Zeitungen, Magazine lesen	36	73
Tätigkeiten im Zusammenhang mit der öffentlichen Verwaltung (in % der Internetnutzer, in den letzten 12 Monaten)	49	71
Online-Einkauf von Produkten / Dienstleistungen	34	55
Online-Verkäufe (inkl. Auktionen)	4	14
E-Banking Nutzung	42	50
Musik herunterladen	19	40
Nachrichten über Chat, Foren, Newsgroups senden	19	31
Eigenes Social Media Profil anlegen / pflegen	–	36
Selbst erstellte Inhalte auf Internetseiten oder Plattformen aufschalten	–	22

Datenquelle: BFS-Bundesamt für Statistik (2011b). Indikatoren Informationsgesellschaft – Internetnutzung. URL: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html (6.3.2012).

Auch wenn die passiv «lesende» Internetnutzung in Form von Informationssuche und Zeitungslesen weiterhin dominiert, so ist die aktive Nutzung eindeutig auf dem Vormarsch. Der Konsum von Produkten und Dienstleistungen ist selbstverständlicher Bestandteil der Internetnutzung geworden. Immer mehr Geschäftsbeziehungen, Transaktionen aber auch Interaktionen mit Behörden, für die es nur noch digitale Nachweise gibt, werden über das Internet abgewickelt.

Neben E-Commerce hat Web 2.0 die Internetnutzung revolutioniert. Internetkonsumenten werden zu «Prosumers»⁵, die Inhalte auf einer neuen Generation von Internetplattformen teilen und Beziehungen über Soziale Netzwerke aufbauen. Nutzergenerierte Inhalte («User-generated/created content») in Form von Texten, Fotos, Videos, Apps etc. werden im Rahmen von Blogs, Wikis, Filesharing Plattformen und Sozialen Netzwerken für einen mehr oder weniger beschränkten Personenkreis im «Participative Web» (OECD, 2007) publiziert. 36% der Schweizer Internetnutzer gaben 2010 an, ein eigenes Social-Media-Profil zu pflegen (Bundesamt für Statistik, 2011b) und der Trend hält an. Im Februar 2012 wurden in der Schweiz stündlich 141 neue Facebook-User registriert (Social Media Schweiz, 2012). Im April 2012 verfügten bereits 41% der gesamten Schweizer Bevölkerung über 14 Jahre über ein Facebook-Profil. Zieht man die durchschnittlichen 5% Fake-Accounts, ab, die Facebook im Börsengangprospekt offengelegt hat (United States Securities and Exchange Commission [SEC], 2012), bleibt eine 39-prozentige Durchdringung.

⁵ Produzent (producer) und Verbraucher (consumer) zugleich (nach Alvin Toffler)

Konsequenz der aktiven Internetnutzung sind die Spuren, die dabei bewusst oder unbewusst hinterlassen werden, sei es in Form eines Blog-Eintrags oder unseres Social Networking Profils, das in Kombination mit dem persönlichen Surfverhalten, viel über unsere (digitale) Identität verrät.

Zum aktuellen Zeitpunkt lässt sich kaum erahnen, wie viele Informationen im Laufe eines aktiven Online-Lebens auf diese Weise akkumuliert, gestreut und weiterverarbeitet werden. Die aktuelle Diskussion um Datenschutz und soziale Netzwerke konzentriert sich darauf, diese Verteilprozesse zumindest transparent zu machen und den Nutzern Kontrollmechanismen in die Hand zu geben. Der Bericht der Europäischen Kommission zur Haltung der EU-Bürger zu Datenschutz und elektronischer Identität basiert auf der grössten jemals durchgeführten Umfrage zum Internet-Nutzungsverhalten der EU-Bürger (älter als 15 Jahre) (European Commission, 2011). Demzufolge betrachten 74% der befragten EU Bürger die Offenlegung persönlicher Daten als zunehmend unvermeidlichen Teil des modernen Lebens. Der Grund, dies zu tun, liegt für 79% in der Nutzung von Online Shopping Angeboten und für 61% in der Nutzung von Sozialen Netzwerken. 70% sind besorgt, dass Internet-Plattformen ihre Daten für andere Zwecke als die, für die sie bereitgestellt wurden, nutzt und nur rund ein Viertel (26%) der Befragten glaubt noch vollständige Kontrolle über persönliche Daten im Internet zu haben. 75% wünschen ein «Recht auf Vergessen», d.h. die Möglichkeit, persönliche Daten im Internet endgültig zu löschen. Eben dies wird jedoch durch technologische Innovationen und neue Nutzungsmuster und Geschäftsmodelle zunehmend un-

«Monatlich werden weltweit durchschnittlich 6 Milliarden Fotos auf Facebook gestellt. Allein in der Silvesternacht 2010/11 wurden 750 Millionen Fotos auf Facebook hochgeladen»

möglich. Ein Foto kann aus dem eigenen Profil entfernt werden, nicht aber ohne weiteres aus den Profilen der Kontakte, mit denen das Foto geteilt wurde⁶, und ebenso wenig aus den Cache-Speichern der Suchmaschinen-Indizes. Viktor Mayer-Schönberger's Buch «Delete: Die Tugend des Vergessens in digitalen Zeiten» widmet sich diesem Thema (2010) und stellt fest, dass diese Entwicklung nicht einfach passiert, sondern zugelassen wird. Der «Trend zur Selbstentblössung» und die «Erosion der Privatsphäre» in Kombination mit einem «allzu gründlichen digitalen Gedächtnis» (Mayer-Schönberger, 2010, pp. 22–23) hält an und lässt den digitalen Nachlass grösser und persönlicher werden. In welchem Ausmass dies geschieht, und welche Relevanz der daraus resultierende digitale Nachlass hat, hängt, im Rahmen der Praktiken der Plattformanbieter und der rechtlichen Rahmenbedingungen, vom individuellen Nutzungsverhalten, der Kompetenz und der daraus resultierenden Vorsicht beziehungsweise Sorglosigkeit des einzelnen Nutzers ab.

⁶ Siehe auch (Wagenknecht, 2011) Was passiert mit unseren Bildern bei Facebook? URL: <http://www.rechtambild.de/2011/05/facebook-was-passiert-mit-unseren-bildern> [Besucht: 9 June 2012].

Der «Trend zur Selbstentblössung» und die «Erosion der Privatsphäre» in Kombination mit einem «allzu gründlichen digitalen Gedächtnis» hält an und lässt den digitalen Nachlass grösser und persönlicher werden.

Mayer-Schönberger, 2010: p.22f

«74% der befragten EU Bürger betrachten die Offenlegung persönlicher Daten als zunehmend unvermeidlichen Teil des modernen Lebens. 26% glauben noch vollständige Kontrolle über persönliche Daten im Internet zu haben. 75% wünschen ein «Recht auf Vergessen»»

European Commission, 2011: Attitudes on Data Protection and Electronic Identity in the European Union

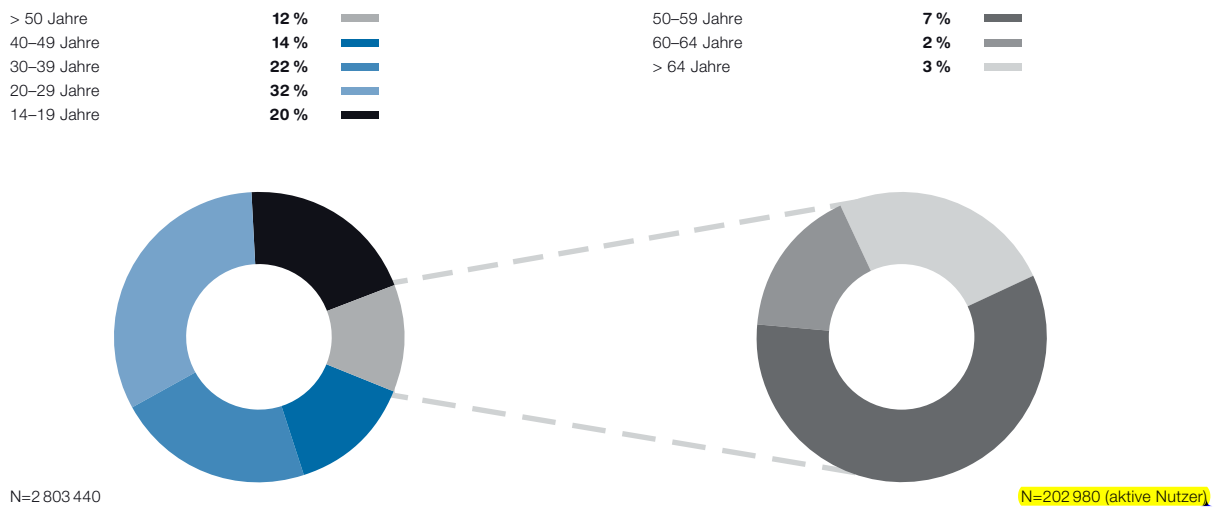
3.3 DIE ONLINEBEVÖLKERUNG IN DER SCHWEIZ ALTERN

«Facebook Schweiz wird älter» überschreibt die NZZ (Langer, 2012) die jüngsten Nutzungsstatistiken des grössten Sozialen Netzwerkes, das weltweit mehr als 800 Millionen und in der Schweiz fast 3 Millionen aktive Mitglieder verzeichnet (Bernet/Serranetga, 2012), Stand September 2012).

Dass Social Media kein Jugendphänomen sind, zeigt die Tatsache, dass rund die Hälfte der Facebook-Mitglieder in der Schweiz über 30 und mehr als ein Viertel über 40 Jahre alt ist. Die über 50-jährigen, die sogenannten «Silver Surfer», stellen erst rund 12% der Facebook-Mitglieder. Doch die enormen Wachstumsraten in dieser Altersgruppe lassen die Facebook-Nutzerschaft in der Schweiz zunehmend altern.

Abb. 1

ALTERSSTRUKTUR AKTIVER FACEBOOK-NUTZER IN DER SCHWEIZ (STAND 29.2.2012)



Datenquelle: Social Media Schweiz (2012) Facebook – die Schweiz in Zahlen (Updates pro Stichtag). URL: http://www.socialmediaschweiz.ch/html/ch_fb_publicationen.html [abgerufen: 22.6.2012].

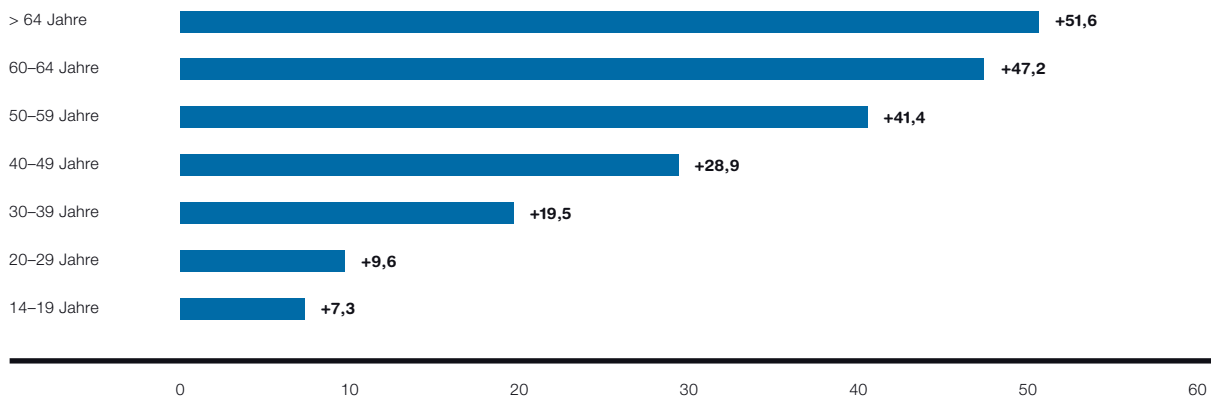
Stagnierende Wachstumsraten zeigen sich bei den Schweizer Mitgliedszahlen lediglich bei den jüngeren Nutzergruppen. Die Nutzergruppen > 30 Jahre wachsen wei-

terhin im zweistelligen Bereich, wobei der deutlich grösste Wachstum bei den über 50-jährigen «Silver Surfern» zu verzeichnen ist.

Abb. 2

JÄHRLICHES WACHSTUM AKTIVER FACEBOOK-NUTZER SCHWEIZ (28.2.2011 BIS 29.2.2012)

in %

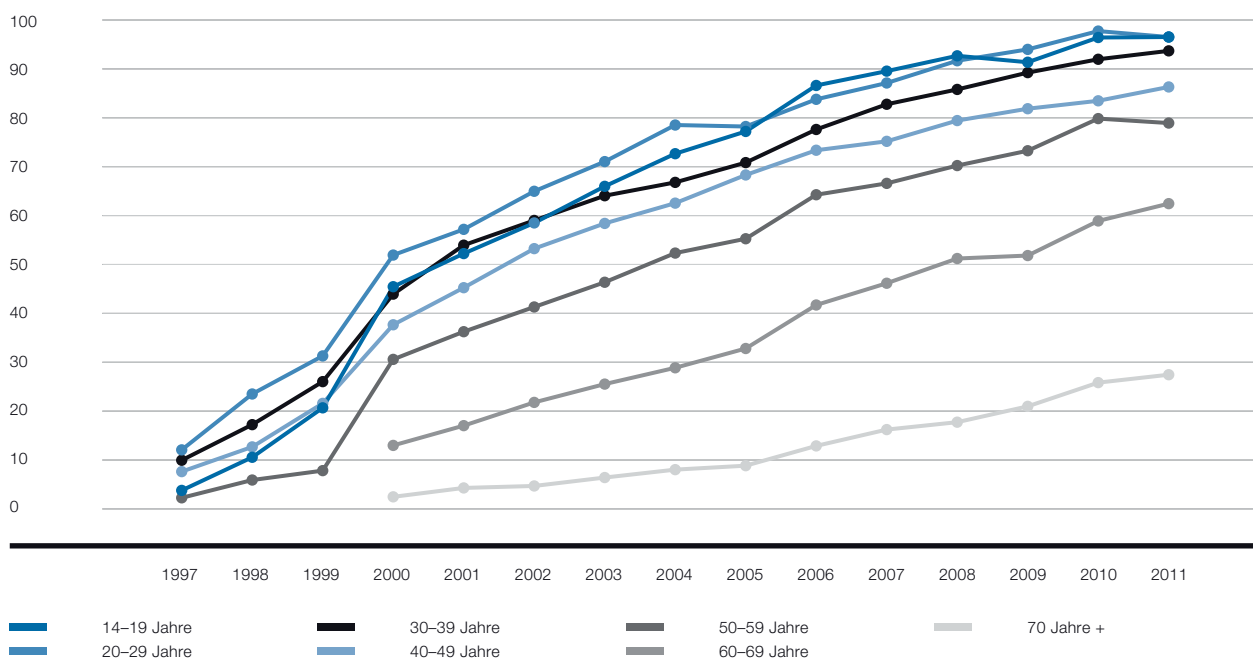


Datenquelle: Social Media Schweiz (2012) Facebook – die Schweiz in Zahlen (Updates pro Stichtag). URL: http://www.socialmediaschweiz.ch/html/ch_fb_publicationen.html [abgerufen: 22.6.2012].

Abb. 3

INTERNETNUTZUNG IN DER SCHWEIZ NACH ALTER VON 1997 BIS 2011

in %



Datenquelle: BFS-Bundesamt für Statistik (2011b). Indikatoren Informationsgesellschaft – Internetnutzung. URL: http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html (6.3.2012)

«Rise of the Silver Surfer»

Die Altersstruktur von Facebook Schweiz ist eine Folgeerscheinung des Aufholeffekts, der bei der Internetnutzung in der Schweiz allgemein für die höheren Altersklassen seit Ende der 90er-Jahre verzeichnet wurde (Bundesamt für Statistik, 2012). **Auch wenn nach wie vor ein digitaler Graben zwischen den über 60-jährigen und der jüngeren Bevölkerung liegt, so nutzen mittlerweile doch mehr als 60% der über 60-jährigen in der Schweiz regelmässig das Internet; bei den 50- bis 59-jährigen sind es fast 80%** (Bundesamt für Statistik, 2011b). Dass diese Altersgruppen in zunehmendem Masse auch Social Media für sich entdecken, ist eine logische Konsequenz.

Dass sich das Nutzungsverhalten der Altersgruppen unterscheidet, zeigen die Ergebnisse verschiedener Studien (Bundesamt für Statistik, 2011b; European Commission, 2011; Franz, 2010; ZHAW, 2010). Verglichen werden dabei häufig die Verhaltensmuster der «Digital Natives» und der «Digital Immigrants». Neben diesen beiden Kategorien, haben sich die nachfolgenden Bezeichnungen für die verschiedenen Internetgenerationen durchgesetzt.

Tabelle 5

INTERNETGENERATIONEN

Internetgeneration	Eigenschaften	Geburtsjahrgang
Digital Natives	Aufgewachsen mit Computern, Mobiltelefonen, Internet, Video Games etc.; Internetnutzung überproportional von hedonistisch-egoistischen Werten geprägt = Spass, Action, Kreativität und Selbstverwirklichung, Kontakte mit anderen; Fokus: Kommunikation und Unterhaltung (Franz 2010)	1980 +
Digital Immigrants	Adaption von Computern, Mobiltelefonen, Internet, Video Games im Laufe des Erwachsenenlebens; Internetnutzung geprägt durch altruistische-soziale und konservativ-traditionelle Werte = soziale Verantwortung, Status, Sicherheit; Fokus: Kommunikation, Transaktionen, gezielte Informationssuche (Franz 2010)	Vor 1980
Generation C64/ Generation Atari	Aufgewachsen mit der ersten Generation der Heimcomputer und PC-Spiele; An der Schwelle von den Digital Immigrants zu den Digital Natives	Ca. 1966–1971
Silver Surfers	Ältere Generation der Internet-Nutzer, die aus Marketingperspektive zur Zielgruppe «Best Agers» gehören, d.h. zwischen 50 und 69 Jahre alt sind	Ca. 1942–1961

Auch wenn Digital Natives sich immer noch häufiger und länger im Internet bewegen (Bundesamt für Statistik, 2012), so sind die Unterschiede doch nicht so massiv, als dass sich daraus auf die Relevanz des digitalen Nachlasses schliessen liesse. (Franz, 2010) stellt dies für die deutsche Online-Bevölkerung fest und interpretiert die Umfrageergebnisse dahingehend, dass die Unterschiede zwischen den Internetgenerationen vielmehr in deren Werthaltung und Motiven für die Internetnutzung liegen. Einen Einfluss dürfte ausserdem die erhöhte Skepsis der «Digital Immigrants» im Vergleich zu den «Digital Natives» in Bezug auf Datenschutz und Kontrolle über persönliche Daten im Internet haben; «Digital Natives» sehen die Offenlegung von persönlichen Daten, um Zugriff auf Soziale Netzwerke und sonstige gratis Internet-Plattformen zu erhalten, als weniger problematisch an als «Digital Immigrants» (European Commission, 2011, p.3). Auf der anderen Seite sind «Digital Natives» aktiver und vermutlich auch kompetenter, wenn es darum geht, Massnahmen zu ergreifen, wie die Sicherheitseinstellungen eines Sozialen Netzwerkes oder des Internet Browsers zu verändern oder bei Plattformen die persönlichen Informationen abzufragen, die dort gespeichert sind (European Commission, 2011, pp.111, 165).

3.4 MEHR ALS 3000 VERSTORBENE FACEBOOK-USER JÄHRLICH IN DER SCHWEIZ

Die Mortalitätsraten von Social Network Mitgliedern zu berechnen hat einen makabren Beigeschmack, insbesondere dann, wenn dies mit Blick auf ein Geschäftsfeld «digitale Nachlassplanung» geschieht.

Vor diesem Hintergrund hat 2010 einer der Gründer des digitalen Vererbungsdienstes Entrusted⁷ hochgerechnet, dass weltweit jede Minute drei Facebook-Mitglieder sterben (Lustig, 2010). Seine Rechnung basierte auf US-amerikanischen altersgruppenspezifischen Sterbeziffern, die er auf die globale Facebook-Mitgliederzahl (2010: 500 Millionen) nach Altersgruppen anwandte und somit rund 1,5 Millionen Facebook-Tote weltweit im Jahr 2010 errechnete⁸. Resultat dieses Zahlenspiels war die eindrückliche Schlagzeile «Three Facebook Users Die Every Minute», die es schaffte, die Thematik «Digital Death» in zahlreichen Blogs und Artikeln zu positionieren, und ins Bewusstsein zu rücken, dass Social Media Nutzer und Nutzerinnen nicht für immer jung und unsterblich sind.

Wendet man dieses Vorgehen auf die Nutzerschaft von Sozialen Netzwerken in der Schweiz am Beispiel von Facebook und Xing an, ergibt sich folgendes Bild:

⁷ Entrusted (Madison, WI) wurde im April 2012 vom Schweizer Anbieter SecureSafe (DSwiss AG) übernommen.

⁸ (Lustig, 2012) aktualisierte diese Hochrechnung kürzlich auf 2,89 Millionen verstorbene Facebook-Mitglieder weltweit im Jahr 2012.



FACEBOOK SCHWEIZ – SCHÄTZUNG DER TODESFÄLLE 2011 UND 2012

Altersgruppe	Sterbeziffer CH (Stand 2010 ^{1,2})	Facebook Schweiz			
		Aktive User (31.12.2011 ³)	Errechnete Todesfälle aktiver User 2011	Aktive User (29.2.2012 ³)	Hochrechnung Todesfälle per Ende 2012 ^{**}
14–19 Jahre	0,022664 %	549 380	125	549 140	124
20–29 Jahre	0,032693 %	880 020	288	892 020	306
30–39 Jahre	0,050378 %	592 300	298	617 460	341
40–49 Jahre	0,127239 %	379 420	483	405 920	591
50–59 Jahre	0,329963 %	181 540	599	202 980	808
60–64 Jahre	0,658749 %	45 020	297	51 580	420
> 64 Jahre	*	73 160	916	84 340	1 328
65–74 Jahre	1,252052 %				
Total:		2 700 840	3 005	2 803 440	3 919



XING SCHWEIZ UND DACH – SCHÄTZUNG DER TODESFÄLLE 2012

Altersgruppe	Sterbeziffer CH (Stand 2010 ^{1,2})	Xing Schweiz		Xing Deutschl., Österr., Schweiz	
		Mitglieder CH (April 2012 ⁴)	Todesfälle Hochrechnung 2012 ^{***}	Mitglieder DACH (April 2012 ⁴)	Hochrechnung Todesfälle 2012 (unter Anwendung CH-Sterbeziffern ^{***})
14–19 Jahre	0,022664 %	128 520	42	1 056 000	345
20–29 Jahre	0,032693 %	287 280	145	2 059 200	1 037
30–39 Jahre	0,050378 %	226 800	289	1 478 400	1 881
40–49 Jahre	0,127239 %	113 400	374	686 400	2 265
50–59 Jahre	0,329963 %				
60–64 Jahre	0,658749 %				
> 64 Jahre	*				
65–74 Jahre	1,252052 %				
Total:		756 000	849	5 280 000	5 529

Quellen:

¹ Für die Facebook-Altersgruppe > 64 wurde die Sterbeziffer CH für die Altersgruppe 65–74 Jahre verwendet, nicht die Sterbeziffer der kompletten Altersgruppe 64–100+ Jahre (3,137404%).

^{**} Unter Anwendung der Mitgliederwachstumsraten des Vorjahres * 0,5

^{***} Xing führt nur eine Altersgruppe > 50 Jahre; Es wurde für alle Xing-User > 50 Jahre die CH-Sterbeziffer der Altersgruppe 50–59 angewandt.

² Bundesamt für Statistik (2010c). Statistik der Bevölkerung und der Haushalte (Ständige Einwohner, Stichtag 31.12.2010). URL: <http://www.bfs.admin.ch/bfs/portal/de/index/themen/01/02/blank/data/01.html> [abgerufen: 6.22.2012].

³ Bundesamt für Statistik (2010b) Bevölkerungsbewegung – detaillierte Daten: Geburten und Todesfälle: Todesfälle (Total) nach Alter. (Todesfallstatistik 2011 zum Analysezeitpunkt noch nicht verfügbar) URL: <http://www.bfs.admin.ch/bfs/portal/de/index/themen/01/06/blank/data/01.html> [abgerufen: 22.6.2012].

⁴ Social Media Schweiz (2011/2012) Facebook – die Schweiz in Zahlen (Updates pro Stichtag). URL: http://www.socialmediaschweiz.ch/html/ch_fb_publicationen.html [abgerufen: 22.6.2012].

⁵ Xing (2012) Xing Mediadata. URL: https://www.xing.com/pdf/xing_medidata_20120404_de.pdf [abgerufen: 22.6.2012].

Demzufolge sind 2011 in der Schweiz schätzungsweise mehr als 3.000 aktive Facebook-Mitglieder verstorben; das bedeutet durchschnittlich 8 Todesfälle täglich. ~~Wächst Facebook in der Schweiz nur halb so stark weiter wie 2011, ist 2012 mit ca. 4.000 Todesfällen zu rechnen. Diese Zahl dürfte deutlich höher liegen, wenn der Wachstum in den Altersgruppen der über 50-jährigen weiter anhält. Ähnlich vorsichtig ist die Schätzung von 849 verstorbenen Xing-Mitgliedern allein in der Schweiz, ausgehend von den Mitgliederzahlen im ersten Quartal 2012. Wendet man die Schweizer Sterbeziffern auf alle Xing-Mitglieder in Deutschland, Österreich und der Schweiz nach Altersgruppen an, ergeben sich schätzungsweise mehr als 5.500 jährliche Todesfälle.~~ Wie viele dieser Profile in Sozialen Netzwerken unverändert bestehen bleiben, gelöscht werden oder im Fall von Facebook in den Gedenkstatus versetzt werden, ist nicht bekannt. Xing legt Profile von Mitgliedern, die als verstorben gemeldet werden, ohne formale Hürden still und löscht sie ohne Wiederruf nach Ablauf von drei Monaten endgültig. Dabei setzt Xing darauf, dass Todesfälle zuverlässig von Netzwerkkontakten oder Angehörigen an den Kundendienst gemeldet werden. Statistisch erfasst werden diese Meldungen nicht, so dass Xing auf Anfrage keine Aussage machen konnte, ob die Anzahl der tatsächlich stillgelegten bzw. gelöschten Profile von verstorbenen

Mitgliedern den hochgerechneten jährlichen Schätzungen entspricht. Weder Xing noch Facebook löschen Profile infolge Inaktivität. Es bleibt zu vermuten, dass ein nicht zu quantifizierender Teil der Profile verstorbener Mitglieder unverändert «weiterlebt» und dies nicht nur für die umsatzrelevanten Mitgliederstatistiken der Sozialen Netzwerke, sondern auch in Form bizarrer Geburtstagserinnerungen oder Kontaktempfehlungen.

Tabelle 8 einfügen (siehe Excel)

4. Szenarien für den digitalen Nachlass

WAS PASSIERT MIT DEN IM INTERNET GESPEICHERTEN DATEN IM TODESFALL?

Was mit den Konten, Profilen und Daten im Internet nach dem Tod einer Person geschieht, hängt im Wesentlichen von den beteiligten Akteuren und vier Faktoren ab:

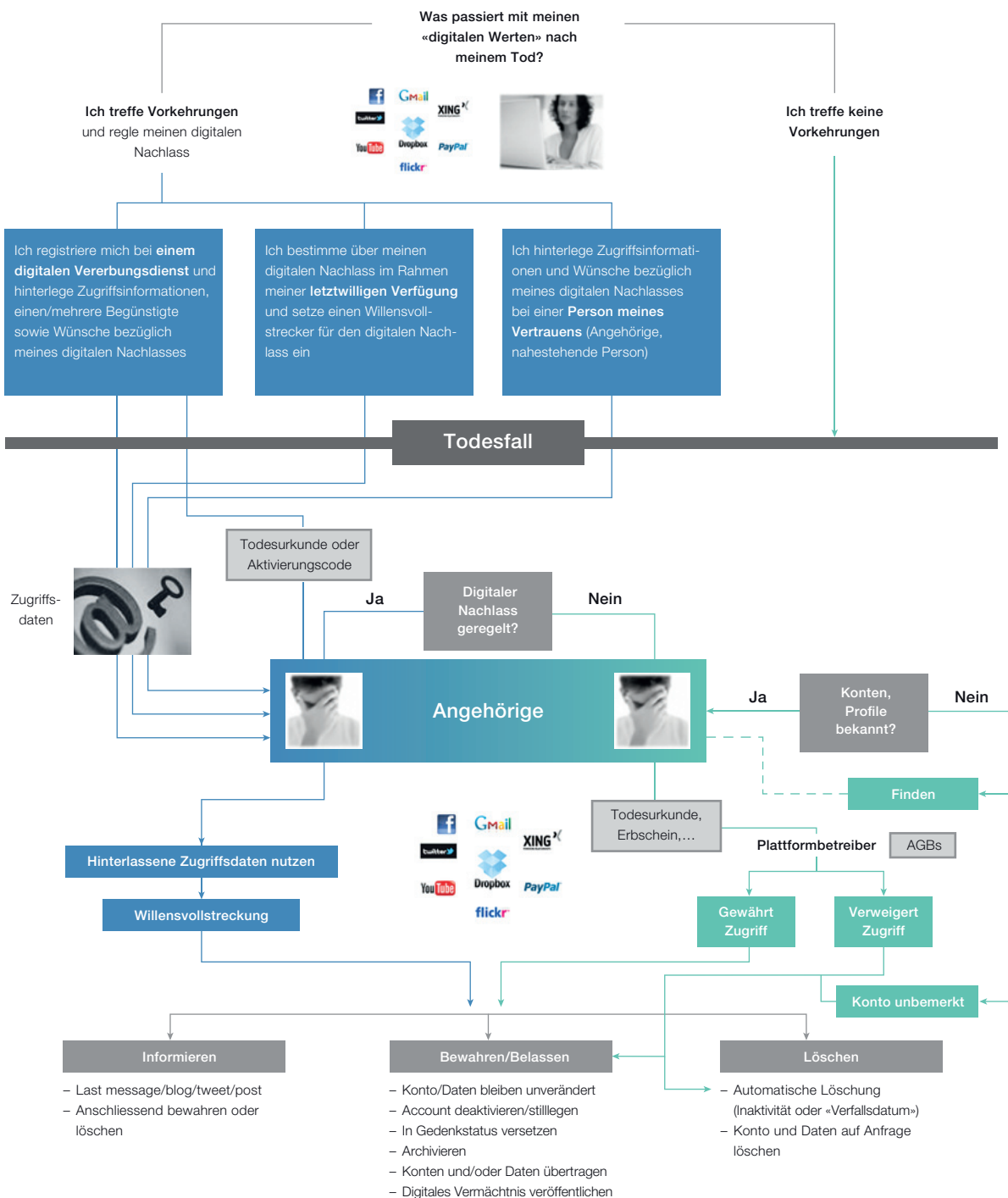
Akteure	Faktoren
Ich Eigenverantwortlicher Nutzer	1. Existiert eine digitale Nachlassplanung? Habe ich meinen digitalen Nachlass zu Lebzeiten geregelt oder nicht? Falls ja, ... <ul style="list-style-type: none"> – Auf welchem Weg habe ich über meinen digitalen Nachlass verfügt (konventionelles Testament, digitaler Vererbungsdienst, Teilen der Zugriffsdaten mit Angehörigen/vertrauten Personen zu Lebzeiten)? – Welche Vorgehensweise habe ich für einzelne Konten, Profile und Datenbestände festgelegt (löschen, bewahren, Gedenkstatus, letzte Botschaft etc.)?
Hinterbliebene (Angehörige, nahestehende Personen)	2. Haben die Hinterbliebenen Zugriff auf den digitalen Nachlass (Username, Login für die Konten)? <ul style="list-style-type: none"> – Haben sie Kenntnis von den verschiedenen Internetkonten, Profilen und Datenbeständen? – Haben sie genügend Internet- und Social-Media-Know-How, um die eigenen Wünsche oder die der verstorbenen Person im Rahmen der digitalen Nachlassplanung formulierten Wünsche auszuführen? – Decken sich die Wünsche der Angehörigen mit denen der verstorbenen Person? – Sind die Wünsche der verstorbenen Person oder der Angehörigen gegenüber den Plattformanbietern durchsetzbar?
Plattformanbieter	3. Was lassen die Plattformanbieter im Umgang mit den Accounts und Daten verstorbener Personen zu? <ul style="list-style-type: none"> – Welche Nutzungsbedingungen/AGB oder sonstigen Regelungen kommen zur Anwendung? – Was sagen diese über die Übertragbarkeit von Zugriffsrechten, Daten oder Nutzungsrechten lebender oder verstorbener Nutzer aus? – Wo ist der Geschäftssitz, Kundendienst und Gerichtsstand für Nutzer in Europa/der Schweiz? – Welche Dokumente (in welcher Sprache) sind notwendig, um den Todesfall nachzuweisen (Todesurkunde, Erbschein, etc.)?
Gesetzgeber, Rechtsprechung	4. Welche rechtlichen Rahmenbedingungen gelten im konkreten Fall für die digitale Nachlassplanung und Willensvollstreckung? <ul style="list-style-type: none"> – Welche rechtliche Relevanz haben die Inhalte des digitalen Nachlasses? Sind sie erbrechtlich, d.h. urheber-, vertrags- oder vermögensrechtlich relevant oder fallen sie unter das Persönlichkeitsrecht? – Wie kann ich formgültig über den digitalen Nachlass verfügen? – Inwiefern greifen Datenschutzbestimmungen, um z.B. die Löschung von Daten zu erzwingen oder Angehörigen den Zugriff auf Daten zu verweigern? – Welche Möglichkeiten und Grenzen bestehen für die Durchsetzbarkeit der Wünsche von Verstorbenen und Angehörigen? – Welcher Gerichtsstand und welches Recht kommen im Konfliktfall zur Anwendung?

Abbildung 4 zeigt in vereinfachter Form die Szenarien, die sich, ausgehend von der Grundsatzentscheidung «digitale Nachlassplanung: ja oder nein», für den Umgang mit dem digitalen Nachlass im Todesfall ergeben. Der Verlauf des Entscheidungsbaums macht deutlich:

- **Internetnutzende haben die Wahl, selbstbestimmt und eigenverantwortlich auf verschiedenen Wegen über ihren digitalen Nachlass zu bestimmen.** Vor- und Nachteile sowie Grenzen dieser Möglichkeiten sind Gegenstand der Analysen existierender Lösungsanbieter (Kapitel 8) sowie der rechtlichen Rahmenbedingungen (Kapitel 6).
- **Wenn Internetnutzende ihren digitalen Nachlass regeln, schaffen sie Transparenz und lösen die Zugriffsproblematik für die Angehörigen im Todesfall. Mit der digitalen Nachlassplanung liegt die Kontrolle und Verfügungsgewalt über den digitalen Nachlass im Todesfall in erster Linie bei den Angehörigen.** Sie können die hinterlegten Zugriffsdaten nutzen, um den Willen des Verstorbenen oder die eigenen Wünsche in Bezug auf den digitalen Nachlass umzusetzen. Einige Vererbungsdienste, (z.B. Ziggur.me) bieten zudem eine «keep private»-Funktion an, d.h. für bestimmte Konten kann bestimmt werden, dass die Angehörigen im Todesfall keine Information und keinen Zugriff auf dieses Konto erhalten. Der digitale Vererbungsdienst agiert in diesem Fall als Willensvollstrecker und löscht z.B. das Konto.
- **Wenn Internetnutzende ihren digitalen Nachlass nicht regeln, sind im Todesfall die Plattformanbieter die taktgebenden Akteure.** Die Angehörigen sind, wenn sie die Zugriffsdaten nicht beschaffen können (z.B. durch Analyse der Endgeräte des Verstorbenen) auf die Kooperation der Plattformanbieter angewiesen, die ihrerseits datenschutzrechtliche Vorgaben erfüllen müssen. Die unterschiedlichen Praktiken der Plattformanbieter sind Gegenstand von Kapitel 5.

Abb. 4

SZENARIEN FÜR DEN DIGITALEN NACHLASS



DIE OPTIONEN

Unabhängig davon, ob und wie der Zugriff erfolgt, gibt es zwei wesentliche Optionen im Umgang mit dem digitalen Nachlass: Löschen oder Bewahren.

Aber löschen ist nicht gleich löschen und bewahren ist nicht gleichbedeutend mit unverändert bestehen lassen. Je nach Plattform gibt es Varianten, die teilweise nur mit Mühe in den Hilfetexten, Einstellungsmenüs oder nur über den Kundendienst des Betreibers ausfindig zu machen sind. Welche Optionen die Plattformanbieter zulassen, ist Gegenstand von Kapitel 5.

LÖSCHEN

Auch wenn die Angehörigen Zugriff auf das Konto erhalten, bedeutet dies noch nicht, dass sie das Konto und die darin enthaltenen Daten einfach und rückstandslos löschen können. Unter dem Druck der Datenschützer ermöglichen zwar immer mehr Plattformen das endgültige Löschen von Konten (zu Lebzeiten), aber die Löschanträge sind nicht bei allen Anbietern direkt bei den Kontoeinstellungen zu finden (z.B. bei Google), sondern oftmals in den Online-Hilfen (z.B. bei Facebook, Xing) aufzuspüren. Das endgültige Löschen erfolgt in der Regel nach Ablauf einer Schutzfrist, in der das Profil lediglich stillgelegt ist. Allerdings ist anschliessend schwer zu kontrollieren, ob nicht nur das Profil, sondern auch die gespeicherten Daten und Spuren endgültig und unwiderruflich gelöscht sind. Fotos in sozialen Netzwerken konnten in Versuchen noch Jahre nach der Löschung über Direktlinks abgerufen werden (Computerbetrug.de, o.J.). Wie der Facebook-Audit Bericht des Irischen Datenschützers zeigt, ist sowohl die Prüfung der unwiderruflichen Datenlöschung als auch die Erarbeitung nachvollziehbarer Löschemechanismen durch den Plattformanbieter mit hohen Aufwänden verbunden (Data Protection Commissioner of Ireland, 2012, p.113). Auf die Problematik ein «Recht auf Vergessen» im Internet durchzusetzen wird in Kapitel 6.3.5 und 8.4 eingegangen.

BEWAHREN

Je stärker die digitale Identität ist, desto grösser kann das Bedürfnis sein, diese nicht einfach zu löschen. Soll der digitale Nachlass komplett oder in Teilen bewahrt werden, stellt sich die Frage in welcher Form, an welchem Speicherort und mit welchem Zugriff⁹ dies geschehen soll. Bleibt ein Konto eines Verstorbenen unberührt und wird vom Plattformanbieter infolge Inaktivität nicht gelöscht, bleiben Konto und Daten unverändert bestehen. Dies kann auch ein Wunsch der verstorbenen Person oder deren Hinterbliebenen sein.

Eine spezielle Variante des Fortbestehens ist der Gedenkstatus bei Facebook. Profile im Gedenkstatus können nur noch von Freunden besucht werden und tauchen in der öffentlichen Suche sowie in den Vorschlägen nicht mehr auf. Facebook hat den Gedenkstatus für Profile in der heutigen Form 2007 in Reaktion auf den Amoklauf an der Virginia Tech in Blacksburg eingerichtet (Krashinsky, 2009). Unter den 35 Todesopfern waren 27 Studierende im College-Alter, die Mehrzahl davon Facebook-User. Die Profile im Gedenkstatus waren ein Bezugspunkt der Trauer für die kurz daraufhin graduierten und in allen Teilen des Landes und weltweit verteilten Studierenden. Ursprünglich wollte Facebook die Profile im Gedenkstatus nach 30 Tagen löschen. Der Protest der Angehörigen und Studenten führte jedoch zur heutigen Praxis, Profile im Gedenkstatus ohne zeitliche Beschränkung bestehen zu lassen, es sei denn ein unmittelbarer Angehöriger verlangt die Löschung.

Eine Variante das digitale Vermächtnis bereits zu Lebzeiten aufzubauen und dessen Fortbestand sicherzustellen, sind digitale Andenkendienste, die Gegenstand von Kapitel 8.3 sind. Digitale Andenkendienste sind nicht zu verwechseln mit «digitalen Friedhöfen» oder «Online Memorials», die im Gedenken an einen Verstorbenen eingerichtet werden.¹⁰

⁹ Die problematische Frage des Zugriffs auf den digitalen Nachlass ist Gegenstand der rechtlichen Analyse (Persönlichkeitsrecht und Datenschutz, Kapitel 6.2 und 6.3).

¹⁰ Der Aspekt des Trauerns und Gedenkens im Internet war nicht Gegenstand des Forschungsprojekts.

Soll der digitale Nachlass ausserhalb des ursprünglichen Kontos oder Profils gesichtet oder archiviert werden (z.B. Fotos aus einem Online-Dienst lokal auf einem Endgerät der Hinterbliebenen), so setzt dies die Übertragung der Daten voraus. Zu Lebzeiten oder mit den Zugriffsdaten ist der Download von Daten beispielsweise aus einem Sozialen Netzwerk oder E-Mail Konto zunehmend unproblematisch. Die grossen Plattformen bieten Download-, Synchronisierungs- oder Archivfunktionalitäten als Bestandteil der Kontoeinstellungen an (z.B. Facebook Archiv, Xing Connector) oder über Drittanbieter (z.B. Google via Data Liberation). Daneben existieren spezialisierte Dienste und Werkzeuge, die Downloads und Archivierung von Daten aus einem oder mehreren Sozialen Netzwerken und Internet-Speichern unterstützen (z.B. SocialSafe, Tweetbook, FlickrBackup).

INFORMIEREN

Die Social Media Präsenz, E-Mail-Konten oder Kontaktlisten des Verstorbenen können genutzt werden, um über das Ableben zu informieren. Die Botschaft wird entweder vom Verstorbenen vorbereitet und hinterlegt oder von den Angehörigen verfasst. Wird die Botschaft vom Verstorbenen zu Lebzeiten formuliert, kann diese bei einem spezialisierten «Last Message»-Dienst (z.B. LastMessageClub.org) oder einem digitalen Vererbungsdienst, der diese Funktion anbietet (z.B. Legacy Locker), hinterlegt und dann durch den Vererbungsdienst oder einen Beauftragten ausgelöst werden. Varianten von Internet-Abschiedsbotschaften sind neben E-Mails z.B. «Last tweets» «last blogs» oder «last posts». Diese Option ist vorgelagert, d.h. es wird lediglich sichergestellt, dass der Todesfall im virtuellen Netzwerk nicht unbemerkt bleibt. Es bleibt jedoch weiterhin zu entscheiden, ob die Accounts und Daten im Anschluss zu löschen oder zu bewahren sind.

4.1 DIE GRUNDSATZENTSCHEIDUNG: DIGITALE NACHLASSPLANUNG JA ODER NEIN

Die wenigsten Nutzer von Social Media und sonstigen Internet-Plattformen stellen sich die Frage, was nach ihrem Tod mit ihren Internetkonten, Profilen und Daten passiert. Konkret darauf angesprochen, würde ein Grossteil mit einer Mischung aus Gleichgültigkeit und Ratlosigkeit reagieren. Ursache ist zum einen eine natürliche Scheu, sich mit dem eigenen Tod auseinanderzusetzen. Zum anderen wird die Relevanz dieser Aktivitäten und Daten auf den ersten Blick eher gering eingestuft.

Das Dilemma der digitalen Nachlassplanung liegt auch in der Demographie der Internet-Nutzerschaft. Für die «Digital Natives» (Prensky, 2001), die mit Computern, Internet, Mobiltelefonen und Video Games aufgewachsen sind, sind Instant Messaging, Social Media und digitale Musik integraler Bestandteil des täglichen Lebens und für viele dieser Generation untrennbarer Teil der eigenen Identität. Für einen «Digital Native» (Geburtsjahrgang 1980+) wäre es hochrelevant, sich über seine digitale Identität nach dem Tod Gedanken zu machen. Aus der Perspektive eines gesunden «Digital Native» erscheint dies jedoch genau so abwegig oder naheliegend, wie die Auseinandersetzung mit Bestattungswünschen oder einer Patientenverfügung. Die «Digital Immigrants» (geboren vor 1980) hingegen, die digitale Technologien erst im Laufe ihres Erwachsenenlebens adaptiert haben, stehen der Nachlassplanung rein altersbedingt grundsätzlich offener gegenüber. Die finanzielle Vorsorge für den Ruhestand oder die Familie ist selbstverständlich. Alter, Arbeits- oder Entscheidungsunfähigkeit und Tod sind konkrete, wenn auch verdrängte Themen. Der digitale Nachlass ist hierbei jedoch nur ein Bereich, der geregelt sein möchte, und sicher nicht der wichtigste. Der Gestaltungsraum, was das eigene Sterben und das Danach angeht, hat sich über Erbe und Bestattungswünsche hinaus um Vorsorgeaufträge im Rahmen des Erwachsenenschutzrechtes, Patientenverfügungen und Organspenden erweitert. Grundsätzlich ist vielen, egal ob «Digital Native» oder «Digital Immigrant» bewusst, dass es sinnvoll und für die Angehörigen entlastend wäre, diese Gestal-

tungs- und Entscheidungsmöglichkeiten zu Lebzeiten zu nutzen. Aber selbst in Bereichen, die rechtlich weitgehend geregelt und mit Instrumenten (Organspendeausweis, Vorsorgeaufträge etc.) unterstützt sind, herrscht Zurückhaltung. Abzuwarten gilt, ob sich diese Haltung mit Einführung des neuen Erwachsenenschutzrechtes in der Schweiz (per Januar 2013) verändern wird und die Bevölkerung zunehmend sensibilisiert und aktiver wird. Eine Lebensversicherung abzuschliessen, ist selbstverständlicher und abstrakter, als Bestattungswünsche zu formulieren oder über das selbstbestimmte Altern und Sterben zu verfügen. Letzteres hat sehr viel mehr mit der eigenen Identität zu tun, als die finanziellen Aspekte der Vorsorge. Ein Indikator für die «Passivität» in Sachen Nachlassplanung ist die Tatsache, dass bei weniger als einem Drittel aller Erbfälle in der Schweiz letztwillige Verfügungen (Testamente) existieren (Breitschmid, 2010). Eben solche Schlüsse lassen sich daraus ziehen, dass in der Stadt Zürich mit mehr als 390 000 Einwohnern beim Bestattungs- und Friedhofsamt nur ca.

6300 Bestattungswünsche hinterlegt sind (Auskunft Bestattungs- und Friedhofsamt Stadt Zürich, Stand März 2012). Es ist selbstverständlich möglich, dass zusätzlich Bestattungswünsche anderenorts deponiert sind, aber grundsätzlich bleibt der Eindruck der Passivität in Bezug auf persönliche Vorkehrungen für den Todesfall. Wenn ich nicht festlege, was mit meinem «analogen» realen Körper nach meinem Tod geschehen soll, weshalb sollte ich dann bezüglich meiner digitalen Identität und Hinterlassenschaft aktiv werden? Die Antwort ist letztlich jedem selbst überlassen. Selbstbestimmung und Kontrolle sind zentrale Forderungen, die bereits zu Lebzeiten von den Nutzern, aber auch an die eigenverantwortliche Internetnutzerschaft gestellt werden. Die digitale Nachlassplanung ist lediglich ein Instrument, um über den Tod hinaus selbstbestimmt mit persönlichen Daten im Internet umzugehen, sofern die Plattformanbieter und rechtlichen Rahmenbedingungen dies zulassen.

«Junge Menschen nutzen das Internet intensiv, denken aber noch nicht an den Tod. Ältere Menschen sind häufiger auf Beerdigungen, das Lebensende kommt in den Blick. Aber für sie befinden sich die virtuellen Treffpunkte auf einem Kontinent, den sie noch nie betreten haben. Deshalb reagieren die meisten mit Daran habe ich noch nie gedacht.»

Birgit Aurelia Janetzky, Geschäftsführerin Semno.de

4.2 WELCHE SZENARIEN GILT ES DURCH DIE DIGITALE NACHLASSPLANUNG ZU VERMEIDEN?

Eine Motivation über digitale Nachlassplanung nachzudenken, ist die Überlegung, was passieren könnte, wenn keine Vorkehrungen getroffen werden, und wie sich dies auf die Hinterbliebenen oder das eigene Andenken auswirkt:

- Den Angehörigen wird der Zugriff auf Fotos, wichtige Dokumente oder Kontakte verwehrt, weil der Plattformanbieter aufgrund einer strikten Regelung auch bei Vorlage einer Sterbeurkunde keinen Zugriff auf die Daten erlaubt (z.B. Yahoo! AGB (Stand: April 2012): «Ein Account ist nicht übertragbar und alle Rechte an dem Account und den gespeicherten Inhalten erlöschen mit dem Tod des Nutzers.» (Yahoo! Deutschland, 2012).
- Wenn sich Angehörige erst Monate nach dem Todesfall um das digitale Erbe kümmern, sind bestimmte Accounts und deren Daten bereits infolge Inaktivität gelöscht worden (z.B. Yahoo! (AGB Abs.14.7) löscht E-Mail-Konten nach 4 Monaten Inaktivität).
- Eine verstorbene Person lebt in Social-Media-Plattformen weiter, z.B. über Xing werden weiterhin Geburtstags- und Erinnerungskarten an die Netzwerkkontakte verschickt oder der Verstorbene wird weiterhin als Netzwerkkontakt von Facebook vorgeschlagen. Als «virtuell Ausgestopfte» wurden diese Social-Media-Profile Verstorbener in einem Artikel auf ORF/Ö1-Online (Dietrich, 2009) makaber, aber durchaus treffend tituliert.
- Vermögenswerte des Erblassers bleiben unentdeckt, z.B. ein Guthaben in einem PayPal-Account oder ein Aktiendepot oder Bankkonto ausserhalb der «Hausbank», über das kein Papiernachweis besteht.
- Es kommt zum Missbrauch mittels hinterlassener Daten und Konten, z.B. Identitätsdiebstahl, der über längere Zeit unentdeckt bleibt.
- Angehörige erhalten nach Vorlage einer Sterbeurkunde vom Plattformanbieter Zugriff auf vertrauliche Daten oder Internet-Aktivitäten der verstorbenen Person, die diese weder zu Lebzeiten noch nach dem Tod mit ihnen teilen wollte (z.B. Zugriff auf ein E-Mail-Konto).
- Verträge mit Website Hosting Providern oder sonstigen kostenpflichtigen Internetdiensten laufen unbemerkt weiter. Zahlungen oder Lieferungen aus Internet-Einkäufen oder Verkäufen (z.B. ebay) stehen noch aus und die Erben erfahren stark verzögert von diesen Verpflichtungen, die im Rahmen der Universalsukzession mit Antritt des Erbes auf sie übergegangen sind.
- Es liegen unbemerkt Dokumente in cloudbasierten Online-Speichern, die für die Angehörigen oder den Arbeitgeber relevant sind.
- Ein Verstorbener hat durch Online-Aktivitäten gegen das Urheberrecht verstossen, z.B. indem er urheberrechtlich geschützte Bilder oder Videos hochgeladen hat oder via filesharing geteilt hat. Daraus resultierende Forderungen gehen an die Erben über, die die Daten unter Umständen nicht löschen können.
- Erben erhalten keinen Zugriff auf urheberrechtlich geschützte Werke, wie im Fall einer Witwe eines Fotografen, die erst drei Jahre nach dem Tod ihres Mannes auf die künstlerisch wertvollen und gefragten Fotos zugreifen konnte, die bei einem ausländischen Hosting-Provider lagen (Von der Horst, 2009).

Alle aufgeführten Szenarien können nicht nur im Todesfall eintreten, sondern auch bei Verlust der Urteils- oder Handlungsfähigkeit infolge eines Unfalls oder einer Erkrankung.

5. Praktiken der Plattformanbieter

Ein Blick auf die Praktiken der E-Mail-Provider in der Schweiz und international zeigt, wie unterschiedlich Regelungen für den Todesfall eines Nutzers gestaltet und begründet sein können. In den Nutzungsbedingungen oder Online-Hilfen kommunizierte Regelungen für den Todesfall sind nur bei grossen, internationalen Plattformen zu finden. Nationale oder europäische Anbieter, wie Xing oder Swisscom haben Regelungen, die im Todesfall über den Kundendienst in Erfahrung gebracht werden können (SR DRS, 2011). Für die Mehrheit der Plattformanbieter scheint noch kein ausreichender «Leidensdruck» zu bestehen, um die Thematik in Form öffentlich kommunizierter Regelungen zu adressieren. Mitglieder-Sterbeziffern oder der Anteil «toter» Profile werden nicht analysiert und nur wenige Anbieter löschen Konten infolge Inaktivität. Sinkende Speicherkosten sind hierfür eine Erklärung, aber auch die gesetzlichen Rahmenbedingungen, die nicht wirklich eine stabile Grundlage für die Formulierung einheitlicher und unanfechtbarer Regelungen für den Todesfall bieten (siehe Kapitel 6). Auf wackligen Beinen die Regelungen der Plattformanbieter im Konfliktfall stehen, hat der Fall des im Irak getöteten US-Soldaten Justin Ellsworth gezeigt, dessen Eltern gerichtlich Zugriff auf die Yahoo!-Email-Daten ihres Sohnes erkämpft haben, nachdem Yahoo! ihnen unter Berufung auf ihre AGB und die Privatsphäre des Verstorbenen den Zugriff verweigert hatte (BBC Online, 2005).

So bewegen sich die Plattformanbieter im Spannungsfeld zwischen Datenschutzaufgaben, den Wünschen von Angehörigen und den Persönlichkeitsrechten der Verstorbenen. Dass die Problematik nicht zuoberst auf der Prioritätenliste steht, leuchtet ein in Zeiten, in denen Plattformanbieter unter starker Beobachtung stehen und Nutzungsbedingungen und Datenverwendungsrichtlinien für ihre lebende Nutzerschaft laufend überarbeiten müssen. Nachfolgend eine Übersicht bestehender Praktiken grosser internationaler und europäischer Internet-Plattformen, die ein breites Nutzungsspektrum abdecken, und deutlich machen, wie unterschiedlich Praktiken sein können, und welch hohes Mass an Internetkompetenz und Durchhaltevermögen sie teilweise verlangen.

Analysiert wurden im Rahmen des Forschungsprojekts die Nutzungsbedingungen, Datenverwendungsrichtlinien und Online-Hilfen von Facebook, Google (Gmail, YouTube), Yahoo! (Flickr), Twitter und PayPal. Xing (Hauptsitz Hamburg/Kommunikation) erteilte auf Anfrage Auskunft. Die detaillierten Ergebnisse sind dokumentiert im Anhang zu diesem Bericht¹¹. Tabelle 8 und 9 zeigen die Optionen und Vorgehensweisen der untersuchten Plattformen im Überblick:

¹¹ sowie online aufbereitet auf der Projektwebseite. URL: <http://ares.zhaw.ch/digitalessterben/?cat=28>

«Der Zugriff auf den Xing-Account kann den Hinterbliebenen nicht ermöglicht werden, da wir keine personenbezogenen Daten an Dritte weiterleiten. Zudem müssen wir auch die Privatsphäre der Kontakte des Verstorbenen wahren, da diese ihre Kontaktdaten ausschliesslich einem bestimmten Mitglied freigegeben haben.»

Tabelle 8

OPTIONEN IM TODESFALL IM ÜBERBLICK

	Optionen zu Lebzeiten oder mit Zugriffsdaten			Optionen der Plattformanbieter im Todesfall					
	Account stilllegen (Profil, Daten bleiben erhalten)	Account und Daten löschen	Download der Daten (Synchro., Archiv etc.)	Hinterbliebene können beantragen:					
				Automatische Löschung infolge Inaktivität	Zugriff auf das Konto	Account stilllegen	Account und Daten löschen	Gedenkstatus	Datenkopien
Facebook	+	+	+	-	-	-	+	+	-
Xing	+	+	+	-	-	+ direkt bei Meldung	+ nach 3 Monaten	-	-
Gmail (Google)	-	+	+	-	-	-	(+)	-	(+)
YouTube (Google Inc.)	-	+	+ Nur eigene Videos, mp4	-	-	-	(+)	-	(+)
Flickr (Yahoo!)	-	+	+	(+) evtl. nach 4 Monaten bei Gratis-Accounts	-	-	+	-	-
Twitter	+ Löschung nach 30 Tagen	+	-	+ nach 6 Monaten	-	+ Löschung nach 30 Tagen	+	-	-
PayPal (ebay)	+	-	-	+ Auflösung nach 3 Jahren	-	+	-	NA	Guthaben werden ausbezahlt (Erben, Vollstrecker)

Legende:
 + möglich
 - nicht möglich
 (+) unter Umständen möglich

Tabelle 9

PRAKTIKEN DER PLATTFORMANBIETER IM ÜBERBLICK

Plattformanbieter

Facebook	<p>Es gibt 2 Optionen:</p> <p>1. Gedenkstatus (Memorialize): Facebook versetzt alle Konten von Nutzern, deren Todesfall gemeldet wird, in den Gedenkzustand. Den Todesfall melden können über das Formular nicht nur Familienmitglieder, sondern auch Freunde. Wenn ein Konto in den Gedenkzustand versetzt wird, können nur bestätigte Freunde das Profil (Chronik) sehen oder in der Suche finden. Ausserdem wird das Profil nicht mehr im «Vorschläge»-Abschnitt der Startseite angezeigt. Freunde und Familienmitglieder können Gedenkbeiträge hinterlassen.</p> <p>2. Profil löschen: Nur nachgewiesene, unmittelbare Familienangehörige können die Entfernung der Konten von Verstorbenen über einen «Besonderen Antrag» und mit einem offiziellen Todesnachweis beantragen.</p>
Xing	<p>Keine publizierte Regelung: Netzwerkkontakte oder Hinterbliebene wenden sich an den Xing Kundendienst. Eine Todesurkunde oder ein sonstiger Nachweis ist nicht notwendig. Profile von Verstorbenen werden inaktiv geschaltet (unsichtbar). Endgültig gelöscht werden sie nach ca. drei Monaten, um fehlerhaftes Löschen (Verwechslung, Falschmeldung) zu vermeiden.</p>
Gmail (Google)	<p>Ein «autorisierter Vertreter» kann unter Umständen Zugriff zum Inhalt des E-Mail Kontos erhalten. Es muss ein zweistufiges Verfahren durchlaufen werden. In Stufe 1 muss der «autorisierte Vertreter» diverse Identitätsnachweise und Dokumente bei Google Support (Mountain View, CA) einreichen, u.a. eine beglaubigte ins Englische übersetzte oder internationale Sterbeurkunde. Nur wenn Google nach Stufe 1 Bereitschaft signalisiert, Zugriff zu gewähren, ist Stufe 2 möglich, wobei keine Garantie gegeben wird, dass der Zugriff zum Inhalt erteilt wird. In Stufe 2 sind weitere Rechtswege erforderlich, einschliesslich einer Anordnung eines US-Gerichts und/oder der Vorlage weiterer Materialien (z.B. Erbschein).</p>
YouTube (Google Inc.)	<p>Da ein YouTube Account, wie alle Google-Produkte (z.B. auch Picasa) an einen Google Account gebunden ist, ist zu vermuten, dass wie beim Zugriff auf Gmail-Konten von Verstorbenen verfahren wird. Google hat nur eine Regelung für den Zugriff auf Gmail-Konten Verstorbener veröffentlicht. Achtung: Wird ein Google-Account gelöscht, ist der Zugang zu allen Google-Produkten gelöscht (z.B. Gmail, Picasa, YouTube).</p>
Flickr (Yahoo!)	<p>Haben die Angehörigen bereits zu Lebzeiten Zugriff auf die Fotos, da sie als Kontakt des Verstorbenen in Flickr hinterlegt wurden, haben Sie weiterhin Zugriff auf die Fotos, für die sie vom Verstorbenen freigeschalten wurden. Der Umfang des Zugriffs (anschauen, herunterladen) hängt davon ab, wie dieser beim Upload der Fotos eingestellt wurde. Problematisch ist, wenn die Angehörigen zu Lebzeiten keinen Zugriff auf die Fotos hatten und zudem keine lokale Kopie der Fotos auf einem Endgerät des Verstorbenen besteht. In diesem Fall haben sie lediglich die Möglichkeit über Freunde oder Kontakte, die Zugriff auf die Fotos haben, zu gehen. Ansonsten erhalten sie keinen Zugriff auf die Fotos und können maximal deren Löschung beantragen. Wünschen die Angehörigen, dass der Flickr-Account bestehen bleibt, ist dies möglich, da die Löschung explizit mit Todesurkunde beantragt werden muss. Aus erbrechtlicher Sicht relevant sind zudem die Lizenzierungsmöglichkeiten, die Flickr beim Upload der Fotos bietet (Creative Commons oder kommerziell).</p>
Twitter	<p>Angehörige oder autorisierte Personen können mit der Todesurkunde und beglaubigten Kopien von Dokumenten, die die Identität des Nutzers sowie die eigene Identität und Autorisierung nachweisen, die Deaktivierung des Accounts beantragen. Der deaktivierte Account wird nach 30 Tagen inklusive Inhalt gelöscht.</p>
PayPal (ebay)	<p>Im Todesfall ist der PayPal Kundendienst zu kontaktieren. Da es sich um erbrechtlich relevante Guthaben handelt und mit der Schliessung von PayPal-Konten betrügerische Absichten verbunden sein können, werden analog der englischsprachigen Hilfe, Dokumente einverlangt, die den Todesfall, die Berechtigung des Willensvollstreckers oder Erben und dessen Identität eindeutig nachweisen. Guthaben werden nach sorgfältiger Prüfung ausbezahlt.</p>



6. Rechtliche Rahmenbedingungen

Die Frage, was mit Daten im Internet nach dem Tod einer Person geschieht, hat verschiedene rechtliche Dimensionen. Es wird hier aufgezeigt, welche Instrumente dem Verstorbenen vor dem Tod zur Verfügung stehen, um den digitalen Nachlass zu regeln, aber auch darauf eingegangen, welche Handlungsmöglichkeiten die Angehörigen haben, sollte der Verstorbene nichts vorgekehrt haben. Insbesondere werden mögliche Konflikte (zwischen Angehörigen und Verstorbenen, unter Angehörigen, zwischen Angehörigen und dem Internet-Plattformanbieter) sowie offene Fragen herausgearbeitet.

Einleitend muss die Frage geklärt werden, was zu einem «digitalen Nachlass» gehört. Dieser kann aus rechtlicher Perspektive grob in folgende Kategorien eingeteilt werden (siehe Abbildung 8):

- Daten, die im Internet gespeichert sind und
 - **Nicht vererbbar sind** – hier handelt es sich um Daten, die (lediglich) eine **persönlichkeitsrechtliche Komponente**, aber keine vermögensrechtliche Komponente aufweisen.
 - **Vererbbar sind** – dabei ist insbesondere an **durch Urheberrechte geschützte Werke** zu denken.
 - **Vermögens- oder vertragsrechtlich** relevant sind
 - beispielsweise eine Homepage, die der Erblasser hinterlässt und an die gewisse Verträge geknüpft sind (z.B. Webhosting-Vertrag).
- Daten, die auf einem Endgerät (PC, Tablet, Mobiltelefon oder dergleichen) lokal gespeichert sind, und mit ihrem materiellen Datenträger, der als Vermögenswert behandelt wird, vererbt werden.

Nachfolgend konzentrieren wir uns auf die vererblichen (siehe Kapitel 6.1) und unvererblichen (siehe Kapitel 6.2 und 6.3) Daten, die im Internet gespeichert sind. Der Umgang mit vererblichen Daten wird dabei aus der Sicht des Erbrechts behandelt, während bei den nicht vererblichen Daten Aspekte des Persönlichkeits- und Datenschutzrechtes dominieren. In Kapitel 6.4 erfolgen prozessuale Hinweise und Einschätzungen zur internationalen Durchsetzbarkeit möglicher Ansprüche.

Abb. 5

ASPEKTE DES DIGITALEN NACHLASSES AUS RECHTLICHER PERSPEKTIVE

		Digitales Erbe			
		Immateriell: im Internet gespeichert			Materiell: lokal auf Endgeräten gespeichert
		Persönlichkeitsrechtlich geschützt	Urheberrechtlich geschützt	Vermögens-/Vertragsrechtlich geschützt	Sachenrechtlich geschützt
Definition, Beispiele	<p>Unter diesen Schutz fallen</p> <ul style="list-style-type: none"> – Recht auf Namen – Recht am eigenen Bild – Schutz der Intim- und Privatsphäre – Recht auf Ehre – Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (Datenschutz), z.B. eigene und fremde Kontaktdaten in Sozialen Netzwerken 	<p>Das Urheberrecht schützt geistige Schöpfungen der Literatur und Kunst, die einen individuellen Charakter haben, sowie Computerprogramme. z.B. Fotos, Videos, die künstlerisch wertvoll sind und durch das Urheberrecht geschützt sind. Bei vielen Fotos und Videos, die auf Internetplattformen gespeichert sind, ist fraglich ob sie diesen Schutz erreichen, ausgeschlossen ist es jedoch nicht.</p>	<p>Der Erblasser hinterlässt eine persönliche Homepage. Daran sind Verträge geknüpft, wie z.B. Hosting-Verträge oder Verträge über einen Domain-Namen.</p> <p>Der Erblasser hinterlässt ein Guthaben z.B. in einem PayPal-Account.</p>	<p>Die Daten, welche auf einem lokalen Endgerät (PC, DVD, Mobiltelefon etc.) gespeichert sind, können mit ihrem Datenträger, welcher als Vermögenswert behandelt wird, vererbt werden.</p>	
Vorsorge fehlt	<p>Die Persönlichkeit geht mit dem Tod unter und kann dementsprechend nach dem Tod nicht mehr verteidigt werden. Die Angehörigen können sich bei Pietätslosigkeiten gegenüber dem Verstorbenen auf ihre eigene Persönlichkeit berufen, um verletzende Handlungen zu unterbinden. Auch der Datenschutz wirkt nach dem Tod nicht mehr.</p>	<p>Urheberrechtlich geschützte Daten bleiben unentdeckt oder der Zugriff fehlt. Das Urheberrecht ist vererblich. Grundsätzlich handelt es sich um Werte, welche beim Tod des Eigentümers ohne Vorkehrungen auf die Erben übergehen.</p>	<p>Ein Guthaben bleibt unentdeckt oder Verträge können unbemerkt weiterlaufen. Die Erben treten nach dem Tod des Erblassers an dessen Stelle bei derartigen Verträgen. Sie werden Vertragspartner und können daher, den Vertrag kündigen, oder auch weiterführen (was z.B. für einen Arbeitsvertrag nicht der Fall wäre).</p>	<p>Die Erben werden kraft der Universalsukzession (Art. 560 ZGB) gemeinsam Eigentümer des Datenträgers. Es stellt sich in der Regel kein Zugriffsproblem, wie bei auf dem Internet gespeicherten Daten. Der Datenträger kann auch als Ausgangspunkt für die Konten- und Spurensuche im Internet dienen (z.B. Semno.de).</p>	
Zweck einer Vorsorge	<p>Die Vorsorge kann verschiedene Zwecke verfolgen:</p> <ul style="list-style-type: none"> – Die Angehörigen über das Bestehen der Online-Werte (Konten, Profile, Daten, Verträge) zu informieren und den Zugriff durch Hinterlegung der Zugangsdaten sicherstellen – Die digitalen Werte einer bestimmten Person zuzuweisen – Instruktionen für den Umgang mit den Konten, Profilen und Daten zu hinterlegen (löschen, bewahren), z.B. dass ein Profil gelöscht wird, eine persönliche Webseite aber weiterhin online gehalten werden soll 	<p>Die Angehörigen müssen nicht über das Bestehen der Daten informiert werden, da ein physischer Träger vorhanden ist. Jedoch kann der Erblasser erreichen wollen, dass nur eine bestimmte Person über den Inhalt des Datenträgers informiert wird.</p>			
Möglichkeiten Vorsorge	<p>Die durch die Persönlichkeit geschützten Aspekte sind nicht vererblich! Möglichkeiten zur Vorsorge bestehen dennoch:</p> <p>In einem Testament:</p> <ul style="list-style-type: none"> – Auflagen – Bestellung eines Willensvollstreckers <p>Ausserhalb des Testaments:</p> <ul style="list-style-type: none"> – Anordnungen von Todes wegen – Information der Angehörigen via digitaler Vererbungsdienst 	<p>Erbrechtliche Instrumente gemäss ZGB:</p> <p>Handschriftliches Testament mit:</p> <ul style="list-style-type: none"> – Auflagen – Vermächnisse – Bestellung eines Willensvollstreckers <p>und/oder «unkonventionelle Vorsorge»:</p> <ul style="list-style-type: none"> – Information über Zugriffsdaten via digitaler Vererbungsdienst (z.B. SecureSafe, Ziggur.me) 	<p>Es stehen die erbrechtlichen Instrumente gem. ZGB zur Verfügung:</p> <ul style="list-style-type: none"> – Erbvertrag – Testament mit – Auflagen – Vermächtnis – Bestellung eines Willensvollstreckers 		
Willensvollstreckung	<p>Problematisch wird die Durchsetzung von persönlichkeitsrechtlichen Anordnungen (egal in welcher Form), sofern die Angehörigen sich nicht an diese halten wollen. Ein Willensvollstreckter kann Abhilfe schaffen. Datenschutzrechtliche Ansprüche durchzusetzen, ist insbesondere im internationalen Verhältnis schwierig</p>	<p>Die Durchsetzung des Willens des Erblassers ist insbesondere gewährleistet, falls ein Testament errichtet wird. Keine Durchsetzungsmöglichkeit des Erbenspruches ist vorhanden, falls die Erben nicht über die Existenz der Daten informiert sind. Mit einer Vorsorge kann zwar erreicht werden, dass eine andere Person von nun an berechtigt ist, aber dieser Person kann keine Garantie auf Durchsetzung der Ansprüche aus diesem Recht gegeben werden.</p>	<p>Sorgt der Verstorbene in einem Testament vor, ist die Durchsetzung seines Willens relativ sicher. Es handelt sich um einen Fall, der vom «klassischen» Erbrecht erfasst ist</p>	<p>Die Durchsetzung des letzten Willens ist in dieser Konstellation relativ sicher, da es sich im Wesentlichen um die Vererbung des Vermögenswertes (PC, Mobiltelefon) handelt und nicht direkt der Daten</p>	

6.1 DIE ERBRECHTLICHE KOMPONENTE DES DIGITALEN TODES

In erster Linie gilt es zu klären, ob das Erbrecht Lösungen für Daten, die im Internet gespeichert sind, vorsieht. In der Schweiz gilt gem. Art. 560 Abs. 1 ZGB¹² das Prinzip der Universalsukzession. Das bedeutet, dass die Erben die Erbschaft eines Verstorbenen zum Todeszeitpunkt als Ganzes erwerben. **Gegenstand dieser Universalsukzession sind alle vererblichen Vermögenswerte und alle Schulden des Erblassers.** Zu diesen vererblichen Vermögenswerten gehören gemäss Art. 560 Abs. 2 ZGB insbesondere (es handelt sich um eine beispielhafte Aufzählung¹³) Eigentum und Besitz.

Das ZGB stellt dem Erblasser verschiedene Möglichkeiten zur Verfügung, um vor seinem Tod über seinen vererblichen Werte zu entscheiden. Die folgenden Kapitel sollen zum einen klären, welche Daten genau unter den erbrechtlichen Schutz fallen, sowie einige Vorsorgemöglichkeiten aufzeigen, und zum anderen auf die spezifischen Probleme eingehen, die sich in der digitalen Welt ergeben können.

«Das Urheberrecht ist übertragbar und vererblich.»

Art. 16 Abs. 1 URG

6.1.1 Vererbung der Daten bei bestehendem urheberrechtlichen Schutz

Urheberrechte sind gemäss Art. 16 Abs. 1 URG¹⁴ vererblich und werden von der Universalsukzession erfasst¹⁵. Diese Regelung ist eine Ausnahme vom Grundsatz der Unvererblichkeit von Persönlichkeitsrechten¹⁶. Das Urheberrecht kann im Kontext digitaler Daten durchaus eine Rolle spielen. Sowohl Fotografien, Videos als auch literarische Texte können den Schutz des Urheberrechtsgesetzes gemäss Art. 2 URG geniessen. Damit dies auch tatsächlich der Fall ist, muss ein Werk eine Schöpfung (geistiger Inhalt – beruhend auf menschlichem Willen und einer menschlichen Gedankenäusserung¹⁷) der Literatur oder Kunst mit individuellem Charakter sein¹⁸. Die in Art. 2 Abs. 2 URG

exemplarisch aufgezählten Kategorien von Werken der Literatur und Kunst, die den Schutz eines Urheberrechts geniessen können, müssen jeweils diese Voraussetzungen des Abs. 1 erfüllen¹⁹. Bei Fotografien (wie sie beispielsweise auf Facebook oder Flickr gestellt werden) ist fraglich, ob sie die Anforderungen der Individualität und des geistigen Inhalts erfüllen. Eine Fotografie erlangt den Schutz des Urheberrechtsgesetzes erst durch die Wahl des abgebildeten Objekts, des Bildausschnitts und des Zeitpunkts des Auslösens, durch den Einsatz von bestimmten Filtern, Objektiven oder die Bearbeitung des Negatives²⁰. So kann auch ein Schnappschuss – ist er gedanklich vorbereitet – eine geistige Leistung darstellen, die den urheberrechtlichen Schutz verdient hat²¹. Dieselbe Frage ist ebenfalls bei der Beurteilung von Filmen relevant – auch diese gelten nur als Werke im Sinne des URG, falls sie eine individuelle, geistige Schöpfung sind. Diese Voraussetzungen sind bei Hobbyfilmen, wie man sie beispielsweise auf YouTube findet, oft nicht erfüllt²². Handelt es sich jedoch um ein Werk im Sinne des URG, so hat der Urheber gemäss Art. 10 URG das ausschliessliche Recht über die Verwendung des Werkes zu bestimmen. Er hat insbesondere das Vervielfältigungsrecht (Art. 10 Abs. 2 lit. a URG) und das Verbreitungsrecht (Art. 10 Abs. 2 lit. b URG). Zudem wird durch

¹² Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210.

¹³ Häuptli, Art. 560 ZGB N 4; Schwander, BSK, Art. 560 ZGB N 8.

¹⁴ Bundesgesetz vom 9. Oktober 1992 über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz), SR 231.1.

¹⁵ Schwander, BSK, Art. 560 ZGB N 8; Häuptli, Art. 560 ZGB N 4.

¹⁶ Breitschmid/Kamp, S. 26.

¹⁷ BGE 130 II 168, E. 4.5.

¹⁸ Cherpillod, Art. 2 URG N 1.

¹⁹ Rehbinder/Viganò, Art. 2 URG N 5.

²⁰ Rehbinder/Viganò, Art. 2 URG N 13; Cherpillod, Art. 2 URG N 9; BGE 130 II 168, E. 4.5.

²¹ Cherpillod, Art. 2 URG N 9;

²² Rehbinder/Viganò, Art. 2 URG N 14.

Art. 11 URG die Werkintegrität geschützt und dem Urheber Schutz vor unbefugten Änderungen seines Werkes (Art. 11 Abs. 1 lit. a URG) und Schutz vor Entstellung seines Werkes (Art. 11 Abs. 2 URG) geboten. Im Internet sind demzufolge viele Urheberrechtsverletzungen denkbar. So kann es zu einer Verletzung der Urheberrechte kommen, wenn ein anderer Nutzer einer Internet-Plattform z.B. ein Bild kopiert und auf seinem Profil veröffentlicht oder auch durch den Plattform-Anbieter, indem das Werk einem grösseren Publikum als durch den Urheber beabsichtigt zugänglich gemacht wird.

Nur wenige Daten, die im Verlauf eines Lebens auf dem Internet landen, geniessen den Schutz des Urheberrechts und gehen ohne Vorkehrungen auf die Erben über.

Zu beachten bleibt, dass falls es sich um urheberrechtlich geschützte Werke handelt, diese allen Erben zu gesamter Hand zukommen und nicht Miturheberschaft begründet wird. Dies hat zur Folge, dass sich bei einer allfälligen Verletzung der Urheberrechte alle Erben gemeinsam – die Erbgemeinschaft – aktiv werden müssen. Eine Klagelegitimation einzelner Erben ist ausgeschlossen.²³

Somit kann festgehalten werden, dass nur wenige Daten, die eine Person im Verlauf ihres Lebens auf dem Internet auch anderen zur Verfügung stellt, den Schutz des Urheberrechts geniessen und somit ohne Vorkehrungen auf die Erben übergehen. Ein Facebook-Statuskommentar kann zum Beispiel nicht als «Werk» im Sinne des Urheberrechts angesehen werden. Dasselbe gilt wohl für die meisten Hobbyfotografien und Filme.

Zusätzlich ist zu beachten, dass auf Urheberrechte und alleinige Nutzungsrechte auch verzichtet werden kann.²⁴ Solche Klauseln können sich in den AGB der sozialen Netzwerke finden (siehe z.B. Facebook Nutzungsbedingungen (Stand Juni 2012): der Nutzer erteilt Facebook eine gebührenfreie Lizenz, womit er von seinem Ausschliesslichkeitsanspruch zurücktritt). Wird auf die Anerkennung der Urheberschaft oder auf die Ausübung bestimmter Rechte verzichtet, entfällt schliesslich die Vererblichkeit des Urheberrechts, bzw. bestimmter Teilrechte.

Ein weiteres Problem – welches die gesamte Thematik des digitalen Sterbens und Erbens belastet – stellt sich, falls die Angehörigen nicht über das Bestehen eines digitalen Wertes informiert sind. Es wird ihnen somit unmöglich, ihre Rechte auszuüben.

6.1.2 Die Handlungsmöglichkeiten des Erblassers

Das Schweizerische Zivilgesetzbuch (ZGB) bietet dem Erblasser verschiedene Möglichkeiten, um vor dem Tod über seinen Nachlass zu verfügen. Dabei stellt der Gesetzgeber teilweise strenge Form- und Inhaltsvorschriften auf. Es werden hier die wichtigsten Instrumente, welche allenfalls für die digitale Nachlassplanung relevant sein können, vorgestellt.

6.1.2.1 Letztwillige Verfügung (Testament)

Das Schweizerische Zivilgesetzbuch gibt dem zukünftigen Erblasser die Möglichkeit, über seinen Nachlass (also über sein vererbliches Vermögen) zu verfügen. Dies kann entweder mit einem Erbvertrag oder mit einer letztwilligen Verfügung (auch Testament genannt) geschehen. Für Daten und Konten im Internet kommt der letztwilligen Verfügung eine zentralere Bedeutung als dem Erbvertrag zu. Es liegt in der Natur der Sache, dass der Erblasser Zugangsdaten solange als möglich geheim halten will, was mit dem Erstellen eines öffentlich zu beurkundenden Vertrages (Art. 512 ZGB i.V.m. Art. 499 ZGB), gerade nicht gewährleistet wird. Was sind jedoch die Möglichkeiten und Grenzen einer letztwilligen Verfügung?

²³ BGE 121 III 118, E. 2.

²⁴ Barrelet/Egloff, Art. 16 URG N 14.

Solange es sich um vermögensrechtliche Aspekte des digitalen Nachlasses – wie z.B. urheberrechtlich geschützte Bilder oder Videos, die auf einer Webseite gespeichert sind – handelt, steht es dem Erblasser frei, darüber in einer letztwilligen Verfügung zu entscheiden. Diese Inhalte gehen zwar mit der Universalsukzession auf die Erben über, jedoch könnte der Erblasser eine bestimmte Person begünstigen wollen oder gar erst dafür sorgen, dass die Angehörigen über das Bestehen der Werte informiert werden. Hierfür kann das Instrument der letztwilligen Verfügung genutzt werden.

«Die eigenhändige letztwillige Verfügung ist vom Erblasser von Anfang bis zu Ende mit Einschluss der Angabe von Jahr, Monat und Tag der Errichtung von Hand niederzuschreiben sowie mit seiner Unterschrift zu versehen.»

Art. 505 ZGB

Damit ein letzter Wille für die Erben bindend ist, muss dieser den Formerfordernissen von Art. 505 ZGB²⁵ gerecht werden. Das heisst insbesondere, dass die Verfügung von Anfang bis Ende von Hand geschrieben werden muss sowie datiert und unterschrieben sein muss. Entscheidet man sich, über seinen digitalen Nachlass ebenfalls digital zu verfügen, wird diesem Formerfordernis nicht Rechnung getragen. Verwandte oder Freunde, die durch einen «digitalen Vererbungsdienst»²⁶ mit der Vollstreckung des digitalen Willens betraut werden, sind also rechtlich nicht verpflichtet, die darin formulierten Wünsche umzusetzen. Folgerichtig empfiehlt beispielsweise der digitale Vererbungsdienst Ziggur.me seinen Nutzern denn auch, die Existenz der digitalen Nachlassplanung bei ziggur.me in das Testament einzuschliessen.²⁷

Breitschmid spricht sich mit dem Verweis auf die Einführung der elektronischen Unterschrift (vgl. Art. 14 Abs. 2^{bis} OR und ZertES) für eine gewisse Offenheit gegenüber «technischen Äquivalenzen» aus²⁸ – also dafür, dass künftig auch Testamente, die nicht den strengen Vorschriften von Art. 505 ZGB gerecht werden, Wirkung entfalten sollen. Die elektronische Signatur für die letztwillige Verfügung ist jedoch (noch) ausgeschlossen. Auch SuisselD, einem zertifizierte Anbieter von qualifizierten elektronischen Signaturen (Art. 2 lit. c ZertEs) – also einer Signatur die eindeutig dem Inhaber zuordenbar ist und die Identifizierung des Inhabers ermöglicht – ist es nicht möglich, die Formerfordernisse von Art. 505 ZGB zu erfüllen. Denn die elektronische Signatur ist nur der eigenhändigen Unterschrift gleichgestellt, jedoch nicht der Handschriftlichkeit eines ganzen Dokuments (Art. 14 Abs. 2^{bis} OR). Unterdessen gibt es zwar ein elektronisches Testamentenregister (www.testamentenregister.ch) des Schweizerischen Notarenverbandes. In diesem kann jedoch nur eine nach den gesetzlichen Formvorschriften erstellte Verfügung von Todes wegen (dazu gehören u.a. Testamente und Erbverträge) registriert werden – sofern sie bei einem Notar oder Anwalt erstellt wurden. Es handelt sich dabei also nicht um eine digitale Aufbewahrung, sondern lediglich um das Festhalten der Existenz einer solchen Verfügung.²⁹

²⁵ Es wird hier nur auf das eigenhändige Testament eingegangen, da die anderen Verfügungsformen in Anbetracht der Problematik nicht zweckmässig erscheinen.

²⁶ Die Funktionsweise von digitalen Vererbungsdiensten ist Gegenstand von Kapitel 8.2

²⁷ <www.ziggur.me> (safe and simple/ Being listed on the register of digital inheritance), besucht am: 22.10.2012.

²⁸ Breitschmid, BSK, Art. 505 ZGB N 1.

²⁹ <www.testamentenregister.ch> (Testamentenregister/Privatpersonen), besucht am 16.07.2012.

6.1.2.2 Bestellung eine Willensvollstreckers

Gemäss Art. 517 ZGB kann der Erblasser mittels letztwilliger Verfügung³⁰ einen oder mehrere Willensvollstrecker einsetzen. «Die Befugnisse des Willensvollstreckers ergeben sich primär aus dem Willen des Erblassers, sekundär aus den gesetzlichen Vorschriften».³¹ Willensvollstrecker können juristische oder natürliche, handlungsfähige Personen sein.³² Ein Willensvollstrecker hat zum Zweck, den schnellen und zuverlässigen Vollzug der in einer letztwilligen Verfügung angeordneten Massnahmen, Teilungsvorschriften und Vermächtnisse sicherzustellen.³³ Weitere Voraussetzungen werden im Gesetz keine genannt, so wird insbesondere kein Wohn- oder Geschäftssitz in der Schweiz verlangt.³⁴ Im internationalen Verhältnis muss jedoch geklärt werden, welches Recht die Handlungsfähigkeit des Willensvollstreckers bestimmt. Für das Nachlassverfahren sind gemäss Art. 86 IPRG³⁵ die schweizerischen Gerichte und Behörden am letzten Wohnsitz des Erblassers zuständig. Sie wenden dabei schweizerisches Recht an (Art. 90 IPRG). Die Rechts- und Handlungsfähigkeit von Gesellschaften wird gemäss Art. 154 und 155 lit. c IPRG nach dem Recht des Staates, nach dessen Vorschriften sie organisiert sind beurteilt. Das heisst, es ist regelmässig ausländisches Recht in Betracht zu ziehen.

Der Erblasser hat somit die Wahl, wen er als Willensvollstrecker einsetzt – solange dieser sich nicht in einem Interessenskonflikt befindet. Denkbar ist insbesondere: einen gewöhnlichen Willensvollstrecker z.B. in der Person eines Anwalts oder Treuhänders zu ernennen, einen Online-Dienst mit der Vollstreckung des digitalen Willens zu beauftragen oder eine nahestehende Person via einen Online-Dienst als Willensvollstrecker für die digitalen Werte vorzusehen.

³⁰ Siehe zur Gültigkeit der letztwilligen Verfügung oben.

³¹ Künzle, BK, Art. 517–518 ZGB N 194.

³² Künzle, BK, Art. 517–518 ZGB N 1.

³³ Karrer/Vogt/Leu, BSK, vor. Art. 517/518 ZGB N 3.

³⁴ Künzle, BK, Art. 517–518 ZGB N 4.

³⁵ Bundesgesetz vom 18. Dezember 1987 über das Internationale Privatrecht, SR 291.

Willensvollstreckung durch einen Online-Dienst?

Digitale Vererbungsdienste unterstützen die digitale Nachlassplanung und Willensvollstreckung, indem sie die Hinterlegung von Zugriffsdaten und Instruktionen für den Umgang mit dem digitalen Nachlass unterstützen. Benannt werden ausserdem Begünstigte, die im Todesfall Zugriff auf die Zugangsdaten erhalten und den «digitalen Willen» vollstrecken. Voraussetzung ist, dass diese Vertrauenspersonen bereits zu Lebzeiten über die Existenz der digitalen Nachlassplanung und ihre Rolle als Willensvollstrecker instruiert wurden. Vereinzelt bieten digitale Vererbungsdienste auch an, als Willensvollstrecker aufzutreten, sobald der Todesfall gemeldet wird. Soll tatsächlich ein Online-Dienst die Willensvollstreckung übernehmen, muss dieser als juristische Person – unter Umständen nach ausländischem Recht – organisiert sein. Das schweizerische Recht schliesst die Willensvollstreckung durch Organisationen ohne eigene Rechtspersönlichkeit gem. Art. 530 OR aus.³⁶ Art. 517 ZGB gibt dem Erblasser die Möglichkeit, mehrere Willensvollstrecker zu ernennen. Tut er dies, kann er ebenfalls bestimmen, wie die Willensvollstrecker zusammen wirken sollen. Ein selbständiges Nebeneinander der Willensvollstrecker empfiehlt sich, wenn einzelne Vermögenswerte separat zu betreuen sind.³⁷ Also eine Lösung, die sich im Bereich der Vollstreckung eines «digitalen Willens» anbieten könnte. Ernennet der Erblasser einen Willensvollstrecker, so hat er die Möglichkeit, dessen Aufgaben im Sinne eines Spezialexekutors einzuschränken. Insbesondere ist es denkbar, eine Beschränkung auf einzelne Vermögensteile vorzunehmen.³⁸

Der in einer letztwilligen Verfügung ernannte Willensvollstrecker hat gem. Art. 517 Abs. 2 ZGB die Möglichkeit binnen vierzehn Tagen zu erklären, dass er das Amt nicht annimmt. Stillschweigen gilt als Annahme. Eine Pflicht zur Annahme besteht für die ernannte Person jedoch nicht.³⁹

³⁶ Künzle, BK, Art. 517–518 ZGB N 1.

³⁷ Künzle, BK, Art. 517–518 ZGB N 12.

³⁸ Künzle, BK, Art. 517–518 ZGB N 94; Christ/Eichner, Art. 518 ZGB N 11.

³⁹ Christ/Eichner, Art. 517 ZGB N 18.

Für den Willensvollstrecker ergibt sich bei Mandatsannahme ein einseitig zwingender Anspruch auf angemessene Vergütung. Dieser Anspruch kann vom Erblasser nicht wegbedungen werden.⁴⁰ Bemessungskriterien für diese Vergütung sind Zeitaufwand, Kompliziertheit der Verhältnisse, Umfang und Dauer des Auftrags und die damit verbundene Verantwortung.⁴¹ Ob ein freiwilliger Verzicht auf eine Vergütung möglich ist, wird in der Literatur nicht diskutiert. Jedoch ist kein Grund ersichtlich, wieso dies nicht der Fall sein sollte.

Die Willensvollstreckung durch einen Online-Service ist grundsätzlich denkbar. Es müsste im Testament klar festgehalten werden, dass es sich um einen Spezialexekutor für den digitalen Nachlass handelt. Jedoch handelt es sich hierbei kaum um eine Lösung, die sich in der Praxis durchsetzen wird. Die Lösungsanbieter haben wohl wenig Interesse daran in die formalistische Position eines Willensvollstreckers (auch nur mit beschränktem Mandat) gehievt zu werden. Beim Erblasser auf der anderen Seite wird wohl regelmässig dennoch das nötige Vertrauen fehlen und ein Online-Dienst wird kaum in einem Testament als Willensvollstrecker erwähnt werden.

Willensvollstreckung durch Private Person

Häufig werden als Willensvollstrecker Banken, Anwälte, Notare oder Treuhänder ernannt – in der Annahme diese seien neutral und unparteiisch. Jedoch steht es dem Erblasser frei, jede natürliche Person aus seinem Umfeld zum Willensvollstrecker zu ernennen. So können auch Erben oder Vermächtnisnehmer zum Willensvollstrecker ernannt

werden.⁴² Dies können problematische Konstellationen sein, da ein Willensvollstrecker, der zugleich Erbe ist, leichter in Interessenskonflikte gerät, welche ein Grund für die Absetzung des Willensvollstreckers sein können. Im Bereich der digitalen Vererbung könnte sich jedoch eine zweckmässige Willensvollstreckung auf die digitalen Werte beschränken und aufgrund der Persönlichkeitsnähe der zu behandelnden Werte, kann auch der Wunsch nach einer vertrauten Person als Willensvollstrecker gerechtfertigt erscheinen.

Ein «Willensvollstrecker» der nur «per Mausclick» ernannt wurde, kann formal nicht als solcher bezeichnet werden.

Formvorschriften

Auch bei der Bestellung eines Willensvollstreckers gilt es die Formvorschriften von Art. 505 ZGB zu beachten. Das heisst, dieser muss in einem Testament, welches handschriftlich erstellt wurde oder öffentlich beurkundet ist, bestellt werden. Der allein online «per Mausclick» ernannte «Willensvollstrecker» kann daher formal nicht als solcher bezeichnet werden.

⁴⁰ Karrer/Vogt/Leu, BSK, Art. 517 ZGB N 27, 28; Christ/Eichner, Art. 517 ZGB N 30.

⁴¹ Christ/Eichner, Art. 517 ZGB N 32.

⁴² Künzle, Interessenskollision, S. 6 f.

6.1.2.3 Ausrichten eines Vermächtnis

Mit einem Vermächtnis wird jemandem, der in der gesetzlichen Erbfolge nicht berücksichtigt wird, ein Vermögensvorteil zugewendet (Art. 483 Abs. 1 ZGB). Es können dabei insbesondere bestimmte Sachen und bestimmte Geldsummen vermacht werden.⁴³ Der Vermächtnisnehmer ist kein Erbe und auch kein Mitglied der Erbengemeinschaft und hat keinen Anspruch an deren Beschlüssen mitzuwirken.⁴⁴ Er haftet zudem auch nicht für allfällige Nachlassschulden.⁴⁵ Das Einsetzen eines Vermächtnisnehmers kann die gesonderte Behandlung des digitalen Nachlasses bewirken. Das heisst, einer Person werden die Urheberrechte übertragen und sie kann diese nutzen. Auch ein Vermächtnis kann mit Auflagen (siehe dazu 6.2.1) verknüpft werden. So kann die gesonderte Behandlung des digitalen Nachlasses im Sinne des Erblassers sichergestellt werden.

6.1.2.4 Vollmacht

Gemäss Art. 35 OR⁴⁶ ist es möglich Vollmachten zu erteilen, die über den Tod hinaus wirken. Mit einer Vollmacht wird jemand ermächtigt, im Namen eines anderen Rechtshandlungen vorzunehmen. Das heisst, der Bevollmächtigte kann – im Rahmen seiner Befugnisse – in einem Rechtsgeschäft wie der eigentlich Berechtigte auftreten. So könnte also mit einer Vollmacht erreicht werden, dass der Bevollmächtigte nach dem Tod wie der Verstorbene über dessen digitalen Daten verfügen könnte. Dies setzt erneut voraus, dass der Bevollmächtigte in Kenntnis der Zugangsdaten gelangt. Geschieht dies zu Lebzeiten und wird auch die Vollmacht noch zu Lebzeiten ausgesprochen, stellt sich die Frage, ob diese eine Wirkung über den Tod haben kann. Dies ist grundsätzlich zu bejahen. Der Bevollmächtigte hat primär die Interessen des Verstorbenen zu vertreten.

Will jedoch der Verstorbene die Zugangsdaten erst nach dem Tod bekannt machen – was eigentlich in der Natur der Sache liegt – muss geklärt werden, unter welchen Voraussetzungen vollmachten ab Todeszeitpunkt gültig sind. Die herrschende Lehre geht davon aus, dass Vollmachten auf den Tod in der Form der letztwilligen Verfügung gemäss Art. 505 ZGB erstellt werden müssen⁴⁷ – somit ist die

Handschriftlichkeit des gesamten Dokuments gefordert. Eine Vollmacht, die über den Tod wirkt, kann zudem von jedem Erben einzeln widerrufen werden.⁴⁸ Es scheint sich deshalb nicht um ein geeignetes Mittel zur Regelung der digitalen Hinterlassenschaft zu handeln.

6.1.3 Fazit – Erbrecht

Zusammengefasst ergibt sich, dass das heute geltende Erbrecht nur beschränkt (geeignete) Möglichkeiten vorsieht, um einen «digitalen Nachlass» zu regeln. Zum einen fallen nur urheberrechtlich geschützte Werke überhaupt in den Nachlass, und zum anderen gelten strenge Formvorschriften für die Gültigkeit von letztwilligen Verfügungen. Problematisch scheint in diesem Bereich das Erfordernis der Handschriftlichkeit der letztwilligen Verfügung, welches so gar nicht in die digitale Welt des Internet passt. Digitale Lösungen, die angeboten werden, mangelt es daher an der fehlenden garantierten Durchsetzbarkeit. Es kann aber dennoch sinnvoll sein, die eigenen digitalen Daten in ein formgültiges Testament aufzunehmen. Wie aufgezeigt ist es den Erben ansonsten nicht oder nur erschwert möglich, die ihnen aus Urheberrecht zustehenden Rechte überhaupt wahrzunehmen – wobei allerdings nicht vergessen werden darf, dass die Durchsetzung von Urheberrechten im Internet nicht einfach ist (siehe dazu auch 6.4). Dem Erblasser steht es auch frei, den digitalen Nachlass im Sinne eines Vermächtnisses gesondert zu behandeln und ihn in einem Testament einer bestimmten Person zuzuteilen und/oder eine Vertrauensperson als Willensvollstrecker für den digitalen Nachlass einzusetzen. Wird ein digitaler Vererbungsdiens für die Erfassung der Datenbestände, Internetkonten sowie von Zugriffsdaten und Instruktionen eingesetzt, empfiehlt es sich, diese digitale Nachlassplanung im Rahmen eines formgültigen letzten Willens zu stützen.

⁴³ Druey, § 11 N 13.

⁴⁴ Druey, § 11 N 22.

⁴⁵ Druey, § 11 N 21.

⁴⁶ Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht), SR 220.

⁴⁷ Watter, BSK, Art. 35 OR N 8, m.w.H.

⁴⁸ Watter, BSK, Art. 35 OR N 11.

6.2 DIE PERSÖNLICHKEITSRECHTLICHE KOMPONENTE DES DIGITALEN TODES

Bei den im Internet gespeicherten Daten handelt es sich nur in seltenen Fällen um Vermögenswerte, welche im Todesfall vererbt werden (können). Viel häufiger relevant sind persönlichkeitsrechtliche Aspekte, welche nicht auf die Erben übergehen.

Die Persönlichkeit einer Person wird durch Art. 28 ZGB geschützt. Bewusst hat der Gesetzgeber darauf verzichtet, aufzuzählen, welche Güter genau in den Schutzbereich fallen. Es handelt sich um einen Begriff, der stetig im Wandel ist. Aus der Rechtsprechung haben sich allerdings unter anderem folgende Bereiche ergeben, die geschützt werden:

- Psychische Integrität
- Recht auf Achtung der Privatsphäre
- (das damit verbundene) Recht auf informationelle Selbstbestimmung (dieser Aspekt erfährt einen besonderen Schutz durch die Datenschutzgesetzgebung)
- die Ehre
- das Recht am eigenen Bild⁴⁹

Daten, welche z.B. in Sozialen Netzwerken gespeichert sind, scheinen also durchaus geeignet, um in die Persönlichkeit einzugreifen und diese zu verletzen. Zum einen sind die Daten, die ein Benutzer von sich selbst auf ein solches Netzwerk stellt, vom Recht auf informationelle Selbstbestimmung erfasst, zum anderen können weitere Nutzer durch ihre Veröffentlichungen z.B. das Recht am eigenen Bild oder auch die Ehre anderer Nutzer verletzen.

Die Persönlichkeit endet gem. Art. 31 Abs. 1 ZGB mit dem Tod. Somit sind insbesondere zwei Fragen zu klären:

- Wie kann vor dem Tod gegen postmortale Persönlichkeitsverletzungen vorgesorgt werden?
- Was können die Angehörigen unternehmen?

6.2.1 Vor dem Tod

6.2.1.1 Widerrechtlichkeit von Persönlichkeitsverletzungen

Art. 28 ZGB sieht die Widerrechtlichkeit jeder persönlichkeitsverletzenden Handlung vor, es sei denn, es kann vom vermeintlichen Urheber der Verletzung ein Rechtfertigungsgrund vorgebracht werden.⁵⁰ Als Rechtfertigung kommen ein überwiegendes privates oder öffentliches Interesse, die Einwilligung des Verletzten oder die Rechtfertigung durch Gesetz in Betracht (Art. 28 Abs. 2 ZGB). Das heisst mit anderen Worten, z.B. jede Veröffentlichung von Bildern die eine Person zeigen, ist eine Persönlichkeitsverletzung, es sei denn der Abgebildete hat eingewilligt, oder es handelt sich um eine Person des öffentlichen Lebens.

Im vorliegenden Kontext ist vor allem die Einwilligung zu betrachten. Damit eine Online-Plattform überhaupt das Recht erlangt, in die Persönlichkeit einzugreifen muss eine Einwilligung vorliegen. Zu Lebzeiten kann eine Einwilligung jederzeit und frei widerrufen werden.⁵¹ So ist es – oder sollte es zumindest – jeder Person freigestellt sein, gewisse Inhalte in einem Sozialen Netzwerk zu veröffentlichen oder eben nicht und sich gegen Veröffentlichungen anderer, welche in eigene Persönlichkeitsrechte eingreifen mit Hilfe der Art. 28 ff. ZGB zur Wehr zu setzen.

⁴⁹ Büchler/Frei, Art. 28 ZGB N 1ff.

⁵⁰ Knellwolf, S. 131; Bucher, N 496.

⁵¹ Haas, N 540.

6.2.1.2 Anordnungen im Testament

Es handelt sich bei in digitalen Netzwerken gespeicherten Daten nur in seltenen Fällen (urheberrechtlich geschützte Werke) um Vermögensrechte, welche in den Nachlass fallen. Häufiger handelt es sich um persönlichkeitsbezogene Rechte und wollte man es eng sehen, ist nur das Vermögen vererblich.⁵²

Der Anspruch auf die verfassungsrechtlich garantierte persönlichen Freiheit (Art. 10 Abs. 2 BV), beinhaltet auch die Möglichkeit, zu Lebzeiten Anordnungen zu treffen, die über den Tod hinaus gelten sollen. Dazu gehört es, durch Anordnungen von Todes wegen, seine religiösen oder weltanschaulichen Auffassungen zur Achtung zu bringen.⁵³ Ebenfalls sollen die Pietätsgefühle von dem Verstorbenen nahe stehenden Personen geschützt werden.⁵⁴ Es leitet sich daraus insbesondere auch die Garantie einer selbstbestimmten Bestattung ab, welche eine postmortale Fortwirkung des verfassungsrechtlichen Persönlichkeitsschutzes des Verstorbenen darstellt.⁵⁵

Ein Beispiel dieser postmortalen Wirkung von Art. 10 Abs. 2 BV bietet BGE 129 I 173. In einem Nachtrag zum Testament traf die Verstorbene Y. Anordnung hinsichtlich ihrer Bestattung. Sie wünschte eine Bestattung in Meilen. Der Vater der Verstorbenen veranlasste die Überführung des Leichnams von Rom nach Meilen. Der Ehemann von Y. hingegen legte gegen die Bestattung in Meilen Beschwerde ein, mit der Begründung, sein Recht auf persönliche Freiheit gem. Art. 10 Abs. 2 BV werde durch eine Bestattung in Meilen verletzt, da es ihm – in Rom lebend – nicht möglich sei, die Totenfürsorge wahrzunehmen. Das Bundesgericht stufte jedoch das Interesse der Verstorbenen, aufgrund von Art. 10 Abs. 2 BV über ihre Bestattung zu entscheiden, als vorrangig ein und stellte fest, dass der Eingriff in die Grundrechte des Beschwerdeführers somit gerechtfertigt sei. Hat der Verstorbene keine Anordnung getroffen, wie mit seinem Leichnam zu verfahren ist, kommt diese Entscheidung den Angehörigen zu.⁵⁶

Anordnungen in einem Testament, die nicht das Vermögen sondern die Persönlichkeit betreffen, sind grundsätzlich möglich.

Somit ist auch bereits klar, dass auch Anordnungen nicht vermögensrechtlicher – sondern persönlichkeitsrechtlicher – Natur in einer letztwilligen Verfügung für die Angehörigen grundsätzlich bindend sind.⁵⁷ Diese sind insbesondere von Bedeutung, falls sich die Angehörigen nicht einig sind, wie sie den Verstorbenen z.B. bestatten möchten. Jedoch ist zu beachten, dass sich auch hier ein Durchsetzungsproblem ergeben kann, falls sich die Angehörigen darin einig sind, nicht mit dem Verstorbenen einig zu sein.

Durch eine **Auflage** im Sinne von Art. 482 ZGB kann der Erblasser die Begünstigten mit seinem Testament zu jeglichem rechtlich und sittlich zulässigen Tun oder Unterlassen verpflichten. Zur Wahrnehmung persönlichkeitsrechtlicher Anliegen wird somit den Erben ein «wirtschaftlicher Köder» gelegt.⁵⁸ Beispiele für Auflagen sind die Anordnung, die Gedichte des Erblassers herauszugeben oder zu vernichten,⁵⁹ Anordnungen über die Abdankung und die Bestattung, oder auch die Vorschriften des Urhebers über die Verwendung und Nutzung seines Urheberrechts.⁶⁰ Es

⁵² Breitschmid, Persönlichkeitsrechtliche Belange, S. 39.

⁵³ BGE 127 I 115, E. 4a).

⁵⁴ Schweizer, N 21.

⁵⁵ Müller/Schefer, S. 163; Auer/Malinverni/Hottelier, N 324; Beretta, BSK, Art. 31 ZGB N 41.

⁵⁶ BGE 123 I 112, E. 4 c).

⁵⁷ Knellwolf, S. 56.

⁵⁸ Breitschmid, Persönlichkeitsrechtliche Belange, S. 41.

⁵⁹ Weimar, BK, Art. 482 ZGB N 12.

⁶⁰ Staehelin, BSK, Art. 482 ZGB N 16.

können auch ganz bestimmte Eingriffe, wie das Lesen eines Tagebuches, verboten werden oder auch die Vernichtung eines Fotoalbums angeordnet werden.⁶¹ **Es wäre also gut vorstellbar, dass der Erblasser auch über die nicht vermögensrechtlichen Aspekte seines digitalen Erbes in einem Testament Anordnungen erlässt.** Ein Blog wäre vergleichbar mit der oben erwähnten Anordnung bezüglich der Gedichte. Bezüglich E-Mails (Korrespondenz) und dem (elektronischen) Fotoalbum könnte ebenfalls eine Anordnung getroffen werden. Die Ausführung oder Überwachung dieser Wünsche kann wiederum einem Willensvollstrecker übertragen werden.⁶² Ein Willensvollstrecker kann und soll auch persönlichkeitsbezogenen Anordnungen, die nicht den Nachlass betreffen, zur Durchsetzung verhelfen.⁶³

6.2.1.3 Anordnungen ausserhalb eines Testaments

Anordnungen in Bezug auf die Bestattung etc. werden auch ausserhalb der Formvorschriften des Testaments als gültig angesehen. Es reicht, dass der Verstorbene seine Wünsche eindeutig geäussert hat.⁶⁴ Dies gilt aus Sicht der Autoren auch für andere die Persönlichkeits- und nicht Vermögensrechte betreffenden Anordnungen. Das heisst, eine Anordnung, wie mit einem Datenbestand oder Internet-Profil zu verfahren ist, die den Angehörigen via einen digitalen Vererbungsdienst mitgeteilt wird, ist grundsätzlich gültig. Verschiedene Organisationen (z.B. der Konsumentenschutz) stellen umfassende Formulare zur Verfügung, in welchen im Hinblick auf den Tod allerlei Anordnungen getroffen werden können. Diese gehen vom Wunsch in welchen Zeitungen eine Todesanzeige gedruckt werden soll, bis zur gewünschten Kleidung im Sarg.

Problematisch sind diese formlosen Anordnungen jedoch dann, wenn sich die Angehörigen aus irgendwelchen Gründen nicht an die Wünsche des Verstorbenen halten wollen.⁶⁵ Sind z.B. die Angehörigen dagegen, ein Facebook-Profil – wie vom Verstorbenen gewünscht – in den Gedenkstatus zu versetzen, fehlt es anderen aussenstehenden Personen an eigenen schützenswerten Interessen, welche sie berechtigen würden, die Einhaltung der Anordnungen zu erzwingen.⁶⁶ Zudem ist auch der Staat nicht verpflichtet, dem Willen des Verstorbenen zur Verwirklichung und Durchsetzung zu verhelfen.⁶⁷ Der Verstorbene ist also darauf angewiesen, dass die Angehörigen seine Wünsche und Vorstellungen freiwillig durchsetzen. Dies wurde auch vom Bestattungs- und Friedhofsamt der Stadt Zürich bestätigt: Wollen sich alle Angehörigen einhellig und nach eingehender Beratung nicht an die Wünsche des Verstorbenen halten, so werden die Wünsche der Angehörigen und nicht diejenigen des Verstorbenen ausgeführt.

⁶¹ Aebi-Müller, N 330. Aebi-Müller und Knellwolf sehen dies als Möglichkeit für den Erblasser seine «postmortale Persönlichkeit» zu pflegen und zu gestalten.

⁶² Siehe auch dazu oben.

⁶³ Christ/Eichner, Art. 518 ZGB N 5; Künzle, Chk, Art. 517–518 ZGB N 50.

⁶⁴ Knellwolf, S. 88 f.

⁶⁵ Knellwolf, S. 89 f.

⁶⁶ vgl. Knellwolf, S. 90; Auch das Bestattungsamt Zürich bestätigt, dass im Konfliktfall die Weisungen der Angehörigen denen des Verstorbenen vorgehen.

⁶⁷ Knellwolf, S. 90.

Der Verstorbene ist auf den «Goodwill» seiner Angehörigen angewiesen.

6.2.2 Nach dem Tod

Während zu Lebzeiten jede Persönlichkeitsverletzung widerrechtlich ist, es sei denn sie sei gerechtfertigt durch beispielsweise eine Einwilligung, verliert die Persönlichkeit mit dem Tod einer Person ihren Schutz beziehungsweise «stirbt» ebenfalls. Eine Persönlichkeit geht mit ihrem Inhaber unter (Art. 31 Abs. 1 ZGB) und kann daher nicht mehr verletzt werden. Dies wiederum bedeutet, dass eine Einwilligung des Abgebildeten zur Veröffentlichung seines Bildes nicht mehr nötig ist.⁶⁸ Das Datenschutzgesetz (DSG)⁶⁹, welches einen bestimmten Aspekt der Persönlichkeit schützt, findet ebenfalls keine unmittelbare Anwendung auf die Daten von Verstorbenen.

«Die Persönlichkeit beginnt mit dem Leben nach der vollendeten Geburt und endet mit dem Tode.»

Art. 31 Abs. 1 ZGB

Ist somit die Persönlichkeit eines Verstorbenen nach dem Tod schutzlos Eingriffen von Dritten ausgesetzt? Die Antwort ist ein «nicht ganz, aber fast», da die in ihrem Andenken geschützten Angehörigen (begrenzte) Handlungsmöglichkeiten haben.

6.2.2.1 Andenkenschutz

Nach dem Untergang der Persönlichkeit kann niemand im Namen des Verstorbenen eine Verletzung der Persönlichkeit des Verstorbenen unterbinden, selbst dann nicht, wenn jemand (z.B. ein Anwalt) vor dem Tod dazu bevollmächtigt wurde.⁷⁰ Denn mit dem Tod verliert eine Person die Parteifähigkeit und auch ein Vertreter kann nicht in ihrem Namen einen Prozess anheben.⁷¹

Die Angehörigen der verstorbenen Person können eine Verletzung der Persönlichkeit derselben nur unterbinden, sofern sie selbst ebenfalls in ihrer Persönlichkeit verletzt und insbesondere ihr Pietätsgefühl verletzt wurde.⁷² Man

spricht in diesem Zusammenhang von Andenkenschutz. So war es z.B. der Witwe des Malers Ferdinand Hodler möglich, in Folge einer Veröffentlichung eines Bildes, welches ihren Mann auf dem Sterbebett zeigt, Genugtuung zu erhalten. Es gelang ihr darzulegen, dass diese Veröffentlichung ihre Pietätsgefühle verletzte.⁷³

Hingegen gelang es Anwalt Ludwig Minelli von der Sterbehilfeorganisation Dignitas nicht, gestützt auf eine vor dem Tod ausgestellte Vollmacht, zwei Verstorbene gegenüber Behörden und vor Gericht zu vertreten. Er konnte nicht in ihrem Namen gegen eine Obduktionsverfügung Beschwerde führen.⁷⁴ Da es sich um eine Obduktion handelte, die zur Aufklärung eines aussergewöhnlichen Todesfalls durch die Staatsanwaltschaft angeordnet wurde, hätten in diesem Fall auch die Angehörigen gestützt auf die Verletzung ihrer Persönlichkeit kein Beschwerderecht gehabt.⁷⁵

Es besteht somit ein indirekter Schutz der Persönlichkeit des Verstorbenen, wobei es zu beachten gilt, dass der Schutzbereich der Persönlichkeit des Verstorbenen nicht mit demjenigen der (andenkengeschützten) Angehörigen zusammenfällt.⁷⁶ Was eine Verletzung der Persönlichkeit des Verstorbenen zu Lebzeiten darstellt, ist nicht immer geeignet, auch die Pietätsgefühle der Angehörigen zu verletzen. Wer alles in den Kreis der Angehörigen gehört und somit klagelegitimiert ist, lässt sich nicht in abstrakter Weise feststellen. Ein geschütztes Andenken setzt kein rechtliches Verhältnis (z.B. Ehe, Verwandtschaft) voraus, sondern beruht auf einer lebendigen und intensiven Kontaktpflege zu Lebzeiten.⁷⁷ Die Legitimation muss dementsprechend im Einzelfall abgewogen werden.⁷⁸ Nicht auszuschliessen

⁶⁸ Haas, N 435.

⁶⁹ Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1; siehe dazu Kapitel 6.3

⁷⁰ Knellwolf, S. 4; Aebi-Müller, N 327; BGE 129 I 302, E. 1.2.1; BGE 127 I 115, E. 6 a).

⁷¹ Beretta, BSK Art. 31 ZGB N 39; BGE 129 I 302 ff.

⁷² BGE 127 I 115, E. 6a); Breitschmid/Kamp, S. 22.

⁷³ BGE 70 II 127, E. 2.

⁷⁴ BGE 129 I 302.

⁷⁵ Rémy, S. 40.

⁷⁶ Breitschmid/Kamp, S. 22.

⁷⁷ Knellwolf, S. 113

⁷⁸ Breitschmid/Kamp, S. 24.

ist, dass mehrere Hinterbliebene – die nicht zwingend Erben sein müssen – ein schützenswertes Andenken geltend machen können. Eine Rangfolge zwischen den Angehörigen lässt sich jedoch nicht rechtfertigen.⁷⁹ BREITSCHMID/KAMP machen darauf aufmerksam, dass es zu einer Interessensabwägung kommen müsste, wenn sich ein Angehöriger (im Sinne des Andenkensschutzes) gegen Dispositionen der Erben wehren würde, da er seine Persönlichkeit dadurch verletzt sieht. In solchen Situationen wäre der mutmassliche Wille des Verstorbenen zu berücksichtigen.⁸⁰ Hier könnte eine auch nicht formgültige Verfügung zum Beispiel in der Form eines Accounts bei einem digitalen Vererbungsdienst eine Rolle spielen.

Eine Grundlage für andenkensrechtliche Ansprüche stellen alle Handlungen dar, welche den erforderlichen Respekt gegenüber der Würde des Toten vermissen lassen.⁸¹ Die Pietätlosigkeit muss jedoch eine gewisse Intensität erreichen, um als Persönlichkeitsverletzung gewertet zu werden. Es ist nicht jedes alltäglich vorkommende, allgemein zu duldende Verhalten eine Verletzung von Persönlichkeitsrechten. So sind z.B. wahre aber kritische Zeitungsberichte über den Verstorbenen hinzunehmen.⁸² So scheint es zumindest fraglich, ob die Angehörigen eine Persönlichkeitsverletzung erleiden, falls eine Online-Plattform das Profil des Verstorbenen nicht löscht, war doch der Verstorbene zu Lebzeiten wohl mit seinem Profil einverstanden. Hier zeigt sich die Diskrepanz, die zwischen dem Schutzbereich der Persönlichkeit des Verstorbenen und demjenigen der andenkensgeschützten Angehörigen liegt: Hätte der Verstorbene zu Lebzeiten die Möglichkeit gehabt, unter Berufung auf die eigene Persönlichkeit, das Profil zu löschen, wird dies den Hinterbliebenen wohl mangels Persönlichkeitsverletzung nicht möglich sein.

Den Angehörigen stehen grundsätzlich alle in Art. 28 ff. ZGB vorgesehenen Rechtsmittel zur Verfügung.⁸³ Der Anspruch auf Genugtuung – wie er bei der Witwe Hodler bejaht wurde – wird nur bei einer hohen Intensität des Eingriffs zugesprochen.⁸⁴

6.2.2.2 Kritik und postmortaler Persönlichkeitschutz

Die Konzeption des Andenkensschutzes wird (immer häufiger) kritisiert. So sei dieser indirekte Schutz durch den Andenkensschutz ungenügend und versage sogar gänzlich, falls die Angehörigen nichts unternehmen oder falls es gar die Angehörigen sind, die in die Persönlichkeit des Verstorbenen eingreifen.⁸⁵ Ebenfalls versage das System, falls jemand keine Angehörige hinterlasse.⁸⁶ Durch den ungleichen Schutzbereich der Persönlichkeit des Verstorbenen und des Andenkensschutzes der Angehörigen, fallen zudem gewisse Ansprüche mit dem Tod endgültig weg.⁸⁷ Im Bereich des digitalen Sterbens zeigt sich diese Diskrepanz an folgenden Beispielen:

Sollte ein Verstorbener eine Auflage in sein Testament aufgenommen haben, welche der Plattformbetreiber nicht ausführen will (z.B. fordert der Verstorbene sein Profil sei endgültig zu löschen, die Plattform sieht jedoch nur eine Stilllegung vor) so scheinen den Angehörigen die Hände gebunden zu sein. Der Verstorbene hätte jedoch seinerseits zu Lebzeiten die Möglichkeit gehabt, die Löschung des Profils zu verlangen – ein höchstpersönliches Recht (sehr wahrscheinlich gestützt auf das DSGVO oder Persönlichkeitsrecht im Allgemeinen). Den Angehörigen wird es jedoch nicht möglich sein, im Namen des Verstorbenen einen Prozess anzustreben. Ob diese Weigerung die Intensität erreicht, um die Persönlichkeit der Angehörigen selbst zu verletzen, scheint fragwürdig.

⁷⁹ Knellwolf, S. 124 ff.

⁸⁰ Breitschmid/Kamp, S. 24.

⁸¹ Knellwolf, S. 128.

⁸² Knellwolf, S. 129.

⁸³ Knellwolf, S. 139; Breitschmid/Kamp, S. 24.

⁸⁴ Breitschmid/Kamp, S. 24.

⁸⁵ Grieder/Ott, S. 628; BGE 129 I 302, E. 1.2.2.

⁸⁶ Grieder/Ott, S. 628; BGE 129 I 302, E. 1.2.2.; Knellwolf, S. 5.

⁸⁷ Breitschmid/Kamp, S. 22; Grieder/Ott, S. 628.

Die Kritik an der Konzeption des Andenkensschutzes erfolgt unter anderem mit dem Verweis auf die Deutsche Rechtsprechung, welche einen postmortalen Persönlichkeitsschutz kennt.⁸⁸ Demzufolge erlischt die Persönlichkeit nicht mit dem Tod, falls noch schutzwürdige Objekte bestehen.⁸⁹

Das Bundesgericht setzte sich soweit ersichtlich zuletzt in BGE 129 I 302 mit der Theorie des postmortalen Persönlichkeitsschutzes auseinander und lehnte diese ab. Es begründet diese Haltung einerseits mit dem klaren Wortlaut von Art. 31 Abs. 1 ZGB, andererseits mit dem Problem bei der Bestimmung des Rechtsträgers und einer Befristung der Ansprüche.⁹⁰ Jedoch steht die Ablehnung des postmortalen Persönlichkeitsschutzes der Verbindlichkeit von Anordnungen über die Bestattung nicht entgegen.⁹¹

Wird der Theorie eines postmortalen Persönlichkeitsschutzes gefolgt, stehen lediglich Unterlassungs- und Beseitigungsansprüche und das Gegendarstellungsrecht zur Verfügung. Eine Entschädigung können die Angehörigen nicht geltend machen.⁹²

6.2.3 Fazit – Persönlichkeitsrecht

Viele Daten, die im Internet gespeichert sind, sind nicht vererblich, da sie eng mit der Persönlichkeit des Verstorbenen zusammenhängen und keine Vermögensrechte darstellen. Die Persönlichkeit geht jedoch mit dem Tod unter und ist danach nahezu schutzlos. Die Angehörigen können sich nicht im Namen des Verstorbenen gegen allfällige Persönlichkeitsverletzungen wehren. Ihnen steht im Sinne des Andenkensschutzes die Möglichkeit auf Beseitigung, Feststellung und Unterlassung zu klagen (gem. Art. 28a ff. ZGB) lediglich offen, falls eine Handlung auch ihre eigene Persönlichkeit verletzt. Die Durchsetzung von Ansprüchen aus Persönlichkeitsverletzung im Internet stellt sich zudem in vielen Fällen schwierig dar (siehe Kapitel 6.4.).

⁸⁸ Grieder/Ott, S. 628.

⁸⁹ Knellwolf, S. 6; Grieder/Ott, S. 628 f.

⁹⁰ BGE 129 I 302, E. 1.2.3; Aebi-Müller, N 327.

⁹¹ Siehe oben BGE 129 I 173.

⁹² Knellwolf, S. 140; Aebi-Müller, N 335.

6.3 DATENSCHUTZ UND DIGITALES STERBEN

Bei der Datenbearbeitung hat der Schutz der Persönlichkeit und der Grundrechte einen hohen Stellenwert. So gewährt Art. 13 Abs. 2 BV ausdrücklich einen Anspruch auf Schutz vor Missbrauch persönlicher Daten und einen Anspruch auf informationelle Selbstbestimmung.⁹³ Dabei ist der Wortlaut dieser Verfassungsbestimmung allerdings zu eng gefasst, denn es wird nicht nur vor Missbrauch geschützt, sondern generell ein Anspruch verliehen, darüber informiert zu sein, wer wann und mit welcher Legitimation über die eigene Person Daten bearbeitet.⁹⁴ Einer Person wird durch dieses Recht der Anspruch gewährt, selbst zu bestimmen, wem und weshalb sie persönliche Lebenssachverhalte, Gedanken, Empfindungen oder Emotionen offenbart. Durch das Bundesgesetz über den Datenschutz (DSG) erfahren die Persönlichkeit und die Grundrechte im Bereich der Datenbearbeitung also eine Konkretisierung und Ergänzung. Es darf dabei nicht vergessen werden, dass der Datenschutz einen Teilaspekt der Persönlichkeit schützt. Diese geht – wie oben erläutert – gem. Art. 31 Abs. 1 ZGB mit dem Tod unter und ist nach dem Tod schutzlos, bis zur Grenze des Andenkensschutzes der Angehörigen.

Die vorliegende Problematik berührt den Datenschutz an verschiedenen Punkten:

Zum einen interessiert, wie die Internet-Plattformen zu Lebzeiten mit den Daten ihrer Mitglieder umgehen und welcher Umgang mit den Daten von Verstorbenen zu pflegen ist. Eine genügende Kontrolle über die Daten scheint eine wichtige Voraussetzung, damit Angehörigen überhaupt zweckdienliche Hinweise zum Umgang mit den Daten nach dem Tod gegeben werden können. Zum anderen haben sich auch Lösungsanbieter für digitale Nachlassplanung an die datenschutzrechtlichen Grundsätze zu halten.

⁹³ Hilty et Al., S. 42; ausführlich dazu: Müller/Schefer, S. 164 ff.

⁹⁴ Hilty et Al., S. 42; Rosenthal, Art. 1 DSGVO N 4.

Im Folgenden wird dargestellt, bei welchen Informationen es sich um «Daten» handelt, wie diese durch das DSG geschützt werden und ob das DSG auch auf Daten von Verstorbenen Anwendung findet, was am Fallbeispiel «E-Mail-Account» veranschaulicht wird. In einem zweiten Teil widmet sich das Kapitel der Diskussion um ein «Recht auf Vergessen» im Internet und beleuchtet kurz die (mögliche) Rolle des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Die Problematik der Durchsetzung der Ansprüche aus dem Datenschutzgesetz werden in Kapitel 6.4 behandelt.

6.3.1 Daten auf Internet-Plattformen

In sozialen Netzwerken und anderen Internet Plattformen, sind diverse Informationen gespeichert, die als «Daten» zu qualifizieren sind und daher auch den Schutz des Datenschutzgesetzes⁹⁵ geniessen. Gemäss Art. 3 lit. a DSG sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen, (Personen-) Daten. Dies sind objektive Informationen (wie z.B. der Beruf einer Person, der Geldbetrag auf ihrem Konto) und subjektive Informationen (z.B. die Kreditwürdigkeit)⁹⁶ ungeachtet des Inhalts der Information: Es werden Informationen über das Privatleben (Freizeitbeschäftigungen, Mitgliedschaft in einem Verein, Einkäufe, ausgeliehene Videos etc.) und Angaben, die sich auf das Wirken einer Person in ihrem Amt oder Beruf beziehen geschützt (z.B. die von einem Arzt verschriebenen Rezepte).⁹⁷ Ebenfalls unerheblich ist das Format oder der Träger der Informationen. In einem wie folgt verfassten Facebook-Statuskommentar sind also zweifelsohne Personendaten enthalten: «Zurück vom Fitness-Studio und den Fussballmatch am geniessen.»

Das DSG bestimmt in Art. 3 lit. c zusätzlich, welche Daten in die Kategorie der «besonders schützenswerten Personendaten» fallen. Dazu gehören (u.a.) religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Informationen über die Gesundheit, Intimsphäre oder die Rassenzugehörigkeit. Die Information «Peter Meier nimmt Teil an der 1. Mai Demonstration in Zürich», wie sie auf Facebook-Profilen zu lesen ist, beinhaltet also besonders schützenswerte Personendaten. Ein Persönlichkeitsprofil liegt gem. Art. 3 lit. d DSG vor, wenn die Zusammenstellung von Daten eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben. Für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen gelten erhöhte Anforderungen.⁹⁸

⁹⁵ Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG), SR 235.1.

⁹⁶ Rosenthal, Art. 3 Bst. a DSG N 9.

⁹⁷ Rosenthal, Art. 3 Bst. a DSG N 10.

⁹⁸ Hilty et Al., S. 48.

Internetnutzer stellen in sozialen Netzwerken diverse Daten – insbesondere auch besonders schützenswerte – zur Verfügung.

6.3.2 Wichtigste Grundsätze der Datenbearbeitung durch Private

Eine Datenbearbeitung durch Private ist zulässig, soweit sie im Rahmen der Datenbearbeitungsgrundsätze erfolgt bzw. ein Rechtfertigungsgrund geltend gemacht⁹⁹ werden kann. Folglich liegt eine widerrechtliche Datenbearbeitung und damit eine Persönlichkeitsverletzung der betroffenen Person vor, falls im Allgemeinen ohne Rechtfertigungsgrund Daten bearbeitet werden, oder im Speziellen ohne Rechtfertigungsgrund entgegen den Grundsätzen des DSGVO Daten bearbeitet werden.¹⁰⁰

Zu den wichtigsten Grundsätzen der Datenbearbeitung durch private gehören:

- Die Bearbeitung hat nach Treu und Glauben zu erfolgen, und muss verhältnismässig sein (Art. 4 Abs. 2 DSGVO)
- Der Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSGVO), wonach Daten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde, oder aus den Umständen ersichtlich ist.
- Die Beschaffung der Daten sowie der Zweck ihrer Bearbeitung muss gem. Art. 4 Abs. 3 DSGVO für die betroffenen Personen erkennbar sein (Transparenzprinzip)

Die Einhaltung dieser elementaren Grundsätze ist auf Internet-Plattformen nicht immer gewährleistet. Internet-Plattformen auf allfällige Verstösse zu untersuchen, ist nicht Gegenstand des vorliegenden Forschungsprojekts. Exemplarisch sei an dieser Stelle auf den Audit-Bericht der irischen Datenschutzbehörde verwiesen, welcher die Klagen des Vereins «Europe versus Facebook» behandelt. Die Behörde veröffentlichte im Dezember 2011 allein zu (behaupteten) Datenschutzverstössen von Facebook einen Bericht von 149 Seiten Umfang und schliesslich im September 2012 einen Nachfolgebericht zur Umsetzung der Empfehlungen.¹⁰¹

Werden Daten in persönlichkeitsverletzender Weise bearbeitet,¹⁰² so stehen der betroffenen Person gem. Art. 15 DSGVO die Klagen aus den Artikeln 28, 28a sowie 28l ZGB zur Verfügung. Der Verletzte hat somit ein Unterlassungs-, Beseitigungs- und Feststellungsanspruch und kann die Mitteilung und Veröffentlichung des Urteils verlangen. Gegebenenfalls hat die Person einen Schadenersatz-, Genugtuungs- und Gewinnherausgabeanspruch und ein Gegendarstellungsrecht. Ausdrücklich in Art. 15 Abs. 1 genannt sind die Ansprüche auf Berichtigung, Vernichtung und eine Sperre der Bekanntgabe der Daten.¹⁰³

Art. 12 Abs. 3 DSGVO sieht zudem vor, dass eine Datenbearbeitung ebenfalls nicht widerrechtlich ist, falls Daten von der betroffenen Person allgemein zugänglich gemacht und die Datenbearbeitung nicht ausdrücklich untersagt wurde. Dazu gilt es festzuhalten, dass die allgemeine Zugänglichkeit mit Wissen und Willen zu erfolgen hat.¹⁰⁴ Das heisst, mangelhafte AGB oder Standardeinstellung, welche die Öffentlichkeit der Information vorsehen, führen dazu, dass dieses Erfordernis nicht erfüllt ist und deshalb nicht davon ausgegangen werden kann, dass jemand der z.B. sein Social-Media-Profil als «öffentlich» eingestellt hat, tatsächlich in eine Datenbearbeitung eingewilligt hat. Schliesslich ist auch fraglich ob die Publikation auf einer passwortgeschützten Plattform bereits als allgemein zugänglich betrachtet werden kann. Klar ist, dass Art. 12 Abs. 3 DSGVO nicht zur Anwendung kommt, falls die betroffene Person eine Veröffentlichung z.B. eines Videos auf dem Internet lediglich duldet – dies genügt nicht, um die Persönlichkeitsverletzung zu rechtfertigen.¹⁰⁵

⁹⁹ Hilty et Al., S. 50.

¹⁰⁰ Vgl. Rosenthal, Art. 12 DSGVO N 16 ff., es ist davon auszugehen, dass Verstösse gegen die Bearbeitungsgrundsätze insbes. durch Einwilligung gerechtfertigt werden können.

¹⁰¹ Data Protection Commissioner Ireland <http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf>, besucht am 16.10.2012.

¹⁰² Unter Bearbeiten versteht man gem. Art. 3 lit. e DSGVO jeden «Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.»

¹⁰³ Rampini, Art. 15 DSGVO N 1.

¹⁰⁴ Rosenthal, Art. 12 DSGVO N 54.

¹⁰⁵ Rosenthal, Art. 12 DSGVO N 56.

6.3.3 Der Umgang mit Daten von Verstorbenen Personen

Das DSG schützt zwar mit dem Recht auf informationelle Selbstbestimmung einen Teilaspekt der Persönlichkeit – jedoch stellt es insbesondere Vorschriften über die Bearbeitung von Personendaten auf. Es gilt daher zu klären, ob unter Personendaten im Sinne von Art. 3 Abs. 1 lit. a DSG auch Daten zu verstehen sind, die sich auf eine tote Person beziehen. Von einer Datenbearbeitung betroffene Personen können natürliche oder juristische Personen sein (Art. 3 Abs. 1 lit. b DSG). Während der Begriff der juristischen Person weit zu verstehen ist,¹⁰⁶ wirft der Begriff der natürlichen Person die Frage auf, ob dabei ebenfalls die Daten von Verstorbenen oder ungeborenen Kindern erfasst werden.¹⁰⁷ Da die Persönlichkeit mit dem Tod endet, und das ungeborene Kind diese nur unter dem Vorbehalt erlangt, lebendig geboren zu werden, findet das DSG grundsätzlich keine Anwendung auf die Daten von Verstorbenen oder Todgeborenen.¹⁰⁸ Diese Feststellung scheint jedoch zu kurz zu greifen, wird doch in der Verordnung zum Datenschutzgesetz (VD SG)¹⁰⁹ in Art. 1 Abs. 7 festgehalten, dass Auskunft über Daten von Verstorbenen nur erteilt wird, falls keine überwiegenden Interessen der Angehörigen oder von Dritten entgegenstehen. Diese Norm schützt zumindest teilweise die Daten einer verstorbenen Person. Zwar werden ihre Interessen nicht mehr direkt in Betracht gezogen, jedoch wird die Wahrung dieser Interessen den Angehörigen übertragen. Denn es scheint, Art. 1 Abs. 7 VD SG gehe weiter als die herkömmlich Andenkensschutztheorie: Angehörige, die sich gegen die Auskunft stellen, müssen nur ein überwiegendes Interesse nachweisen und nicht eine Verletzung der eigenen Persönlichkeitsrechte. Auf der anderen Seite stellt diese Norm auch klar, dass nahe Verwandte und Ehepartner der verstorbenen Person grundsätzlich ein Interesse an der Auskunft über Daten der verstorbenen Person haben. Zu beachten bleibt jedoch, dass es spezialgesetzliche Regelungen gibt, die eine Auskunft an Angehörige und Dritte ausschliessen. So bleibt das Arztgeheimnis (Art. 321 StGB¹¹⁰) nach dem Tod bestehen und ein Patientendossier kann nicht an die Angehörigen weitergegeben werden.¹¹¹ Dasselbe gilt für das Bankgeheimnis (Art. 47 BankG¹¹²).¹¹³

Die kantonalen Datenschutzgesetze, die auf die Datenbearbeitung kantonalen Behörden Anwendung finden, sehen teilweise weiterreichende Regelungen zum Umgang mit Daten Verstorbener vor, so z.B. das solothurnische Informations- und Datenschutzgesetz (InfoDG).¹¹⁴ Dieses Gesetz sieht in § 21 Abs. 5 vor, dass besonders schützenswerte Daten verstorbener Personen erst nach einer Schutzfrist herausgegeben werden dürfen, es sei denn, es bestehe eine gesetzliche Grundlage, die etwas anderes vorsieht. Die Schutzfrist beträgt 30 Jahre seit dem Tod oder, wenn der Tod ungewiss ist, 110 Jahre seit der Geburt. Zudem ist die Herausgabe in den 80 Jahren seit der letzten Aufzeichnung nicht erlaubt, falls weder Todes- noch Geburtsdatum festzustellen sind. Ausnahmen können von der Behörde bewilligt werden, wenn schützenswerte private oder wichtige öffentliche Interessen vorliegen oder die Daten für die wissenschaftliche Forschung erforderlich sind. Ähnliche Regelungen kennen die Datenschutzgesetzgebungen des Kantons Aargau¹¹⁵ und des Kantons Wallis¹¹⁶, wobei diese beiden Kantone eine Schutzfrist von lediglich 10 Jahren vorsehen und nicht explizit darauf eingehen, dass eine Herausgabe auch vor Ablauf der Schutzfrist unter Angabe von privaten oder öffentlichen Interessen möglich ist. Der Kanton Genf sieht vor, dass die Angehörigen

¹⁰⁶ Rosenthal, Art. 3 DSG N 7; Belsler/Noureddine, N 42.

¹⁰⁷ Rosenthal, Art. 3 DSG N 7.

¹⁰⁸ Rosenthal/Jöhri, Art 2 DSG N 5; Belsler, BSK, Art. 3 DSG N 9.

¹⁰⁹ Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VD SG), SR 235.11.

¹¹⁰ Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (StGB), SR 311.0.

¹¹¹ Breitschmid/Kamp, S. 22; Hofer, S. 34; Gramigna/Maurer-Lambrou, BSK, Art. 9 DSG N 19.

¹¹² Bundesgesetz vom 8. November 1934 über die Banken und Sparkassen (Bankengesetz, BankG), SR 952.0.

¹¹³ Gramigna/Maurer-Lambrou, BSK, Art. 9 DSG N 19.

¹¹⁴ Informations- und Datenschutzgesetz des Kantons Solothurn vom 21. Februar 2011, BGS 114.1.

¹¹⁵ Art. 46 Abs. 2 Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) des Kantons Aargau vom 24. Oktober 2006, SAR 150.700.

¹¹⁶ Art. 43 Gesetz über die Information der Öffentlichkeit, den Datenschutz und die Archivierung (GIDA) des Kantons Wallis vom 9. Oktober 2008, 170.2.

einer Verstorbenen Person nur Zugang zu den Daten erhalten, falls sie ein schutzwürdiges Interesse geltend machen können, und sich die Interessen von Dritten nicht gegen eine Bekanntgabe stellen. Zudem sieht die Genfer Gesetzgebung auch vor, dass die Rechte auf Beseitigung, Feststellung und Unterlassung zu klagen, in Bezug auf die Datenbearbeitung, die einen Verstorbenen betreffen, seinen Angehörigen zustehen. Letzteres auch, falls sie ein schutzwürdiges Interesse geltend machen können, und sich keine anderen privaten oder öffentlichen Interessen dagegenstellen.¹¹⁷

Dieser Ansatz zum Umgang mit besonders schützenswerten Personendaten Verstorbener ist auf die vorliegende Thematik nicht direkt übertragbar. Zum einen handelt es sich um besonders schützenswerte Personendaten und zum anderen um Daten, die von Behörden bearbeitet wurden. Die Position des Verstorbenen scheint jedoch in angemessener Weise dadurch gestärkt zu werden, dass zur Erteilung der Auskunft schützenswerte private Interessen vorliegen müssen, während im Kontext von Art. 1 Abs. 7 VDSG die Auskunft grundsätzlich möglich ist, es sei denn es liegen entgegengesetzte Interessen vor. Die Schutzfristen von 30 Jahren, wie sie der Kanton Solothurn vorsieht, scheint in Bezug auf besonders schützenswerte Daten angemessen, es wäre jedoch zu prüfen, ob für nicht besonders schützenswerte Daten eine kürzere Frist gewählt werden sollte. Besonders interessant scheint aber die Genfer Regelung. Die Übertragung der Klagemöglichkeiten an die Angehörigen geht eindeutig über die Andenkenschutz-Theorie hinaus und erlaubt es den Angehörigen, den Verstorbenen vor gesetzwidrigen Datenbearbeitungen zu schützen. Dies scheint gerechtfertigt, denn wie oben dargestellt, schützt zwar der Datenschutz einen Teilaspekt der Persönlichkeit, jedoch stellt er grundsätzlich Regelungen zur Bearbeitung von (Personen-)Daten auf. Dass dabei jemand legitimiert wird, um gegen gesetzeswidrige Datenbearbeitungen von Daten, die Verstorbene betreffen vorzugehen, drängt sich auf. Eine vorgängige Interessenabwägung kann dabei gerechtfertigt sein, jedoch könnte gar der Verzicht auf diese Voraussetzung diskutiert werden.

6.3.4 Das Auskunftsgesuch der Angehörigen am Beispiel E-Mail Account

Wie die Analyse der Praktiken der Plattformanbieter gezeigt hat (Kapitel 5), wird mit der Auskunft über die Zugangsdaten und/oder Inhalte, die sich hinter einem digitalen Account befinden ganz unterschiedlich umgegangen. Die Plattformanbieter befinden sich in einem Spannungsfeld: Zum einen haben sie dem Nutzer bei Abschluss des Vertrags den Schutz seiner Persönlichkeit und Daten versprochen, zum anderen haben die Angehörigen tatsächliche Interessen an der Auskunft. In der Presse diskutiert wurde insbesondere der Fall eines US-Soldaten, der im Krieg im Irak gefallen war. Während seiner Zeit im Irak verschickte er viele E-Mails – er nutzte das Kommunikationsmittel quasi als Tagebuch. Die Eltern ersuchten daher beim E-Mail-Anbieter des Verstorbenen, Yahoo!, um Einsicht in sein E-Mail-Konto mit der Absicht, die E-Mails evtl. zu veröffentlichen. Yahoo! weigerte sich jedoch Zugangsdaten oder Inhalt bekannt zu geben. Ein US-Gericht musste schliesslich entscheiden und tat dies zu Gunsten der Angehörigen.¹¹⁸

Die Praktiken der Plattformanbieter in Bezug auf die Behandlung von Auskunftsgesuchen von Angehörigen können in folgende Kategorien aufgeteilt werden:

1. Zugriff wird bei Vorlage der Sterbeurkunde und/oder des Erbscheins gewährt

Dabei kann zusätzlich unterschieden werden, ob der Zugriff in Form von Sicherungskopien des E-Mail-Verkehrs und evtl. der Kontaktdaten gewährt wird, oder ob der generell das Konto übertragen wird und dieses unter Umständen gar weiterverwendet werden darf.

¹¹⁷ Art. 48 Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) du canton de Genève du 5 octobre 2001, A 2 08.

¹¹⁸ Siehe <http://news.bbc.co.uk/2/hi/uk_news/magazine/4164669.stm>, besucht am 21. Juni 2012; Darrow/Ferrera, Who Owns a Decedent's E-Mails: Inherent Probate Assets or Property of the Network?, New York University Journal of Legislation and Public Policy, Vol. 10 S. 281ff, New York 2007.

2. Zugriff wird nur in begründeten Ausnahmen unter Angabe von triftigen Gründen und nach Vorlage der Sterbeurkunde und/oder des Erbscheins gewährt

3. Der Zugriff wird verweigert

4. Das E-Mail-Konto wird gelöscht, entweder in Folge Inaktivität oder auf Wunsch der Angehörigen unter Vorlage der Sterbeurkunde und/oder des Erbscheins

Falls die Angehörigen den Tod nicht melden und es sich um einen Anbieter handelt, der keine automatische Löschung vornimmt, bleibt ein E-Mail-Account in diesem Fall bestehen.

Rechtlich betrachtet interessant und zugleich problematisch scheinen die «Extrem-Lösungen» (3. kein Zugriff gegenüber 1. Zugriff bis hin zur Übernahme des Kontos).

Eine Verweigerung des Zugriffs kann sich entweder auf das Argument des Persönlichkeits- und Datenschutzes (a) stützen, wird aber teilweise auch mit Geheimhaltungspflichten (b) begründet.

a) Rufen wir uns erneut in Erinnerung, dass in der Schweiz die Persönlichkeit mit dem Tod untergeht und auch der Datenschutz seine grundsätzliche Wirkung mit dem Tod einer Person verliert, scheint es fragwürdig, ob den Angehörigen der Zugriff gestützt auf das Argument des Daten- und Persönlichkeitsschutzes verweigert werden kann. Art. 1 Abs. 7 VDSG spricht ebenfalls eher gegen diese Argumentation. Diese Norm stellt klar, dass nahe Verwandte und Ehegatten grundsätzlich ein Interesse an der Auskunft über Daten des Verstorbenen haben – entgegenstehende Interessen, die eine Ablehnung des Auskunftsgesuches rechtfertigen, sind sodann nicht die Interessen des Verstorbenen, sondern nur diejenigen von Dritten. Das Argument müsste somit lauten, dass die Auskunft verweigert wird, weil die Persönlichkeit der Korrespondenz-Partner geschützt werden soll. Das Interesse des Dritten muss je-

doch überwiegen. Aber: geht man als Korrespondenzpartner nicht – wie früher in der nicht digitalen Welt – das Risiko ein, dass der Empfänger die E-Mails (oder Briefe) für seine Nachwelt zugänglich aufbewahrt oder sogar veröffentlicht?

b) Andere Anbieter verweigern den Zugriff, indem sie sich auf übergeordnete Geheimhaltungspflichten berufen. In der Schweiz dient z.B. der Swisscom¹¹⁹ das Fernmeldegeheimnis zu diesem Zweck. Es ist zwar richtig, dass auch die elektronische Post vom Fernmeldegeheimnis erfasst wird und das Verletzen dieses Geheimnisses strafrechtlich verfolgt wird (Art. 321^{ter} StGB).¹²⁰ Jedoch wird vom Post- und Fernmeldegeheimnis lediglich der Kommunikationsvorgang bzw. der Kommunikationsfluss erfasst. Für das Postgeheimnis heisst das, dass Briefe oder Pakete, die noch beim Absender oder schon beim Adressaten sind, noch nicht bzw. nicht mehr dem Postgeheimnis unterstehen.¹²¹ Analog sind E-Mails die noch oder bereits in der Mailbox gespeichert sind nicht vom Fernmeldegeheimnis geschützt, da der Kommunikationsfluss fehlt. Umstritten scheint, ob das Fernmeldegeheimnis auf E-Mails Anwendung findet, die bereits in der Mailbox sind, jedoch noch nicht gelesen wurden.¹²² Diese Frage kann hier zumindest teilweise offen bleiben. Denn eine pauschale Zugriffsverweigerung gestützt auf das Fernmeldegeheimnis scheint nicht gerechtfertigt, da es nicht auf bereits gelesene E-Mails in der Mailbox angewendet werden kann.

119 SR DRS, 2011. Passwörter: Auch nach dem Tod eine Plage. Digital. URL: <http://www.drs.ch/www/de/drs/themen/digital/ratgeber-die-digitalen-spuren-nach-dem-tod/296310.296769.passwoerter-auch-nach-dem-tod-eine-plage.html> [besucht am: 16.6.2012]

120 Bettex et Al., Art. 321^{ter} CP N 11; Donatsch/Schmid, S. 152.

121 Donatsch/Schmid, S. 157.

122 Donatsch/Schmid, S. 159 mit weiteren Hinweisen. Die Frage wurde, soweit ersichtlich, bisher vor allem im Zusammenhang mit dem Strafprozess diskutiert: sobald ein Brief oder eine E-Mail nicht mehr unter das Fernmeldegeheimnis fällt kann dieser beschlagnahmt werden – in der Zeit in der die Sendung jedoch durch das Geheimnis geschützt ist, kann sie nur durch die Überwachung des Fernmeldeverkehrs eingesehen werden.

Wird in der anderen Extrem-Lösung der Zugriff auf das Konto bzw. sogar die Übernahme des Kontos bedingungslos gewährt, ist fraglich, ob der E-Mail-Provider seinen rechtlichen Verpflichtungen genügend nachkommt. So hat beispielsweise entsprechend der VDSG wie oben ausgeführt zumindest eine Interessensabwägung zu erfolgen. Eine Weiterführung einer persönlichen E-Mail-Adresse durch eine andere Person ist kaum zu rechtfertigen.

Soziale Netzwerke befinden sich aus der Sicht des Datenschutzes in einem Spannungsverhältnis: Zum einen versprechen sie ihren Nutzern den Schutz von Persönlichkeit und Daten, zum anderen haben Angehörige nach dem Tod ein Interesse an der Auskunft.

Eine zu prüfende, wenn auch mit erheblichen Aufwänden verbundene Lösung wäre: Beim Vorlegen der Sterbeurkunde oder des Erbscheins ist den Angehörigen Auskunft über die auf einem E-Mail-Account gespeicherten Daten zu gewähren. Jedoch sind dabei die Interessen von Dritten zu berücksichtigen. Diese können insbesondere berührt sein, falls über E-Mail Informationen, die durch ein Geheimnis (z.B. Berufsgeheimnis) geschützt sind, ausgetauscht wurden. Es ist zudem zu bevorzugen, dass nicht die Zugangsdaten herausgegeben werden, sondern lediglich eine Kopie der Daten, und der E-Mail-Account nach erfolgter Auskunft gelöscht wird. Hier kann auch der Kreis zur digitalen Vorsorge geschlossen werden: Eine ideale (testamentarische) Vorsorge würde die Aussortierung des Inhalts im Hinblick auf Verletzung von Geheimhaltungspflichten (Berufsgeheimnis) einem Willensvollstrecker übertragen.

6.3.5 «Recht auf Vergessen(werden)»

Das «Recht auf Vergessen» gebietet, dass nicht ohne bedeutende Rechtfertigung erneut über Tatsachen berichtet wird, die sich in der Vergangenheit abspielten und die geeignet sind, den Ruf oder die Ehre der betroffenen Person zu schädigen. Es geht dabei um wahrheitsgetreue Aussagen und das Schutzziel eines Rechts auf Vergessen ist, allenfalls einst fehlbaren Personen eine Chance einzuräumen, um ihr Leben in andere Bahnen zu leiten.¹²³ In der Schweiz besteht ein Recht auf Vergessen grundsätzlich gestützt auf Art. 28 ZGB. Wie jedoch noch gezeigt wird, stösst dieses im Internet an seine Grenzen.

6.3.5.1 Ein «Recht auf Vergessen» basierend auf dem Persönlichkeitsschutz

Der Bundesgerichtsentscheid 109 II 353 illustriert das Schutzkonzept des «Rechts auf Vergessen» basierend auf dem Persönlichkeitsschutz sehr deutlich: Paul Irniger wurde 1939 in Zug wegen Mordes verurteilt und hingerichtet. 1980 wollte die Schweizerische Radio- und Fernsehgesellschaft eine Dokumentarhörfolge mit dem Titel «Das Leben und Sterben des unwürdigen Dieners Gottes und mörderischen Vagabunden Paul Irniger» senden. Der Sohn des Hingerichteten reichte gegen dieses Vorhaben Klage ein und wollte die Ausstrahlung verbieten. Das Bundesgericht prüfte zuerst, ob Paul Irniger selbst, sollte er noch leben, sich gegen die Ausstrahlung der Sendung hätte wehren können. Es gelangte dabei zum Schluss, dass die geplante Ausstrahlung einen Eingriff in den Intim- und Privatbereich darstelle. Zwar sei Irniger zur Zeit, zu der er die fraglichen Verbrechen begangen hatte, eine Person der Zeitgeschichte gewesen, und dies rechtfertige wohl ein tieferes Eindringen in seine Persönlichkeit und Lebensgeschichte, was jedoch nicht bedeute, dass die Person eines Straftäters für alle Zukunft der Öffentlichkeit in gleich umfangreichem Masse zugänglich gemacht werde.¹²⁴ Durch die Ausstrahlung hätte also eine Verletzung der persönlichen Verhältnisse stattgefunden, da die Tatsachen – obwohl vormals von öffentlichem Interesse – durch den Zeitablauf erneut der Geheim- und Privatsphäre der betroffenen Person zuzuschreiben seien.

¹²³ Langer, N 1.

¹²⁴ BGE 109 II 353, E. 3.

Das heisst mit anderen Worten: Früher bekannt gemachte Informationen werden «informationsunwürdig», wenn das Interesse der Öffentlichkeit daran gering geworden ist, und durch die erneute Veröffentlichung die betroffene Person stark beeinträchtigt werden könnte.¹²⁵ Diese Rechtsprechung wurde konkretisiert in BGE 111 II 209, in dem das Bundesgericht festhielt, dass eine Interessenabwägung zwischen den Interessen der betroffenen Person und dem Interesse der Öffentlichkeit informiert zu sein, stattfinden müsse.¹²⁶ 2003 ergänzte das Bundesgericht in einem Entscheid 5C.156/2003 vom 23. Oktober 2003, dass sich nach dem Ablauf von 10 Jahren nur schwierig ein überwiegendes öffentliches Interesse an den Informationen finden lasse, falls es sich um strafrechtliche Verurteilungen handle, die wieder hervorgezerrt werden.¹²⁷ Das «Recht auf Vergessen» ist jedoch auch nach 10 Jahren nicht absolut.¹²⁸

Schliesslich hat das Gericht im «Irniger-Fall» entschieden, dass die Ausstrahlung auch in die Persönlichkeitsrechte des Sohnes eingreift. Somit können Angehörige ein «Recht auf Vergessen» geltend machen – jedoch nur in Berufung auf die Verletzung ihrer eigenen Persönlichkeit.¹²⁹

6.3.5.2 «Recht auf Vergessen» – auch im Internet?

Im Internet wird dieses «Recht auf Vergessen» jedoch vor besondere Herausforderungen gestellt, beziehungsweise geschwächt: Immer bessere Such- und Analyseprogramme verbunden mit nahezu unbegrenzten (und immer günstigeren) Speicherkapazitäten führen dazu, dass im Internet nichts vergessen geht. So können uns auch «unbedeutende Jugendsünden» ein Leben lang verfolgen, sofern sie einmal auf dem Netz sind.¹³⁰ Zudem stellt sich die Frage, wer die Verantwortung trägt, um den Inhalt zu löschen, sobald das Interesse an einer Publizität verloren geht.

Der Schweizerische Presserat beschäftigte sich im Mai 2011 mit der Frage, wie es sich bei digitalen (Zeitungs-) Archiven mit dem «Recht auf Vergessen» verhalte, und wel-

che berufsethischen Pflichten den Journalistinnen und Journalisten in diesem Zusammenhang zukommen.¹³¹ Insbesondere ging es um die Frage, ob eine Pflicht zur nachträglichen Anonymisierung von Online zugänglichen Artikeln bestehe oder ob die Digitalisierung von Zeitungsarchiven das «Recht auf Vergessen» gar überhole, und wen eine Anonymisierungspflicht treffen solle. Der Presserat hielt in seinen Überlegungen zwar, in Analogie zum Google-Streetview Entscheid¹³², fest, dass, wie nützlich ein Service auch immer sei, der Anbieter den Persönlichkeitsschutz der Betroffenen zu beachten habe. Zu diesem Schutz gehöre auch das «Recht auf Vergessen».¹³³ Jedoch ist der Presserat auch der Ansicht, dass es für Presshäuser unzumutbar ist Artikel, die via Suchmaschinen zugänglich sind, von sich aus regelmässig unter dem Gesichtspunkt «Recht auf Vergessen» zu überprüfen und nachträglich Artikel zu anonymisieren.¹³⁴ Gesuche um nachträgliche Anonymisierung sollen jedoch sorgfältig geprüft werden und die Anonymisierung soll vorgenommen werden, falls der Betroffene glaubhaft macht, dass ihm aus der Identifizierung ein aktueller und gewichtiger Nachteil droht.¹³⁵

¹²⁵ Weber, S. 103.

¹²⁶ Langer, N 16.

¹²⁷ Langer, N 16.

¹²⁸ Langer, N 18.

¹²⁹ BGE 109 II 353; Langer, N 13.

¹³⁰ Edöb, Die Privatsphäre im Zeitalter der digitalen Revolution, <<http://www.edoeb.admin.ch/dokumentation/00898/01704/index.html?lang=de>>, besucht am 3.5.2012.

¹³¹ Stellungnahme des Schweizer Presserates vom 11. Mai 2011 (29/2011; Berichtigung/Gegendarstellung/Nachträgliche Anonymisierung in Online-Medien und digitalen Archiven)

¹³² BVGer, A-7040/2009. Die Datenbearbeitung durch Google im Bereich von Streetview wurde als unverhältnismässig eingestuft und es wurde für Google zumutbar erklärt, die Anonymität der Personen die auf den aufgenommenen Bildern zu sehen sind sicherzustellen – wenn notwendig mit manuellen Nachbearbeitungen. Siehe dazu insbesondere E. 10.4.6. Das Bundesgericht ging auf Beschwerde von Google in derselben Frage davon aus, dass es genüge eine einfache, gut sichtbar Widerspruchsmöglichkeit zu schaffen, die auch von ungeübten Internetbenutzern problemlos in Anspruch genommen werden kann. Siehe dazu: BGE 138 II 346, E. 10.6.3.

¹³³ Presserat 29/2011, E. 6, d.

¹³⁴ Presserat 29/2011, E. 6, e.

¹³⁵ Presserat 29/2011, E. 6, e.

Das Datenschutzgesetz sieht in Art. 15 Abs. 1 DSGVO einen Anspruch auf Vernichtung von Daten vor. Dies lässt zwar an ein «Recht auf Vergessen» denken, jedoch muss zur Durchsetzung des Anspruchs nachgewiesen werden, dass Daten in persönlichkeitsverletzender Weise bearbeitet wurden und werden. Damit lässt sich der Anspruch auf Löschen nicht verwirklichen.¹³⁶ Zwar kann argumentiert werden, es läge eine Persönlichkeitsverletzung vor, da mit einer zu langen Aufbewahrung oder Bearbeitung der Daten gegen den (Datenbearbeitungs-) Grundsatz der Verhältnismässigkeit und Zweckmässigkeit verstossen werde. Jedoch darf nicht vergessen werden, dass es der betroffenen Person zukommt, die Persönlichkeitsverletzung zu beweisen.

Die Verankerung eines ausdrücklichen Rechts auf Löschung von Daten könnte dem «Recht auf Vergessen» zur Durchsetzung verhelfen.¹³⁷ Ein solches Grundrecht könnte z.B. vorsehen, dass Daten mit «Verfallsdaten» versehen werden.¹³⁸ Das heisst, Daten werden nach Ablauf einer – vertraglich vereinbarten oder gesetzlich festgelegten Frist – durch den Datenbearbeiter automatisch gelöscht.¹³⁹ Denkbar wäre auch, dass nach Ablauf der Frist aktiv die Zustimmung zur Löschung der Daten einzuholen wäre.¹⁴⁰

(evtl. für besonders schützenswerte Daten). Die Löschung sollte dabei eine irreversible Vernichtung der Daten darstellen, wobei unter keinen Bedingungen die Wiederherstellung der Daten möglich sein sollte.¹⁴¹

Eine solche Umsetzung des Rechts auf Vergessen würde sodann für den verstorbenen Internet-Plattform-Nutzer bedeuten, dass seine Daten z.B. spätestens 10 Jahre nach seinem Tod auch ohne Vorkehrungen nicht mehr zugänglich sind. Es könnte dann tatsächlich von einem «Recht auf Vergessenwerden» (right to be forgotten), das aktiv durch den Datenbearbeiter sichergestellt werden muss, gesprochen werden. Dies anstelle eines «Rechts auf Vergessen» (right to forget) welches den Daten- und Persönlichkeitsschutz weitgehend dadurch sicherstellt, dass unter Umständen ein erneutes Aufgreifen der Daten unterlassen werden muss.

136 Hilty et Al., S. 196.

137 Hilty et Al., S. 196.

138 Weber, S. 105; Hilty et Al., S. 196.

139 Hilty et Al., S. 195; Weber, S. 105.

140 Hilty et Al., S. 195.

141 Hilty et Al., S. 196.

Das «Recht auf Vergessen» stösst im Internet an seine Grenzen: Das Löschen von Informationen wird unnötig, da immer mehr und günstigerer Speicherplatz zur Verfügung steht – Jugendsünden, einmal in Netz, können uns ein Leben lang und darüber hinaus verfolgen.

6.3.5.3 Entwicklung des «Rechts auf Vergessenwerden» in der EU

Im Gemeinschaftsrecht der EU enthält bereits die Datenschutzrichtlinie 95/46/EG einige Elemente eines «Rechts auf Vergessen», insbesondere durch eine weitreichende Definition des Begriffs «Datenbearbeitung». Diese umfasst gem. Art. 2 lit. b RL 95/46/EG u.a. das Speichern, die Aufbewahrung, die Veränderung, das Abfragen, die Benutzung, Weitergabe, Verbreitung sowie auch das Sperren, Löschen oder Vernichten von Daten. Dies umfasst somit die Veröffentlichung von Online-Archiven, das Erstellen von «deep-links», die via Suchmaschinen zu Online-Archiven führen und das Aufbewahren von persönlichen Daten in Sozialen Netzwerken.¹⁴²

Gem. Art. 6 Abs. 1 lit. b RL 95/46/EG dürfen personenbezogene Daten nur «für festgelegte eindeutige und rechtmässige Zwecke erhoben» werden und nicht in einer Art weiterverarbeitet werden, die dieser Zweckbestimmung widerspricht. Eine Weiterverarbeitung zu historischen, statistischen oder wissenschaftlichen Zwecken bleibt vorbehalten.

In der EU wächst das Bewusstsein dafür, dass der Datenschutz durch den technologischen Wandel (vermehrte Nutzung von Sozialen Netzwerken, Fernspeicherung von Daten) vor neue Herausforderungen gestellt wird und die jetzigen Instrumente weder genügend harmonisiert noch genügen wirksam sind, um das Recht auf den Schutz personenbezogener Daten zu garantieren. Dieses Recht ist sowohl in der Charta der Grundrechte der EU (Art. 8 GRC) als auch im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) verankert. Zwischen September und Dezember 2011 ging aus Gesprächen zwischen den Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten deutlich hervor, dass Bürger und Unternehmen eine Reform der EU-Datenschutzvorschriften (Richtlinie 95/46/EG und Rahmenbeschluss 2008/977/JI) befürworten.

¹⁴² Langer, N 22.

Vorgeschlagene Revision der Datenschutzrichtlinie der EU

Diese Revision soll folgende Aspekte neu oder ausführlicher regeln:

- Kontrolle über die personenbezogenen Daten soll dem Einzelnen zukommen
 - In der bestehenden Richtlinie ist Art und Weise, in der die betroffenen Personen ihr Recht auf Datenschutz wahrnehmen können – insbesondere über die Grenzen der Mitgliedstaaten – nicht ausreichend vereinheitlicht. Eine einheitliche und wirksame Anwendung der Vorschriften ist ebenfalls nicht gewährleistet. Online ist die Ausübung der Datenschutzrechte in einigen Mitgliedstaaten schwieriger als in anderen. Im Bereich von sozialen-online-Netzwerken will die EU deshalb insbesondere sicherstellen, dass die Menge der erfassten und verarbeiteten personenbezogenen Daten auf ein Mindestmass begrenzt wird.
 - Die Standardeinstellungen von Sozialen Netzwerken sollen vorsehen, dass Daten nicht veröffentlicht werden.
 - Verlangt die betroffene Person das Löschen von Daten, soll dies durch die für die Verarbeitung Verantwortlichen durchgeführt werden, sofern keine legitimen Gründe für die Aufbewahrung der Daten vorliegen. Auf einer Internetplattform müsste der Verwalter die «Freunde» der Person die das Löschbegehren stellt, darüber informieren, dass die betreffenden Daten auch von ihren Konten gelöscht werden.¹⁴³ Es handelt sich also bei diesem Vorschlag um ein «Recht auf Vergessenwerden».
- Verbesserte Möglichkeiten für den Einzelnen seine Rechte wahrzunehmen

Die EU scheint auch erkannt zu haben, dass der Datenschutz an einem Durchsetzungsproblem leidet. Insbesondere kann es heute vorkommen, dass derselbe Sachverhalt in einem Mitgliedstaat als Verstoß gegen den Datenschutz gewertet wird und in einem anderen nicht.¹⁴⁴ Folgende Massnahmen werden vorgeschlagen, um den materiellen Rechten zur Durchsetzung zu verhelfen:

- Die vorzuschlagende EU-Verordnung soll unmittelbare Anwendung in der gesamten Union finden.
- Die Unabhängigkeit der nationalen Datenschutzbehörden soll gestärkt und ihre Befugnisse sollen ausgebaut werden. Die Behörden sollen damit ermächtigt werden, Ermittlungen vorzunehmen, verbindliche Beschlüsse zu fassen und wirksame abschreckende Sanktionen zu erlassen. Die Mitgliedstaaten müssen die Behörden daher mit ausreichenden Ressourcen ausstatten.
- Die Zuständigkeit, um Verletzungen der Datenschutzverordnung festzustellen, soll nur bei der Datenschutzbehörde des Staates liegen, in dem das Unternehmen seinen Hauptsitz hat. Damit wird nur diese Behörde zuständig für Personen aus verschiedenen Mitgliedstaaten, was eine zügige und wirksame Abstimmung zwischen Datenschutzbehörden verschiedener Mitgliedstaaten notwendig macht und eine einheitliche Rechtsanwendung fördert.¹⁴⁵

Ein weiterer Vorschlag besteht darin, ein Zertifizierungsverfahren für Datenbearbeiter aufzubauen. Es soll abgeklärt werden, ob Initiativen zur Selbstregulierung zu einer besseren Durchsetzbarkeit führen und schliesslich auch, welche Voraussetzungen ein «Datenschutzsigel» zu erfüllen hätte.¹⁴⁶

¹⁴³ Langer, N 29; Art. 17 Abs. 2 der vorgeschlagenen Verordnung.

¹⁴⁴ So geschehen in Bezug auf Google-Streetview.

¹⁴⁵ Siehe zum Ganzen: Kom (2012) 9 endg.

¹⁴⁶ Kom (2010) 609 endg.

6.3.5.4 Kritik und Auswirkungen auf die Schweiz

Die Initiative zur Überarbeitung der Datenschutzrichtlinie in der EU ist zu begrüßen und scheint in wesentlichen Punkten in die richtige Richtung zu zielen. Insbesondere ist positiv festzuhalten, dass versucht wird, das Problem des Datenschutzes im Internet und auf Internet-Plattformen einheitlich zu lösen und dem Benutzer die Herrschaft über seine Daten zurückzugeben. Jedoch ist zu bemängeln, dass das vorgeschlagene Recht auf Vergessen in diesem Kontext zu wenig weit geht. Es ist allgemein festzuhalten, dass das Schicksal der auf Internet-Plattformen gespeicherten Daten nach dem Tod der betroffenen Person nicht nur nicht geregelt wird, sondern, dass darüber keine Bemerkungen in den Mitteilungen zu finden sind.¹⁴⁷

In diesem Bereich ist also anzunehmen, dass es weiterhin in der Kompetenz der Mitgliedstaaten liegt, festzulegen, wem die Klagelegitimation zukommt: Besteht ein postmortaler Persönlichkeitsschutz, werden die Angehörigen das «Recht Vergessenwerden» durchsetzen können. Besteht kein solcher, werden sich die Angehörigen nach dem Tod kaum gegen den Internet-Plattformbetreiber durchsetzen können. Würde sich die EU für ein weitergehendes Grundrecht aussprechen, welches – wie z.B. wie von WEBER und auch HILTY ET AL. diskutiert wird – mit Verfallsdaten von Daten arbeiten würde, könnte auch in diesem Bereich eine Vereinheitlichung bewirkt werden.

Sollte die EU die Datenschutz-RL überarbeiten, könnte sich dadurch für die Schweiz aufgrund der Schengen- und Dublin-Verträge ein Handlungsbedarf ergeben und eine Integration der Änderungen in die schweizerischen Gesetze nötig werden.¹⁴⁸ Das Thema gewinnt derzeit auch unter den Bundesparlamentarierinnen vermehrt Beachtung, wie das Postulat von Jean Christophe Schwaab¹⁴⁹ zeigt. Das Postulat, welches sich in seiner Begründung auch auf die Entwicklungen in der EU bezieht, will den Bundesrat beauftragen, die Aufnahme eines «Recht auf Vergessen im Internet» in die Gesetzgebung zu überprüfen. Dies insbesondere im Zusammenhang mit sozialen Netzwerken und Suchmaschinen. Zudem soll die bessere Durchsetzbarkeit dieser Rechte überprüft werden. Der Bundesrat selbst beantragt die Annahme des Postulats. Diesem Antrag ist der Nationalrat am 15. Juni 2012 gefolgt, womit der Bundesrat zur Ausarbeitung eines Berichts zu den aufgeworfenen Fragen beauftragt wurde. Auf diesen kann gespannt gewartet werden.

¹⁴⁷ Vgl. Kom (2010) 609 endg.; Kom (2012) 9 endg.

¹⁴⁸ Langer, N 31; Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz, BBl 2012 335, S. 349

¹⁴⁹ 12.3152 – Postulat, Recht auf Vergessen im Internet, 14.3.2012

6.3.6 Die Rolle des Eidgenössischen Datenschutzbeauftragten EDÖB

In seiner Funktion als Aufsicht über private Datenbearbeiter hat der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) gemäss Art. 29 DSG die Möglichkeit, Sachverhalte näher abzuklären, wenn Bearbeitungsmethoden gewählt wurden, die geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen – es sich also um Systemfehler handelt (Art. 29 Abs. 1 lit. a DSG). Basierend auf diesen Abklärungen kann der EDÖB Empfehlungen an die datenbearbeitende Stelle richten, das Datenbearbeiten sei zu unterlassen oder anzupassen (Art. 29 Abs. 3 DSG). Werden die Empfehlungen nicht oder nur teilweise befolgt, ist der EDÖB berechtigt, die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorzulegen (Art. 29 Abs. 4 DSG). Illustrativ für dieses Vorgehen ist der Entscheid «Google-Streetview» des Bundesverwaltungsgerichtes. Umstritten war in dieser Sache auch das Vorliegen eines Systemfehlers, also die Gefahr, dass durch die Wahl der Bearbeitungsmethode, die Persönlichkeit einer grösseren Anzahl von Personen verletzt werden könnte. Sowohl das Bundesverwaltungsgericht als auch das Bundesgericht hielten fest, dass es sich um einen möglichen Systemfehler im Sinne von Art. 29 Abs. 1 lit. a DSG handle, wenn Bilder und andere Daten, welche direkt oder nur mit geringem Aufwand bestimmten Personen zugeordnet werden können, im Internet einem grossen Publikum zur Verfügung gestellt werden.¹⁵⁰ Eine Einwilligung in einen Systemfehler ist nicht möglich, da er – wird sein Vorliegen bejaht – im öffentlichen Interesse beseitigt werden muss.¹⁵¹ Ein Systemfehler müsste wohl angenommen werden, falls eine Internet-Plattform Daten eines Nutzers anderen Nutzern ohne Einwilligung zugänglich macht. Insbesondere problematisch scheint die Praxis, AGB zu ändern, neue Anwendungen einzuführen und die neuen Standardeinstellungen so zu setzen, dass die Nutzer in das Verwenden ihrer Daten für den neuen Dienst automatisch einwilligen. Ein solches Vorgehen scheint geeignet, um die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen.¹⁵²

Ein Vorgehen des EDÖB nach Art. 29 DSG könnte für den Umgang mit digitalen Daten nach dem Tod insofern relevant sein, als dass den Nutzern bereits zu Lebzeiten eine effektivere Kontrolle über ihre Daten zukommen könnte. Zudem könnte allenfalls auch beim Umgang mit den Daten von Verstorbenen von einem Systemfehler ausgegangen werden, da – wie oben dargestellt – der Datenschutz nach dem Tod nicht vollständig versagt. Letzteres muss jedoch kritisch beurteilt werden, da es wie ausgeführt in solchen Fällen meistens an einer Persönlichkeitsverletzung fehlt.

Des Weiteren sieht Art. 11 DSG ein Zertifizierungsverfahren für System, Verfahren und Organisation der Datenbearbeitung vor. Zertifizieren lassen können sich sowohl private Organisationen als auch Bundesorgane, die Personendaten bearbeiten. Mit der Zertifizierung soll ein Beitrag zur Selbstregulierung geleistet werden.¹⁵³ Das durch die Zertifizierung verliehene Datenschutz-Qualitätszeichen soll deren Träger von der Pflicht, eine Datensammlung zu melden, entbinden (Art. 11a Abs. 5 lit. f DSG). Die Arbeiten an einer Produktezertifizierung, wie sie durch das DSG ebenfalls vorgesehen ist, wurden auf Eis gelegt. Der EDÖB wies dabei auf Unklarheiten in der Gesetzgebung hin.¹⁵⁴ Die Zertifizierung von Organisationen wurde unterdessen umgesetzt.¹⁵⁵ Die Anreize zur Selbstregulierung, die durch diese Zertifizierung geschaffen werden, werden jedoch als zu wenig weitgehend kritisiert.¹⁵⁶

¹⁵⁰ Urteil BGer vom 31. Mai 2012 1C_230/2011, E. 6.5; BVGer A-7040/2009 vom 30. März 2011, E. 7.6.3.

¹⁵¹ Schweizer/Glut von Blotzheim, N 13.

¹⁵² Es wird in diesem Zusammenhang vom «Opt-In-Prinzip» gesprochen, welches die Anforderungen an die Einwilligung präzisieren soll: Die Grundeinstellung soll auf eine minimale Verwendung der vom Nutzer zur Verfügung gestellten Daten voreingestellt sein. In eine weitergehende Nutzung muss danach explizit eingewilligt werden. Vgl. dazu: Bolliger/Féraud/Epiney/Hänni, S. 246

¹⁵³ Pärli, S. 67.

¹⁵⁴ Edöb, <www.edoeb.admin.ch> (Dokumentation/Tätigkeitsberichte/18-2010/2011/Entwicklung der Zertifizierung von Produkten und Dienstleistungen), besucht am: 22.10.2012.

¹⁵⁵ Edöb, <www.edoeb.admin.ch> (Dokumentation/Tätigkeitsberichte/17-2009/2010/Zertifizierung von Datenschutzmanagementsystemen: Akkreditierungen), besucht am: 22.10.2012.

¹⁵⁶ Pärli, S. 65.

6.4 DURCHSETZUNG DES DIGITALEN LETZTEN WILLENS

Da im Internet regelmässig ein internationaler Sachverhalt vorliegt, stellt sich die Frage der gerichtlichen Zuständigkeit und des anwendbaren Rechts. Es gilt herauszufinden, ob die schweizerischen Gesetze (ZGB und DSGVO insbesondere) auf den Sachverhalt anwendbar sind und Betroffene gegen eine unrechtmässige Datenverarbeitung (zu Lebzeiten) oder gegen Persönlichkeitsverletzungen (die Angehörigen wegen verletzter Pietätsgefühle) vor den schweizerischen Gerichten vorgehen können. Die Zuständigkeit des Gerichts entscheidet sich entweder nach dem schweizerischen Gesetz über das Internationale Privatrecht (IPRG) oder nach völkerrechtlichen Verträgen. Das konkrete Vorgehen kann am Beispiel Facebook veranschaulicht werden: Facebook hat einen Sitz in Irland. Irland und die Schweiz sind Vertragsstaaten des Lugano-Übereinkommens (LugÜ), welches somit zur Anwendung kommt. Die EU ist mit Wirkung für alle ihre Mitgliedsstaaten Vertragspartner des LugÜ. Dementsprechend ist für unerlaubte Handlungen – wie eine nicht zu rechtfertigende Datenbearbeitung – eine Zuständigkeit des Gerichts am Handlungs- oder Erfolgsort gegeben (Art. 5 Ziff. 3 LugÜ). Entsprechend hat der Europäische Gerichtshof (EuGH) im Oktober 2011 seine Rechtsprechung konkretisiert: Bei Persönlichkeitsverletzungen im Internet soll neben dem Handlungsort – welcher unter Umständen schwierig zu identifizieren ist – auch eine Zuständigkeit für den Gesamtschaden am Haupterfolgsort gegeben sein. Der Erfolgsort wird dabei mit dem Ort des gewöhnlichen Aufenthalts des Geschädigten gleichgesetzt.¹⁵⁷ In der früheren Rechtsprechung des EuGH wurde nur die Möglichkeit am Handlungsort den Gesamtschaden einzuklagen, anerkannt. Der Erfolgsort wurde dabei auf verschiedene Staaten aufgeteilt und daher war es nur möglich, den Schaden, der in einem bestimmten Staat verursacht wurde, auch in demselben einzuklagen, was natürlich die Durchsetzung des Schadenersatzes erheblich erschwerte.¹⁵⁸

Nun haben jedoch viele Internetplattformen in ihren AGB auch eine Gerichtsstandsvereinbarung aufgenommen. Auch die einzige im Projektrahmen untersuchte Plattform,

welche in der Schweiz einen Sitz hat, Xing, hat eine Gerichtsstands-Klausel zugunsten des Amtsgerichts Hamburg in seine AGB eingefügt. Im Falle von Facebook lautet die Gerichtsstands-Klausel (Stand Juni 2012):

16. Streitfälle

«Du wirst sämtliche Ansprüche, Klagegegenstände oder Streitfälle («Anspruch»), die du uns gegenüber hast und die sich aus dieser Erklärung oder aus Facebook oder in Verbindung damit ergeben, ausschliesslich vor einem Staats- oder Bundesgericht in Santa Clara County, Kalifornien, klären. Diese Erklärung sowie alle Ansprüche, die möglicherweise zwischen dir und uns entstehen, unterliegen den Gesetzen des Bundesstaates Kalifornien, unter Ausschluss der Grundsätze des Kollisionsrechts. Du erklärst dich damit einverstanden, dich bei einem Prozess über alle derartigen Ansprüche der personenbezogenen Zuständigkeit der Gerichte in Santa Clara County, Kalifornien, zu unterwerfen.»

Die Gültigkeit dieser Vereinbarung ist im (für Facebook) besten Fall wohl als unsicher einzustufen. Gerichtsstandsvereinbarungen sind zwar grundsätzlich möglich. Sich jedoch der Anwendung des gesamten Kollisionsrechts¹⁵⁹ entziehen zu wollen, scheint gewagt. Eine Gerichtsstandsvereinbarung für eine Haftung aus unerlaubter Handlung wird gemäss dem LugÜ aufgrund von Art. 23 Abs. 1 nur akzeptiert, falls das prorogierte Gericht seinen Sitz ebenfalls in einem LugÜ Vertragsstaat hat. Somit hält die Gerichtsstandsvereinbarung von Facebook bzw. mit dessen irischer Tochtergesellschaft Facebook Ireland Ltd., welche Vertragspartnerin von allen europäischen Nutzern ist, dem LugÜ nicht stand.¹⁶⁰ Jedoch kann nicht generell festgehalten werden, inwieweit solche und ähnliche Klauseln

¹⁵⁷ Kernen, N 10.

¹⁵⁸ Kernen, N 11.

¹⁵⁹ Unter Kollisionsrecht versteht man die Normen, die bei internationalen Streitigkeiten das zuständige Gericht und das anwendbare Recht bestimmen.

¹⁶⁰ Hilty et Al., S. 59.

überhaupt zulässig sind. Es muss jeweils auf die konkreten Umstände des Einzelfalls abgestellt werden.¹⁶¹

Sollte die fragliche Plattform keinen Sitz in der Schweiz oder in einen LugÜ-Vertragsstaat haben, so wird ein angerufener Schweizer Richter seine Zuständigkeit i.d.R. nach dem IPRG prüfen. Dieses sieht in Art. 5 IPRG insbesondere auch vor, dass eine Gerichtsstandsvereinbarung, bevor der Streit entsteht, nur in Bezug auf vermögensrechtliche Ansprüche möglich ist. Im Bereich des Datenschutzes wird es sich kaum um vermögensrechtliche Ansprüche handeln – einzige Ausnahme bildet wohl der Anspruch auf Genugtuung im Sinne von Art. 15 DSGVO i.V.m. Art. 28 a Abs. 3 ZGB und Art. 49 OR. Art. 129 IPRG sieht zudem eine zum LugÜ analoge Regelung in Bezug auf die Zuständigkeit der schweizerischen Gerichte vor und es ist zu erwarten, dass die vom EuGH liberalisierte Rechtsprechung bezüglich des Klägergerichtsstandes am Erfolgsort (=Ort des gewöhnlichen Aufenthalts) für den Gesamtschaden übernommen werden wird.¹⁶²

Somit dürfte eine Zuständigkeit der schweizerischen Gerichte gegeben sein, wenn das datenbearbeitende Unternehmen keinen Sitz in einem EU-Vertragsstaat hat. Die schweizerischen Gerichte beurteilen das anwendbare Recht bei Persönlichkeitsverletzungen gemäss Art. 139 IPRG. Der Geschädigte kann dabei wählen zwischen

- a. dem Recht des Staates, in dem der Geschädigte seinen gewöhnlichen Aufenthalt hat, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste;
- b. dem Recht des Staates, in dem der Urheber der Verletzung seine Niederlassung oder seinen gewöhnlichen Aufenthalt hat, oder
- c. dem Recht des Staates, in dem der Erfolg der verletzenden Handlung eintritt, sofern der Schädiger mit dem Eintritt des Erfolges in diesem Staat rechnen musste.

Somit ist im Ergebnis die Anwendbarkeit des schweizerischen Datenschutzrechts in praktisch allen internationalen Konstellationen möglich.¹⁶³

Schliesslich ist jedoch zu beachten, dass ein Urteil im Ausland auch anerkannt werden muss um vollstreckt zu werden. Die Gerichte einiger US-Bundesstaaten scheinen die Tendenz zu haben Urteile, die gegen ein US-amerikanisches Unternehmen im Ausland ergangen sind weder anzuerkennen noch zu vollstrecken. Somit kann es unter Umständen unumgänglich sein im Sitzstaat des betreffenden Unternehmens zu klagen.¹⁶⁴

Auch Parlament und Regierung scheinen sich der Problematik der fehlenden oder zumindest ungenügenden Durchsetzbarkeit von Ansprüchen aus Persönlichkeits- und Datenschutzverletzung im Internet und dabei insbesondere in Social-Media-Plattformen bewusst zu sein. Mit der Annahme des Postulats Amherd (11.3912) wurde der Bundesrat mit der Ausarbeitung eines Berichts beauftragt, der die Rechtslage in Bezug auf Social Media beleuchtet. **Dabei erkennt der Bundesrat: «(...) die Betreiber von Social-Media-Plattformen sind häufig international tätig und die nationale Gesetzgebung stösst daher an ihre Grenzen». Der Bericht soll daher insbesondere untersuchen, in welchen Bereichen (Gesetzes-)Lücken im DSG, ZGB, StGB und URG bestehen, und wie diese geschlossen werden können.** Ob dabei jedoch auch auf die Rechtsdurchsetzung durch Angehörige eines verstorbenen Nutzers eingegangen wird, ist derzeit noch offen. Schliesslich ist noch zu bemerken, dass die Evaluation des DSG ergeben hat, dass die Durchsetzungsrechte des DSG relativ selten genutzt werden. Dies könne auf den «beträchtlichen Aufwand einer Klage» bei «einem diffusen und nicht gesicherten Nutzen bei ihrer Gutheissung» zurückgeführt werden. Der Rechtsweg könne für die Betroffenen mit Risiken verbunden sein. Die spezifischen Durchsetzungsrechte des DSG erlangen gegenüber privaten Datenbearbeitern nur zusammen mit Art. 28 ZGB Bedeutung. Auch die Wirksamkeit der Tätigkeiten des EDÖB werde teilweise durch die Zunahme intransparenter und grenzüberschreitender Datenbearbeitungen bestimmt und nur schwer beeinflussbar.¹⁶⁵

¹⁶¹ Hilty et Al., S. 192.

¹⁶² Kernen, N 40.

¹⁶³ Hilty et Al., S. 60.

¹⁶⁴ Meili, S. 29.

¹⁶⁵ Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, in: BBl 2012 335 ff., 343.

7. Anknüpfungspunkte bei der Administration von Todesfällen

Der Schwedische digitale Vererbungsdienst Mywebwill, der seine Dienste 2011 nach zwei Jahren wieder eingestellt hat, verfügte über einen Mechanismus, der die digitale Nachlassplanung und Willensvollstreckung vereinfachte. Kunden, die ihre digitale Nachlassplanung bei Mywebwill hinterlegt hatten, waren dort mit ihrer Personennummer, über die alle Schwedischen Bürger eindeutig identifizierbar sind, registriert. Wurde der Tod eines Mywebwill-Kunden im nationalen amtlichen Melderegister verzeichnet, wurde der Vererbungsdienst automatisch benachrichtigt und konnte den Prozess der digitalen Willensvollstreckung starten, das heisst die hinterlegten Zugangsdaten und Wünsche für den Umgang mit den Daten und Internetprofilen an die benannten Vertrauenspersonen weiterleiten.

Ein solcher Automatismus, basierend auf einer Integration mit einem amtlichen Registersystem, vereinfacht den Prozess und erhöht die Wahrscheinlichkeit der Willensvollstreckung in zweierlei Hinsicht: Durch die, im Fall von Mywebwill, «amtliche Meldung» entfällt zum einen die Notwendigkeit, dass die Hinterbliebenen den Todesfall an den Vererbungsdienst melden und mit einer Todesurkunde bestätigen müssen. Zum anderen müssen die Hinterbliebenen oder Vertrauenspersonen (=digitalen Willensvollstrecker) nicht zwangsläufig von der nachlassplanenden Person zu Lebzeiten über die Existenz der digitalen Nachlassplanung informiert werden, vorausgesetzt die Instruktionen für die Willensvollstreckung im Todesfall sind selbst erklärend oder der Vererbungsdienst unterstützt die Hinterbliebenen bei Bedarf.

Bietet das amtliche Melde- und Registerwesen in der Schweiz derartige Anknüpfungspunkte für die digitale Nachlassplanung?

In der Schweiz existieren bereits Anwendungsbeispiele, in denen amtliche Stellen und Systeme eine Rolle in der Vorsorgeplanung spielen. So besteht mit Einführung des neuen Erwachsenenschutzrechtes (1.1.2013) die Mög-

lichkeit, die Existenz und den Hinterlegungsort eines Vorsorgeauftrages im eidgenössischen Zivilstandsregister (System Infostar) eintragen zu lassen. Dies ist jedoch Ergebnis eines mehrjährigen Revisionsprozesses und bedurfte der Anpassung und Erweiterung der Rechtsgrundlagen (Revision ZGB nArt. 361 Abs. 3, ZStV Art. 23a). Auf Ebene des Meldewesens auf Gemeindeebene erlaubt beispielsweise das Einwohnerregister der Stadt Zürich (TopaZ) einen Vermerk «HT» (hinterlegtes Testament), der bei der Registrierung des Todesfalls einen Brief an das Notariat auslöst. In diesem Kontext ebenfalls zu nennen sind die in Kapitel 6.2.1.3 beschriebenen «Anordnungen ausserhalb eines Testaments». Das Bestattungs- und Friedhofsamt der Stadt Zürich beispielsweise ermöglicht die Hinterlegung von Bestattungswünschen, die den Angehörigen bei der Anmeldung des Todesfalls zur Kenntnis gebracht werden.

Es stellt sich die Frage, ob amtliche Stellen und Systeme eine vergleichbare Funktion bei der digitalen Vorsorgeplanung einnehmen könnten. Im Rahmen des Projekts wurde die **Machbarkeit aus organisatorischer, technischer und rechtlicher Sicht** für folgende Möglichkeiten geprüft:

- **Vermerk** in einem amtlichen Personenregister, der auf die **Existenz einer digitalen Nachlassplanung** hinweist sowie allenfalls auf die Person oder Institution (z.B. Online-Dienst, Notar), durch die bzw. den die Willensvollstreckung ausgelöst wird.
- **Automatisierte Mitteilung eines Todesfalls** an einen Online-Dienst oder eine sonstige mit der digitalen Willensvollstreckung betraute Institution.
- **Beurkundung eines Todesfalls in digitaler Form**, um die Kommunikation mit Plattformanbietern und Vererbungsdiensten für die Hinterbliebenen zu vereinfachen. Sowohl Plattformanbieter (z.B. Google, siehe Kapitel 5) als auch die Mehrzahl der digitalen Vererbungsdienste (siehe Kapitel 8.2) verlangen einen offiziellen Nachweis für den Todesfall. In der Regel handelt es sich hierbei um die beglaubigte Kopie einer Todesurkunde, bei Geschäftssitz im Ausland die Kopie einer beglaubigten Übersetzung bzw. eine internationale Todesurkunde.

Infrastrukturelle Voraussetzungen: Das elektronische Register- und Meldewesen in der Schweiz

In der Schweiz wurden seit 2008 die gesetzlichen und systemischen Grundlagen für ein elektronisches Meldewesen durch das Projekt «Registerharmonisierung»¹⁶⁶ und das Folgeprojekt «e-MISTAR» (elektronische Meldungen aus Infostar) geschaffen. Die Datenübermittlungsplattform des Bundes «sedex» (=secure data exchange) stellt seit Januar 2008 den gesetzlich geregelten, sicheren und standardisierten Datenaustausch zwischen den angeschlossenen amtlichen Registern sicher (siehe Abbildung 6).

Infostar (= Informatisiertes Standesregister, *2004) ist das zentrale vom Bundesamt für Justiz betriebene elektronische Zivilstandsregister, an das alle schweizerischen Zivilstandsämter angeschlossen sind. Alle Zivilstandsereignisse, so auch Todesfälle, werden in Infostar dezentral in den Zivilstandsämtern erfasst. Neben der vereinfachten Lieferung statistischer Daten aus den kantonalen und kommunalen Einwohnerregistern an das Bundesamt für Statistik,

ermöglichen die Registerharmonisierung und sedex auch die Ablösung der traditionellen Papiermeldungen aus Infostar an die Einwohnerdienste und weitere amtliche Register. So erfolgt die Meldung eines Todesfalls an die AHV-Behörde (Art. 53 ABs.1 ZStV) sowie an das Bundesamt für Statistik (Art. 52 ZStV) elektronisch und automatisiert, sobald ein Todesfall in Infostar vom zuständigen Zivilstandsamt registriert wird. Auch die Meldung eines Todesfalls aus Infostar an das Einwohnerregister des Wohnsitzes oder Aufenthaltsorts der verstorbenen Person in der Schweiz kann elektronisch erfolgen, vorausgesetzt das jeweilige Einwohnerregister ist für das elektronische Meldewesen aktiviert.¹⁶⁷

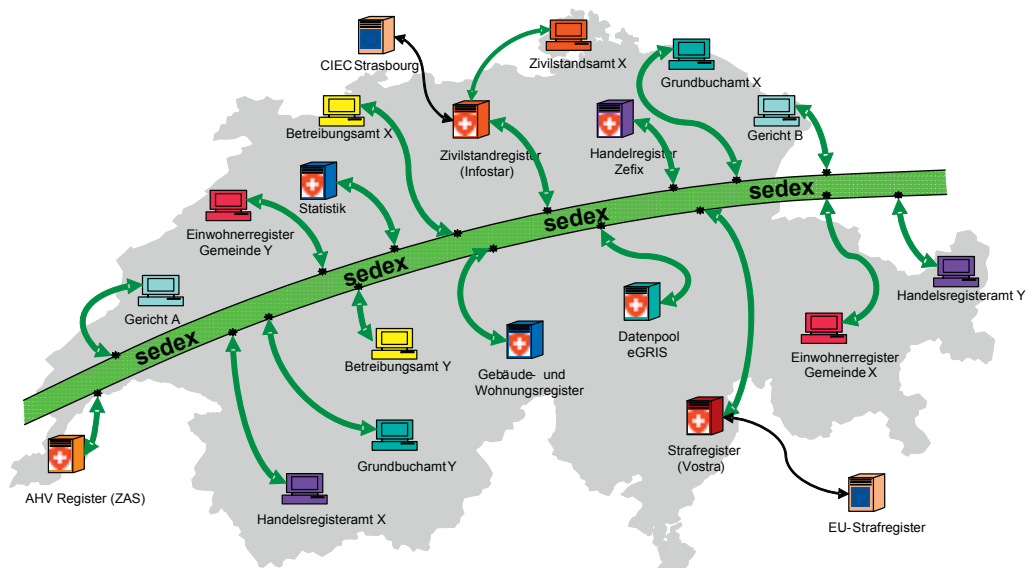
¹⁶⁶ RHG, Registerharmonisierungsgesetz in Kraft seit 1. Januar 2008

¹⁶⁷ Stand Ende September 2012 haben 741 Gemeinden das elektronische Meldewesen mit Infostar aktiviert, dies entspricht rund 30% aller politischen Gemeinden der Schweiz (Steimer, 2012). Voraussichtlich bis 2014 wird das Meldewesen aus Infostar an die EWR der Schweizer Gemeinden und Städte flächendeckend elektronisch erfolgen. Zum aktuellen Stand des elektronischen Meldewesens siehe <http://www.bj.admin.ch/content/bj/de/home/themen/gesellschaft/zivilstand/einwohnerkontrolle.html>

¹⁶⁸ Vereinfachte Darstellung ohne kantonale Datenplattformen

Abb. 6

ELEKTRONISCHER DATENAUSTAUSCH VIA SEDEX ¹⁶⁸



Prozesse und Rechtsgrundlagen für die Beurkundung und Meldung von Todesfällen ¹⁶⁹

Im Rahmen des Forschungsprojekts ermöglichte das Bevölkerungsamt der Stadt Zürich Einblicke in die Meldung, Registrierung und Beurkundung von Todesfällen¹⁷⁰. Todesfälle müssen gemäss Art. 35 ZStV (eidgenössische Zivilstandsverordnung) innert zwei Tagen dem zuständigen Zivilstandsamt gemeldet werden. In der Stadt Zürich erfolgt die Anmeldung des Todesfalls persönlich beim Bestattungs- und Friedhofsamt oder durch eine schriftliche Mitteilung des Spitals, Heims oder sonstigen Institution, in der die Person verstorben ist (Art. 34a ZStV, Art. 18–21 ZVO des Kantons Zürich). Anschliessend wird der Todesfall ohne Verzug im Zivilstandsamt der Stadt Zürich in Infostar elektronisch beurkundet. Die Zuständigkeit für die Beurkundung des Todesfalls richtet sich nach dem Ereignisort, d.h. der Tod wird im Zivilstandskreis beurkundet, in dem die Person verstorben ist (Art. 20a ZStV, Art. 1, 21 ZVO des Kantons Zürich). Nach Abschluss der Beurkundung in Infostar erfolgen die oben erwähnten amtlichen Mitteilungen an die zuständige Einwohnerkontrolle, an das Bundesamt für Statistik und an die AHV-Behörde sowie an weitere Stellen gemäss Art. 48a–57 ZStV. Bezugsberechtigte Personen können eine Todesurkunde oder einen Auszug aus dem Todesregister CIEC (Commission Internationale de l'Etat Civil, internationale Todesurkunde) für den Verkehr mit ausländischen Behörden beim Zivilstandsamt bestellen. Die detaillierten Abläufe und Rechtsgrundlagen für die Beurkundung von Todesfällen durch die Zivilstandsämter ist in den Fachprozessen zum Geschäftsfall «Tod» des Eidgenössisches Amtes für das Zivilstandswesen dokumentiert (EAZW, 2011).

Die Analyse der Abläufe, Rechtsgrundlagen und Systeme führt in Bezug auf die oben genannten Anknüpfungspunkte zu folgenden Schlussfolgerungen:

- Elektronische Todesurkunden (CH/dreisprachig und international) sind im eidgenössischen Zivilstandswesen momentan nicht möglich. Die Urkunden werden ausschliesslich auf speziellem Sicherheitspapier (Art. 6 ZStV, Festlegung des EAZW) ausgedruckt.
- Die ZStV unterscheidet Bekanntgaben von Amtes wegen und Bekanntgaben auf Bestellung. Zusätzliche Meldungen eines Todesfalls bedürfen einer Rechtsgrundlage des Bundes oder der Kantone (Art. 56 ZStV). Todesurkunden und Auszüge aus dem Todesregister (CIEC, internationale Todesurkunden) werden nur auf Bestellung für bezugsberechtigte Personen ausgestellt. Daher besteht für eine Meldung eines Todesfalls direkt aus Infostar an einen privaten digitalen Vererbungsdienst, wie dies vergleichsweise in Schweden der Vererbungsdienst Mywebwill eingerichtet hatte, momentan keine Rechtsgrundlage in der Schweiz.
- Eine Anpassung des Datenschemas von Infostar, um z.B. die Existenz eines «digitalen Willens» zu vermerken (analog Hinterlegungsort des Vorsorgeauftrags in Infostar ab 1.1.2013) erscheint nicht aufwandsgerecht. Jede Anpassung des Infostar-Datenschemas erfordert eine Prüfung und gegebenenfalls Anpassung der Rechtsgrundlagen.

¹⁶⁹ Einen zentralen Einstieg zu den Zuständigkeiten und Vorgehensweisen im Todesfall auf kantonaler und kommunaler Ebene bietet das Portal [ch.ch](http://www.ch.ch/private/00029/00037/index.html?lang=de) der Schweizerischen Bundeskanzlei: <http://www.ch.ch/private/00029/00037/index.html?lang=de>

¹⁷⁰ Das Projektteam dankt dem Bevölkerungsamt der Stadt Zürich, Direktor Sergio Gut und den beteiligten Experten des Zivilstandsamtes sowie des Bestattungs- und Friedhofsamts (Profile siehe Anhang) für das Interesse an der Thematik und die wertvolle Zusammenarbeit.

- Alternativ bietet sich die Nutzung der Einwohnerregister für einen solchen Zweck, analog zum Vermerk «Hinterlegtes Testament» im Einwohnerregister der Stadt Zürich (TopaZ), der bei der Registrierung des Todesfalls einen Brief an das Notariat auslöst. Zu prüfen wäre die rechtlichen und technischen Voraussetzungen direkter Todesfall-Meldungen aus Einwohnerregistern an digitale Vererbungsdienste.
- Ebenfalls zu prüfen wäre die Rolle der Notare, Notariate oder sonstiger Institutionen, bei denen letztwillige Verfügungen hinterlegt sein können, und die unter Umständen von den Meldebehörden über Todesfälle benachrichtigt werden. Die Problematik der beschränkten Möglichkeiten des Erbrechts und der formgültigen Verfügung über den digitalen Nachlass wurde in Kapitel 6.1

detailliert beschrieben. Auch auf die Existenz eines zentralen elektronischen Testamentenregisters des Schweizerischen Notarenverbandes wurde hingewiesen. In diesem können jedoch lediglich Notare, Anwälte und amtliche Aufbewahrungsstellen die Existenz einer formgültigen letztwilligen Verfügung registrieren, nicht jedoch Private. Nichtsdestotrotz könnten Notariate, Notare oder sonstige mit der Vorsorgeplanung betraute Institutionen mit zunehmender Relevanz der Thematik eine Rolle in der digitalen Nachlassplanung spielen. Sei es, indem sie die digitale Nachlassplanung in eine formgültige letztwillige Verfügung einbetten (siehe Kapitel 6.1.3), und/oder indem sie mit digitalen Vererbungsdiensten kooperieren.

8. Lösungsansätze für den digitalen Nachlass

Die digitale Nachlassplanung und Willensvollstreckung ist ein Pionierfeld. Es existieren weder bewährte Geschäftsmodelle noch dem Medium Internet angepasste rechtliche Rahmenbedingungen, die es erlauben würden, perfekt durchdachte und zukunftssichere Lösungen zu entwerfen. Die in den vorangegangenen Kapiteln entworfenen Szenarien für den digitalen Nachlass, die Analyse der Praktiken der Plattformanbieter und insbesondere die detaillierte Bewertung der rechtlichen Handlungsmöglichkeiten bieten dennoch eine Grundlage, aktuell existierende Lösungsansätze fundiert zu beurteilen. Angesichts der Defizite und des geringen Reifegrades der digitalen Nachlassplanung wird deutlich, dass der Lösungsraum für den digitalen Nachlass weiter zu fassen ist. Kontrollverlust über

Daten beginnt bereits zu Lebzeiten. Wirksame und praktikable Ansätze setzen daher im «digitalen Alltag» an und helfen, Übersicht und Kontrolle über persönliche Daten zu bewahren.

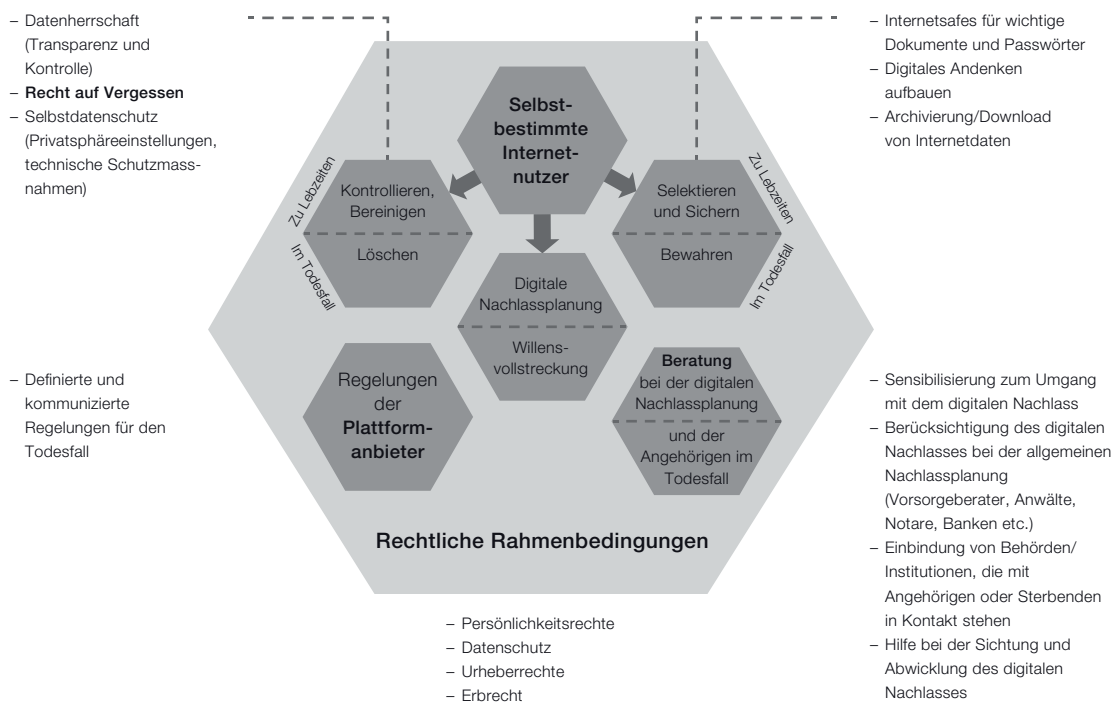
8.1 DER ERWEITERTE LÖSUNGSRAUM

Der erweiterte Lösungsraum, der im Rahmen des Forschungsprojekts entworfen wurde, stellt den selbstbestimmten Nutzer in den Mittelpunkt und schließt die Datenherrschaft zu Lebzeiten mit ein (Abb. 7).

Auch wenn der selbstbestimmte und eigenverantwortliche Internet-Nutzer im Zentrum aller Lösungsansätze steht, so entbindet dies die Plattformanbieter nicht von der Verantwortung, Regelungen für den Todesfall eines Mitglieds bzw. Kunden zu erarbeiten und zu kommunizieren.

Abb. 7

DER ERWEITERTE LÖSUNGSRAUM FÜR DEN DIGITALEN NACHLASS



Nicht zu vernachlässigen ist die Tatsache, dass die nachfolgend beschriebenen Möglichkeiten der digitalen Nachlassplanung, aber auch die Umsetzung der darin festgelegten Wünsche, gewisse Kompetenzen voraussetzen. Daraus ergibt sich ein **Bedarf an Beratung**, zum einen für Internetnutzer, die den digitalen Nachlass regeln wollen, und zum anderen für die Angehörigen, denen unter Umständen das Know-how im Umgang mit dem Internet und Social Media fehlt, um die Wünsche umzusetzen. Institutionen, die sich mit der Vorsorgeplanung befassen, werden nicht umhin kommen, diese Beratungskompetenz mit zunehmender Relevanz der Thematik aufzubauen.

Der erweiterte Lösungsraum umfasst zwei grundlegende Ansätze im selbstbestimmten Umgang mit dem digitalen Nachlass:

1. Instrumente der digitalen Nachlassplanung und Willensvollstreckung, die konkret den Aspekt der Weitergabe von Zugriffsdaten und von Instruktionen für den Not- und Todesfall adressieren:

- Digitale Vererbungsdienste (siehe Kapitel 8.2)
- Die Regelung des digitalen Nachlasses im Rahmen einer formgültigen letztwilligen Verfügung (siehe Kapitel 6.1.2 / erbrechtliche Handlungsmöglichkeiten)
- Die direkte Weitergabe von Zugriffsdaten an enge Vertraute («lifetime sharing»)

2. Massnahmen, die zu Lebzeiten im digitalen Alltag helfen Transparenz und Herrschaft über die im Internet gespeicherten Daten aufrecht zu erhalten, ohne den Aspekt der «Vererbung» zu adressieren:

2a. Selektieren, sichern und bewahren

- Passwortsafes und Online-Dokumentensafes, die helfen Zugriffsinformationen sowie wichtige Daten zu selektieren und somit für die alltägliche Nutzung (und potentiell auch für den Not- oder Todesfall) zu sichern
- Digitale Andenkendienste, die helfen zu Lebzeiten Daten für ein «digitales Vermächtnis» zu selektieren und für die Nachwelt zugänglich zu bewahren (siehe Kapitel 8.3)

- Archivierungswerkzeuge und Synchronisierungsdienste, die das Herunterladen und Sichern von Internetdaten unterstützen

2b. Kontrollieren, bereinigen und löschen

- Als konkrete Lösungsansätze für die Datenherrschaft zu Lebzeiten sind Massnahmen zum Selbstdatenschutz zu nennen, wie sie z.B. vom Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten empfohlen werden (EDÖB, o.J.) Dazu zählen Browsereinstellungen, Webfilter oder sonstige Massnahmen, um Datenspuren im Internet zu vermeiden.
- Schaffung und Umsetzung eines «Rechts auf Vergessen» im Internet (siehe Kapitel 6.3.5 und 8.4)

Tabelle 10 beurteilt die aufgeführten Lösungsansätze im Überblick. **Die dargestellten Defizite und Vorteile zeigen auf, dass die Kombination verschiedener Ansätze bereits heute wirksame Lösungen für den digitalen Nachlass bietet:** Wer einen digitalen Vererbungsdienst nutzt, schafft Transparenz und emanzipiert sich mit der Weitergabe der Zugriffsdaten im Todesfall bis zu einem gewissen Grad von der Verfügungsgewalt der Plattform-Anbieter. Wird dieser «digitale Wille» zusätzlich in ein konventionelles Testament integriert und allenfalls einem dedizierten Willensvollstrecker anvertraut, ist das Kriterium der Formgültigkeit erfüllt und somit die Wahrscheinlichkeit der Durchsetzbarkeit erhöht. Eine weitere erfolgsversprechende Kombination von Ansätzen stellen Passwort- und Dokumentensafes dar, die über eine Vererbungsfunktionalität verfügen und somit nicht nur das Management wichtiger Daten und Passwörter im Alltag unterstützen, sondern auch deren Weitergabe im Not- oder Todesfall (siehe Kapitel 8.1). Ob die aufgeführten Massnahmen im Konfliktfall (Erbstreitigkeiten, Konflikte mit Plattformanbietern) durchsetzbar sind, und welche Hürden für die formgültige Verfügung über den digitalen Nachlass bestehen, war Gegenstand der rechtlichen Analysen in Kapitel 6.

Tabelle 10

OPTIONEN IM UMGANG MIT DEM DIGITALEN NACHLASS

Optionen für die digitale Nachlassplanung

Zweck und Vorteile

Nachteile

1. Instrumente der digitalen Nachlassplanung und Willensvollstreckung

Digitale Vererbungsdienste
(siehe Kapitel 8.2)

- ➔ Transparenz und Zugriff: Ermöglichen die Hinterlegung existierender Internetkonten inklusive Zugriffsdaten und Wünsche für den Umgang mit den Konten/Profilen/Daten nach dem Tod
- ⬆️ Verfügungsgewalt durch Weitergabe der Zugriffsdaten an die Hinterbliebenen, d.h. geringe Abhängigkeit vom Plattformanbieter
- ⬆️ Tritt der Vererbungsdienst auch als Willensvollstrecker auf, können Daten gelöscht werden, ohne dass die Angehörigen Zugriff erhalten
- ⬆️ Know-how des Vererbungsdienstes zu Nachlassplanung, Willensvollstreckung und Praktiken der Plattformanbieter

- ⬇️ Keine Garantie, dass der Vererbungsdienst bis zum Tod existiert
- ⬇️ Kumulierte Zugriffsdaten können zum Sicherheitsrisiko werden, wenn der Anbieter die Daten nicht optimal sichert
- ⬇️ Mit der Willensvollstreckung bedachte Hinterbliebene müssen zu Lebzeiten instruiert werden
- ⬇️ Wenn der Vererbungsdienst nicht als Passwortsafe aktiv genutzt wird, veralten die Zugriffsinformationen
- ⬇️ Die hinterlegten Wünsche und Begünstigten genügen den Formerfordernissen an ein Testament nicht (Art. 505 ZGB: Handschriftlichkeit oder öffentliche Beurkundung)

Im Testament über den digitalen Nachlass verfügen und einen Willensvollstrecker einsetzen (siehe Kapitel 6.1)

- ⬆️ Erhöht die Wahrscheinlichkeit der Willensvollstreckung
- ⬆️ Formerfordernisse (Art. 505 ZGB: Handschriftlichkeit oder öffentliche Beurkundung) sind erfüllt
- ⬆️ Empfohlen insbesondere bei urheberrechtlich geschützten und somit erbrechtlich relevanten Datenbeständen
- ⬆️ Erleichtert unter Umständen die Durchsetzbarkeit gegenüber dem Plattformanbieter

- ⬇️ Die Persönlichkeit endet mit dem Tod. Testamentarische Verfügungen über Daten die unter das Persönlichkeitsrecht fallen, und erbrechtlich nicht relevant sind, sind unter Umständen nicht oder nur über Bedingungen durchsetzbar
- ⬇️ Zugriffsdaten im Testament veralten
- ⬇️ Mediengerechte, digitale Testamente sind in der Schweiz noch nicht möglich (Formerfordernis der Handschriftlichkeit)

Zugriffsinformationen und Wünsche bei einer Person des Vertrauens hinterlegen («lifetime sharing»)

- ⬆️ Unkompliziert
- ⬆️ Relevant insbesondere für Personen, die z.B. aufgrund einer schweren Erkrankung oder dem absehbaren Verlust der Urteilsfähigkeit Vorsorge treffen

- ⬇️ Begünstigte haben bereits zu Lebzeiten Zugriff auf die Daten
- ⬇️ Zugriffsdaten veralten

Last Message- /E-Mail- /Tweet-Dienste
(z.B. LastMessageClub.org)

- ➔ Erlauben die Hinterlegung von Abschiedsbotschaften, die nach dem Tod verschickt werden

- ⬇️ Kein sicheres Instrument für das Hinterlegen und postmortale Versenden von Zugriffsdaten

Tabelle 10

OPTIONEN IM UMGANG MIT DEM DIGITALEN NACHLASS

Optionen für die digitale Nachlassplanung

Zweck und Vorteile

Nachteile

2. Erweiterter Lösungsraum: Datenherrschaft und Transparenz zu Lebzeiten schaffen

Passwortsafes (lokale SW, Browser, USB oder im Internet)	↑ Zugriffsdaten bleiben aktuell, wenn der Passwortsafe zu Lebzeiten konsequent genutzt wird	↓ Lösen die Vererbungsproblematik nicht. Angehörige müssten Zugriff auf den Passwortsafe und das Masterpasswort erhalten ↓ Kumulierte Zugriffsdaten können zum Sicherheitsrisiko werden, wenn die SW/der Anbieter die Daten nicht optimal verschlüsselt und sichert ↓ Dokumente oder Anweisungen zum Umgang mit dem digitalen Nachlass können bei einem reinen Passwortsafe nicht hinterlegt werden
Dokumentensafes (z.B. preventix, SecureSafe)	➔ Sichere und geordnete Ablage von wichtigen Dokumenten in Online-Dokumentenspeichern	↓ Ohne integrierten Vererbungsmechanismus wird die Zugriffsproblematik im Todesfall nicht gelöst
Digitale Andenkendienste	➔ Helfen, wichtige Erinnerungstücke (z.B. Fotos, Musik, Texte), die im digitalen Nachlass untergehen würden, bewusst zu Lebzeiten zu selektieren und zugänglich zu machen	↓ Nur für einen kleinen Ausschnitt des digitalen Nachlasses relevant ↓ Lösen die Vererbungs- und Zugriffsproblematik für den Grossteil des digitalen Nachlasses nicht (Profile, E-Mail-Konten, etc.)
Archivierung / Downloads von Internetdaten (z.B SocialSafe, dataliberation)	➔ Lokale Sicherung von Internetdaten (Profile, E-Mails, Kontakte) ↑ Erleichtert im Todesfall unter Umständen den Zugriff auf die Daten über ein Endgerät des Verstorbenen	↓ Daten veralten rasch, falls keine laufende Synchronisation stattfindet ↓ Zugriff oder Löschen der Internet-Konten im Todesfall ist nicht gelöst
«Recht auf Vergessen» im Internet (Verfallsdaten für Daten und Profile im Internet, «Digitaler Radiergummi»)	↑ Setzen bei der Entstehung bzw. Speicherung der Daten an ➔ Bedingen, dass sich der Nutzer mit der Relevanz und Lebenszeit seiner Daten auseinandersetzt	↓ Wird von den Plattform- und Softwareanbietern noch nicht angeboten ↓ Aktuelle technische Lösungen sind nicht praktikabel und weisen Sicherheitslücken auf

8.2 DIGITALE VERERBUNGSDIENSTE

Seit etwa 2006 sind verschiedene Anbieter, die sich als «digitale Nachlassplaner», «digitale Vererbungsdienste» oder «Digital Estate Planner» bezeichnen im Internet aufgetaucht und in einigen Fällen auch rasch wieder verschwunden. Ziel dieser Dienste ist es, den digitalen Nachlass transparent und greifbar zu machen, indem sie die Hinterlegung folgender Informationen zu Lebzeiten unterstützen:

- **Zugriffsdaten** (Username und in der Regel Passwort) für Internet-Konten (Facebook, Gmail etc.) und sonstige zugriffsgeschützte Datenbestände
- **Anordnungen oder Wünsche**, was mit dem jeweiligen Konto/Profil/Datenbestand im Todesfall geschehen soll
- **Vertrauenspersonen**, die den Todesfall melden, die Zugriffsdaten erhalten und die Wünsche des Verstorbenen ausführen sollen. Sie können sich mit den Zugriffsdaten in die jeweilige Plattform einloggen und beispielsweise ein Profil eigenhändig löschen, ohne den Todesfall an den Plattform-Anbieter melden zu müssen

Diese Grundfunktionalitäten sind den existierenden digitalen Vererbungsdiensten gemeinsam. Jedoch gibt es in der Umsetzung durch die Anbieter **unterschiedliche Ausprägungen und Varianten von Geschäftsmodellen**:

a. Nach Art der hinterlegten Daten und Informationen:

In der Regel werden Name und URL sowie Username und Passwort des Kontos verschlüsselt hinterlegt. Bestimmte Dienste, wie z.B. Ziggur.me, ermöglichen lediglich die Ablage des Benutzer-Namens bzw. der E-Mail-Adresse, die mit dem Konto verknüpft ist. Die Ablage des kompletten Logins garantiert den unkomplizierten Zugriff für die Begünstigten im Todesfall, vorausgesetzt die hinterlegten Passwörter wurden laufend aktuell gehalten. Allerdings sind die Sicherheitsgarantien des Dienstes kritisch zu prüfen, da die Ablage aller Zugriffsdaten an einem Ort ein hohes Sicherheitsrisiko darstellt.

Zusätzlich zur Hinterlegung der Zugriffsdaten ermöglichen manche Dienste die Ablage von Dateien. Der Schweizer Anbieter preventix.ch unterstützt neben der Hinterlegung von Passwörtern, den Upload wichtiger Dokumentkopien und Informationen (z.B. Ausweisdaten, Policen, Verträge, Patientenverfügung etc.) und wird so zur virtuellen Vorsorge- und Notfallmappe. Der Dienst kann durch seine vorgegebene Ordnerstruktur (Abdankung, Bestattung, Testament etc.) sowie die bereitgestellten Formulare und Vorlagen (z.B. Organspendeausweis, Patientenverfügung) wie eine Checkliste für die Vorsorge für den Not- und Todesfall genutzt werden.

Abb. 8

LEGACY LOCKER: HINTERLEGUNG VON ZUGRIFFSDATEN

Add a new digital asset

This digital asset is a...

Name your digital asset (ex: gmail)

Digital Asset Website/URL (ex: www.gmail.com)

My username is (ex: jtoeman)

My password is (ex: 12345) [Why this is safe](#)

[Show password!](#)

Add any notes or directives about this digital asset

b. Nach der Zuständigkeit für die Willensvollstreckung

Im in Abbildung 10 dargestellten Beispiel von Ziggur.me ermöglicht die «Keep private»-Funktion dem Kunden, bestimmte Konten nicht an die Hinterbliebenen zu melden. Dies könnte beispielsweise im Fall eines E-Mail Kontos zum Schutz der Privatsphäre auch über den Tod hinaus gewünscht sein. Will der Kunde dennoch sicherstellen, dass dieses Konto gelöscht wird, kann er Ziggur.me als «digitalen Willensvollstrecker» beauftragen, das heisst nicht die Angehörigen, sondern der Vererbungsdienst setzt die Wünsche des Verstorbenen um. Diese Form der erweiterten Dienstleistung ist wenig verbreitet. Ziggur.me kann ihn anbieten, da keine Passwörter hinterlegt sind, sondern Kooperationen mit den grossen Internet-Plattformen genutzt werden, um die Wünsche ausführen zu lassen. Anbieter wie Legacy Locker oder SecureSafe betreiben bewusst keine Willensvollstreckung, da ihnen die zugrundeliegenden Sicherheitsmechanismen jeglichen Zugriff auf die hinterlegten Daten zu Lebzeiten und im Todesfall verunmöglichen. Willensvollstrecker sind in diesem Fall die hinterlegten Vertrauenspersonen oder Begünstigten, die vom Kunden zu Lebzeiten über ihre Rolle informiert sein müssen. Als Begünstigte müssen nicht zwangsläufig Hinterbliebene benannt werden. Denkbar wäre auch einen sonstigen Kontakt, der mit dem Nachlass betraut ist (z.B. Anwalt, Notar) zu hinterlegen und mit der digitalen Willensvollstreckung zu beauf-

tragen. Dieser könnte zudem sicherstellen, dass die digitale Nachlassplanung zusätzlich in einem formgültigen Testament festgehalten wird, um die Wahrscheinlichkeit der Durchsetzbarkeit im Konfliktfall zu erhöhen.

Abb. 10

ZIGGUR.ME: EINGABEMASKE FÜR WÜNSCHE BETREFFEND FACEBOOK-PROFIL

My Profile **Network Profiles** Entrusted People More Services

Add network profile

On this page you can add an online profile and indicate your wishes regarding this profile. We use the e-mail address linked to this online profile as your unique identification. This is why it's important to have a verification e-mail sent to the address you entered. This e-mail allows you to confirm that your details are correct with just one click.

Mark this profile as private

A Ziggur account allows you to keep certain profiles private. This means that Ziggur will never divulge the existence of these profiles to your trusted representatives or your surviving relatives. If you have a free Ziggur account, nothing will be done with these online profiles after you are deceased. If you have a Ziggur Plus account, Ziggur will carry out your wishes relating to these profiles without informing your surviving loved ones.

Facebook

My current email address for this website

My wishes for this profile after my death

Do not take action
 Close my account
 Memorialize my account
 Keep it private

Save Cancel

«Damit man seine digitalen Werte pflegt, braucht man einen täglichen Nutzen. SecureSafe hat hierfür den Passwort- und Dokumentensafe geschaffen und auch via Mobile App zur Verfügung gestellt. Im SecureSafe kommen die Benutzer erstmalig mit Datenvererbung in Kontakt. Es braucht aber wohl noch ein paar Jahre, bis sich Nutzen und Notwendigkeit der Datenvererbung auch ausserhalb von Anwendungen wie SecureSafe durchsetzt.»

c. Nach Art des Vorgehens im Todesfall

Im Todesfall muss der Vererbungsdienst darüber in Kenntnis gesetzt werden, damit die beauftragten Begünstigten in einem nächsten Schritt Zugriff auf die hinterlegten Zugriffsdaten und gegebenenfalls Dokumente erhalten und den Willen vollstrecken können. Bei den momentan verfügbaren Diensten können drei Formen der Auslösung der digitalen Vererbung unterschieden werden, die alle voraussetzen, dass die auslösende Partei im Vorfeld vom Verstorbenen über die digitale Nachlassplanung und ihre Rolle in diesem Prozess informiert wurde, sei es persönlich und/oder über eine E-Mail-Benachrichtigung vom Vererbungsdienst:

1. Die hinterlegte Vertrauensperson meldet den Todesfall beim digitalen Vererbungsdienst zusammen mit einer Todesurkunde oder einem sonstigen amtlichen Nachweis. Manche Vererbungsdienste, z.B. Legacy Locker erfordern zwei Vertrauenspersonen, um den Todesfall unabhängig voneinander zu bestätigen.
2. Der Vererbungsdienst arbeitet mit einer Behörde oder einem amtlichen Register zusammen, bei dem die Existenz der digitalen Nachlassplanung registriert ist, und der den Todesfall an den Vererbungsdienst meldet. Der Schwedische Anbieter Mywebwill, der nicht mehr aktiv ist, hatte eine solche Kooperation mit dem schwedischen Einwohnerregister. Schwedische Kunden konnten sich mit der eindeutig identifizierenden Personenummer bei Mywebwill registrieren und dort den digitalen Nachlass planen. Die Meldung des Todesfalls eines registrierten Nutzers vom Einwohnerregister an Mywebwill erfolgte auf dieser Grundlage automatisch. Die eidgenössische Zivilstandsverordnung bietet momentan keine rechtliche Grundlage für derartige Meldungen an nicht-amtliche Stellen, ohne dass die Angehörigen diese bestellen und übergeben (siehe Kapitel 7). Eine andere Art der Kooperation mit Registern versucht der niederländische Anbieter Ziggur.me zu etablieren. Ziggur.me kooperiert mit Notaren und nimmt Kunden auf Wunsch in das Ziggur.me Notariatsregister auf. Notare, die das Register nutzen, können prüfen, ob eine digitale Nachlassplanung vorliegt und den Todesfall an Ziggur.me melden.

3. Ein Bevollmächtigter erhält vom Kunden des Vererbungsdienstes zum Zeitpunkt der Nachlassplanung einen Aktivierungscode und Instruktionen, wie im Todesfall vorzugehen ist. Im Todesfall löst der Aktivierungsbevollmächtigte durch Eingabe des Codes beim Vererbungsdienst den Prozess aus. Der Vererbungsdienst versucht, innerhalb einer vordefinierten Sperrfrist den mutmasslich verstorbenen Kunden zu kontaktieren. Erfolgt kein Wiederruf wird der digitale Vererbungsprozess ausgelöst. Bei diesem Prinzip, das bei SecureSafe zum Einsatz kommt, ist keine Todesurkunde als Nachweis notwendig.

Anbieterlandschaft «digitale Vererbung»

Das Themenportal «The Digital Beyond» stellt, ohne Anspruch auf Vollständigkeit, eine Liste von digitalen Vererbungsdiensten, Last-E-Mail-Diensten und Online-Gedenkstätten bereit, die sich international in diesem jungen Geschäftsfeld bewegen (The Digital Beyond, 2012). Die sechzehn gelisteten Dienste, die digitale Nachlassplanung anbieten, wurden mehrheitlich in den Jahren 2008 bis 2010 gegründet. Mit Gründungsdatum 2011 sind lediglich zwei neue Anbieter für digitale Nachlassplanung hinzugetreten. Drei der aufgeführten Anbieter haben ihren Dienst bereits wieder eingestellt (z.B. Mywebwill), wurden akquiriert (z.B. Entrusted von SecureSafe) oder sind offline und kündigen einen Release an (z.B. MentoMori). Es entsteht der Eindruck, dass die erste Gründungswelle vorüber und eine gewisse Ernüchterung und Konsolidierung eingetreten ist. Sofern der Vererbungsdienst nicht in ein breiteres Angebot eingebettet ist, das bereits zu Lebzeiten Nutzen verspricht, oder ein Investor bzw. eine Muttergesellschaft den Dienst trägt, scheint das Überleben insbesondere in Europa und nationalen Märkten momentan noch schwierig. So steht hinter dem niederländischen Anbieter Ziggur.me die Marketingagentur Calanza. SecureSafe der DSwiss AG (Zürich) bietet Datenvererbung als Funktionalität im Rahmen eines sicheren Online-Dokumenten- und Passwortsafe an, der bereits zu Lebzeiten aktiv genutzt wird.

Preisgestaltung

Viele digitale Vererbungsdienste bieten eine Gratis-Version an, die funktional oder zeitlich eingeschränkt ist. So kann man in einem SecureSafe «Free Account», 50 Passwörter und 10 MB Dateien ohne zeitliche Begrenzung speichern. Es kann jedoch nur ein Begünstigter für die Datenvererbung hinterlegt werden, und diverse fortgeschrittene Funktionalitäten stehen nicht zur Verfügung. Die kostenpflichtigen Accounts werden, wie bei anderen Online-Speichern,

aufgrund der erweiterten Speicherkapazität und zusätzlicher Funktionalität angeboten. Die Preise reichen von CHF 1.50 bis CHF 12.– pro Monat (Stand Juni 2012). Auch Ziggur.me lässt gratis Konten eröffnen, allerdings wird Ziggur.me bei dieser Variante nicht als Willensvollstrecker aktiv. Die kostenpflichtige Version schliesst die Willensvollstreckung und die Registrierung im Notariatsregister ein. Beim Abonnement kann zwischen monatlich (EUR 19.90) oder lebenslänglich (EUR 199.–) gewählt werden. Ähnliche Modelle bieten Legacy Locker (USD 29.99 jährlich, USD 299.99 lebenslang) und preventix.ch. Preventix offeriert eine funktional eingeschränkte basic-Variante für CHF 78.–jährlich und CHF 780.– auf Lebenszeit und die premium-Variante mit voller Funktionalität für CHF 130.– jährlich und CHF 1 300.– auf Lebenszeit (Stand Juni 2012). Zusätzlich erhebt preventix eine einmalige Registrierungsgebühr (CHF 90.– bzw. CHF 150.–).

Anforderungen und Erfolgsfaktoren

Eine Grundanforderung an einen digitalen Vererbungsdienst ist, dass er noch besteht, wenn der nachlassplanende Kunde verstirbt. Angesichts des Zeithorizonts der digitalen Nachlassplanung kann das Überleben des digitalen Vererbungsdienstes in keinem Fall garantiert werden. Vertraute man seine digitale Nachlassplanung einem Startup an, das unter Umständen in wenigen Jahren den Dienst wieder einstellt, werden die Daten im günstigsten Fall sorgfältig vernichtet oder auf Wunsch an einen anderen Dienst übertragen, der die Dienstleistung fortführt. Ebenso kann der Dienst plötzlich offline und nicht mehr erreichbar sein, der Verbleib der Daten ist ungewiss und die bereits bezahlten monatlichen, jährlichen oder gar lebenslangen Gebühren bleiben ohne Gegenleistung. Die Tragfähigkeit des Geschäftsmodells und die Unternehmensgrösse, können Hinweise auf die **Überlebenswahrscheinlichkeit und Zuverlässigkeit** des Dienstes sein. Eine Überlebensgarantie gibt es letztlich nicht.

Sicherheit ist ein entscheidendes Kriterium, das für Techniklaien nur schwer zu überprüfen ist. Alle Anbieter bezeichnen ihre Dienste als sicher. Ob die Verschlüsselung der Daten ausreicht, die Infrastruktur hohe Sicherheitsanforderungen erfüllt, und ob der Anbieter keinerlei Zugriff auf die Daten hat, ist sorgfältig zu prüfen, bevor alle Zugriffsdaten bei einem Dienst abgelegt werden.

Aus den **Nutzungsbedingungen** und **Datenschutzrichtlinien** des Vererbungsdienstes sollte klar hervorgehen, dass der Kunde die Rechte an den Daten behält und der Vererbungsdienst die Daten alleinig für den vorgesehenen Zweck speichert und verarbeitet. Wünschenswert sind zudem Mechanismen, die es dem Kunden ermöglichen, den Wunsch nach Privatsphäre in der digitalen Nachlassplanung umzusetzen, z.B. indem er den digitalen Vererbungsdienst als Willensvollstrecker für bestimmte Konten einsetzt (z.B. E-Mail-Konto löschen) oder bestimmte Konten als privat und nicht für die Begünstigten zugänglich deklarieren kann.

Zweckmässigkeit ist gefordert im Sinne einer benutzerfreundlichen Bedienungsfläche für die einfache Hinterlegung der Daten, aber insbesondere bei der unkomplizierten Abwicklung für die Angehörigen im Todesfall. Falls nicht automatisiert, wie z.B. durch den Aktivierungscode bei SecureSafe, so zumindest durch durchdachte Prozesse und einen gut organisierten Kundendienst, der die Angehörigen beratend unterstützt.

Ein zentraler Faktor, der die Erfolgswahrscheinlichkeit des Vererbungsdienstes erhöht, ist, ob der Dienst nicht nur für die digitale Nachlassplanung und im Todesfall genutzt wird, sondern darüber hinaus einen **Mehrwert zu Lebzeiten** bietet, wie etwa die sichere digitalisierte Ablage von wichtigen Dokumenten oder ein Passwortsafe, der auch für die Passwortverwaltung im Alltag genutzt und somit laufend aktuell gehalten wird.

«Der Gebrauch von Online-Diensten für die Speicherung von wichtigen oder persönlichen Informationen wird zweifelsfrei weiter zunehmen. Dadurch wird das Bedürfnis, diese Informationen gezielt, einfach und sicher an Dritte zu vererben an Bedeutung gewinnen. Im Idealfall bietet der Dienst selbst eine entsprechende Vererbungsfunktion an (z.B. SecureSafe) und es ist denkbar, dass die Verfügbarkeit einer solchen Funktion in Zukunft einen Wettbewerbsvorteil im Konkurrenzkampf der verschiedenen Dienstanbieter darstellt.»

8.3 BEWAHREN – DIGITALE ANDENKENDIENSTE

Neben «Online-Memorial-Diensten», die es trauernden Angehörigen ermöglichen, eine Gedenkstätte im Internet einzurichten, gibt es Dienste, die den Aufbau eines «digitalen Andenkens» zu Lebzeiten unterstützen. Ziel ist die eigenhändige Selektion von wesentlichen digitalen Inhalten und Stationen im Leben, die ansonsten in der Menge des digitalen Nachlasses untergehen würden. Während einige Social-Media-Dienste, dieses Bedürfnis erkannt und als Feature eingebaut haben (z.B. Facebook Timeline), haben die nachfolgenden Beispiele das «digitale Andenken» zum Geschäftsmodell gemacht:

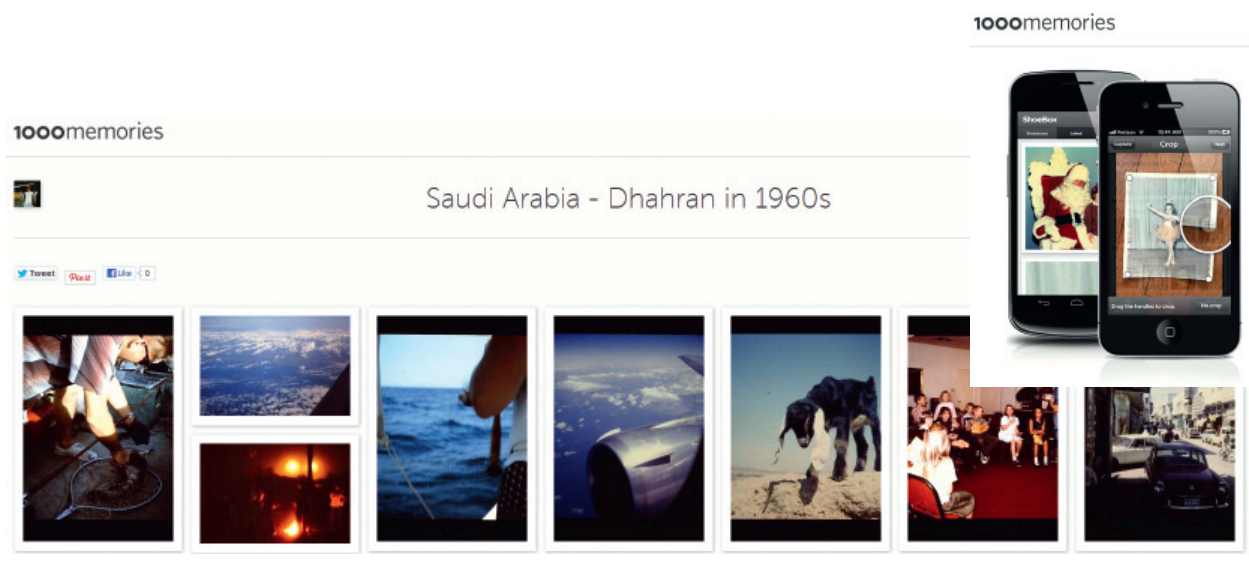
- Lifonaut (Bristol, VT): Ein Dienst der Stiftung Terasem, die sich der «digitalen Unsterblichkeit» verschrieben hat. Lifonaut ermöglicht in einem «Mindfile»-Speicher, diverse Informationen (Fotos, Dokumente etc.) bis hin zur tiefgefrorenen DNA-Probe zu hinterlegen. Hintergrund ist der Glaube, dass mittels dieser Informationen irgendwann in der Zukunft die Identität repliziert und sogar in einen, wie auch immer gearteten Körper «geladen» werden kann.

- Virtual Eternity (Huntsville, AL): Unterstützt die interaktive Programmierung eines «Intellitar», eines Avatars, der möglichst «lebensecht» die eigene Persönlichkeit, Aussehen, Stimme und Lebenserfahrungen widerspiegelt. Technische Grundlage ist die Intelligent Avatar Plattform, die auf Spracherkennungs- und Künstlicher Intelligenz-Technologie aufbaut.

- 1000memories (San Francisco, CA): Bietet sich an als «digitale Schuhschachtel» (ShoeBox), die sich auf die Bewahrung und thematische Zusammenstellung alter, d.h. nicht digitaler Fotos, spezialisiert hat. iPhone- und Android-Apps unterstützen die Digitalisierung alter Fotos. Digitale Fotos können ebenfalls in die «ShoeBox» hochgeladen werden. Zugriffsberechtigungen (privat, Gruppen, öffentlich) können für jede ShoeBox vergeben werden. Keine reiner Andenkendienst, sondern ein Online-Fotoalbum, dass sich durch die Scan-App für analoge Fotos anbietet, Lebensstationen zu dokumentieren.

Abb. 11

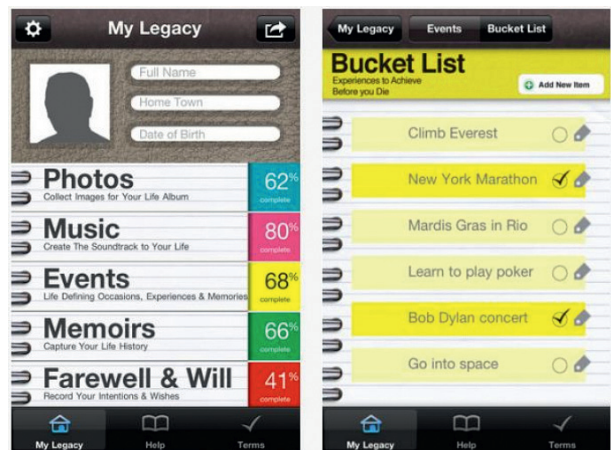
1000MEMORIES: BEISPIEL EINER SHOEBOX SITE UND APP



- Chronicle of Life (Santa Cruz, CA): Unterstützt die Hinterlegung eines «digitalen Andenkens», d.h. Fotos, Dokumente, Botschaften sowie die Führung eines Tagebuches.
- Legacy Organiser (UK): iPhone App der Epitapp Ltd., die es ermöglicht wesentliche Erinnerungen in Form von Fotos, Musik oder Notizen festzuhalten. Die «Bucket List» soll sicherstellen, dass kein Lebenstraum unerledigt bleibt. Abschiedsbotschaften und Nachlassplanung sind zusätzliche Funktionen.

Abb. 12

LEGACY ORGANISERS IPHONE APP



Quelle: iTunes

8.4 LÖSCHEN – LÖSUNGSMÖGLICHKEITEN FÜR EIN RECHT AUF VERGESSEN

Das Internet und seine Innovationen haben ein Vergessen, im Sinne einer endgültigen und vollständigen Löschung von Informationen, fast unmöglich gemacht. Das Internet ist zu einer «riesenhaften Erinnerungs- und Kopiermaschine aus sozialen Netzwerken, Wikis, Weblogs, Websites, online verfügbaren Nachrichten, Filmen und Fotos» geworden (Pörksen, 2012). Ein Bild, das einmal in sozialen Netzwerken geteilt und in den Caches der Suchmaschinen gespeichert wurde, ist, wenn überhaupt, nur mit grossen Mühen wieder zu spurlos zu beseitigen. Aber auch die alltägliche «Datenhygiene» ist nicht selbstverständlich. Während besonders wichtige Informationen im besten Fall speziell gesichert werden, geht das Löschen von veralteten Daten vergessen. Regelmässiges Aussondern, wie es physische Bücherregale und Kommodenschubladen verlangen, ist im Internet angesichts sinkender digitaler Speicherkosten und verteilter Datenablagen nicht zwangsläufig Bestandteil des «Online-Alltags».

Es liegt nahe, dass man die Technologien, die das grenzenlose Abspeichern und unüberlegte Streuen von Informationen ermöglichen, auch für das «digitale Vergessen» einsetzt. Nachfolgend sind Lösungsansätze diskutiert, die jedoch noch weit von einem flächendeckenden Einsatz und der Verankerung im Alltag entfernt sind. Kritisch für die Akzeptanz ist die Praktikabilität dieser Mechanismen. Selbst wenn die rechtlichen Grundlagen für ein Recht auf Vergessen im Internet geschaffen sind (siehe Kapitel 6.3.5), funktioniert das «digitale Vergessen» erst, wenn Anbieter- und Nutzerseite ihre Verantwortung wahrnehmen, sowie alltagstaugliche Techniken und Praktiken für das einfache, zuverlässige Aussondern von Daten zum Einsatz kommen.

Verfallsdatum für digitale Daten

Eine naheliegende Lösung wäre ein Verfallsdatum für Informationen, wie es (Mayer-Schönberger, 2010, p.210ff) skizziert. Das Verfallsdatum könnte z.B. einem Dokument, einer Bilddatei, einem Blogbeitrag oder gar einem Konto

bereits bei der Erstellung beziehungsweise Speicherung oder Veröffentlichung auf einer Social-Media-Plattform als Metainformation mitgegeben werden. Denkbar wäre, dass der Urheber oder Verteiler das Verfallsdatum festlegt, oder dass die Information automatisch mit einem Verfallsdatum versehen wird, ausgehend von einem voreingestellten Standardwert für die Lebensdauer. Revisions sichere Records Management Systeme und bestimmte Speichermedien erlauben seit langem die automatische fristgesteuerte Löschung von Daten. Auch die automatische Vergabe von Metainformationen ist bereits Standard (z.B. Versandzeitpunkt einer E-Mail oder Erstellungsdatum oder Autor in den Dokumenteneigenschaften eines Textverarbeitungsprogramms). Solche Metadaten schemata um ein festgelegtes oder automatisch berechnetes Verfallsdatum zu erweitern, ist technisch relativ einfach zu realisieren. Fraglich ist die Notwendigkeit einer gesetzlichen Grundlage, die Softwarehersteller oder Plattformbetreiber verpflichtet, solche Mechanismen zur Durchsetzung eines «Rechts auf Vergessen» zwingend in ihre Angebote einzubauen, oder ob es den Anwendern überlassen wird, spezielle Werkzeuge für die Vergabe von Verfallsdaten einzusetzen. Beide Wege setzen voraus, dass sich Menschen, die Informationen erstellen, speichern und im Internet teilen, mit der Lebensdauer und somit der Relevanz dieser Informationen bewusst auseinandersetzen und entsprechend handeln. (Mayer-Schönberger, 2010, p.203) hält diesen Aspekt für sehr viel kritischer als die technische Umsetzung des Verfallsdatums. Ein solches selbstbestimmtes Verfallsdatum greift jedoch nur bei bewusst gespeicherten oder geteilten Informationen, nicht aber bei Informationen, die bei der Internetnutzung in Form von Registrierungen, Suchabfragen oder sonstiger Profil- und Bewegungsdaten unbewusst oder gezwungenermassen hinterlassen werden. (Mayer-Schönberger, 2010, p.213) stellt klar, dass die «Wiederbelebung des Vergessens» durch Verfallsdaten «keine Lösung des Datenschutzproblems» darstellen kann.

Selbsterstörende Daten und digitale Radiergummis

Die zeitgesteuerte nicht wiederherstellbare Löschung von Daten ist eine Herausforderung, mit der sich IT Sicherheitsexperten schon seit langem auseinandersetzen. So wurde «Vanish» als Daten-Selbsterstörungsmechanismus zunächst für elektronische Nachrichten an der Universität Washington entwickelt (Markoff, 2009). «Vanish» basiert auf sogenannten VDOs (vanishing data objects), d.h. auf verschlüsselten Datenelementen, die nur für einen definierten Zeitraum lesbar und anschliessend nicht mehr rekonstruierbar sind. Der Verschlüsselungs-Algorithmus wurde jedoch kurz nach seiner Ankündigung umgangen und bereits zerstörte VDOs konnten wiederhergestellt werden (Felten, 2009).

Ebenfalls auf Verschlüsselung basiert der digitale Radiergummi «X-pire», der vom deutschen Verbraucherschutzministerium propagiert wurde (Die Zeit, 2011). Mit X-pire können Personen, die Bilder im Internet (z.B. in Facebook, Flickr) teilen wollen, diese vorab mit «X-pire» verschlüsseln und den Schlüssel zusätzlich mit einem Verfallsdatum für das Bild versehen. Das so verschlüsselte Bild kann entschlüsselt und betrachtet werden, solange das Verfallsdatum nicht erreicht ist. Mit Erreichen des Verfallsdatums ist das Bild nicht mehr abrufbar (Backes, 2011). Aber auch X-Pire ist bereits Gegenstand der Kritik in Sachen Sicherheit und Praktikabilität (Ruef, 2011).

Benachrichtigung zur Überprüfung auf Aktualität

Ein Ansatzpunkt, der bereits genutzt wird, sind Aufforderungen zur Überprüfung von Informationen auf Aktualität. So erinnern Wiki-Plattformen ihre Autoren in regelmässigen Abständen, Artikel zu prüfen und gegebenenfalls zu löschen oder zu aktualisieren (Karla, 2010, p.2). Auch hier mangelt es nicht an der technischen Möglichkeit, sondern an der Umsetzung durch die Plattformbetreiber und vor allem an Praktikabilität. Der Ansatz funktioniert nur für klar begrenzte Informationsbestände. Die Massen und Vielfalt an produzierten und verteilten Informationen aktiv regelmässig auf Aktualität zu überprüfen, kann kein Mensch leisten.

Durchsetzbarkeit und gesetzliche Grundlagen

Die Lebensdauer und der Schutz von Daten im Internet sind nicht primär technische Probleme. Technologien können jedoch wirksame Hebel für die Durchsetzbarkeit eines Rechts auf Vergessen im Internet darstellen, vorausgesetzt sie sind praktikabel und garantieren die unwiderrufliche Löschung. Dies entspricht dem Prinzip «Privacy by Design» (Cavoukian, 2009), das auch im Grundsatzpapier «A Digital Agenda for Europe» (European Commission, 2010) vertreten wird. Es fordert, Datenschutz und die Privatsphäre in den gesamten Lebenszyklus von Informationstechnologien und Informationen einzubetten, vom Entwurf bis hin zur Vernichtung. Eine solche Konkretisierung erfordert nicht nur Bereitschaft und Druck von Seiten der Internetnutzerschaft, sondern eine Überprüfung und gegebenenfalls Anpassung gesetzlicher Grundlagen, wie sie in der Schweiz aktuell diskutiert wird (siehe Kapitel 6.3.5).

Die Lebensdauer und der Schutz von Daten im Internet sind nicht primär technische Probleme. Technologien können jedoch wirksame Hebel für die Durchsetzbarkeit eines Rechts auf Vergessen im Internet darstellen, vorausgesetzt sie sind praktikabel.

8.5 ENTSCHEIDEN – BERATUNG BEI DER DIGITALEN NACHLASSPLANUNG UND WILLENSVOLLSTRECKUNG

Angesichts des geringen Reifegrads der digitalen Nachlassplanung und der unterschiedlichen beziehungsweise grösstenteils nicht existenten Regelungen von Plattformanbietern spielt die Beratung bei der digitalen Nachlassplanung und Willensvollstreckung eine wichtige Rolle. Auch die Gespräche im Rahmen der Forschungsarbeiten mit Institutionen und Personen, die täglich mit Sterbenden oder Hinterbliebenen zu tun haben, haben gezeigt, dass Aufklärung und Beratung ein wesentliches Element des Lösungsraums für den digitalen Nachlass darstellen. Dies können Hilfestellungen in Form von Aufklärung und Informationen von Behörden oder Dienstleistern (z.B. EDÖB, Sterbe-Vorsorgeberatern, Anwälten, Notaren, Bestattungsjämtern) zu Lebzeiten oder bei Meldung des Todesfalls sein, oder eine Dienstleistung, die Hinterbliebene bei der Sichtung und Abwicklung des digitalen Nachlasses unterstützt. Beratungs- und Aufklärungsbedarf wurde in den nachfolgenden Bereichen identifiziert.

Sensibilisierung der Internetnutzer für die Relevanz der digitalen Nachlassplanung und die möglichen Konsequenzen, wenn der digitale Nachlass ungeregelt bleibt

Das Bewusstsein über die Relevanz des digitalen Nachlasses und die Möglichkeiten der digitalen Nachlassplanung ist in der Bevölkerung noch sehr gering ausgeprägt. Es steht selbstverständlich jedem frei, den eigenen digitalen Nachlass als so geringwertig einzustufen, dass er ungeregelt bleiben kann (siehe auch Kapitel 4.1 «Die Grundsatzentscheidung: digitale Nachlassplanung ja oder nein»). Gespräche zur Thematik zeigen jedoch, dass sich kaum jemand bewusst Gedanken macht, welche Konten, Daten und Spuren er oder sie im Internet bereits angesammelt

hat, und was es für die Angehörigen und das eigenen Andenken bedeuten kann, wenn diese im Todesfall fortbestehen. «Will ich nach meinem Tod weiterhin als Freund oder Kontakt in Sozialen Netzwerken vorgeschlagen werden? Und wie werden die Hinterbliebenen dies empfinden? Haben meine Angehörigen nach meinem Tod die Möglichkeit, an alle wichtigen Dokumente, Fotos, Adresslisten etc. zu gelangen?» (siehe Kapitel 4.2 «Welche Szenarien gilt es durch die digitale Nachlassplanung zu vermeiden?»). Wünschenswert ist eine informierte Entscheidung, ausgehend vom Wissen über:

- Die Gesamtheit und Relevanz eigenen Internetaktivitäten, d.h. Konten, Profile, Datenspeicher etc. (siehe Kapitel 2.1 «Vom E-Mail-Konto zur digitalen Identität – Welche Daten sammeln sich im Laufe eines Lebens an?»)
- Die Möglichkeiten der digitalen Nachlassplanung (siehe Kapitel 8.1 «Der erweiterte Lösungsraum»)
- Die Praktiken der Plattformanbieter (siehe Kapitel 5). Um bei einem digitalen Vererbungsdienst und/oder in einem Testament umsetzbare Wünsche für den digitalen Nachlass formulieren zu können, muss die nachlassplanende Person zum Zeitpunkt der Planung die Möglichkeiten kennen, die die Plattformanbieter zulassen (z.B. Löschen, Stilllegen, Gedenkstatus).

Ansatzpunkte für eine solche Sensibilisierung und konkrete Hilfestellungen bieten die Informationsangebote, Ratgeber und Vordrucke z.B. von Konsumentenschutzorganisationen oder Seniorennetzwerken, die um die digitale Nachlassproblematik erweitert werden könnten.

Auch die Aufklärung und konkrete Unterstützung zu den Themen Datenherrschaft und Selbstdatenschutz zu Lebzeiten spielt in diesen Zusammenhang eine Rolle (EDÖB, o.J.). Die Bereitschaft, sich mit der digitalen Nachlassplanung auseinanderzusetzen, setzt letztlich voraus, dass bereits zu Lebzeiten ein Bewusstsein für die im Internet gespeicherten Daten und Spuren und deren Verwendung besteht.

Beratung bei der digitalen Nachlassplanung

Wie die Analyse der rechtlichen Handlungsmöglichkeiten gezeigt hat, ist die formgültige Verfügung über den digitalen Nachlass momentan nur bedingt möglich (siehe Kapitel 6.1.2). Um die Wahrscheinlichkeit der Durchsetzbarkeit zu erhöhen, braucht es Fachwissen über die erbrechtlichen Handlungsmöglichkeiten und die Rechtsnatur des digitalen Nachlasses. Je relevanter der digitale Nachlass wird, desto grösser wird der Bedarf an kompetenter Beratung zur digitalen Nachlassplanung werden. Institutionen oder Berufsgruppen, die bereits in der Vorsorgeberatung aktiv sind (z.B. Sterbe-Vorsorgeberater, Banken, Anwälte, Notare), könnten sich dieses neue Tätigkeitsfeld erschliessen, vorausgesetzt sie haben das notwendige Know-how zu den Möglichkeiten und Grenzen der digitalen Nachlassplanung und Willensvollstreckung.

Beratung der Plattformanbieter bei der Formulierung von Regelungen im Todesfall

Die Analyse der Nutzungsbedingungen und Praktiken hat gezeigt, dass nur die grossen internationalen Plattformen Regelungen zum Vorgehen im Todesfall online publiziert haben. Für die digitale Nachlassplanung, aber insbesondere für die Angehörigen im Todesfall, wäre es wünschenswert, wenn auch grosse nationale oder regionale Anbieter in der Schweiz solche Regelungen definieren und einfach zugänglich machen würden.

«Im Wachstumsmedium Internet sind die Anbieter nicht auf sterbende Nutzer und Kontakte mit trauernden Angehörigen und Freunden vorbereitet. Deshalb benötigen die Plattformen eine Beratung, wie sie sich in der Nutzerfreundlichkeit und im Service auf den Tod einstellen können. Die Angehörigen beraten wir über Funktionsweisen und Spielregeln der Internetwelt und wie man sich in Zeiten der Trauer dort unbeschadet bewegt.»

Birgit Aurelia Janetzky, Geschäftsführerin Semno.de

Beratung der Angehörigen im Todesfall

Im Rahmen der Forschungsarbeiten haben das Bestattungs- und Friedhofsamt sowie das Zivilstandsamt der Stadt Zürich Einblick in die Bearbeitung, Meldung und Beurkundung von Todesfällen sowie die Beratung von Angehörigen gewährt. Auch wenn der digitale Nachlass in dieser frühen Phase nicht im Vordergrund steht, besteht dennoch die Möglichkeit, Informationen (z.B. in Form eines Info-Flyers über die digitale Nachlassabwicklung) abzugeben, die zu einem späteren Zeitpunkt hilfreich sein können. Auch Einrichtungen, die mit der Palliativpflege betraut sind, haben signalisiert, dass sie für derartige Informationen offen sind.

Einen weiteren Lösungsansatz, der Angehörigen bei der Regelung des digitalen Nachlasses unterstützt, hat der momentan nur in Deutschland aktive Dienstleister Semno umgesetzt. Hinterbliebene überlassen Semno den Computer der verstorbenen Person, um diesen hinsichtlich vorhandener Datenbestände und Internetaktivitäten zu analysieren. Erstellt wird ein Gutachten, aufgrund dessen die Angehörigen entscheiden können, was mit den gefundenen Daten und Internetprofilen geschehen soll. Semno versteht sich nicht als technische Dienstleistung, sondern steht den Angehörigen beratend zur Seite und unterstützt diese auf Wunsch auch bei der Umsetzung ihrer Wünsche für den digitalen Nachlass, z.B. bei der Schliessung eines E-Mail-Kontos oder dem Versetzen eines Facebook-Profiles in den Gedenkstatus. Wenn Angehörige mit dem digitalen Nachlass überfordert sind und selbst über wenig Internetkenntnisse verfügen, ist dieser beratende Aspekt nicht zu unterschätzen.

«Abschied und Trauer hat etwas mit Beziehung, Freundschaft und Liebe zu tun. Deshalb sind rein technische Lösungen für den digitalen Nachlass nur die eine Seite der Medaille. Manche brauchen eine einfühlsame Begleitung, um im Dschungel des Internets nicht von Raubtieren angefallen zu werden oder sich dort zu verlaufen.»

Birgit Aurelia Janetzky, Geschäftsführerin Semno.de

9. Fazit

Die initiale Zielsetzung des Forschungsprojekts war, neue oder angepasste Geschäftsmodelle für die digitale Nachlassplanung und Willensvollstreckung zu entwerfen, die als Grundlage für eine neue oder erweiterte Dienstleistung in der Schweiz (z.B. ein Start-up) dienen können. Die Analysen ergaben jedoch ein sehr viel differenzierteres Bild der grundlegenden Problematik, der unterschiedlichen Interessensgruppen und der rechtlichen Rahmenbedingungen. Digitale Nachlassplanung und Willensvollstreckung allein ist (noch) kein Geschäft. Pioniere unter den digitalen Vererbungsdiensten, wie Mywebwill oder Entrusted, haben den Betrieb wieder eingestellt oder wurden akquiriert. Erfolg versprechen Lösungsansätze, die im Rahmen eines breiter angelegten Geschäftsmodells einen Mehrwert zu Lebzeiten ermöglichen (z.B. Online-Speicher und Passwortsafes mit Datenvererbungsmechanismen) oder bereits bei der Entstehung, Speicherung und Verteilung der Daten ansetzen («Recht auf Vergessen», Verfallsdaten für Daten im Internet). Fazit der Analysen ist, dass der Lösungsraum weiter gefasst werden muss, um mit der zwangsläufig zunehmenden Relevanz der Thematik in den nächsten Jahren, den Herausforderungen des digitalen Nachlasses gewachsen zu sein.

Nachfolgend werden die zentralen Schlussfolgerungen zu den im Rahmen des Projekts bearbeitenden Forschungsfragen zusammengefasst sowie Anknüpfungspunkte für Lösungsansätze und offene Fragen aufgezeigt.

Tabelle 11

FAZIT UND ANKNÜPFUNGSPUNKTE

Forschungsfragen

Fazit

Der digitale Nachlass: Eigenschaften und Problematik (Kapitel 2)

Was umfasst ein digitaler Nachlass? Welche Umstände erschweren den Umgang mit den verteilt im Internet gespeicherten Daten und Konten von Verstorbenen?

- Es geht beim digitalen Nachlass nicht nur um die eigentlichen Inhalte/Daten, sondern um die Gefässe (Internetplattformen, Konten, Profile), an die sie gebunden sind sowie die Spuren, die wir im Rahmen unserer Internetaktivitäten hinterlassen.
- Die spezifischen Problematiken des digitalen Nachlasses lassen sich in 5 Faktoren zusammenfassen: Kenntnis, Zugriff, Eigentum/Kontrolle, Archivierungswürdigkeit, Lösbarkeit/Vergessen.

Vom Datenspeicher zum Datenfriedhof (Kapitel 3)

Welche Faktoren beeinflussen Grösse und Relevanz des digitalen Nachlasses?

- Die zunehmende Bedeutung des digitalen Nachlasses ist unbestritten (quantitativ, Soziodemographie/hohe Wachstumsraten der Internetnutzung in den älteren Altersgruppen, Durchdringung aller Lebensbereiche, aktive Nutzung). Dies allein lässt jedoch noch keine Rückschlüsse auf die Bereitschaft zur und Nachfrage nach digitaler Nachlassplanung zu.

Szenarien für den digitalen Nachlass (Kapitel 4)

Was passiert mit dem digitalen Nachlass im Todesfall mit und ohne digitale Nachlassplanung? Welche proaktiven und reaktiven «Anwendungsfälle» im Umgang mit digitalen Werten im Todesfall sind grundsätzlich denkbar?

- Die massgeblichen Akteure sind: Nutzer, Hinterbliebene, Plattformanbieter und ggfs. Behörden (Beurkundung und Meldung von Todesfällen).
- Schlüssel der digitalen Nachlassplanung ist die Übertragung der Zugriffsrechte auf Hinterbliebene (oder sonstigen Willensvollstrecker), die somit Herrschaft über den digitalen Nachlass erhalten.
- Bei fehlender Nachlassplanung sind die Plattformbetreiber die bestimmenden Akteure im Umgang mit dem digitalen Nachlass.

Die Praktiken der Plattformanbieter (Kapitel 5)

Wie gehen Plattformanbieter momentan mit Todesfällen von Mitgliedern um?

- Kommunizierte Regelungen für den Todesfall sind nur bei grossen, internationalen Plattformen zu finden. Nationale oder europäische Anbieter haben keine Regelungen oder Regelungen, die im Todesfall über den Kundendienst in Erfahrung gebracht werden müssen.
 - Die Plattformanbieter bewegen sich im Spannungsfeld zwischen Datenschutzaufgaben, den Wünschen von Angehörigen und den Persönlichkeitsrechten der Verstorbenen. Die gesetzlichen Rahmenbedingungen bieten den Plattformen momentan keine klare Grundlage für die Formulierung einheitlicher und unanfechtbarer Regelungen für den Todesfall.
-

Rechtliche Rahmenbedingungen (Kapitel 6)

Wie sehen die rechtlichen Rahmenbedingungen für die digitale Nachlassplanung und Willensvollstreckung in der Schweiz aus? Welche offenen Fragen gibt es?

Welche **erbrechtlichen Möglichkeiten** und Grenzen gibt es, über den digitalen Nachlass zu verfügen und den Willen zu vollstrecken?

- Das heute geltende Erbrecht in der Schweiz bietet nur beschränkt Möglichkeiten, um einen digitalen Nachlass formgültig und dennoch mediengerecht zu regeln. Zum einen sind nur Daten, die urheberrechtlich relevant sind, überhaupt vererbbar, und zum anderen gelten strenge Formvorschriften für die Gültigkeit von letztwilligen Verfügungen.
-

Welche **persönlichkeitsrechtlichen Aspekte** hat der digitale Nachlass und welche Grenzen und Möglichkeiten der Durchsetzbarkeit von Rechtsansprüchen gibt es für Angehörige nach dem Tod?

- Die Mehrheit der im Rahmen der privaten Internetnutzung im Internet gespeicherten Daten fallen unter das Persönlichkeitsrecht. Die Persönlichkeit endet gemäss Art. 31 Abs.1 ZGB mit dem Tod. Das Persönlichkeitsschutzrecht bietet somit kaum geeignete Hebel, um einen digitalen Willen durchzusetzen oder sich gegen Persönlichkeitsverletzungen im Namen eines Verstorbenen zu wehren. Angehörigen steht im Sinne des Andenkenschutzes die Möglichkeit auf Beseitigung, Feststellung und Unterlassung zu klagen (gem. Art. 28a ff. ZGB) lediglich offen, falls eine Handlung auch ihre eigene Persönlichkeit verletzt.
-

Welche **datenschutzrechtlichen Fragestellungen** wirft der digitale Nachlass auf? Gibt es ein «**Recht auf Vergessen**» im Internet?

- Der geeignetste Ansatzpunkt um die Ausgangslage für die digitale Nachlassplanung und Willensvollstreckung zu optimieren, scheint das Datenschutzrecht zu sein. Zum einen gilt es, die Datenherrschaft zu Lebzeiten auch bei grenzüberschreitender und zunehmend intransparenter Datenverarbeitung im Internet sicherzustellen. Zum anderen muss die Einführung eines wirk-samen «Rechts auf Vergessen(werden)» vertieft geprüft werden. Somit sind die aktuell in verschiedenen parlamentarischen Vorstössen anvisierten Revisionen des Datenschutzgesetzes auch für die Thematik des digitalen Nachlasses von hoher Relevanz. Rechtsgrundlagen betreffend die Auskunft über Personendaten von Verstorbenen, wie sie in gewissen Kantonen bereits bestehen, können Orientierung bieten, um der Persönlichkeit postmortal zu einem vernünftigen Schutz zu verhelfen, ohne dass damit deren grundsätzlicher Untergang mit dem Tod in Frage gestellt würde.
-

Welche Möglichkeiten und Grenzen gibt es bei der Durchsetzbarkeit von hinterlegten Wünschen des Verstorbenen oder Ansprüchen der Angehörigen gegenüber Plattformanbietern? Welches Recht und welcher Gerichtsstand sind anwendbar?

- Einige jüngere Entscheide haben Klarheit darüber verschaffen, dass zum einen bei Persönlichkeitsverletzungen im Internet ein Gerichtsstand am Ort des gewöhnlichen Aufenthalts des Verletzten zu bejahen ist und zum anderen, dass falls – selbst wenn die Datenbearbeitung nicht in der Schweiz erfolgt – die Schweizerischen Gesetze anwendbar sind. Viele Gerichtsstandsklauseln in den AGB der Plattformanbieter sind vor diesem Hintergrund als kaum durchsetzbar zu beurteilen.
- Die spezifischen Durchsetzungsrechte des DSG erlangen gegenüber privaten Datenbearbeitern nur zusammen mit Art. 28 ZGB Bedeutung. In Bezug auf die Wünsche, die ein Verstorbener geäußert hat, bleibt jedoch festzuhalten, dass die Angehörigen – zumindest in der Schweiz aufgrund des Untergangs der Persönlichkeit mit dem Tod – einen schweren Stand haben, um diese durchzusetzen.

Anknüpfungspunkte bei der Administration von Todesfällen (Kapitel 7)

Wie werden Todesfälle in der Schweiz administriert?
Gibt es Anknüpfungspunkte für die digitale Nachlassplanung und Willensvollstreckung?

- Elektronische Todesurkunden (CH/dreisprachig und international) sind im eidgenössischen Zivilstandswesen momentan nicht möglich. Die Urkunden werden ausschliesslich auf speziellem Sicherheitspapier ausgedruckt.
- Für die automatische Meldung eines Todesfalls aus dem eidgenössischen Zivilstandsregister (Infostar) an einen privaten digitalen Vererbungsdienst, wie dies vergleichsweise in Schweden der Vererbungsdienst Mywebwill eingerichtet hatte, besteht momentan keine Rechtsgrundlage in der Schweiz.
- Alternativ bietet sich die Nutzung der Einwohnerregister für einen solchen Zweck (analog Vermerk «Hinterlegtes Testament» im Einwohnerregister der Stadt Zürich (TopaZ), der bei der Registrierung des Todesfalls einen Brief an das Notariat auslöst. Zu prüfen wäre die rechtlichen und technischen Voraussetzungen direkter Todesfall-Meldungen von Einwohnerregistern an digitale Vererbungsdienste. Ebenfalls zu prüfen wäre die Rolle der Notare, Notariate oder sonstiger Institutionen, bei denen letztwillige Verfügungen hinterlegt sein können.

Lösungsansätze für den digitalen Nachlass (Kapitel 8)

Welche Möglichkeiten und Angebote existieren bereits für die digitale Nachlassplanung und Willensvollstreckung?

Welche Ansatzpunkte bestehen für praktikable und den rechtlichen Rahmenbedingungen in der Schweiz angepasste Lösungen?

- Die digitale Nachlassplanung und Willensvollstreckung ist ein Pionierfeld. Es existieren weder bewährte Geschäftsmodelle noch dem Medium Internet angepasste rechtliche Rahmenbedingungen, die es erlauben würden, perfekt durchdachte und zukunftssichere Lösungen zu entwerfen.
- Wer einen digitalen Vererbungsdienst nutzt, schafft Transparenz und emanzipiert sich mit der Weitergabe der Zugriffsdaten im Todesfall bis zu einem gewissen Grad von der Verfügungsgewalt der Plattform-Anbieter. Wird dieser «digitale Wille» zusätzlich in ein konventionelles Testament integriert und allenfalls einem dedizierten Willensvollstreckter anvertraut, ist das Kriterium der Formgültigkeit erfüllt und somit die Wahrscheinlichkeit der Durchsetzbarkeit erhöht.
- Kontrollverlust über Daten beginnt bereits zu Lebzeiten. Der erweiterte Lösungsraum für den digitalen Nachlass stellt den selbstbestimmten Nutzer in den Mittelpunkt und schliesst die Datenherrschaft zu Lebzeiten sowie ein «Recht auf Vergessen» mit ein.
- Angesichts des geringen Reifegrads der digitalen Nachlassplanung spielt die Sensibilisierung der Bevölkerung sowie die Beratung bei der digitalen Nachlassplanung und Willensvollstreckung eine wichtige Rolle. Institutionen oder Berufsgruppen, die bereits in der Vorsorgeberatung aktiv sind, könnten sich dieses zunehmend relevante Tätigkeitsfeld erschliessen, vorausgesetzt sie bauen das notwendige Know-how zu den Möglichkeiten und Grenzen der digitalen Nachlassplanung und Willensvollstreckung auf.

Literaturverzeichnis

KAPITEL 2

Bundesamt für Statistik (2011b) Indikatoren Informationsgesellschaft – Internetnutzung. 2011b. http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html [abgerufen: 2012-06-22].

Ethority (o.J.) Social Media Prisma – ethority Social Media Intelligence Blog. Ethority.de. <http://www.ethority.de/weblog/social-media-prisma/> [abgerufen: 2012-06-16].

Facebook (2012) Legal terms / Nutzungsbedingungen (deutsche Übersetzung), Stand 8.6.2012. <https://www.facebook.com/legal/terms> [abgerufen: 2012-06-22].

Google (o.J.) Eine Seite oder Website aus den Suchergebnissen von Google entfernen – Webmaster-Tools-Hilfe. <http://support.google.com/webmasters/bin/answer.py?hl=de&answer=164734> [abgerufen: 2012-11-13].

Mayer-Schönberger, Viktor (2010) Delete: Die Tugend des Vergessens in digitalen Zeiten. 1. Auflage. Berlin University Press.

OECD (2007) Participative Web: User-Created Content. <http://www.oecd.org/dataoecd/57/14/38393115.pdf> [abgerufen: 2012-06-22].

Schwaab, Jean Christophe (2012) Postulat: Recht auf Vergessen im Internet. Eingereicht: 14.3.2012, Plenum: Nationalrat, Status: 9.5.2012: Annahme des Postulats. http://www.parlament.ch/d/suche/seiten/geschaeft.aspx?gesch_id=20123152 [abgerufen: 2012-06-22].

Wall Street Journal Online (o.J.) What They Know. <http://online.wsj.com/public/page/what-they-know-digital-privacy.html> [abgerufen: 17. Oktober 2012].

Yahoo! Deutschland (2012) Allgemeine Geschäftsbedingungen. Bearbeitungsstand: April 2012. <http://info.yahoo.com/legal/de/yahoo/tos.html> [abgerufen: 22-06-2012].

KAPITEL 3

Bernet/Serranetga 2012. Facebook Zahlen Schweiz: Bald 3 Millionen Profile | bernetblog.ch. bernetblog. <http://bernetblog.ch/2012/10/01/facebook-zahlen-schweiz-bald-3-millionen-profile/> [abgerufen: 2012-10-19].

Bundesamt für Statistik 2010a. Indikatoren Informationsgesellschaft. http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.html [abgerufen: 2012-06-22].

Bundesamt für Statistik 2011b. Indikatoren Informationsgesellschaft – Internetnutzung. http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30106.301.html [abgerufen: 2012-06-22].

Bundesamt für Statistik 2012. Internet in den Schweizer Haushalten: Ergebnisse der Erhebung Omnibus IKT 2010. Bundesamt für Statistik. <http://www.bfs.admin.ch/bfs/portal/de/index/themen/16/22/publ.html?publicationID=4742> [abgerufen: 2012-06-22].

European Commission 2011. Attitudes on Data Protection and Electronic Identity in the European Union. Brüssel: European Commission. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf [abgerufen: 2012-06-22].

Franz, Gerhard 2010. Digital Natives und Digital Immigrants: Social Media als Treffpunkt von zwei Generationen. http://www.media-perspektiven.de/uploads/tx_mppublications/09-2010_Franz.pdf [abgerufen: 2012-06-22].

Langer, Marie-Astrid 2012. Facebook Schweiz wird älter: Entwicklung vom Jugend-zum Allgemein-Medium. Neue Zürcher Zeitung. 2012-05-12. <http://www.nzz.ch/nachrichten/wirtschaft/aktuell/facebook-schweiz-wird-aelter-1.16861769> [abgerufen: 2012-06-25].

Lustig, Nathan 2010. How We Calculated That Three Facebook Users Die Every Minute. no longer available online.

Lustig, Nathan 2012. 2.89 m Facebook Users Will Die in 2012, 580,000 in the USA. <http://www.nathanlustig.com/2012/06/06/2-89m-facebook-users-will-die-in-2012-580000-in-the-usa/> [abgerufen: 2012-06-30].

Mayer-Schönberger, Viktor 2010. Delete: Die Tugend des Vergessens in digitalen Zeiten. 1. Auflage. Berlin University Press.

OECD 2007. Participative Web: User-Created Content. <http://www.oecd.org/dataoecd/57/14/38393115.pdf> [abgerufen: 2012-06-22].

Pixable 2011. Facebook Photo Trends [INFOGRAPHIC] | Pixable Blog. <http://blog.pixable.com/2011/02/14/facebook-photo-trends-infographic/> [abgerufen: 2012-11-18].

Social Media Schweiz 2012. Facebook – Die Schweiz in Zahlen (Updates pro Stichtag). http://www.socialmediaschweiz.ch/html/ch_fb_publicationen.html [abgerufen: 2012-06-22].

United States Securities and Exchange Commission [SEC] 2012. Amendment No. 6 to Form S-1 Registration – Facebook Inc. – Prospectus subject to completion (Börsengangprospekt, Status 6. Mai, 2012). Washington D. C.: SEC. <http://www.sec.gov/Archives/edgar/data/1326801/000119312512223668/d287954ds1a.htm> [abgerufen: 2012-06-22].

Wagenknecht, Florian 2011. Was passiert mit unseren Bildern bei Facebook? | Recht am Bild. <http://www.rechtambild.de/2011/05/facebook-was-passiert-mit-unseren-bildern-%E2%80%93-ein-einblick-in-die-nutzungsbestimmungen/> [abgerufen: 2012-11-9].

ZHAW 2010. JAMES-Studie: Jugend, Aktivitäten, Medien – Erhebung Schweiz. <http://www.psychologie.zhaw.ch/psychologie/forschung-und-entwicklung/medienpsychologie/medienumgang-von-kindern-und-jugendlichen/james.html> [abgerufen: 2012-05-21].

KAPITEL 4

Breitschmid, P. 2010. Organspende, Sektion und Bestattung – zivilrechtliche Streifzüge. In Symposium Tod und toter Körper, Zürich 13./14. Januar 2010.

Computerbetrug.de o.J. Facebook und das Löschen: So entfernen Sie Daten, Nachrichten, Account – computerbetrug.de – Infos über Gefahren des Internet. <http://www.computerbetrug.de/2012/05/facebook-und-das-loschen-so-entfernen-sie-daten-nachrichten-account-6288/> [abgerufen: 2012-11-16].

Data Protection Commissioner of Ireland 2012. Report of Data Protection Audit of Facebook Ireland – Data Protection Commissioner – Ireland. http://dataprotection.ie/docs/21/12/11_-_Report_of_Data_Protection_Audit_of_Facebook_Irela/1182.htm [abgerufen: 2012-06-30].

Dietrich, Nicole 2009. Untote im Internet. Internet Text ORF Ö3. <http://oe1.orf.at/artikel/214846> [abgerufen: 2012-06-22].

Von der Horst, Rutger 2009. Rechtlicher Schutz und technische Verfügbarkeit digitaler Werte (In Idivus Blog). <http://www.idivus.com/content/2009-11-24-Fachbeitrag-Dr-von-der-Horst-Massensterben-in-Digitalien> [abgerufen: 2012-06-22].

Krashinsky, Susan 2009. How to die on Facebook. Globe and Mail. <http://www.theglobeandmail.com/technology/how-to-die-on-facebook/article4215861/> [abgerufen: 2012-06-22].

Prensky, Marc 2001. Digital natives, digital immigrants Part 1. On the horizon 9, 5, 1–6.

Yahoo! Deutschland 2012. Allgemeine Geschäftsbedingungen. Bearbeitungsstand: April 2012. <http://info.yahoo.com/legal/de/yahoo/tos.html> [abgerufen: 2012-06-22].

KAPITEL 5

BBC Online 2005. Who owns your e-mails? BBC. http://news.bbc.co.uk/2/hi/uk_news/magazine/4164669.stm [abgerufen: 2012-06-30].

Facebook 2012a. Datenverwendungsrichtlinien (Status: 8.6.2012). <https://www.facebook.com/about/privacy/other> [abgerufen: 2012-06-26].

Facebook o.J. Datenverwendungsrichtlinien. Was Du sonst noch wissen musst. Facebook. <https://www.facebook.com/about/privacy/other> [abgerufen: 2012-06-26].

Facebook o.J. How do I report a deceased person or an account that needs to be memorialized or deleted? | Facebook Help Centre. <https://www.facebook.com/help/150486848354038/?q=deceased&sid=0NZelqyvUCr0HFG1p> [abgerufen: 2012-04-25].

Facebook 2012b. Nutzungsbedingungen / Legal terms (deutsche Übersetzung), Status: 8.6.2012. <https://www.facebook.com/legal/terms> [abgerufen: 2012-06-22].

Facebook Nutzungsbedingungen für Nutzer mit Wohnsitz in Deutschland (Stand: 20.4.2012). <https://www.facebook.com/terms/provisions/german/index.php> [abgerufen: 2012-b-06-26].

Facebook 2012c. Terms – Statement of Rights and Responsibilities (Status: 8.6.2012). <https://www.facebook.com/legal/terms> [abgerufen: 2012-10-25].

Facebook 2012d. Wie melde ich einen verstorbenen Nutzer oder ein Konto, das in den Gedenkzustand versetzt bzw. gelöscht werden muss? – Facebook Hilfebereich. <https://www.facebook.com/help/?faq=150486848354038#Wie-melde-ich-einen-verstorbenen-Nutzer-oder-ein-Konto.-das-in-den-Gedenkzustand-versetzt-bzw.-gel%C3%B6scht-werden-muss?> [abgerufen: 2012-06-26].

Facebook 2012e. Wie übermittle ich einen besonderen Antrag im Zusammenhang mit dem Konto eines Verstorbenen? – Facebook Hilfebereich. <https://www.facebook.com/help/?faq=265593773453448> [abgerufen: 2012-06-26].

Google 2012a. Google Nutzungsbedingungen – Datenschutzerklärung & Nutzungsbedingungen (Status: 1.3.2012). <http://mail.google.com/intl/de/policies/terms/> [abgerufen: 2012-06-27].

Google 2012b. Google-Konto löschen oder wiederherstellen – Google-Konten-Hilfe. <http://support.google.com/accounts/bin/answer.py?hl=de&answer=32046&topic=2382753&ctx=topic> [abgerufen: 2012-06-28].

Google 2011. Zugriff auf die E-Mails einer verstorbenen Person – Google Mail-Hilfe. <http://support.google.com/mail/bin/answer.py?hl=de&answer=14300> [abgerufen: 2012-06-27].

Google o.J. Accessing a deceased person's mail – Gmail Help. <http://support.google.com/mail/bin/answer.py?hl=en&answer=14300&topic=1669055&ctx=topic> [abgerufen: 2012-10-25].

PayPal o.J. How do I close the PayPal account of a relative? [no longer available online]. [abgerufen: 2012-06-30].

PayPal 2011. PayPal-Datenschutzgrundsätze (Status: 28.3.2011). https://cms.paypal.com/ch/cgi-bin/marketingweb?cmd=_render-content&content_ID=ua/Privacy_full&locale.x=de_DE [abgerufen: 2012-06-30].

SR DRS 2011. Passwörter: Auch nach dem Tod eine Plage. Digital. <http://www.drs.ch/www/de/drs/themen/digital/ratgeber-die-digitalen-spuren-nach-dem-tod/296310.296769.passwoerter-auch-nach-dem-tod-eine-plage.html> [abgerufen: 2012-06-26].

Twitter 2012. Allgemeine Geschäftsbedingungen (gültig ab 25.6.2012). <https://twitter.com/tos> [abgerufen: 2012-06-27].

Twitter o.J. Hilfe-Center | How to Contact Twitter About a Deceased User. <http://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/87894-how-to-contact-twitter-about-a-deceased-user#> [abgerufen: 2012-06-27].

Xing 2012a. AGB | XING. <https://www.xing.com/terms> [abgerufen: 2012-06-26].

Xing 2012b. Datenschutz | XING. <https://www.xing.com/privacy> [abgerufen: 2012-06-26].

Yahoo! 2012. Allgemeine Geschäftsbedingungen (Stand April 2012). <http://info.yahoo.com/legal/de/yahoo/tos.html> [abgerufen: 2012-06-27].

Yahoo! 2008. Yahoo! Terms of Service (Status: 24.11.2008). <http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html> [abgerufen: 2012-06-27].

Yahoo! Deutschland 2012a. Allgemeine Geschäftsbedingungen. Bearbeitungsstand: April 2012. <http://info.yahoo.com/legal/de/yahoo/tos.html> [abgerufen: 2012-06-22].

Yahoo! Deutschland 2012b. Datenschutzcenter. <http://info.yahoo.com/privacy/de/yahoo/> [abgerufen: 2012-06-27].

YouTube 2010. Terms of Service (Stand: 9.6.2010). <http://www.youtube.com/t/terms> [abgerufen: 2012-06-28].

KAPITEL 6

Aebi-Müller Regina, Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes – Unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland, Bern 2005.

Auer Andreas / Malinverni Giorgio / Hottelier Michel, Droit constitutionnel suisse, volume II, Les droits fondamentaux, 2. Aufl., Bern 2006.

Belser Eva Maria, Kommentar zu Art. 3 DSG, in: Maurer-Lambrou Urs / Vogt Nedim Peter (Hrsg.), Basler Kommentar zum Datenschutzgesetz, 2. Auflage, Basel 2006.

Belser Eva Maria / Hussein Noureddine, § 7 Die Datenschutzgesetzgebung des Bundes, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, S. 412 ff.

Barrelet Denis / Egloff Willi, Das neue Urheberrecht – Kommentar zum Bundesgesetz über das Urheberrecht und verwandte Schutzrechte, 3. Aufl., Bern 2008.

Beretta Piera, Kommentar zu Art. 31 ZGB, in: Honsell Heinrich / Vogt Nedim Peter / Geiser Thomas (Hrsg.), Basler Kommentar, Zivilgesetzbuch I, Art. 1–456 ZGB, Basel 2010.

Bettex Christian et Al., Kommentar zu Art. 312^{ter} StGB, in: Dupuis Michel et al. (Hrsg.), Petit commentaire Code pénal, Basel 2012.

Bolliger Christian / Féraud Marius / Epiney Astrid / Hänni Julia, Schlussbericht Evaluation DSG, Bern 2011 http://www.ejpd.admin.ch/content/dam/data/staat_buerger/evaluation/bj/schlussber-datenschutzeval-d.pdf, besucht am: 17.10.2012.

Breitschmid Peter, Einsatz des Willensvollstreckers bei persönlichkeitsrechtlichen Belangen, in: Künzle Hans Rainer (Hrsg.), Willensvollstreckung – Aktuelle Rechtsprobleme (2), Referate der Weiterbildungsseminare an der Universität St. Gallen, Zürich 2006, S. 37 ff. (zit. persönlichkeitsrechtliche Belange).

Ders., Kommentar zu Art. 505 ZGB, in: Honsell Heinrich / Vogt Nedim Peter / Geiser Thomas (Hrsg.), Basler Kommentar, Zivilgesetzbuch II, Art. 457–977 ZGB; Art 1–61 SchIT ZGB, 4. Aufl. Basel 2011 (zit. BSK).

Breitschmid Peter / Kamp Annasofia, Persönlichkeitsschutz Verstorbener – Urheberpersönlichkeitsschutz im Besonderen, Successio 1/2011, S. 19 ff.

Bucher Andreas, Natürliche Personen und Persönlichkeitsschutz, 4. Aufl. Basel 2009.

Büchler Andrea / Frei Marco, Kommentar zu Art. 28 ZGB, in: Kren Kostkiewicz Jolanta / Nobel Peter / Schwander Ivo / Wolf Stephan (Hrsg.), Kommentar Schweizerisches Zivilgesetzbuch, 2. Aufl., Zürich 2011.

Cherpillod Ivan, Kommentar zu Art. 2 URG, in: Müller Barbara K. / Oertli Reinhard (Hrsg.), Stämpfli's Handkommentar, Urheberrechtsgesetz (URG), Bern 2006.

Christ Bernhard / Eichner Mark, Kommentar zu Art. 517 ZGB, in: Abt Daniel / Weibel Thomas (Hrsg.), Praxiskommentar Erbrecht, Basel 2011.

Donatsch Andreas / Schmid Albert, Der Zugriff auf E-Mails im Strafverfahren – Überwachung (BÜPF) oder Beschlagnahme? in: Schwarzenegger Urs / Arter Oliver / Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, S. 151 ff.

Druey Jean Nicolas, Grundriss des Erbrechts, 5. Aufl., Bern 2002.

Gramigna Ralph/Maurer-Lambrou Urs, Kommentar zu Art. 9 DSG, in: Maurer-Lambrou Urs/Vogt Nedim Peter (Hrsg.), Basler Kommentar zum Datenschutzgesetz, 2. Auflage, Basel 2006.

Grieder Thomas/Ott Walter, Plädoyer für den postmortalen Persönlichkeitschutz, Aktuelle Juristische Praxis (AJP), 6/2001, S. 627ff.

Haas Raphaël, Die Einwilligung in eine Persönlichkeitsverletzung nach Art. 28 Abs. 2 ZGB, Luzerner Beiträge zur Rechtswissenschaft, Band 18, Zürich, Basel, Genf, 2007.

Hauptli Matthias, Kommentar zu Art. 560 ZGB, in: Abt Daniel/Weibel Thomas (Hrsg.), Praxiskommentar Erbrecht, 2. Aufl., Basel 2011.

Hilty Lorenz/Oertel Britta/Wölk Michaela/Pärli Kurt, Lokalisiert und identifiziert, Wie Ortungstechnologien unser Leben verändern, Zürich 2011.

Hofer Martin, Die Crux der Auskunft über Verstorbene, digma 1/2008, S. 34 ff.

Karrer Martin/Vogt Nedim Peter/Leu Daniel, Vorbemerkung zu Art. 517/518 ZGB, in: Honsell Heinrich/Vogt Nedim Peter/Geiser Thomas (Hrsg.), Basler Kommentar, Zivilgesetzbuch II, Art. 457–977 ZGB; Art. 1–61 SchIT ZGB, 4. Aufl. Basel 2011.

Kernen Alexander, Schützenhilfe für Opfer von Persönlichkeitsverletzungen im Internet, in: Jusletter vom 6. Februar 2012.

Knellwolf Esther, Postmortaler Persönlichkeitsschutz – Andenkensschutz der Hinterbliebenen, Diss., Zürich 1990.

Künzle Hans Rainer, Kommentar zu Art. 517–518 ZGB, in: Hausheer Heinz, Walter Hans Peter, Berner Kommentar, Kommentar zum schweizerischen Privatrecht, Das Erbrecht, Band III, 1. Abteilung, 2. Teilband, 2. Teil Die Willensvollstrecker, Bern 2011. (zit. BK)

Ders., Kommentar zu Art. 517–518 ZGB, in: Breitschmid Peter/Rumo-Jungo Alexandra (Hrsg.), Handkommentar zum Schweizer Privatrecht, Erbrecht, 2. Aufl., Zürich, Basel, Genf, 2012 (zit. CHK).

Ders., Interessenskollision im Erbrecht: Willensvollstrecker, Notar, Anwalt. Schweizerische Juristen Zeitung 1/2012 (108), S. 1 ff. (zit. Interessenskollision).

Langer Dirk, Le droit à l'oubli à l'épreuve d'Internet, in: Jusletter vom 12. März 2012.

Meili Andreas, Kann man das Persönlichkeitsrecht im Internet durchsetzen? Plädoyer 5/2009, S. 29.

Müller Jörg Paul/Schefer Markus, Grundrechte in der Schweiz, im Rahmen der Bundesverfassung, der EMRK und der UNO-Pakte, 4. Aufl., Bern 2008.

Pärli Kurt, Datenschutz durch Selbstregulierung, digma 2/2011, S. 66 ff.,

Rehbinder Manfred/Viganò Adriano, Kommentar Urheberrecht, 3. Auflage, Zürich 2008.

Rampini Corrado, Kommentar zu Art. 15 DSG, in: Maurer-Lambrou Urs/Vogt Nedim Peter, Basler Kommentar zum Datenschutzgesetz, 2. Auflage, Basel 2006.

Rémy Marc, L'ordre d'autopsie médico-légale: le droit d'opposition et le contrôle judiciaire en procédure pénale suisse, forumpoenale 1/2012, S. 38 ff.

Rosenthal David, Kommentar zu Art. 1, Art. 3 und Art. 12 DSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich, Basel, Genf, 2008.

Rosenthal David/Jöhri Yvonne, Kommentar zu Art. 2 DSG, in: Rosenthal David/Jöhri Yvonne (Hrsg.), Handkommentar zum Datenschutzgesetz, Zürich, Basel, Genf, 2008.

Schwander Ivo, Kommentar zu Art. 560 ZGB, in: Honsell Heinrich/Vogt Nedim Peter/Geiser Thomas (Hrsg.), Basler Kommentar, Zivilgesetzbuch II, Art. 457–977 ZGB, Art. 1–61 SchIT ZGB, 4. Aufl., Basel 2011.

Schweizer Rainer J., § 43 Verfassungsrechtlicher Persönlichkeitschutz, in: Thürer Daniel/Aubert Jean-François/Müller Jörg Paul (Hrsg.), Verfassungsrecht der Schweiz, Droit constitutionnel suisse, Zürich 2001, 691 ff.

Schweizer Rainer J./Glutz von Blotzheim Alexander M., Wie die Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gegenüber privaten Datenbearbeitern umgesetzt werden, in: Jusletter vom 21. Februar 2011

Stahelin Daniel, Kommentar zu Art. 482 ZGB, in: Honsell Heinrich/Vogt Nedim Peter/Geiser Thomas (Hrsg.), Basler Kommentar, Zivilgesetzbuch II, Art. 457–977 ZGB; Art. 1–61 SchIT ZGB, 4. Aufl. Basel 2011.

Watter Rolf, Kommentar zu Art. 35 OR, in: Honsell Heinrich/Vogt Nedim Peter/Wiegand Wolfgang (Hrsg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 5. Aufl., Basel 2011

Weber Rolf H., Der Ruf nach einem Recht auf Vergessen, digma 3/2011, S. 102 ff.

Weimar Peter, Kommentar zu Art. 482 ZGB, Berner Kommentar zum schweizerischen Privatrecht, Band III, 1. Abteilung, 1. Teilband, 1. Teil, Bern 2009.

KAPITEL 7

Bestattungs- und Friedhofamt – Stadt Zürich. http://www.stadt-zuerich.ch/prd/de/index/bevoelkerungsamt/bestattungs-und_friedhofamt.html [abgerufen: 2012-03-25].

Bestattungs- und Friedhofamt – Stadt Zürich. Bestattungswünsche. http://www.stadt-zuerich.ch/content/prd/de/index/bevoelkerungsamt/bestattungs-_und_friedhofamt/bestattungswuensche.html [abgerufen: 2012-11-24].

Bundesamt für Justiz. Meldewesen Einwohnerkontrolle. <http://www.bj.admin.ch/content/bj/de/home/themen/gesellschaft/zivilstand/einwohnerkontrolle.html> [abgerufen: 2012-11-25].

Bundesamt für Statistik 2012. Einführung sedex. http://www.bfs.admin.ch/bfs/portal/de/index/news/00/00/02_parsys.49026.downloadList.64534.DownloadFile.tmp/introde.pdf [abgerufen: 2012-11-25].

Bundesamt für Statistik 2011. Meldungen der Bundesregister an die Einwohnerregister. http://www.bfs.admin.ch/bfs/portal/de/index/news/00/00/12/09_parsys.74130.downloadList.40139.DownloadFile.tmp/meldungenderbranewrv.1.425.08.2011.pdf [abgerufen: 2012-11-25].

EAZW 2011. Fachprozess EAZW: Tod einer Person mit bekannter Identität im Inland. Eidgenössisches Amt für das Zivilstandswesen, 15.12.2004 (Stand 1.1.2011). http://www.ejpd.admin.ch/content/dam/data/gesellschaft/eazw/weisungen/aktuelleprozesse/31_4-d.pdf [abgerufen: 2012-05-5].

EJPD, Bundesamt für Justiz BJ, Direktionsbereich Privatrecht Fachbereich Infostar FIS 2013. Releasenotes Infostar (per 9.1.2013), Releasewechsel von 7.0.0 auf 8.0.0. <http://www.ejpd.admin.ch/content/dam/data/gesellschaft/eazw/support/releasewechsel-8-0-0-d.pdf> [abgerufen: 2012-11-8].

Kantonale Zivilstandsordnung (ZVO) (vom 1. Dezember 2004). Kanton Zürich. [http://www2.zhlex.zh.ch/app/zhlex_r.nsf/0/D1CA01F0B6987ABCC12577FC002663C3/\\$file/231.1_1.12.04_71.pdf](http://www2.zhlex.zh.ch/app/zhlex_r.nsf/0/D1CA01F0B6987ABCC12577FC002663C3/$file/231.1_1.12.04_71.pdf) [abgerufen: 2012-09-25].

Notariate im Kanton Zürich – Erbrecht. http://www.notariate.zh.ch/not_erb.php [abgerufen: 2012-11-12].

Schweizerische Bundeskanzlei. ch.ch – Schweizer Portal von Bund, Kantonen und Gemeinden – Todesfall. <http://www.ch.ch/private/00029/00037/index.html?lang=de> [abgerufen: 2012-06-1].

Schweizerischer Verband für Zivilstandswesen 2012. Revision der Eidgenössischen Zivilstandsverordnung und der Verordnung über die Gebühren im Zivilstandswesen, Schriftliche Anhörung. http://www.zivilstandswesen.ch/webautor-data/21/2012-04-24_d_Anhoerung---Revision-ZStV-und-ZStGV.pdf [abgerufen: 2012-11-24].

SNV Schweizerischer Notarenverband o.J. Testamentenregister – Register der Schweizer Notare. http://www.testamentenregister.ch/index.cfm?parents_id=979 [abgerufen: 2012-07-1].

Steimer, Thomas 2010. eMISTAR Projektinformation Ausgabe 1 / November 2010. <http://www.bj.admin.ch/content/dam/data/gesellschaft/eazw/meldewesen/newsletter-1-2010-d.pdf> [abgerufen: 2012-11-25].

Steimer, Thomas 2011a. Elektronisches Meldewesen Infostar. http://www.einwohnerdienste.ch/fileadmin/mitgliederbereich/download/eMISTAR_VSED_GV.pdf [abgerufen: 2012-11-25].

Steimer, Thomas 2011b. eMISTAR Projektinformation Ausgabe 2 / September 2011. <http://www.bj.admin.ch/content/dam/data/gesellschaft/eazw/meldewesen/newsletter-2-2011-d.pdf> [abgerufen: 2012-11-25].

Steimer, Thomas 2012. eMISTAR Projektinformation Ausgabe 4 / November 2012. <http://www.bj.admin.ch/content/dam/data/gesellschaft/eazw/meldewesen/newsletter-4-2012-d.pdf> [abgerufen: 2012-11-25].

Zivilstandsamt – Stadt Zürich. <http://www.stadt-zuerich.ch/prd/de/index/bevoelkerungsamt/zivilstandsamt.html> [abgerufen: 2012-03-20].

Zivilstandsverordnung (ZStV) (vom 28.4.2004, Stand 1.1.2011) http://www.admin.ch/ch/d/sr/211_112_2/index.html [abgerufen: 2012-11-8].

Zivilstandsverordnung (ZStV). Änderung (per 1.1.2013). <http://www.ejpd.admin.ch/content/dam/data/gesellschaft/gesetzgebung/namensrecht/zstv-d.pdf> [abgerufen: 2012-11-24].

KAPITEL 8

Backes, Michael 2011. X-pire! – Wie man dem Internet das «Vergessen» beibringt. <http://www.infsec.cs.uni-saarland.de/projects/forgetful-internet/> [abgerufen: 2012-10-17].

Cavoukian, Ann 2009. Privacy by design. Ontario. <http://privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-german.pdf> [abgerufen: 2012-10-17].

Die Zeit 2011. Digitales Vergessen: Aigner präsentiert Verfallsdatum für Fotos. Die Zeit. <http://www.zeit.de/digital/datenschutz/2011-01/digitaler-radiergummi> [abgerufen: 2012-06-1].

DSwiss AG SecureSafe – Preserve what matters. <http://www.securesafe.com/de/> [abgerufen: 2012-06-25].

EDÖB o.J. Surfen und Privatsphäre. Tipps zum Selbstschutz. <http://www.edoeb.admin.ch/themen/00794/00928/00930/00956/index.html?lang=de> [abgerufen: 2012-06-25].

European Commission 2010. A Digital Agenda for Europe. Brussels. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF> [abgerufen: 2012-10-17].

Felten, Ed 2009. Breaking Vanish: A Story of Security Research in Action. <https://freedom-to-tinker.com/blog/felten/breaking-vanish-story-security-research-action/> [abgerufen: 2012-10-17].

Karla, Jürgen 2010. Digitales Vergessen im Web 2.0. WIRTSCHAFTSINFORMATIK 52, 2, 105–108.

Legacy Locker – The safe and secure way to pass your online accounts to your friends and loved ones. <http://legacylocker.com/> [abgerufen: 2012-05-03].

Markoff, John 2009. New Technology to Make Digital Data Self-Destruct. The New York Times. <http://www.nytimes.com/2009/07/21/science/21crypto.html> [abgerufen: 2012-10-17].

Mayer-Schönberger, Viktor 2010. Delete: Die Tugend des Vergessens in digitalen Zeiten. 1. Auflage. Berlin University Press.

preventiX Homepage. <https://www.preventix.ch> [abgerufen: 2012-07-1].

Pörksen, Bernhard 2012. Das gnadenlose Gedächtnis – Essay. Tages-Anzeiger. <http://www.tagesanzeiger.ch/kultur/diverses/Das-gnadenlose-Gedaechtnis/story/16536606> [abgerufen: 2012-10-19].

Ruef, Marc 2011. Erfolgreicher Angriff gegen X-pire! <http://www.scip.ch/?labs.201110131> [abgerufen: 2012-11-9].

Semno – regelt den digitalen Nachlass. <http://www.semno.de/startseite.html> [abgerufen: 2012-06-26].

The Digital Beyond 2012. Digital Death and Afterlife Online Services List. <http://www.thedigitalbeyond.com/online-services-list/> [abgerufen: 2012-03-01].

Xsen – Für einen sicheren digitalen Nachlass. <https://xsen.de/> [abgerufen: 2012-11-25].

Ziggur – What is your online legacy? <http://www.ziggur.me/en/home.aspx> [abgerufen: 2012-05-03].

Autoren der Studie



Elke Brucker-Kley

Dipl. inf. wiss.
Wissenschaftliche Mitarbeiterin
mbA, Projektleiterin



Thomas Keller

Prof. Dr. Dipl. Ing. ETH
Dipl. Informatik UZH
Leiter Institut für Wirtschafts-
informatik (ZWI)
Professor für Wirtschaftsinformatik



Lukas Kurtz

BSc in Business Administration
with a Major in Business
Information Technology
Master of Advanced Studies ZFH
Business Analysis



Kurt Pärli

PD Prof. (FH), Dr. iur.
Leiter Zentrum für Sozialrecht
und Forschungsleiter Institut für
Wirtschaftsrecht
Dozent für Europarecht, Arbeits-
und Sozialrecht

Elke Brucker-Kley ist wissenschaftliche Mitarbeiterin am Institut für Wirtschaftsinformatik an der ZHAW School of Management and Law. Sie ist Mitglied der Forschungsgruppe Knowledge und Information Management, Dozierende für IT Service Management und leitet Forschungs- und Beratungsprojekte in den Themenbereichen Informations-, Prozess- und Wissensmanagement.

Thomas Keller ist Leiter des Instituts für Wirtschaftsinformatik (ZWI) und Professor für Wirtschaftsinformatik an der ZHAW School of Management and Law. Zu seinen Forschungs- und Beratungsschwerpunkten zählen Prozessautomatisierung, Business Integration und Software-Architektur.

Lukas Kurtz ist wissenschaftlicher Mitarbeiter am Institut für Wirtschaftsinformatik an der ZHAW School of Management and Law. In dieser Funktion ist er als Teil-Projektleiter in unterschiedlichen Beratungs- und Umsetzungsprojekten im Internet-Umfeld tätig und ist Mitglied der Forschungsgruppe Prozessautomatisierung.

Kurt Pärli ist Leiter des Zentrums für Sozialrecht und Forschungsleiter der Abteilung Business Law an der ZHAW School of Management and Law. Er ist Dozent für Europarecht, Arbeits- und Sozialrecht. Darüber hinaus liegen seine Forschungsschwerpunkte im Bereich Diskriminierungsschutzrecht (www.non-discrimination.ch), Recht der beruflichen Wiedereingliederung, HIV/Aids und Recht sowie Gesundheits- und Datenschutzrecht.



Matthias Schweizer
lic. iur., RA
Wissenschaftlicher Mitarbeiter



Melanie Studer
BSc (ZFH) in Business Law
Wissenschaftliche Assistentin

Matthias Schweizer ist assoziierter wissenschaftlicher Mitarbeiter der Abteilung Business Law an der ZHAW School of Management and Law. Er beschäftigt sich in Forschung und Lehre mit Fragen zum Immaterialgüter- und Technologierecht.

Melanie Studer ist wissenschaftliche Assistentin am Zentrum für Sozialrecht an der ZHAW School of Management and Law. Sie ist dabei insbesondere in Forschungs- und Publikationsprojekten im Diskriminierungsschutzrecht (u.a. Datenbanken auf www.non-discrimination.ch) und Datenschutzrecht tätig.

Beteiligte Experten



Tobias Christen
CTO DSwiss AG
www.securesafe.com



Birgit Aurelia Janetzky
Diplom-Theologin,
Geschäftsführerin Semno UG
(Freiburg, Deutschland)
www.semno.de



Roland Peterhans
Leiter des Zivilstandsamts
der Stadt Zürich
[www.stadt-zuerich.ch/
zivilstandsamt](http://www.stadt-zuerich.ch/zivilstandsamt)



Barbara Bachmann
Gruppenleitung «Geburt und Tod»
des Zivilstandsamts der
Stadt Zürich
[www.stadt-zuerich.ch/
zivilstandsamt](http://www.stadt-zuerich.ch/zivilstandsamt)

Tobias Christen ist CTO der DSwiss AG. Die DSwiss bietet mit ihrem Produkt SecureSafe Endkunden und Geschäftspartnern weltweit die hochsichere Ablage wichtiger Dokumente und Passwörter an, auf die über Web, iPhone und Android App zugegriffen werden kann. Die Datenvererbungsfunktion bietet zudem die Möglichkeit, Dateien und Passwörter im Not- oder Todesfall Partnern, Freunden und Angehörigen automatisch und sicher zukommen zu lassen.

Birgit Aurelia Janetzky ist Geschäftsführerin der Semno UG, Trauerrednerin und Spezialistin für digitalen Nachlass, Tod und Trauer im Internet. Sie kennt nicht nur die psychologischen und philosophischen sondern auch die praktischen Aspekte von Tod, Trauer und Bestattung. Semno unterstützt Angehörige bei der Regelung des digitalen Nachlasses.

Roland Peterhans ist Leiter des Zivilstandsamts der Stadt Zürich.

Barbara Bachmann hat die Gruppenleitung «Geburt und Tod» inne. Das Zivilstandsamt der Stadt Zürich begleitet alle Zivilstandsereignisse in der Stadt Zürich von der Geburt, über die Heirat bis hin zum Tod. Nach der Meldung eines Todesfalls sorgt das Zivilstandsamt für die Registrierung und Beurkundung des Todes und löst die amtlichen Mitteilungen aus.



Rolf Steinmann

Leiter des Bestattungs- und Friedhofsamts der Stadt Zürich
www.stadt-zuerich.ch/bestattungsamt



Prof. Dr. Marc Rennhard

Dozent für Informatik am Institut für angewandte Informationstechnologie an der ZHAW School of Engineering
www.init.zhaw.ch



Thomas Steimer

Umsetzungsprojektmanager E-Government im Bundesamt für Justiz
www.emistar.ch



Yee Wah Tsoi

Manager Corporate Communications, XING AG
www.xing.com

Rolf Steinmann ist Leiter des Bestattungs- und Friedhofsamts der Stadt Zürich. Das Bestattungs- und Friedhofamt erbringt alle Dienstleistungen rund um die Anmeldung von Todesfällen sowie die Bestattung eines verstorbenen Menschen und organisiert nach den Wünschen der Hinterbliebenen die Abschiedsfeier.

Prof. Dr. Marc Rennhard ist Dozent für Informatik am Institut für angewandte Informationstechnologie an der ZHAW School of Engineering. Er ist Leiter des Schwerpunktes Information Security und Projektleiter in diversen F&E Projekten. Er war unter anderem verantwortlich für F&E Projekte in Kooperation mit DSwiss, die die Weiterentwicklung des Datensafes, der Vererbungsfunktion und der mobilen Plattform von SecureSafe zum Gegenstand hatten.

Thomas Steimer ist Dipl. Informatikingenieur FH und hat Rechtswissenschaften studiert. Heute ist er Umsetzungsprojektmanager E-Government im Bundesamt für Justiz. Dort befasst er sich mit verschiedenen Themen im Bereich E-Government und Justiz, im Speziellen mit Fragestellungen rund um das Zivilstandswesen.

Yee Wah Tsoi ist Manager Corporate Communications bei der Xing AG. Xing ist das führende berufliche Online-Netzwerk im deutschsprachigen Raum.

Hildegard Egolf-Zett (MAS Palliative Care FHO) ist Fachexpertin Pflege im Kompetenzzentrum Palliative Care des Universitätsspitals Zürich.

Anhang

Praktiken und Regelungen der Plattformanbieter zum Vorgehen im Todesfall

Die Online-Version dieses Anhangs findet sich auf der Projektwebseite: <http://ares.zhaw.ch/digitalessterben/?cat=28>

ANALYSE PRAKTIKEN UND REGELUNGEN DER PLATTFORMEN

Facebook (Status: Juni 2012)

Unternehmensdaten

URL	https://www.facebook.com
Land (Adresse HQ)	Facebook Inc. (International): USA (Menlo Park, CA); HQ Europa/EMEA: Irland (Dublin)
Rechtsform, Konzernstruktur	Facebook, Inc. ist eine nach dem Recht des States Delaware gegründete und registrierte Gesellschaft. Facebook Ireland Ltd. bietet die Facebook Plattform allen Usern ausserhalb der USA an und ist gleichzeitig EMEA HQ von Facebook

Vorgehen im Todesfall

Gibt es eine kommunizierte Regelung für Todesfälle?	Ja, in den Datenverwendungsrichtlinien. Sowie in der Facebook Hilfe «Wie melde ich einen verstorbenen Nutzer oder ein Konto, das in den Gedenkzustand versetzt bzw. gelöscht werden muss?»
Erhalten Angehörige Zugriff? In welcher Form?	Nein, Facebook Hilfe: «Zum Schutz der Privatsphäre eines verstorbenen Nutzers können wir niemandem die Anmeldeinformationen für das Konto mitteilen. Sobald ein Konto in den Gedenkzustand versetzt wurde, ist es vollständig gesichert und niemand kann mehr darauf zugreifen oder es ändern.» Achtung: Dies bedeutet, dass selbst wenn Angehörige die Facebook-Zugangsdaten haben, sie nicht mehr auf das Konto zugreifen können, sobald das Profil im Gedenkstatus ist. Wenn die Angehörigen zu Lebzeiten nicht als Facebook-Freunde bestätigt waren, können sie das Profil im Gedenkstatus nicht einsehen.
Ablauf aus Sicht der Angehörigen	Es gibt 2 Optionen: 1. Gedenkstatus (Memorialize): Facebook versetzt alle Konten von Nutzern, deren Todesfall gemeldet wird, in den Gedenkzustand. Den Todesfall melden können über das Formular nicht nur Familienmitglieder, sondern auch Freunde. Wenn ein Konto in den Gedenkzustand versetzt wird, können nur bestätigte Freunde das Profil (Chronik) sehen oder in der Suche finden. Ausserdem wird das Profil nicht mehr im «Vorschläge»-Abschnitt der Startseite angezeigt. Freunde und Familienmitglieder können Gedenkbeiträge hinterlassen. 2. Profil löschen: Nur nachgewiesene, unmittelbare Familienangehörige können die Entfernung der Konten von Verstorbenen über einen «Besonderen Antrag» und mit einem offiziellen Todesnachweis beantragen.
Voraussetzungen, zu erbringende Dokumente	Für das Versetzen in den Gedenkstatus reicht eine Todesanzeige oder Nachrichtenmeldung. Das Löschen kann nur von unmittelbaren Familienangehörigen beantragt werden und erfordert: – Geburtsurkunde des Verstorbenen – Sterbeurkunde des Verstorbenen – Rechtsgültiger Nachweis darüber, dass du der rechtmässige Vertreter des Verstorbenen oder von dessen Nachlass bist.
Gibt es Kooperationen mit Vererbungsdiensten?	Ja, diverse Vererbungsdienste (z.B. Ziggur in Europa/NL) berufen sich darauf, Kooperationen mit Facebook zu haben, d.h. diese vollstrecken dann den digitalen Willen bzgl. Facebookprofil. Wurde das Profil jedoch bereits von Freunden/Angehörigen in den Gedenkstatus versetzt, kann der Vererbungsdienst die hinterlegten Zugriffsdaten nicht mehr nutzen, um das Profil zu löschen, falls dieser Wunsch vom Verstorbenen hinterlegt wurde.

Post-mortem Szenarien: Welche Optionen ermöglicht der Plattformanbieter?

A Nachwelt informieren

A1 Last Message / email / blog / tweet / auto response	Nein, nicht direkt; Angehörige können über die Wall des Verstorbenen über den Todesfall informieren; evtl. in Kombination mit dem Versetzten des Profils in den Gedenkstatus
---	--

B Daten / Accounts löschen

B1 Account und Daten löschen	Ja, über eine «Besondere Anfrage»; jedoch nur für unmittelbare Familienangehörige und mit offiziellem Dokument zwecks Todesnachweis; Die finale und permanente Löschung der Daten erfolgt verzögert (ca. 90 Tage). Zu Lebzeiten ist das endgültige Löschen des Facebook-Profiles inkl. Daten durch den Nutzer selbst möglich bzw. durch die Angehörigen im Todesfall, falls diese die Zugangsdaten haben
-------------------------------------	--

B2 Automatische Löschung (bei Inaktivität, Frist?)	Nein, Facebook löscht keine inaktiven Konten
---	--

C Bewahren

C1 Account / Daten bleiben unverändert (unbegrenzt, ohne Nachricht)	Ja, falls der Todesfall nicht gemeldet wird
--	---

C2 Account wird deaktiviert / stillgelegt, Daten bleiben erhalten	Ja, über Kontoeinstellungen/Sicherheit kann das Konto deaktiviert werden, ohne dass die Daten gelöscht werden. Das Konto kann wieder reaktiviert werden. Nur möglich, falls die Angehörigen die Zugriffsdaten haben
--	---

C3 Gedenkstatus	Ja, auch durch Freunde oder Arbeitskollegen. Als Nachweis reicht eine Todesanzeige oder ein Nachrichtentext; Formular zur Versetzung eines Profils in den Gedenkstatus: https://www.facebook.com/help/contact/?id=305593649477238
------------------------	---

C4 Archivierung (Verschiebung der Daten, Archivierung über speziellen Dienst z.B. SocialSafe, FlickrEdit)	Zu Lebzeiten ja oder falls die Angehörigen die Zugriffsdaten haben. Unter den Account-Einstellungen hat jeder Facebook-Nutzer die Möglichkeit, seine Facebook-Inhalte in ein Archiv herunterzuladen, d.h. eine Kopie der Inhalte zu erstellen (vom Nutzer eingestellte Fotos, Videos, Pinnwandbeiträge, Nachrichten, Chatunterhaltungen, Namen von Freunden und E-Mail-Adressen, falls hinterlegt). Facebook gibt Angehörigen weder die Zugriffsdaten noch erstellt es für die Angehörigen ein Archiv. Daneben gibt es Freeware Tools wie ArchiveFacebook oder SocialSafe, mit denen ein Facebook-Archiv erstellt werden kann.
--	--

C5 Datenkopien werden den Angehörigen überlassen	Nein
---	------

C6 Guthaben werden den Angehörigen überlassen	Es existiert keine kommunizierte Regelung zum Verbleib von Facebook Credits
--	---

C7 Veröffentlichung des digitalen Erbes (Aufhebung Zugriffsbeschränkungen)	Nein, Profile im Gedenkstatus sind nur für die bestätigten Freunde noch sichtbar
---	--

Durchsetzbarkeit gemäss AGB o.ä.

Gerichtsstand	Gemäss Nutzungsbedingungen (Stand 8. Juni 2012): 16.1: USA: Staats- oder Bundesgericht in Santa Clara County, Kalifornien; «Du wirst sämtliche Ansprüche, Klagegegenstände oder Streitfälle (Ansprüche), die du uns gegenüber hast und die sich aus dieser Erklärung oder aus Facebook oder in Verbindung damit ergeben, ausschliesslich vor einem Staats- oder Bundesgericht in Santa Clara County, Kalifornien, klären bzw. klären lassen. Diese Erklärung sowie alle Ansprüche, die möglicherweise zwischen dir und uns entstehen, unterliegen den Gesetzen des Bundesstaates Kalifornien, unter Ausschluss der Bestimmungen des internationalen Privatrechts. Du erklärst dich damit einverstanden, dich bei einem Prozess über alle derartigen Ansprüche der personenbezogenen Zuständigkeit der Gerichte in Santa Clara County, Kalifornien, zu unterwerfen.» Ausnahme: Für Nutzer mit Wohnsitz in Deutschland gelten spezielle Bedingungen (Stand 20.4.2012) und das deutsche Recht. Gemäss dem «Facebook Ireland Ltd – Report of Audit. Appendix 4 – Structure of European Offices» (Data Protection Commissioner of Ireland, 2011: S. 213) reguliert das Irische Recht die Nutzung aller nicht-US-Amerikanischer Facebook-Nutzer «Irish data protection law regulates the use of all non-North American Facebook user data». Die sonstigen europäischen Facebook Offices haben lediglich Vertriebs/Marketing-funktionen (Amsterdam, Hamburg, London, Madrid, Milan, Paris, Stockholm).
---------------	---

Aussagen zum Eigentum der gespeicherten Daten/ Inhalte, Urheberrechte, Nutzungsrechte etc.	Nutzungsbedingungen Abs.2 (Stand 8. Juni 2012): «Du bist Eigentümer aller Inhalte und Informationen, die du auf Facebook postest. Zudem kannst du mithilfe deiner Privatsphäre- und Anwendungseinstellungen kontrollieren, wie diese Informationen ausgetauscht werden. Ferner: Für Inhalte wie Fotos und Videos («IP-Inhalte»), die unter die Rechte an geistigem Eigentum fallen, erteilst du uns durch deine Privatsphäre- und Anwendungseinstellungen die folgende Erlaubnis: Du gibst uns eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest («IP-Lizenz»). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löschst, ausser deine Inhalte wurden mit anderen Nutzern geteilt und diese haben die Inhalte nicht gelöscht. – Wenn du IP-Inhalte löschst, werden sie auf eine Weise entfernt, die dem Leeren des Recyclingbehälters auf einem Computer gleichkommt. Allerdings sollte dir bewusst sein, dass entfernte Inhalte für eine angemessene Zeitspanne in Sicherheitskopien fortbestehen (für andere jedoch nicht zugänglich sind).» Für deutsche Nutzer gilt die Einschränkung, dass Facebook's Nutzung der Inhalte auf die Verwendung auf oder in Verbindung mit Facebook beschränkt ist (https://www.facebook.com/terms/provisions/german/index.php). Abs. 17 «Wir versuchen eine globale Gemeinschaft zu schaffen, deren Standards einheitlich sind und für alle Mitglieder gelten. Allerdings bemühen wir uns dabei auch die regionalen Gesetze zu berücksichtigen. Die folgenden Bestimmungen sind für Nutzer ausserhalb der USA bindend: Du bist damit einverstanden, dass deine persönlichen Daten in die USA weitergeleitet und dort verarbeitet werden.»
--	---

Quellen, Bedingungen, rechtliche Grundlagen

URL AGBs, Nutzungsbedingungen, legal terms	Nutzungsbedingungen international (in deutsch, Stand 8.6.2012): https://www.facebook.com/legal/terms
Spezielle AGBs, z.B. für bestimmte Geographien	Spezielle Nutzungsbedingungen für Nutzer mit Wohnsitz in Deutschland: https://www.facebook.com/terms/provisions/german/index.php
URL zu Datenschutzrichtlinien	Datenverwendungsrichtlinien (in deutsch) Stand 8. Juni 2012: https://www.facebook.com/about/privacy/
Sonstige relevanten URLs/Online Hilfen des Anbieters zur Problematik	Facebook Hilfe «Wie melde ich einen verstorbenen Nutzer oder ein Konto, das in den Gedenkzustand versetzt bzw. gelöscht werden muss?»: https://www.facebook.com/help/?faq=150486848354038#Wie-melde-ich-einen-verstorbenen-Nutzer-oder-ein-Konto,-das-in-den-Gedenkzustand-versetzt-bzw.-gel%C3%B6scht-werden-muss?

Xing (Status: Mai 2012)

Unternehmensdaten

URL	https://www.xing.com
Land (Adresse HQ)	Deutschland (Hamburg)
Rechtsform, Konzernstruktur	AG

Vorgehen im Todesfall

Gibt es eine kommunizierte Regelung für Todesfälle?	Auf der Xing Website (AGB, FAQ etc.) ist keine Regelung oder Hilfestellung für Angehörige kommuniziert. Auskunft erhalten Angehörige über den Kundenservice von Xing.
Erhalten Angehörige Zugriff? In welcher Form?	Nein, da XING keine personenbezogenen Daten an Dritte weitergibt.
Ablauf aus Sicht der Angehörigen	Netzwerkkontakte oder Hinterbliebene wenden sich an den Xing Kundendienst. Eine Todesurkunde oder sonstiger Nachweis ist nicht notwendig. Profile von Verstorbenen werden inaktiv geschaltet (unsichtbar). Endgültig gelöscht werden sie erst nach ca. drei Monaten, um fehlerhaftes Löschen (Verwechslung, Falschmeldung) zu vermeiden.
Voraussetzungen, zu erbringende Dokumente	Keine, da Xing das Profil zunächst stilllegt und erst nach 3 Monaten löscht. So können Löschungen infolge Falschmeldungen verhindert werden
Gibt es Kooperationen mit Vererbungsdiensten?	Nein

Post-mortem Szenarien: Welche Optionen ermöglicht der Plattformanbieter?

A Nachwelt informieren**A1** Last Message/ email/ blog/ tweet/
auto response

Nein

B Daten/Accounts löschen**B1** Account und Daten löschenIm Todesfall: Ja nach Meldung und Ablauf von 3 Monaten nach der Stilllegung wird das Profil gelöscht.
Zu Lebzeiten: Über Hilfe «Rücktritt von der kostenlosen Basis-Mitgliedschaft».**B2** Automatische Löschung (bei Inaktivität, Frist?)

Nein, Xing löscht keine Profile bei Inaktivität.

C Bewahren**C1** Account/Daten bleiben unverändert
(unbegrenzt, ohne Nachricht)

Ja, falls der Todesfall nicht gemeldet wird.

C2 Account wird deaktiviert/ stillgelegt,
Daten bleiben erhaltenJa, direkt bei Meldung wird das Konto stillgelegt, d.h. es ist nicht mehr sichtbar;
Löschung nach 3 Monaten.**C3** Gedenkstatus

Nein

C4 Archivierung (Verschiebung der Daten,
Archivierung über speziellen Dienst z.B.
SocialSafe, FlickrEdit)Zu Lebzeiten ja oder falls die Angehörigen die Zugriffsdaten haben: mit dem
XING Connector als kostenloses Plug-in für den Microsoft Outlook Social
Connector (OSC) können Kontakte mit Microsoft Outlook synchronisiert werden.**C5** Datenkopien werden den Angehörigen
überlassen

Nein, keine Abgabe personenbezogener Daten an Dritte.

C6 Guthaben werden den Angehörigen überlassen

NA

C7 Veröffentlichung des digitalen Erbes
(Aufhebung Zugriffsbeschränkungen)

Nein

Durchsetzbarkeit gemäss AGB o.ä.

Gerichtsstand

Amtsgericht Hamburg; Gemäss AGB Xing: «12.4 Erfüllungsort ist der Sitz von XING.,
12.5 Gerichtsstand für Kaufleute im Sinne des Handelsgesetzbuches (HGB) ist der
Sitz von XING. 12.6 Es gilt deutsches Recht unter Ausschluss des Internationalen
Privatrechts und des ins deutsche Recht übernommenen UN-Kaufrechts.»Aussagen zum Eigentum der gespeicherten Daten/
Inhalte, Urheberrechte, Nutzungsrechte etc.In den AGBs und ergänzenden Dateschutzbestimmungen verpflichtet sich Xing, die
Daten nicht weiterzugeben. Die Kontrolle über die Freigabe liegt beim Nutzer selbst.
«XING unterwirft sich folgenden Grundsätzen beim Schutz Ihrer personenbezogenen
Daten: XING erhebt, verarbeitet und nutzt Ihre personenbezogenen Daten unter
Einhaltung der Datenschutzgesetze der Bundesrepublik Deutschland und der
Datenschutzbestimmungen der Europäischen Union. XING nutzt Ihre personen-
bezogenen Daten ausschliesslich, um Ihnen die Inanspruchnahme der registrie-
rungspflichtigen Internet-Dienste von XING zu ermöglichen. In keinem Fall wird XING
Ihre personenbezogenen Daten zu Werbe- oder Marketingzwecken oder unbefugt
zu anderen Zwecken Dritten übermitteln (das heisst zum Beispiel zur Kenntnis geben
oder weitergeben).» Aussagen zu Eigentum oder Urheberschaft werden in den
AGBs oder Dateschutzbestimmungen nicht gemacht.**Quellen, Bedingungen, rechtliche Grundlagen**

URL AGBs, Nutzungsbedingungen, legal terms

AGB (abgerufen, Stand 14.5.2012): <https://www.xing.com/terms>

Spezielle AGBs, z.B. für bestimmte Geographien

URL zu Datenschutzrichtlinien

Datenschutzbestimmungen von Xing (abgerufen, Stand 14.5.2012):
<https://www.xing.com/privacy>Sonstige relevanten URLs/Online Hilfen des
Anbieters zur Problematik

Gmail (Google) (Status: Juni 2012)**Unternehmensdaten**

URL	https://www.google.com
Land (Adresse HQ)	USA (Mountain View, CA)
Rechtsform, Konzernstruktur	Gmail ist ein Produkt der Google Inc.

Vorgehen im Todesfall

Gibt es eine kommunizierte Regelung für Todesfälle?	Ja, nicht in den Nutzungsbedingungen, aber über die Google Mail Hilfe: «Zugriff auf die E-Mails einer verstorbenen Person»
Erhalten Angehörige Zugriff? In welcher Form?	Unter Umständen ja; jedoch liegt dies im Ermessen von Google und ist erst nach Durchlaufen eines langwierigen Verfahrens möglich (s.u.).
Ablauf aus Sicht der Angehörigen	Ein «autorisierter Vertreter» kann unter Umständen Zugriff zum Inhalt des Email-Kontos erhalten. Es muss ein zweistufiges Verfahren durchlaufen werden. In Stufe 1 muss der «autorisierte Vertreter» die unter «Voraussetzungen» gelisteten Dokumente bei Google Support (Mountain View, CA) einreichen, u.a. eine englischsprachige Sterbeurkunde. Nur wenn Google nach Stufe 1 Bereitschaft signalisiert Zugriff zu gewähren, ist Stufe 2 möglich, wobei keine Garantie gegeben wird, dass der Zugriff erteilt wird. In Stufe 2 sind weitere Rechtswege erforderlich, einschliesslich einer Anordnung eines US-Gerichts und/oder der Vorlage weiterer Materialien (z.B. Erbschein).
Voraussetzungen, zu erbringende Dokumente	Google verlangt folgende Informationen: «1. vollständigen Namen 2. Ihre Anschrift 3. Ihre E-Mail-Adresse 4. Eine Fotokopie des amtlichen Ausweises oder Führerscheins 5. Die Google Mail-Adresse des verstorbenen Nutzers Die Sterbeurkunde des verstorbenen Nutzers. Sofern das Dokument nicht auf Englisch verfasst ist, benötigen wir eine von einem entsprechend beeidigten Übersetzer ausgestellte, beglaubigte Übersetzung ins Englische. 6. Die folgenden Informationen aus einer E-Mail, die Sie unter Ihrer E-Mail-Adresse von dem betreffenden Google Mail-Konto erhalten haben: Die vollständigen Kopfzeilen (Header) der E-Mail. Informationen zum Anzeigen der Kopfzeilen bei Google Mail und anderen Webmail-Anbietern finden Sie in dieser Anleitung. Kopieren Sie bitte sämtlichen Text von der Zeile «Delivered-To:» bis zur Zeile «References:». Den vollständigen Inhalt der Nachricht 7. Schicken Sie diese Informationen per Post oder Telefax an: Google Inc., Gmail User Support – Decedents' Accounts, c/o Google Custodian of Records, 1600 Amphitheatre Parkway, Mountain View, CA 94043»
Gibt es Kooperationen mit Vererbungsdiensten?	Nicht bekannt

Post-mortem Szenarien: Welche Optionen ermöglicht der Plattformanbieter?**A Nachwelt informieren**

A1 Last Message /email/ blog/ tweet/ auto response	Nein, grundsätzlich wäre es möglich Gmail und die darin abgelegten Kontakte für die Abschiedsbotschaft zu nutzen, falls die Hinterbliebenen Zugriff auf das E-Mail Konto und entsprechende Anweisungen haben.
---	---

B Daten/Accounts löschen

B1 Account und Daten löschen	Nein; Google Konto löschen ist grundsätzlich möglich jedoch nur zu Lebzeiten, d.h. durch den Nutzer selbst oder wenn die Angehörigen die Zugriffsdaten haben; Wird ein Google Konto gelöscht, werden automatisch alle davon abhängigen Konten von Google-Produkten (z.B. YouTube, Picasa) ebenfalls gelöscht.
B2 Automatische Löschung (bei Inaktivität, Frist?)	Google löscht keine ruhenden oder inaktiven Konten.

C Bewahren

C1 Account /Daten bleiben unverändert (unbegrenzt, ohne Nachricht)	Ja
---	----

C2 Account wird deaktiviert / stillgelegt, Daten bleiben erhalten	Nein; Google kann Konten deaktivieren/sperrern. Dies ist jedoch keine Option für Nutzer.
C3 Gedenkstatus	Nein
C4 Archivierung (Verschiebung der Daten, Archivierung über speziellen Dienst z.B. SocialSafe, FlickrEdit)	Zu Lebzeiten ja, gemäss Nutzungsbedingungen, oder falls die Angehörigen die Zugriffsdaten haben: «Ihre Daten gehören Ihnen und wir halten es für wichtig, dass Sie auf diese Daten zugreifen können. Sollten wir einen Dienst einstellen, werden wir, sofern vernünftigerweise möglich, Sie im Voraus angemessen darüber informieren und Ihnen die Möglichkeit geben, Ihre Daten aus diesem Dienst zu exportieren.» Google verlinkt für den Export von Daten aus Googleprodukten auf http://www.dataliberation.org/ .
C5 Datenkopien werden den Angehörigen überlassen	Nein
C6 Guthaben werden den Angehörigen überlassen	NA
C7 Veröffentlichung des digitalen Erbes (Aufhebung Zugriffsbeschränkungen)	Nein
Durchsetzbarkeit gemäss AGB o.ä.	
Gerichtsstand	Nutzungsbedingungen (Stand:1. März 2012): «Alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesen Nutzungsbedingungen oder Diensten ergeben, unterliegen dem Recht des US-Bundesstaats Kalifornien, mit Ausnahme der Regelungen des Internationalen Privatrechts. Alle Ansprüche, die sich aus oder im Zusammenhang mit diesen Nutzungsbedingungen oder Diensten ergeben, werden ausschliesslich vor Bundesgerichten oder den Gerichten des Verwaltungsbezirks Santa Clara, Kalifornien, USA, verhandelt und Sie und Google erklären sich mit der Zuständigkeit dieser Gerichte einverstanden. Gemäss den deutschen Nutzungsbedingungen, gilt deutsches Recht.
Aussagen zum Eigentum der gespeicherten Daten / Inhalte, Urheberrechte, Nutzungsrechte etc.	Nutzungsbedingungen (Stand: 1. März 2012): «Bei einigen unserer Dienste können Sie Inhalte einstellen. Sie behalten alle bestehenden gewerblichen Schutzrechte an den Inhalten, die Sie in unsere Dienste einstellen. Kurz gesagt: Was Ihnen gehört, bleibt auch Ihres. Wenn Sie Inhalte in unsere Dienste hochladen oder auf andere Art und Weise in diese einstellen, räumen Sie Google (und denen, mit denen wir zusammenarbeiten) das Recht ein, diese Inhalte weltweit zu verwenden, zu hosten, zu speichern, zu vervielfältigen, zu verändern, abgeleitete Werke daraus zu erstellen (einschliesslich solcher, die aus Übersetzungen, Anpassungen oder anderen Änderungen resultieren, die wir vornehmen, damit Ihre Inhalte besser in unseren Diensten funktionieren), zu kommunizieren, zu veröffentlichen, öffentlich aufzuführen, öffentlich anzuzeigen und zu verteilen. Diese von Ihnen im Rahmen dieser Lizenz gewährten Rechte dienen ausschliesslich zur Durchführung, Förderung und Verbesserung unserer Dienste sowie zur Entwicklung neuer Dienste. Diese Rechteinräumung bleibt auch dann bestehen, wenn Sie unsere Dienste nicht mehr verwenden, z.B. bei einem Brancheneintrag, den Sie in Google Maps eingefügt haben. Bei einigen Diensten können Sie auf von Ihnen bereitgestellte Inhalte zugreifen und diese aus dem entsprechenden Dienst entfernen. In einigen unserer Dienste wird unsere Nutzung der von Ihnen bereitgestellten Inhalte durch die Nutzungsbedingungen oder Einstellungen eingeschränkt. Achten Sie darauf, dass Sie über die notwendigen Rechte verfügen, um uns eine entsprechende Lizenz für alle Inhalte zu erteilen, die Sie in unsere Dienste hochladen.»
Quellen, Bedingungen, rechtliche Grundlagen	
URL AGBs, Nutzungsbedingungen, legal terms	Nutzungsbedingungen (international, in deutsch, (Stand 1. März 2012): https://www.google.com/intl/de/policies/terms/
Spezielle AGBs, z.B. für bestimmte Geographien	Für Deutschland gelten spezielle Nutzungsbedingungen: https://www.google.de/policies/terms/regional.html
URL zu Datenschutzrichtlinien	Per 1.3.2012 hat Google die Datenschutzbestimmungen für ihre > 60 Produkte vereinheitlicht und eine einheitliche Datenschutzerklärung veröffentlicht: https://www.google.com/intl/de/policies/privacy/
Sonstige relevanten URLs / Online Hilfen des Anbieters zur Problematik	Google Mail Hilfe / Zugriff auf die E-Mails einer verstorbenen Person: http://support.google.com/mail/bin/answer.py?hl=de&answer=14300

YouTube (Google Inc.) (Status: Juni 2012)

Unternehmensdaten

URL	https://www.youtube.com
Land (Adresse HQ)	USA (San Bruno, CA)
Rechtsform, Konzernstruktur	YouTube LLC; gehört seit 2006 zu Google Inc.; die Nutzung von YouTube erfordert einen Google Account

Vorgehen im Todesfall

Gibt es eine kommunizierte Regelung für Todesfälle?	Nicht speziell für YouTube (eine 2011 noch existierende YouTube Hilfeseite zu diesem Thema ist nicht mehr abrufbar). Da ein YouTube Account an einen Google Account gebunden ist, ist zu vermuten, dass wie beim Zugriff auf Gmail-Konten von Verstorbenen verfahren wird. Google hat nur diese Regelung kommuniziert, jedoch keine Regelung für Google Accounts insgesamt oder für YouTube im Speziellen.
Erhalten Angehörige Zugriff? In welcher Form?	Siehe Gmail
Ablauf aus Sicht der Angehörigen	Siehe Gmail
Voraussetzungen, zu erbringende Dokumente	Siehe Gmail
Gibt es Kooperationen mit Vererbungsdiensten?	Ja, Ziggur; ansonsten nicht bekannt

Post-mortem Szenarien: Welche Optionen ermöglicht der Plattformanbieter?

A Nachwelt informieren

A1 Last Message / email / blog / tweet / auto response	Nein; grundsätzlich hätte man die Möglichkeit ein «Abschiedsvideo» bei YouTube einzustellen und dies als «private» zu deklarieren und bis zu 50 Gäste dazu einzuladen. Der Upload und die Einladung müsste jedoch zu Lebzeiten oder durch einen Beauftragten erfolgen.
---	--

B Daten/Accounts löschen

B1 Account und Daten löschen	YouTube Account hängt am Google Konto; Google Konten können gelöscht werden; jedoch nur zu Lebzeiten, d.h. durch den Nutzer selbst oder wenn die Angehörigen die Zugriffsdaten haben; Die gelöschten Videos tauchen noch einige Zeit in den Suchlisten und als Thumbnail auf, bis die Löschung technisch abgeschlossen ist.
B2 Automatische Löschung (bei Inaktivität, Frist?)	YouTube Account hängt am Google Konto; Google löscht keine ruhenden oder inaktive Konten.

C Bewahren

C1 Account / Daten bleiben unverändert (unbegrenzt, ohne Nachricht)	Ja
C2 Account wird deaktiviert / stillgelegt, Daten bleiben erhalten	Nein, eine Variante wäre die Grundeinstellung eines oder mehrerer Videos von «public» auf «privat» zu ändern. Die erfordert jedoch Zugriff auf den Account.
C3 Gedenkstatus	Nein
C4 Archivierung (Verschiebung der Daten, Archivierung über speziellen Dienst z.B. SocialSafe, FlickrEdit)	Das Herunterladen von Videos wird in YouTube grundsätzlich nicht unterstützt. Ausgenommen sind nur eigene Videos, die als MP4 heruntergeladen werden können. Dies erfordert jedoch den Zugriff auf den Account.
C5 Datenkopien werden den Angehörigen überlassen	Nein
C6 Guthaben werden den Angehörigen überlassen	NA

C7 Veröffentlichung des digitalen Erbes (Aufhebung Zugriffsbeschränkungen)	Die Grundeinstellung von Youtube Videos ist «Public». Der Zugriff kann beschränkt werden, indem man ein Video auf «Private» setzt (Zugriff für max. 50 eingeladene Gäste). Dieser Status kann geändert werden, vorausgesetzt man hat Zugriff auf den Account.
Durchsetzbarkeit gemäss AGB o.ä.	
Gerichtsstand	Youtube Terms of Service (Stand bei Abruf: 9. Juni 2010) Art.14: «These Terms of Service shall be governed by the internal substantive laws of the State of California, without respect to its conflict of laws principles. Any claim or dispute between you and YouTube that arises in whole or in part from the Service shall be decided exclusively by a court of competent jurisdiction located in Santa Clara County, California.»
Aussagen zum Eigentum der gespeicherten Daten/ Inhalte, Urheberrechte, Nutzungsrechte etc.	Youtube Terms of Service (Stand bei Abruf: 9. Juni 2010) Abs.6.C.: «For clarity, you retain all of your ownership rights in your Content. However, by submitting Content to YouTube, you hereby grant YouTube a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the Content in connection with the Service and YouTube's (and its successors' and affiliates') business, including without limitation for promoting and redistributing part or all of the Service (and derivative works thereof) in any media formats and through any media channels. You also hereby grant each user of the Service a non-exclusive license to access your Content through the Service, and to use, reproduce, distribute, display and perform such Content as permitted through the functionality of the Service and under these Terms of Service. The above licenses granted by you in video Content you submit to the Service terminate within a commercially reasonable time after you remove or delete your videos from the Service. You understand and agree, however, that YouTube may retain, but not display, distribute, or perform, server copies of your videos that have been removed or deleted. The above licenses granted by you in user comments you submit are perpetual and irrevocable.»
Quellen, Bedingungen, rechtliche Grundlagen	
URL AGBs, Nutzungsbedingungen, legal terms	Youtube Nutzungsbedingungen (Stand bei Abruf: 9. Juni 2010): http://www.youtube.com/t/terms
Spezielle AGBs, z.B. für bestimmte Geographien	–
URL zu Datenschutzrichtlinien	Es gilt die Datenschutzerklärung von Google; Per 1.3.2012 hat Google die Datenschutzbestimmungen für ihre > 60 Produkte vereinheitlicht und eine einheitliche Datenschutzerklärung veröffentlicht. (Stand bei Abruf: 1. März 2012): https://www.google.com/intl/de/policies/privacy/
Sonstige relevanten URLs/Online Hilfen des Anbieters zur Problematik	–

Flickr (Yahoo!) (Status: Juni 2012)**Unternehmensdaten**

URL	https://www.flickr.com
Land (Adresse HQ)	International USA (Sunnyvale, CA); Schweiz/Deutschland: Yahoo! Deutschland GmbH (München)
Rechtsform, Konzernstruktur	Seit 2005 im Besitz von Yahoo! Corporation; Flickr wurde von Ludicorp entwickelt, einem 2002 in Kanada gegründeten Unternehmen mit Sitz in Vancouver, Canada

Vorgehen im Todesfall

Gibt es eine kommunizierte Regelung für Todesfälle?	Ja, in den AGB von Yahoo! Deutschland: (Stand bei Abruf: April 2012), die auch für Flickr gelten. «Abs. 5.4 Ein Account ist nicht übertragbar und alle Rechte an dem Account und den gespeicherten Inhalten erlöschen mit dem Tod des Nutzers.» In den internationalen Yahoo! AGB (Stand bei Abruf 24.11.2008) wird präzisiert: «No Right of Survivorship and Non-Transferability. You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted.»
Erhalten Angehörige Zugriff? In welcher Form?	Nein, Konto und Inhalte sind nicht übertragbar. Die Angehörigen können nur die Löschung beantragen. Ansonsten bleibt das Konto bestehen, aber die Angehörigen haben gemäss AGB keinerlei Rechte mehr am Konto oder Inhalt, da diese mit dem Tod des Inhabers enden. Siehe Abs. 5.4 der AGB von Yahoo! Deutschland: «Ein Account ist nicht übertragbar und alle Rechte an dem Account und den gespeicherten Inhalten erlöschen mit dem Tod des Nutzers.»
Ablauf aus Sicht der Angehörigen	Haben die Angehörigen bereits zu Lebzeiten Zugriff auf die Fotos, da sie als Kontakt des Verstorbenen in Flickr hinterlegt wurden, haben Sie weiterhin Zugriff auf die Fotos, für die sie vom Verstorbenen freigeschalten wurden. Der Umfang des Zugriffs (anschauen, herunterladen) hängt davon ab, wie dieser beim Upload der Fotos eingestellt wurde, d.h. Fotos können nur heruntergeladen werden, sofern der Inhaber diese Einstellung gewählt hat. Problematisch wird es, wenn die Angehörigen zu Lebzeiten weder als Gast noch als aktiver Flickr-User Zugriff auf die Fotos hatten und zudem keine lokale Kopie der Fotos auf einem Endgerät des Verstorbenen besteht. In diesem Fall haben sie lediglich die Möglichkeit über Freunde oder Kontakte, die Zugriff auf die Fotos haben, zu gehen. Ansonsten erhalten sie keinen Zugriff auf die Fotos und können maximal deren Löschung beantragen. Wünschen die Angehörigen, dass der Flickr-Account bestehen bleibt, ist dies möglich, da die Löschung explizit mit Todesurkunde beantragt werden muss. Jedoch haben die Angehörigen keinerlei Rechte am Konto oder den Fotos, da diese gemäss Abs. 5.4 der AGB von Yahoo! Deutschland mit dem Tod des Inhabers enden.
Voraussetzungen, zu erbringende Dokumente	Todesurkunde («death certificate»)
Gibt es Kooperationen mit Vererbungsdiensten?	Ja, Ziggur; ansonsten nicht bekannt.
Post-mortem Szenarien: Welche Optionen ermöglicht der Plattformanbieter?	
A Nachwelt informieren	
A1 Last Message / email / blog / tweet / auto response	Nein
B Daten / Accounts löschen	
B1 Account und Daten löschen	Ja, wenn die Löschung mit Todesurkunde beantragt wird.
B2 Automatische Löschung (bei Inaktivität, Frist?)	Flickr Hilfe: Flickr löscht keine Accounts aufgrund von Inaktivität. Grundsätzlich behält sich Flickr vor, kostenlose Accounts nach 4 Monaten Inaktivität zu löschen (analog Yahoo!-E-mail-Konten). Jedoch kommuniziert Flickr im Hilfeforum, dass sie dies noch nie getan hätten. Auch ein kostenpflichtiger Pro Account wird nicht gelöscht, falls das Abo nicht verlängert wird. Diese Angaben reflektieren jedoch die momentane Geschäftspraxis von Flickr (Stand Mai 2012); die offiziellen Yahoo!-Policies sehen die Löschung nach 4 Monaten Inaktivität vor AGB von Yahoo! Deutschland: «Abs. 14.7: Soweit Sie Ihren E-Mail-Account mehr als 4 Monate nicht genutzt haben, kann Yahoo! Ihren E-Mail-Account inaktiv stellen und alle darin enthaltenen Inhalte löschen.»
C Bewahren	
C1 Account / Daten bleiben unverändert (unbegrenzt, ohne Nachricht)	Ja

C2 Account wird deaktiviert / stillgelegt, Daten bleiben erhalten	Nein
C3 Gedenkstatus	Nein
C4 Archivierung (Verschiebung der Daten, Archivierung über speziellen Dienst z.B. SocialSafe, FlickrEdit)	Das Herunterladen von Fotos ist ein Feature von Flickr und ist möglich sofern der Kontoinhaber diese Option als globale Einstellung für seine Fotos erlaubt hat. Dies ist jedoch nur möglich, wenn die Angehörigen als Kontakt oder Gast auf die Sammlungen bzw. Fotos berechtigt waren. Daneben gibt es diverse Freeware Tools, die es erlauben Fotos oder ganze Alben aus Flickr herunterzuladen, vorausgesetzt man ist berechtigt (z.B. Downloadr, FlickrEdit, Flickr Backup), d.h. zu Lebzeiten oder falls die Angehörigen die Zugriffsdaten haben.
C5 Datenkopien werden den Angehörigen überlassen	Nein
C6 Guthaben werden den Angehörigen überlassen	NA
C7 Veröffentlichung des digitalen Erbes (Aufhebung Zugriffsbeschränkungen)	Nein, kein Feature, aber grundsätzlich könnten Angehörige, falls sie die Zugriffsdaten haben, bestimmte oder alle Fotos der Allgemeinheit zugänglich machen.
Durchsetzbarkeit gemäss AGB o.ä.	
Gerichtsstand	Es ist für den Nutzer schwer ersichtlich, welche Yahoo! AGBs für welchen Dienst und welchen Nutzungsort gelten. Nutzer in der Schweiz werden bei Aufruf der Nutzungsbedingungen auf Flickr auf die AGB von Yahoo! Deutschland (Stand bei Abruf: April 2012) geführt «Abs. 23.5 Für Streitigkeiten aus oder im Zusammenhang mit der Nutzung der Dienste und/oder dem Nutzungsvertrag sind die Gerichte in München ausschliesslich zuständig, sofern Sie Ihren Wohnsitz oder gewöhnlichen Aufenthaltsort nicht in Deutschland haben, nach Vertragsschluss ins Ausland verlegt haben oder ihr Wohnsitz oder gewöhnlicher Aufenthalt im Zeitpunkt der Klageerhebung nicht bekannt ist.»
Aussagen zum Eigentum der gespeicherten Daten/ Inhalte, Urheberrechte, Nutzungsrechte etc.	Die Fotos sind Eigentum der Kontoinhaber; jedoch hat Yahoo automatisch eine weltweite nicht-exklusive Lizenz für Inhalte die in öffentliche und nicht öffentliche Bereiche von Yahoo! eingestellt werden*. Die Yahoo terms gehen in diesem Zusammenhang nicht konkret auf Flickr ein. Flickr ermöglicht über eine Standardeinstellung die Fotos beim Upload frei verwertbar zu halten oder zu lizenzieren (http://www.flickr.com/account/prefs/license/). Diese sogenannte Creative Commons Lizenz ermöglicht mittels 6 verschiedenen Standardlizenzen, Fotos zur Nutzung mit mehr oder weniger starken Einschränkungen freizugeben (z.B. nur mit Namensnennung, keine kommerzielle Nutzung, keine Bearbeitung etc.). Durch eine Kooperation mit Getty Images können Flickr-Nutzer ihre Fotos auch kommerziell lizenzieren. *AGBs Yahoo! Deutschland (Stand bei Abruf: April 2012): Art. 9.2 «Wenn Sie einen Inhalt in einen nicht öffentlich zugänglichen Bereich eingeben, gewähren Sie Yahoo!, den mit Yahoo! gemäss § 15 AktG verbundenen Unternehmen sowie Vertragspartnern von Yahoo! das gebührenfreie, nicht ausschliessliche, unbefristete Recht, diesen Inhalt (ganz oder teilweise) weltweit zu nutzen, soweit dies allein zur Erbringung der im Rahmen des betreffenden Dienstes angebotenen Leistungen geschieht. Hierfür ist es insbesondere erforderlich, dass die von Ihnen eingegebenen Inhalte von Yahoo! gespeichert, zum Abruf bereitgehalten, auf Servern gehostet, technisch vervielfältigt, dargestellt und den Personen zur Verfügung gestellt werden, die Zugang zu dem nicht öffentlich zugänglichen Bereich haben. Dieses Recht gilt nur so lange, wie Sie den Inhalt in dem betreffenden nicht öffentlich zugänglichen Bereich zugänglich machen wollen, und erlischt, sobald Sie den Inhalt aus dem nicht öffentlich zugänglichen Bereich entfernen.»
Quellen, Bedingungen, rechtliche Grundlagen	
URL AGBs, Nutzungsbedingungen, legal terms	Yahoo! International (Stand bei Abruf: 24. November 2008): http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html
Spezielle AGBs, z.B. für bestimmte Geographien	Flickr Nutzer in der Schweiz werden bei Aufruf der Nutzungsbedingungen auf Flickr auf die AGB von Yahoo! Deutschland (Stand bei Abruf: April 2012) geführt: http://info.yahoo.com/legal/de/yahoo/tos.html
URL zu Datenschutzrichtlinien	Yahoo! Datenschutzcenter: http://info.yahoo.com/privacy/de/yahoo/
Sonstige relevanten URLs / Online Hilfen des Anbieters zur Problematik	–

Twitter (Status: Juni 2012)

Unternehmensdaten

URL	https://www.twitter.com
Land (Adresse HQ)	USA (San Francisco, CA)
Rechtsform, Konzernstruktur	Inc.

Vorgehen im Todesfall

Gibt es eine kommunizierte Regelung für Todesfälle?	Ja, jedoch nur in der englischsprachigen Hilfe: «How to Contact Twitter About a Deceased User».
Erhalten Angehörige Zugriff? In welcher Form?	Nein; Twitter Help: «Please note: We are unable to provide login information for the account to anyone regardless of his or her relationship to the deceased.»
Ablauf aus Sicht der Angehörigen	Angehörige oder autorisierte Personen können mit der Todesurkunde und beglaubigten Kopien von Dokumenten, die die Identität des Nutzers sowie die eigene Identität und Autorisierung nachweisen, die Deaktivierung des Accounts beantragen. Der deaktivierte Account wird nach 30 Tagen inklusive Inhalt gelöscht.
Voraussetzungen, zu erbringende Dokumente	Angehörige oder autorisierte Personen, die einen Account deaktivieren lassen wollen. müssen nachfolgende Dokumente an Twitter (San Francisco, CA) faxen oder per Post schicken: «– The Twitter account's username (e.g., @username and twitter.com/username) – A copy of the deceased user's death certificate – A copy of your government-issued ID (e.g., driver's license) – A signed, notarized statement including: Your first and last name, Your current contact information, Your email address, Your relationship to the deceased user – Action requested (e.g., 'please deactivate the Twitter account') – A link to an online obituary or a copy of the obituary from a local newspaper (optional)»
Gibt es Kooperationen mit Vererbungsdiensten?	Ja, Ziggur; ansonsten nicht bekannt

Post-mortem Szenarien: Welche Optionen ermöglicht der Plattformanbieter?

A Nachwelt informieren

A1 Last Message/email/blog/tweet/ auto response	Nein, nicht von Twitter; diverse Vererbungsdienste oder «Last-Message»-Dienste bieten «last tweet»-Services an.
---	---

B Daten/Accounts löschen

B1 Account und Daten löschen	Ja, deaktivierte Accounts werden nach 30 Tagen inklusive Daten permanent gelöscht.
B2 Automatische Löschung (bei Inaktivität, Frist?)	Twitter Regelung für inaktive Konten: «Ein Twitter Konto, das länger als 6 Monate nicht eingeloggt oder aktualisiert wurde, gilt als inaktiv. Inaktive Konten können von Twitter gelöscht werden.»

C Bewahren

C1 Account/Daten bleiben unverändert (unbegrenzt, ohne Nachricht)	Nein, inaktive Konten werden nach 6 Monaten deaktiviert und dann nach 30 Tagen gelöscht.
C2 Account wird deaktiviert/stillgelegt, Daten bleiben erhalten	Ja, in einer ersten Stufe wird das Konto deaktiviert und nach 30 Tagen permanent inklusive Daten gelöscht.
C3 Gedenkstatus	Nein
C4 Archivierung (Verschiebung der Daten, Archivierung über speziellen Dienst z.B. SocialSafe, FlickrEdit)	Nicht Feature von Twitter; es gibt jedoch diverse Tools um Tweets zu archivieren, z.B. BackupMyTweets, Tweetake, TweetBackup, Tweetscan, Tweetbook.
C5 Datenkopien werden den Angehörigen überlassen	Nein, in Sekundärquellen wird erwähnt, dass Twitter Angehörigen Kopien der Tweets überlässt. In der offiziellen Policy ist diese Möglichkeit jedoch nicht erwähnt.

C6 Guthaben werden den Angehörigen überlassen	NA
C7 Veröffentlichung des digitalen Erbes (Aufhebung Zugriffsbeschränkungen)	Nein, Twitter-Konten/Tweets sind per Grundeinstellung immer öffentlich. Jedoch kann der Zugriff über die Einstellungen geändert werden. Dies jedoch nur zu Lebzeiten bzw. falls die Angehörigen Zugriff haben. Jedoch werden inaktive Konten nach 6 Monaten deaktiviert und nach 30 Tagen gelöscht. Will man die Tweets eines Verstorbenen bewahren und veröffentlichen, bleibt nur die Nutzung eines Tools zur Archivierung von Tweets bevor diese gelöscht werden, vorausgesetzt man hat Zugriff zum Account.
Durchsetzbarkeit gemäss AGB o.ä.	
Gerichtsstand	Twitter AGB: «Die vorliegenden Bedingungen sowie alle damit verbundenen Handlungen unterliegen dem Recht des US-Bundesstaates Kalifornien, wobei die Anwendung der kollisionsrechtlichen Vorschriften von Kalifornien oder Ihrem Wohnsitzstaat oder -land ausgeschlossen sind. Sämtliche Ansprüche, Gerichtsverfahren oder Rechtsstreitigkeiten im Zusammenhang mit den Diensten werden ausschliesslich vor die bundes- oder einzelstaatlichen Gerichte im Verwaltungsbezirk San Francisco, USA gebracht, und Sie erklären sich mit der Zuständigkeit dieser Gerichte und dem Gerichtsstand einverstanden und verzichten auf die Einrede der örtlichen oder sachlichen Nichtzuständigkeit der Gerichte.»
Aussagen zum Eigentum der gespeicherten Daten/ Inhalte, Urheberrechte, Nutzungsrechte etc.	Twitter AGB Abs.5: «Sie behalten die Rechte an allen Inhalten, die Sie über die Dienste übermitteln, veröffentlichen oder anzeigen. Durch Übermittlung, Veröffentlichung oder Anzeigen von Inhalten über die Dienste gewähren Sie uns eine weltweite, nicht exklusive, unentgeltliche Lizenz (mit dem Recht zur Unterlizenzierung), diese Inhalte in sämtlichen Medien und über sämtliche Verbreitungswege, die gegenwärtig bekannt sind oder in Zukunft bekannt sein werden, zu verwenden, zu vervielfältigen, zu reproduzieren, zu verarbeiten, anzupassen, abzuändern, zu veröffentlichen, zu übertragen, anzuzeigen und zu verbreiten.»
Quellen, Bedingungen, rechtliche Grundlagen	
URL AGBs, Nutzungsbedingungen, legal terms	Twitter AGB (Gültigkeitsdatum bei Abruf: ab dem 25. Juni 2012): https://twitter.com/tos
Spezielle AGBs, z.B. für bestimmte Geographien	–
URL zu Datenschutzrichtlinien	Twitter Datenschutzbestimmungen (Stand bei Abruf: 17. Mai 2012): https://twitter.com/privacy
Sonstige relevanten URLs/Online Hilfen des Anbieters zur Problematik	Hilfe: «How to Contact Twitter About a Deceased User»: http://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/87894-how-to-contact-twitter-about-a-deceased-user#

PayPal (ebay) (Status: Juni 2012)

Unternehmensdaten

URL	https://www.paypal.ch/ch
Land (Adresse HQ)	Vertragspartner für Kunden in der Schweiz ist PayPal Ltd. mit Sitz in Singapore Für Kunden in EU-Ländern ist der Vertragspartner PayPal (Europe) S.à r.l. & Cie, S.C.A, Luxemburg
Rechtsform, Konzernstruktur	Ltd., seit 2002 eine Tochtergesellschaft von ebay; PayPal hat seit dem 2. Juli 2007 PayPal in Europa den Status einer Bank (Banklizenz der luxemburgischen Bankbehörde). Die europäischen Konten wurden von PayPal (Europe) Ltd. auf PayPal Luxemburg übertragen. Die Europäische Banktochter mit Sitz in Luxemburg fungiert unter dem Namen PayPal (Europe) S.à r.l. & Cie, S.C.A mit speziellen Nutzungsbedingungen. Registriert man sich als Nutzer mit Wohnsitz in der Schweiz, wird jedoch weiterhin PayPal Ltd. in Singapore als Geschäftspartner in den AGBs genannt, Im Unterschied zu den AGBs für Nutzer in Deutschland, die PayPal (Europe) aufführen.

Vorgehen im Todesfall

Gibt es eine kommunizierte Regelung für Todesfälle?	Ja, jedoch nur in der PayPal-Hilfe mit unklarem geographischen Bezug. PayPal Hilfe: «How do I close the PayPal account of a relative?» Only the account owner can close their account, unless the owner is deceased. Only the account owner can close their account, unless the owner is deceased. To close the account of someone who has died, the estate executor needs to fax the following to (02) 8223 9508: «– A cover sheet that states the account holder is deceased and the executor wants to close the PayPal account. – A copy of the death certificate for the account holder. A copy of the deceased account holder's will or legal documentation that provides the information regarding the executor. – A copy of a photo ID of the executor. The documentation will be reviewed and, if approved, the account will be closed. If there are funds in the PayPal account, a cheque will be issued in the account holder's name.»
Erhalten Angehörige Zugriff? In welcher Form?	Nein; bei PayPal gibt es zwei Arten von Konten: «Konto für Käufer und private Verkäufer», das ausschliesslich privat genutzt werden darf (ein «Privatkonto»), und einem «Geschäftskonto». Bei einem Geschäftskonto können zu Lebzeiten mehrere Zugriffsberechtigte eingerichtet werden. Diesen Zugriff im Todesfall zu erweitern ist jedoch nicht möglich. Das Konto muss aufgelöst werden und ggfs. neu eröffnet werden. Dies kann zu Komplikationen führen, wenn das Konto gewerblich genutzt wurde, mit einer bestimmten E-Mail-Adresse verknüpft war, und nur der Verstorbene Zugriff auf das gewerbliche Konto hatte.
Ablauf aus Sicht der Angehörigen	Es empfiehlt sich im Todesfall die für die Schweiz angegebene Kundendienstnummer zu kontaktieren. Da es sich um erbrechtlich relevante Guthaben handelt und mit der Schliessung von PayPal-Konten betrügerische Absichten verbunden sein können, werden analog der englischsprachigen Hilfe, Dokumente einverlangt, die den Todesfall, die Berechtigung des Willensvollstreckers oder Erben und dessen Identität eindeutig nachweisen. Guthaben werden nach sorgfältiger Prüfung ausbezahlt.
Voraussetzungen, zu erbringende Dokumente	1. Anschreiben mit der Todesmitteilung und der Bitte den Account zu schliessen 2. Kopie der Todesurkunde 3. Eine Kopie des Testaments und/oder Erbscheins oder eines sonstigen rechtsgültigen Dokuments, das die Berechtigung des Erben oder Willensvollstreckers nachweist 4. Eine Kopie eines amtlichen Ausweises (ID) des Willensvollstreckers/Erben
Gibt es Kooperationen mit Vererbungsdiensten?	Nicht bekannt

Post-mortem Szenarien: Welche Optionen ermöglicht der Plattformanbieter?

A Nachwelt informieren

A1 Last Message / email / blog / tweet / auto response	Nein
---	------

B Daten / Accounts löschen

B1 Account und Daten löschen	<p>PayPal Konten werden nicht gelöscht, sondern geschlossen, d.h. die Kontodaten werden nicht gelöscht, sondern lediglich der Kontostatus auf «geschlossen» gesetzt. Dies soll betrügerische Aktivitäten durch Schliessen und Neueröffnen von Konten unterbinden.</p> <p>Zu Lebzeiten oder wenn die Angehörigen die Zugriffsdaten haben, kann ein Konto jederzeit geschlossen werden. Guthaben, die bei Schliessung noch vorhanden sind, zahlt PayPal gemäss angekündigter überarbeiteter Nutzungsbedingungen (gültig ab 10.7.2012) aus Abs. 9.2 (neu): «Gelder, die wir zum Zeitpunkt der Schliessung für Sie verwalten, werden Ihnen, abzüglich eventueller Gebühren, auf das Bankkonto ausgezahlt, das mit Ihrem PayPal Konto verbunden ist. Nach dem Datum der Beendigung verwenden wir die bereitgestellten persönlichen Angaben, um Ihnen eventuell verbleibende Gelder zu senden. Sind diese Angaben falsch und kann die Zahlung nicht erfolgen, unterliegen Ihre Gelder den entsprechenden Gesetzen hinsichtlich der Rückgabe von herrenlosem Besitz.» Sind die Daten für die Auszahlung des Guthabens nicht mehr gültig, müssen die Erben dem oben beschriebenen Ablauf für die Auszahlung von Guthaben eines Verstorbenen folgen.</p>
-------------------------------------	---

B2 Automatische Löschung (bei Inaktivität, Frist?)	<p>Nutzungsbedingungen Abs. 9: «Greifen Sie länger als drei Jahre nicht mehr auf Ihr Konto zu, wird dieses beendet. Nach dem Datum der Beendigung verwenden wir die bereitgestellten persönlichen Angaben, um Ihnen eventuell verbleibende Gelder zu senden. Sind diese Angaben falsch und kann die Zahlung nicht erfolgen, unterliegen Ihre Gelder den entsprechenden Gesetzen hinsichtlich der Rückgabe von herrenlosem Besitz.»</p> <p>Dieser Passus ist in den überarbeiteten Nutzungsbedingungen in Abs. 9 «Beenden und Schliessen eines Kontos» (gültig ab 10.7.2012) gemäss Ankündigung nicht mehr enthalten.</p>
---	--

C Bewahren

C1 Account / Daten bleiben unverändert (unbegrenzt, ohne Nachricht)	Nein, nach 3 Jahren Inaktivität wird das Konto beendet, d.h. geschlossen (zu prüfen ob dies mit den neuen Nutzungsbedingungen ab dem 10.7.2012 noch gilt).
C2 Account wird deaktiviert / stillgelegt, Daten bleiben erhalten	Ja, Konten werden geschlossen, d.h. sie sind nicht mehr nutzbar, aber die Daten bleiben erhalten.
C3 Gedenkstatus	NA
C4 Archivierung (Verschiebung der Daten, Archivierung über speziellen Dienst z.B. SocialSafe, FlickrEdit)	Nein
C5 Datenkopien werden den Angehörigen überlassen	Nein
C6 Guthaben werden den Angehörigen überlassen	Ja, Guthaben werden nach Prüfung der Dokumente (Identität, Erbberechtigung) ausbezahlt.
C7 Veröffentlichung des digitalen Erbes (Aufhebung Zugriffsbeschränkungen)	NA

Durchsetzbarkeit gemäss AGB o.ä.

Gerichtsstand	In den Nutzungsbedingungen (Stand 7.9.2011; in deutsch bei Login aus einem in der Schweiz registrierten Konto) wird PayPal Ltd. als Geschäftspartner und Singa-pore als Gerichtsstand aufgeführt: Abs. 15.2 «Gerichtsstand. Ansprüche können aber auch vor einem Gericht mit Sitz in Singapur, oder am Sitz des Beklagten (für PayPal Singapur und für Sie Ihr Wohnsitz oder Ihr Hauptgeschäftssitz) geltend gemacht werden. Sie und PayPal vereinbaren, sich der örtlichen Zuständigkeit der Gerichte in Singapur zu unterwerfen». In EU-Ländern, z.B. Deutschland, gelten spezielle Nutzungsbedingungen und der Vertragspartner ist PayPal (Europe) S.à r.l. & Cie, S.C.A («Für die vorliegende Vereinbarung und das zwischen uns bestehende Rechtsverhältnis gilt das Recht von England und Wales. Im Falle von Beschwer-den, die nicht anderweitig beigelegt werden können, haben englische Gerichte eine nicht-ausschliessliche Zuständigkeit. Das bedeutet, Sie können in England klagen, können aber auch einen anderen Gerichtsstand wählen.Ihre deutschen Verbraucherschutzrechte sowie Ihr Recht, gerichtliche Verfahren vor Luxemburger Gerichten einzuleiten, bleiben von dieser Regelung unberührt.»)
Aussagen zum Eigentum der gespeicherten Daten/Inhalte, Urheberrechte, Nutzungsrechte etc.	Nutzungsbedingungen Abs. 6.3 «Lizenz. Damit PayPal die uns zur Verfügung gestellten persönlichen Angaben nutzen kann, ohne Ihre Rechte zu verletzen, gewähren Sie PayPal eine nicht-ausschliessliche, weltweite, gebührenfreie, unbe-fristete, unwiderrufliche und über mehrere Ebenen unterlizenzierbare Lizenz zur Ausübung Ihrer, Urheberrechte, Werbe- und Datenbankrechte (aber keinerlei anderen Rechte), Ihnen an Ihren persönlichen Angaben zustehen, in Bezug auf sämtliche Medien, die derzeit bekannt oder noch nicht bekannt sind. PayPal verwendet und schützt Ihre persönlichen Angaben in Einklang mit unseren Datenschutzgrundsätzen.»
Quellen, Bedingungen, rechtliche Grundlagen	
URL AGBs, Nutzungsbedingungen, legal terms	PayPal AGB (bei Login aus einem in der Schweiz registrierten Konto)
Spezielle AGBs, z.B. für bestimmte Geographien	Nutzungsbedingungen (Stand 7.9.2011; in deutsch bei Login aus einem in der Schweiz registrierten Konto). PayPal hat per 10.7.2012 überarbeitete Nutzungsbedingungen angekündigt (https://cms.paypal.com/ch/cgi-bin/?cmd=_render-content&content_ID=ua/upcoming_policies_full&locale.x=de_DE)
URL zu Datenschutzrichtlinien	Datenschutzgrundsätze (Stand 28.3.2011; in deutsch bei Login aus einem in der Schweiz registrierten Konto): https://cms.paypal.com/ch/cgi-bin/marketingweb?cmd=_render-content&content_ID=ua/Privacy_full&locale.x=de_DE
Sonstige relevanten URLs/Online Hilfen des Anbieters zur Problematik	PayPal Hilfe: «How do I close the PayPal account of a relative?» (geographischer Bezug unklar): https://www.paypal.com/helpcenter/main.jsp?sessionid=pJvFPnyRw1ffSyK2PvdGWGTyPbmJthlv2pJJtbnvhKW4KhfBdLI-235400226?locale=en_AU&dyncharset=UTF-8&countrycode=AU&cmd=_help&serverInstance=9018&t=browseTab&sidetopic=57400018&opentopic=57400018

the 1990s, the number of publications on the topic has increased steadily, and the number of authors has increased from 1 to 100.

There are a number of reasons for the increase in research on the topic. One reason is the growing awareness of the importance of the topic. Another reason is the increasing availability of data and methods for studying the topic. A third reason is the increasing interest in the topic by the general public.

The following sections will discuss the history of research on the topic, the current state of research, and the future of research on the topic.

The history of research on the topic can be traced back to the 1950s, when the first studies were published.

In the 1960s, research on the topic was largely limited to descriptive studies.

In the 1970s, research on the topic began to focus on the underlying mechanisms.

In the 1980s, research on the topic began to focus on the development of interventions.

In the 1990s, research on the topic began to focus on the evaluation of interventions.

In the 2000s, research on the topic began to focus on the implementation of interventions.

In the 2010s, research on the topic began to focus on the sustainability of interventions.

In the 2020s, research on the topic began to focus on the impact of interventions.

The current state of research on the topic is characterized by a number of key findings.

One key finding is that the topic is a complex and multifaceted issue.

Another key finding is that the topic is a global issue that affects people in all parts of the world.

A third key finding is that the topic is a public health issue that has a significant impact on the quality of life of many people.

A fourth key finding is that the topic is a social issue that is influenced by a number of factors, including culture, economics, and politics.

A fifth key finding is that the topic is a scientific issue that is being studied by a number of different disciplines, including psychology, sociology, and public health.

The future of research on the topic is bright, and there are a number of exciting opportunities for researchers in the field.

One opportunity is to continue to explore the underlying mechanisms of the topic.

Another opportunity is to develop and evaluate new interventions.

A third opportunity is to focus on the implementation of interventions.

A fourth opportunity is to focus on the sustainability of interventions.

A fifth opportunity is to focus on the impact of interventions.

In conclusion, research on the topic has a long and rich history, and there are a number of exciting opportunities for researchers in the field.

Zürcher Hochschule
für Angewandte Wissenschaften

School of Management and Law

St.-Georgen-Platz 2
Postfach
8401 Winterthur
Schweiz

www.sml.zhaw.ch

