universität wien

DISSERTATION

Titel der Dissertation

„Ausgewählte Rechtsprobleme im Zusammenhang mit Social network-Plattformen“

Verfasserin

Mag. iur. Caterina Hartmann

angestrebter akademischer Grad

Doktorin der Rechtswissenschaften (Dr. iur.)

Wien, 2015

Studienkennzahl lt. Studienblatt:	A 083 101
Dissertationsgebiet lt. Studienblatt:	Rechtswissenschaften
Betreuer:	ao. Univ.-Prof. Dr. Wolfgang Zankl

DANKSAGUNG

„Keine Schuld ist dringender als die, Dank zu sagen."
Marcus Tullius Cicero (106 – 43 v Chr)

Meinen besonderen Dank möchte ich zunächst meinem Erstbetreuer, Herrn Univ.-Prof. Dr. Wolfgang Zankl, aussprechen, der mir die Möglichkeit gab, dieses interessante Thema behandeln und diese Abhandlung verfassen zu dürfen. Nach meinem Magisterstudium begann ich, neben meiner Arbeit als Rechtsanwaltsanwärterin, im E-Center, dem Europäischen Zentrum für E-Commerce und Internetrecht in Wien, zu arbeiten, wo ich immer wieder wertvolle Anregungen erhielt. Ich möchte mich auch dafür bedanken. Durch meine Tätigkeit im E-Center konnte ich viele interessante Persönlichkeiten und Unternehmen kennenlernen und durfte auch eine Studie zum Thema „Facebook" leiten.

Danken möchte ich auch Herrn Priv.-Doz. Dr. Konrad Lachmayer für die Übernahme der Zweitbetreuung und die Erstellung des Zweitgutachtens.

Mein besonderer Dank gilt jedoch auch jenen Menschen, die mich über die Jahre hinweg unterstützt, mich unermüdlich motiviert, an mich geglaubt und auch einen gewissen – wenngleich positiven – Druck auf mich ausgeübt haben, die Arbeit zu verfassen bzw zu beenden.

Mein unermesslicher Dank gilt meiner gesamten Familie, insbesondere meinen Eltern, meiner Großmutter und meinem Freund Alexander, welche immer an mich und meine Arbeit geglaubt haben.

Danke!

Wien, im Juni 2015 Caterina Hartmann

VORWORT

Gleichzeitig ist eine neue Generation von Nutzern entstanden:
Die erste Generation, die aufgewachsen ist, während das Internet bereits existierte.
*Diese **„digitalen Eingeborenen“** haben ihre eigene Art der Nutzung von Internet-Diensten*
entwickelt, und eigene Ansichten darüber, was sie als der Privat- bzw der öffentlichen Sphäre zugehörig
empfinden. Darüber hinaus könnten sie – da die meisten von ihnen im Teenager-Alter sind
*– eher bereit sein, Datenschutzrisiken einzugehen, als die älteren **„digitalen Einwanderer“**.*
Generell scheint es, als seien jüngere Leute eher zur Veröffentlichung
(manchmal intimer) Einzelheiten über ihr Leben im Internet bereit.[1]

In den letzten Jahren konnte ein Wandel unserer Gesellschaft, insbesondere im Umgang mit Daten, Informationen, Kommunikation und generell mit dem Internet und unserer Beziehung dazu, beobachtet werden. Sprach man noch vor einiger Zeit von einer Revolution des Kommunikationswesens durch das Phänomen Internet, ist aus dem Internet eine Selbstverständlichkeit geworden und unsere Gesellschaft immer mehr eine sog Informationsgesellschaft.[2] Das Internet, insbesondere das World Wide Web, ist allgegenwärtig und wird nicht mehr nur von technisch versierten Personen verwendet. Das Internet ist in der Zwischenzeit zu einem der wichtigsten und unentbehrlichsten Informationsbeschaffungs- und Kommunikationsmedien geworden. Es werden immer mehr Massenprogramme entwickelt, welche eine schnelle und einfache Kommunikation zwischen den Menschen über das Internet ermöglichen sollen.

Als eine der größten Errungenschaften der letzten Jahre im Bereich Kommunikation und Vernetzung können mA nach Social network-Plattformen[3] (in der Folge kurz „SNP“) genannt werden. SNP sind geradezu das Spiegelbild unserer neuen Gesellschaft: Immer und überall über alles informiert sein zu wollen und alles kommentieren und beobachten zu können. Aus der speziell von Technikern für Techniker entwickelten Kommunikationsplattform Internet

---

[1] Aus dem Bericht und der Empfehlung zum Datenschutz in sozialen Netzwerkdiensten, „Rom Memorandum“, 43. Sitzung der Arbeitsgruppe vom 3.– 4.3.2008, Rom (Italien); http://www.llv.li/pdf-llv-sds-675.36.13

[2] Es gibt keine allgemein gültige Definition des Begriffs Informationsgesellschaft, doch wird ua im § 3 Z 1 ECG der „Dienst einer Informationsgesellschaft“ definiert als „ein in der Regel gegen Entgelt elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst, insbesondere der Online-Vertrieb von Waren und Dienstleistungen, Online-Informationsangebote, Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern“. Grds kann festgehalten werden, dass eine Informationsgesellschaft eine auf Information und Kommunikation ausgerichtete Gesellschaft ist.

[3] Der Begriff „Plattform“ wurde von Microsoft-Gründer *Bill Gates* in die Technik-Welt eingeführt als eine Art „Plateau, auf dem andere Firmen aufbauen“. Microsoft hat seine Plattform „Windows“ als Basis geschaffen, auf der andere Software-Entwickler ihre Produkte aufsetzen können, ohne die erste Stufe, ein Betriebssystem für die Hardware, aufbauen zu müssen. Vgl auch *Steinschaden*, Phänomen Facebook (2010) 27.

der 1990er Jahre entstanden moderne, allgegenwärtige und für fast jedermann zugängliche Kommunikationsplattformen in Form von SNP.

SNP bringen aber nicht nur Vorteile eines erleichterten Informationszuganges und Kommunikationsaustausches, sondern auch Probleme, wie insbesondere Rechtsprobleme, mit sich, welche nicht nur in nationaler, sondern auch in internationaler Hinsicht ernst genommen und denen entgegengewirkt werden muss.

So aufregend und innovativ die technischen Entwicklungen der letzten Jahre waren, so notwendig ist die Rechtssicherheit der Nutzer der neuen Medien, insbesondere auch deshalb, weil der Wissensumfang der Nutzer von SNP (noch immer) sehr unterschiedlich ist, speziell im Hinblick auf den Schutz der Privatsphäre, die Gefahren des Internets, generell die Schutzmöglichkeiten etc.

In diesem Zusammenhang werden einige rechtliche Fragestellungen aufgeworfen, die es anzusprechen gilt, insbesondere im Hinblick auf die Rechtssicherheit und den Umgang und die Vereinheitlichung der rechtlichen Rahmenbedingungen im Internet, und soll daher mit dieser Arbeit versucht werden, einige Fragestellungen zu thematisieren bzw Lösungsansätze aufzuzeigen:

- Was passiert mit auf SNP online gestellten bzw gespeicherten Daten? Wer erhält diese Daten, wo und wie lange werden sie gespeichert? Können einmal online gestellte Daten wieder gelöscht werden. Gibt es ein „Recht auf Vergessen“ im Internet?
- Welche Gesetze und Vorschriften können zur Lösung von Rechtsproblemen und zur Schaffung von Rechtssicherheit im Zusammenhang mit SNP herangezogen werden bzw besteht ein Bedarf an neuen gesetzlichen Regelungen? Was sind die größten rechtlichen Unterschiede zur realen Welt bzw gibt es überhaupt rechtliche Unterschiede zwischen der digitalen (virtuellen) und der realen Welt? Wie ist die Verwendung, Speicherung und Beseitigung von Daten und Informationen zivilrechtlich zu bewerten? Gewährt das Grundrecht auf Datenschutz einen ausreichenden Schutz vor möglichen Gefahren, welche durch das unerlaubte Verwenden bzw Vernetzen preisgegebener Daten entstehen (können)?
- Wie und welche internationalen und nationalen Regelungen können im Zusammenhang mit SNP angewendet werden?

- Wie müssen allgemeine Geschäftsbedingungen gestaltet sein, um rechtsgültig abgeschlossen zu werden, und gibt es Mindestanforderungen an allgemeine Geschäftsbedingungen im Internet?
- Wie kann sich ein Nutzer einer SNP bei Rechtsverletzungen wehren bzw wo kann er diese aufzeigen? Welches Recht kommt iZm SNP in Österreich zur Anwendung?
- In welchen Bereichen muss das nationale Recht auf all die neuen Entwicklungen in diesem Zusammenhang reagieren?

Im Laufe dieser Arbeit soll versucht werden, mit Hilfe der Analyse von Gesetzestexten, Lehre und Rechtsprechung auf obige Fragen einzugehen, mit dem Ziel, ausgewählte Rechtsprobleme im Zusammenhang mit SNP kritisch aufzuzeigen und Problematiken und Risiken hervorzuheben und zu analysieren. Es soll versucht werden, herauszuarbeiten, was Grund und Auslöser der Veränderung betreffend Datenpreisgabe und -sicherheit waren und was aus dem instinktiven Selbstschutz der Privatsphäre und dem Schutz privater Daten der Menschheit geworden ist?

Auch soll herausgearbeitet werden, ob es der aktuellen Rechtsordnung überhaupt (noch) möglich ist, auf all diese neuen technischen Herausforderungen des Internets einzugehen und die Nutzer vor ihrer eigenen Sorglosigkeit zu schützen, und aufgezeigt werden, wie der (europäische) Gesetzgeber versucht, auf die neuen Entwicklungen zu reagieren. Denn mit der Flut dieser technischen Neuerungen ist auch das Rechtssystem gefordert, die damit in Verbindung stehenden Risikofaktoren und Gefahren einzugrenzen, für Rahmenbedingungen bzw Grenzen zu sorgen.

Mark Zuckerbergs Aussage *„We cannot let poorly thought out laws get in the way of the internet development, we will continue to oppose any laws that will hurt the internet. The world needs ‚political leaders who are pro-internet'"*, zeigt meiner Ansicht nach Problem und Spannungsfeld auf:

Auf der einen Seite gibt es die Nutzer, deren Daten und Privatsphäre allgemein geschützt gehören, und auf der anderen Seite gibt es die Entwickler/Programmierer und

Diensteanbieter, die verhindern wollen, dass ihre Dienste durch Gesetze und Verordnungen „beschränkt“ werden (sollen).[4]

Meines Erachtens sind die zentrale Aufgabe und das Ziel der Rechtsordnung, eine Art „Gleichgewicht“ zwischen den Bürgern/Nutzern bzw deren Privatsphäre und den neuen Medien und deren Entwicklern zu schaffen.

[4] Posting von *Mark Zuckerberg* vom 18.1.2012, dem CEO und Gründer von Facebook, auf der Facebook-Webseite.

INHALTSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

ABGB	Allgemeines Bürgerliches Gesetzbuch
ABl	Amtsblatt der Europäischen Gemeinschaften
Abs	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art	Artikel
BG	Bundesgesetz
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
bzw	beziehungsweise
ca	circa
CH	Schweiz
d(t)	deutscher, -es, -e
dt AGBG	deutsches AGB-Gesetz
dh	das heißt
DSG	Datenschutzgesetz
DSK	Datenschutzkommission
E	Entscheidung
ECG	E-Commerce Gesetz
ecolex	Fachzeitschrift für Wirtschaftsrecht
EDV	elektronische Datenverarbeitung
E-Mail	Eletronic Mail, elektronische Post
etc	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EuGVÜ	Übereinkommen über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen, Brüsseler Übereinkommen
EuGVVO	VO (EG) 44/2001 des Rates vom 22.12.2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen
EWR	Europäischer Wirtschaftsraum
ff	und die folgenden
gem	gemäß
grds	grundsätzlich
hM	herrschende Meinung
Hrsg	Herausgeber
HTML	Hypertext Markup Language
idF	in der Fassung
idR	in der Regel

Inc.	Incorporated
IP	Internetprotokoll
iSd	im Sinne des/der
JN	Jurisdiktionsnorm
KSchG	Konsumentenschutzgesetz
lit	Litera
maW	mit anderen Worten
mE	meines Erachtens
MedienG	Mediengesetz
Nr	Nummer
OGH	Oberster Gerichtshof
ÖJZ	Österreichische Juristenzeitung
OLG	Oberlandesgericht
RL	Richtlinie der EU
RZ	Österreichische Richterzeitung
Rz	Randziffer
S	Seite
SN	Social Network
SNP	Social Network-Plattform
sog	sogenannte/r
StGB	Strafgesetzbuch
TMG	(dt) Telemediengesetz
ua	und andere/r/s
uä	und ähnliche/r/s
udgl	und dergleichen
UGB	Unternehmensgesetzbuch
UrhG	Urheberrechtsgesetz
US(A)	United States (of America)
USD	US-Dollar
vgl	vergleiche
VO	Verordnung
www	World Wide Web
Z	Ziffer
zB	zum Beispiel

GLOSSAR[5]

Zum besseren Verständnis dieser Arbeit werden nachfolgend einige Begriffe erklärt:

Access-Provider:	Zugangsanbieter zum Internet.
Account:	Konto eines individuellen Bereichs einer EDV-Anwendung.
Anwendung:	Bezeichnung für ein Programm oder eine Software.
Applikation (App):	Anwendungsprogramm.
Browser:	Client-Programm zur Benutzung eines Datensystems.
Button:	Ein Button ist eine optisch als Schaltknopf erkennbare Grafik, welche verlinkt ist.
Cookie:	Ein Cookie ist ein kurzer Eintrag auf dem Computer eines Nutzers, welcher dem Austausch von Informationen zwischen dem Computer des Nutzers und der aufgerufenen Seite durch diesen dient. Dank Cookies „erkennt“ eine Webseite, ob sie durch einen Nutzer bereits einmal aufgerufen wurde. Ein Cookie ist wie ein „virtuelles Lesezeichen“, welches einem Nutzer zugeteilt wird und sich auf eine besuchte Webseite „legt“. Facebook verwendet Cookies, um eingeloggte Mitglieder auf fremden Webseiten, die ein Social Plugin (siehe unten) installiert haben, wiederzuerkennen.
Datei:	Unter Datei versteht man eine Sammlung personenbezogener Daten, die nach mindestens einem Suchkriterium zugänglich sind (siehe Legaldefinition § 4 Z 6 DSG 2000).
Disclaimer:	Haftungsausschluss auf einer Webseite.
Domain:	Name eines Hosts oder ganzen Netzwerkes im Internet. Der Domain-Name ist Teil einer Internetadresse.
E-Mail:	E-Mail ist die Abkürzung für electronic mail = elektronische Post. E-Mail ist eine auf elektronischem Weg in Computernetzwerken übertragene briefähnliche Nachricht.

[5] ZT (wörtlich) übernommen aus *Steinschaden*, Phänomen Facebook (2010) 198 ff; *Emich*, Internet – ein rechtsfreier Raum (1999) 135 ff; *Ehmann/Kramer*, Datenschutzglossar (2005); *Welser*, Fachwörterbuch (2005) und Wikipedia (http://de.wikipedia.org/) sowie Glossar auf der Facebook-Webseite unter http://www.facebook.com/help/333140160100643/#!/help/219443701509174/

Facebook-Page:	Eine Facebook-Page (Webseite) ist ausschließlich für Unternehmen bzw Produkte, Marken oder Personen von öffentlichem Interesse konzipiert worden. Facebook-Pages sollen einen Ersatz für eine Homepage bilden und dienen primär der Anwerbung bzw dem Marketing. Facebook-Pages haben in der Regel einen korrespondierenden Like-Button auf einer externen Webseite, über welchen Facebook-Nutzer die jeweilige Page „liken“ und damit unterstützen bzw Werbung machen können.
Homepage:	Startseite eines Internetauftritts im World Wide Web.
Host:	Zentralrechner im Internet.
Hyperlink:	Verweisung in einer Hypertext-Datei zu einer anderen Datei.
Icon:	Darunter versteht man im Computerbereich ein Piktogramm, das als Bestandteil einer grafischen Benutzeroberfläche einer Software oft eine Datei oder ein Verzeichnis repräsentiert, oder das auf einer grafischen Schaltfläche („Button“) einen Befehl an die Software symbolisiert.
Internet:	Das Internet ist ein weltweites Netzwerk von Rechnern, welche untereinander Daten austauschen. Über einen Access Point bzw einen Provider wird ein Zugang zum Netzwerk ermöglicht. Das Internet dient primär der elektronischen Kommunikation und dem Austausch von Informationen.
IP Internet Protocol:	Das Internet-Protokoll erlaubt es Datenpaketen, auf dem Weg vom Sender zum Empfänger mehrere verschiedene Netzwerke nutzen zu dürfen.
IP-Adresse:	Computer, welche auf das Internet zugreifen, werden grundsätzlich mit einer mehrstelligen Zahlenkombination ausgestattet, damit der Standort eines Servers ausfindig gemacht werden kann, über welchen auf eine bestimmte Webseite zugegriffen wurde. Zurzeit werden IP-Adressen als 32 Bit-Binärzahlen dargestellt. Es wird zwischen dynamischen und statischen IP-Adressen unterschieden. Dynamische IP-Adressen werden aus einem Vorrat von IP-Adressen bei jedem Internetaufruf vergeben, während statische IP-Adressen unverändert bleiben und eine permanente Verbindung zum Internet bieten.
Like-Button:	Facebook-Spezifikum: Ein sog Social Plugin, welches von Facebook angeboten wird. Der Like-Button wird durch ein

	blaues „Daumen hoch“-Symbol auf fremden Webseiten angezeigt und damit können Facebook-Nutzer zeigen, dass sie an einer bestimmten Webseite Gefallen finden.
Link:	Verknüpfung. Verweis von einer Datei auf eine andere.
Log-File:	Die Logdatei (im Englischen: log file) enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem.
News Feed:	Facebook-Spezifikum: Darunter versteht man eine Liste von Aktionen (vom Status-Update über Foto- oder Video-Uploads) von Facebook-Freunden auf dem jeweiligen Profil. Unter News Feed werden auch Nachrichtenkanäle aus dem Internet verstanden, welche kostenlos abonniert werden können.
Nutzer:	Jene Personen, welche das Internet für ihre Kommunikation und den Informationsaustausch nutzen.
Opt-In, Opt-Out:	Unter Opt-In kann ein „Bestellen“ und unter Opt-Out ein „Abbestellen“ von Funktionen, Programmen etc. verstanden werden.
PDF:	Portable Document Format. Plattformunabhängiges Dateiformat für Dokumente.
Persönliche Daten:	Informationen, die direkt oder indirekt eine Identifikation von Personen ermöglichen: Vorname, Nachname, E-Mail, Foto, IP-Adresse etc.
Post(ing):	Postings sind Mitteilungen bzw Beiträge. Auf einer Facebook-Pinnwand können Beiträge (Postings) veröffentlicht und mit anderen Personen geteilt werden.
Screenshot:	Bildschirmkopie, Bildschirmfotokopie.
Sensible Daten:	Daten natürlicher Personen über ihre religiöse, philosophische Überzeugung, Gesundheit, sexuelle Orientierung, politische Herkunft etc (siehe Legaldefinition § 4 Z 2 DSG 2000).
Server:	Der Begriff Server kann die Software eines Computers (Programm) bezeichnen oder eine Hardware (Computer), auf welcher diese Software (das Programm) arbeitet.
Service Provider:	Anbieter von Mehrwertdiensten im Internet.
Shitstorm:	Der Begriff Shitstorm bezeichnet im Deutschen das Auftreten des als Flamewar bekannten Phänomens bei Diskussionen im Rahmen von sozialen Netzwerken, Blogs oder

	Kommentarfunktionen von Internetseiten. Typisch für einen Shitstorm ist, dass die Teilnehmer Dysphemismen verwenden. Dabei richtet sich „in kurzem Zeitraum eine subjektiv große Anzahl von kritischen Äußerungen […], von denen sich zumindest ein Teil vom ursprünglichen Thema ablöst und [die] stattdessen aggressiv, beleidigend, bedrohend oder anders attackierend geführt [werden]“ gegen Unternehmen, Institutionen, Einzelpersonen oder in der Öffentlichkeit aktive Personengruppen, etwa Parteien oder Verbände.
Social Media/ Soziale Medien:	Darunter können grob zusammengefasst Webdienste subsumiert werden, welche es dem Nutzer erlauben, selbst erstellte Inhalte wie Texte, Fotos, Videos etc. zu publizieren.
Social Plugins:	Kleine Schaltflächen (sog „buttons“), welche auf fremden Webseiten eingebettet werden können, damit Facebook-Mitglieder Funktionen des Online-Netzwerkes auch außerhalb des Netzwerkes nutzen können. Plugins sind „Verbindungen“ von einer Webseite zu einer anderen. Der Like-Button ist ein typisches Social Plugin, mit welchem Online-Inhalte wie Texte, Videos, Fotos, Kommentare etc. bewertet werden können.
Statusmeldungen:	Beiträge von Nutzern, welche über das Eingabefeld auf der Profilseite eingegeben werden.
Tags:	Unter „taggen“ wird ein „online markieren“ von Personen auf Fotos oder Videos („to tag sth = etwas markieren“) verstanden.
Top-Level-Domain:	Bezeichnung für den äußerst rechten Teil eines Domain-Namens (.com, .at, .de etc).
User-generated-content:	Als nutzergenerierte Inhalte werden Inhalte einer Website bezeichnet, welche von den Nutzern der Website zur Verfügung gestellt werden, wie Texte, Bilder, Audios, Videos etc und welche in der Regel ohne erwerbsmäßige Absicht von den Nutzern verfasst bzw erstellt werden (siehe dazu auch Web 2.0).
Verlinken:	Unter Verlinken wird das Verknüpfen mit einem anderen Dokument auf einer anderen Webseite verstanden.
Wall:	Auf der Facebook „Pinnwand“ (engl.: „wall“) können Beiträge online gestellt und mit anderen geteilt werden. Die Pinnwand befindet sich direkt auf der jeweiligen „Profilseite“ des Nutzers. Der Nutzer kann selbst entscheiden, ob online gestellte Beiträge auf der Pinnwand mit „allen“ Nutzern oder nur „bestimmten Freunden“ geteilt werden sollen. Auch kann eingestellt werden,

	dass nur der Inhaber die Wall-Einträge seiner Freunde sehen kann, dh Wall-Einträge nur für ihn sichtbar sind. Auf der Pinnwand kann ein Nutzer angeben, was er gerade macht, und Videos, Links etc veröffentlichen.
Web 2.0:	Der Begriff Web 2.0 bezeichnet eine neue Generation des Internets und grenzt diese von früheren Nutzungsarten ab. Das Hauptmerkmal ist, dass Nutzer ihre Inhalte selbst erstellen und verbreiten können. Beispiele sind Blogs, Social Network-Plattformen, Media Sharing-Plattformen etc.
www:	World Wide Web. Ein auf Hypertext basierendes System zum Auffinden von Ressourcen im Internet.
Zuckerberg, Mark:	Gründer von Facebook. Zuckerberg gehören etwa 28% des Online Netzwerks (Stand Jänner 2013).

ABBILDUNGSVERZEICHNIS

Ich habe mich bemüht, sämtliche Inhaber der Bildrechte ausfindig zu machen und ihre Zustimmung zur Verwendung der Bilder in dieser Arbeit einzuholen. Sollte dennoch eine Urheberrechtsverletzung bekannt werden, ersuche ich um Meldung bei mir.

I. EINLEITUNG

A. ALLGEMEINE BEGRIFFLICHKEIT

Die Beliebtheit von SNP ist in den vergangenen Jahren enorm gestiegen. 1995 waren es noch speziell für US-amerikanische Schüler konzipierte „Online-Communities", wie etwa Classmates.com, welche die Möglichkeit schaffen sollten, nach der Beendigung der Schule mit Klassenkollegen digital in Kontakt treten zu können. Ab den 2000er Jahren kam es zu einer richtigen SNP-Blütezeit und die Diensteanbieter konnten immer mehr Nutzer auf ihren Webseiten verzeichnen. Es entstanden unzählige Social networks (ie SNP), wie im Jahr 2003 „MySpace"[6], im Jahr 2004 „Orkut"[7] und „TheFacebook.com"[8] und im Jahr 2005 „StudiVZ"[9].

Es gibt in der Zwischenzeit eine Vielzahl von SNP, wie beispielsweise „Xing"[10], „Twitter"[11], „ASmallworld" etc[12], um nur einige zu nennen. Aus den ursprünglich speziell für Schüler und Studenten konzipierten Webdiensten sind unlimitierte Webdienste für jedermann geworden, welche auch für andere Bevölkerungsgruppen geöffnet und zugänglich gemacht wurden.

Im Aufbau sind sich alle SNP relativ ähnlich, auch Sinn und Zweck sind zumeist gleich. Unterschiede gibt es primär bei den jeweiligen Mitgliedern und der Möglichkeit, Mitglied zu werden. Um zB Mitglied von ASmallworld[13] werden zu können, muss man von einem Mitglied mittels E-Mail eingeladen bzw vorgeschlagen werden. ASmallworld reduziert die Auswahl seiner Mitglieder, um eine gewisse „Elite" der Mitglieder erhalten zu können: ASmallworld schreibt in seinen Terms of use (den Allgemeinen Geschäftsbedingungen), dass die Mitglieder einen ähnlichen Background (dh eine ähnliche Ausbildung, gesellschaftlichen Status etc) sowie ähnliche Interessen und Ziele haben sollen.

Die Grafiken in Abbildung 1 veranschaulichen die Anzahl von Nutzern verschiedener SNP. Es ist ganz deutlich erkennbar, wie die Plattform Facebook alleine zwischen 2009 und 2010 Nutzer-Neuzugänge und damit an Popularität dazugewinnen konnte.

---

6 http://www.myspace.com
7 http://www.orkut.com
8 http://www.facebook.com
9 http://www.studivz.net
10 http://www.xing.com
11 http://twitter.com
12 Einige weitere SNP sind ua Google+, SmallWorld, Blogster, Faces.com, Flickr, Friendster, Google Buzz, hi5, Last.fm, LinkedIn, MyHeritage, MySpace, WAYN etc.
13 http://www.asmallworld.net/membership

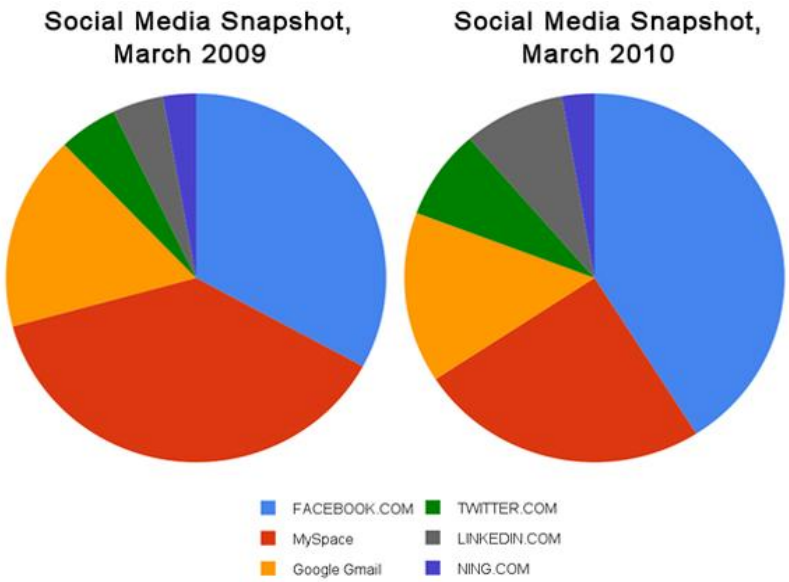

Abbildung 1: Verteilung der Nutzer auf die bekanntesten SNP (Stand: 26.10.2011)[14]

SNP sind mittlerweile omnipräsent geworden. Es gibt kaum noch Mobiltelefone, die nicht SNP-tauglich sind, was dazu führt, dass Nutzer ständig und überall Zugang zu ihren Plattformen haben und Daten hochladen können.

Doch was bedeuten all diese Entwicklungen für die Privatsphäre der Menschen und welche generellen Auswirkungen und Gefährdungen sind mit der Sammlung von Informationen und deren Vernetzung im Hinblick auf die Privatsphäre verbunden?

Personen verloren bereits ihre Arbeit, weil sie unpassende bzw delikate Fotos von sich selbst auf Facebook hochluden oder unpassende Kommentare oder Fragen auf ihrer „wall“[15] posteten. Auch wurden bereits Personen entlassen, weil sie Urlaubsfotos auf Facebook posteten, obwohl sie angaben, krank zu sein. Alle dies sind Beispiele dafür, was passieren kann, wenn man die Reichweite der Veröffentlichung von Daten, Fotos oder anderer Informationen auf einer SNP unterschätzt oder fahrlässig damit umgeht.

In den obigen Fällen war das gemeinsame Problem, dass Informationen, welche der Nutzer grundsätzlich nur einem bestimmten Adressatenkreis zugänglich machen wollte, in der Folge

[14] Untersuchung von Comscore auf http://www.ethority.de/weblog/2010/04/20/facebook-beherrscht-weiterhin-das-social-web (Quelle Comscore).

[15] http://www.facebook.com/help/glossary. Auf der „Pinnwand“ (engl.: „wall“) kann man Beiträge online stellen und mit anderen teilen. Die Pinnwand befindet sich direkt auf der jeweiligen „Profilseite“ des Nutzers. Es kann gewählt werden, ob auf der Pinnwand online gestellte Beiträge mit „allen“, „bestimmten Freunden“ oder „niemandem“ geteilt werden sollen und dementsprechend kann man den Adressatenkreis wählen. Man kann auf der Pinnwand angeben, was man gerade macht, Videos und Links veröffentlichen etc.

Dritten, wie zB dem Arbeitgeber[16], Kollegen oder anderen Personen, zugegangen sind, die davon eigentlich keine Kenntnis erlangen hätten sollen und diese Informationen erhebliche Auswirkungen auf den Beruf, die Laufbahn und den Ruf des Nutzers hatten.

Die „Standardeinstellungen" eines SN-Profils verlangen in der Regel die Preisgabe bestimmter, meist heikler Daten, wie den echten Namen, Wohnort, Ausbildung udgl, sowie das Hochladen eines Profilfotos, um ein leichtes Finden von Personen zu ermöglichen. Bei den meisten SNP führen deren „Standardeinstellungen nicht zu einer größtmöglichen Geheimhaltung, sondern zu einer größtmöglichen Preisgabe von Informationen", wie der *Verein für Konsumenteninformation* bereits feststellte.[17]

Der US-Amerikaner *Matt McKeon*[18] erstellte unter Bezugnahme auf die SNP Facebook Grafiken (Abbildungen 2 bis 4), aus welchen ersichtlich ist, wie sich die Privatsphäre-Einstellungen und auch die „Standardeinstellungen" iZm persönlichen Daten auf Facebook in den Jahren 2005 bis 2010 veränderten.

In Abbildung 2 ist ganz deutlich zu erkennen, dass im Jahr 2005 anderen Nutzern „nur" Daten wie Name, Profilfoto, Geschlecht und Mitgliedschaften angezeigt wurden bzw zugänglich waren (siehe blaue Markierungen – „Availability of your personal data on Facebook").

[16] Einer amerikanischen Studie zufolge suchen etwa 20% aller Arbeitgeber vor der Aufnahme neuen Personals nach „Spuren", welche Bewerber im Internet hinterlassen haben, insbesondere in social networks wie Facebook oder MySpace. Siehe auch *Staudinger* in *Jaksch-Ratajczak,* Aktuelle Rechtsfragen der Internetnutzung (2010) 234.

[17] *Verein für Konsumenteninformation,* Ihr Recht im Internet (2011) 101.

[18] *McKeon* ist Entwickler im IBM Research Center for Social Software.

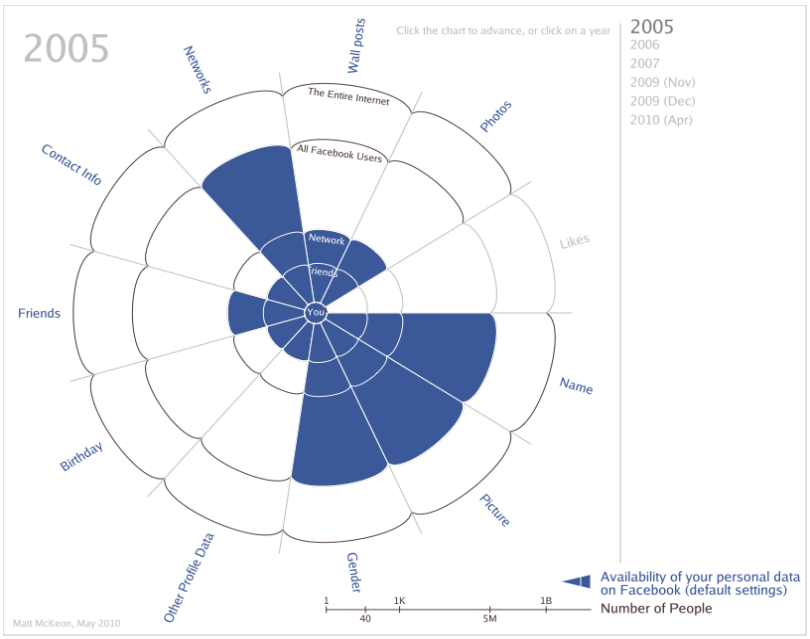

Abbildung 2: Standardeinstellungen im Jahr 2005 (Stand: 26.10.2011)[19]

Im November 2009 (Abbildung 3) wurden ua auch Freunde von Nutzern anderen Facebook-Nutzern angezeigt und Name, Geschlecht und Profilfoto für das gesamte Internet zugänglich gemacht.

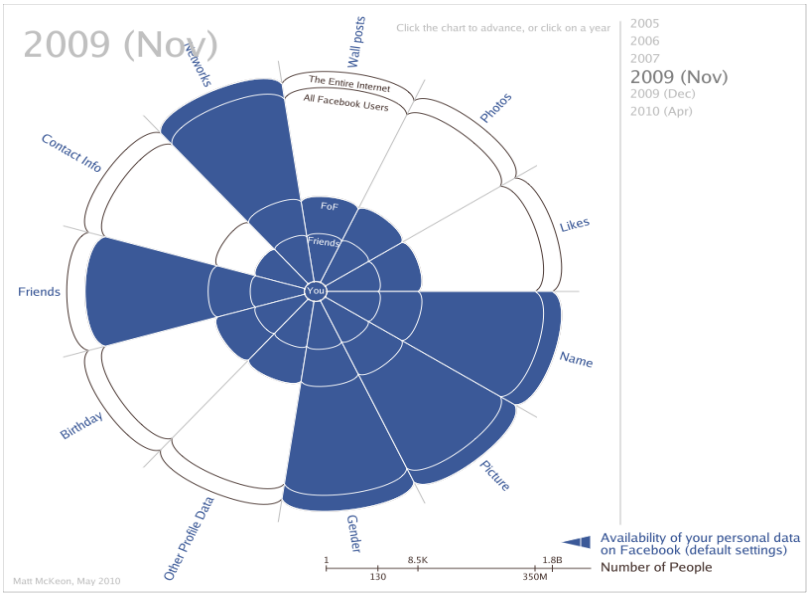

Abbildung 3: Standardeinstellungen im Jahr 2009 (Stand: 26.10.2011)[20]

[19] „Changes in default profile settings over time“, Quelle Matt McKeon, http://mattmckeon.com/facebook-privacy

[20] „Changes in default profile settings over time“, Quelle Matt McKeon,

Für das Jahr 2010 (Abbildung 4) ist schließlich erkennbar, dass auch Fotos, Freunde, Geschlecht, Profilbild und Statusmeldungen teilweise nicht mehr nur noch für Nutzer von Facebook, sondern für alle Internetnutzer zugänglich gemacht wurden.[21]

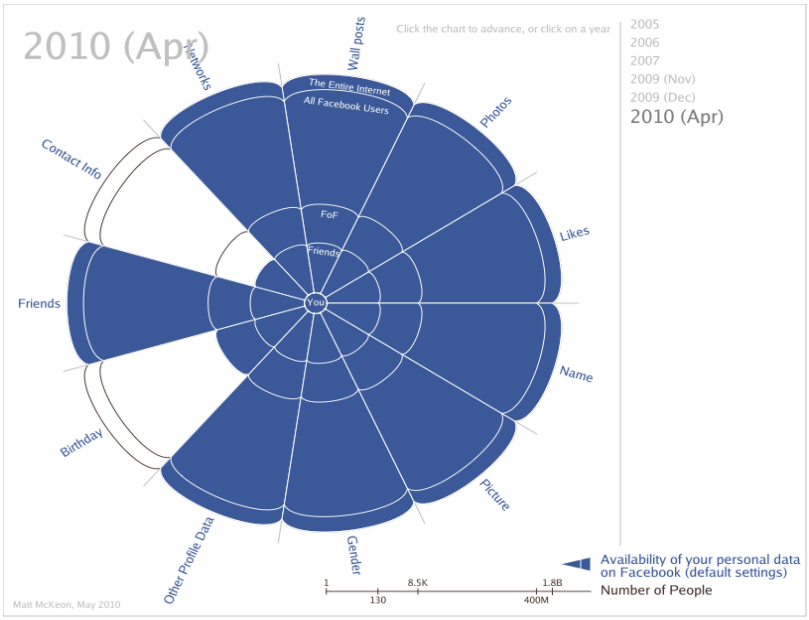

Abbildung 4: Standardeinstellungen im Jahr 2010 (Stand: 26.10.2011)[22]

Die Abbildungen 2 bis 4 zeigen mE ganz deutlich die Veränderungen iZm den Standard- bzw Voreinstellungen bei Facebook in den Jahren 2005 bis 2010.

In diesem Zusammenhang möchte ich auf ein Zitat von *Steinschaden* hinweisen, welcher bereits im Jahr 2010 in seinem Werk „Phänomen Facebook" davon sprach, dass *Zuckerberg* eine „radikale Transparenz" der Menschheit plane, welche zum Ziel habe, dass unsere Welt „transparenter und offener" werde, damit die Menschen ehrlicher und offener handeln würden und gezwungen wären, für ihr Verhalten einzustehen. Nach Ansicht von *Zuckerberg* sei damit ein „besseres Zusammenleben" möglich.[23]

---

http://mattmckeon.com/facebook-privacy/

[21] *Steinschaden*, Phänomen Facebook (2010) 157.

[22] „Changes in default profile settings over time", http://mattmckeon.com/facebook-privacy/

[23] *Steinschaden*, Phänomen Facebook (2010) 158.

Aber bedeutet diese „radikale Transparenz“ nur Gutes und ist der einzige, löbliche Gedanke von Facebook „ein besseres Zusammenleben“ oder bedeutet eine „radikale Transparenz“ doch primär das Sammeln möglichst vieler offengelegter Informationen?

Es ist mittlerweile erwiesen, dass SNP bei der Verbrechensbekämpfung helfen (indem zB Suchbilder auf einer Plattform veröffentlicht werden), soziale Bewegungen leichter unterstützt und öffentlich gemacht und Themen schneller verbreitet werden können (wie zB Suchaktionen).

Transparenz hat aber auch „Schattenseiten“ und sie kann auch als „Waffe“ zum Nachteil der Menschen wirken. Man denke nur an Mobbing, Kündigungen, weil etwas Ungünstiges auf einer SNP gepostet wurde, Selbstjustiz, Morddrohungen etc.

Die neue Ausgangslage der Gefährdung der Privatsphäre durch SNP liegt damit zum einen in der Speicherung und Verwendung von Informationen und zum anderen in der Verknüpfung, Vernetzung und Weiterverarbeitung der preisgegebenen Daten durch globale Unternehmen, welche ohne gesetzliche Ermächtigung Daten in großen Mengen sammeln, welche sie entweder direkt vom Nutzer erhalten haben oder ohne seine Mitwirkung vernetzen und speichern, dh ohne dazu gesetzlich ermächtigt zu sein.

II. ÜBERBLICK ÜBER AUSGEWÄHLTE SOCIAL NETWORK-PLATTFORMEN

Zum besseren Verständnis dieser Arbeit ist es unerlässlich, den Aufbau von SNP näher zu beschreiben. Erst eine kurze technische Darstellung von SNP bzw deren Hauptfunktionen und Diensten lässt eine genauere Behandlung datenschutzrechtlicher Fragen bzw der anwendbaren Rechtsbereiche iZm SNP zu.

SNP sind internetbasierte Netzgemeinschaften, welche ein Verknüpfen bereits bestehender Freundschaften und ein Suchen und Finden von neuen Bekanntschaften, Gleichgesinnten und/oder Geschäftskontakten ermöglichen sollen.[24] SNP sind der Inbegriff des Web 2.0[25], Nutzer können eigenständig Inhalte erstellen, bearbeiten und online stellen (social media[26]) und sind damit sowohl „Konsumenten" als auch „Produzenten" der zur Verfügung gestellten Informationen. Das Internet wandelte sich seit dem Jahr 2004 von statischen Web 1.0-Webseiten zu dynamischen Web 2.0-Webseiten. Unter statisch versteht man in diesem Zusammenhang, dass das Internet früher lediglich „konsumiert" und passiv genutzt wurde und dieses nun „dynamisch" mitgestaltet und verändert werden kann.[27] Der Nutzer ist Akteur, Entwickler und Lenker der Dynamik einer Webseite. SNP sind ein sog Web im Web geworden. Das Web 2.0 gestattet seinen Nutzern, eigene Inhalte im Internet bereitzustellen, in SNP zu interagieren, gemeinsame Inhalte zu schaffen und ganz allgemein stärker im Internet mitzumachen[28]. *Hansen* stellte richtig fest, dass dieses „Mitmach-Netz per Web 2.0 eine

[24] http://de.wikipedia.org/wiki/Soziales_Netzwerk_(Internet)

[25] Der Begriff „Web 2.0" wurde im Jahr 2004 von *Tim O'Reilly* (O'Reilly Media) geschaffen, um eine neue Generation von interaktiven Internet- und Webanwendungsmöglichkeiten zu erklären und zu beschreiben. Web 2.0 bedeutet, dass Nutzer eigene Inhalte auf einfache Art und Weise im Internet publizieren und damit das Internet selbst mitgestalten können: *„Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an architecture of participation, and going beyond the page metaphor of Web 1.0 to deliver rich user experiences."*

[26] Social media ist ein Sammelbegriff für Webdienste, die dem Nutzer das einfache Veröffentlichen selbst erstellter Inhalte (Texte, Fotos, Videos) erlauben. Siehe *Steinschaden,* Phänomen Facebook (2010) 203.

[27] So zB das von Internetbenutzern erstellte Online-Lexikon Wikipedia, (http://de.wikipedia.org/wiki/Wikipedia:Hauptseite).

[28] Zum Web 2.0 gehören ua Soziale Netzwerke, Blogs, Videoportale etc., siehe *Hansen* in *De Meer/Herkenhöner,* Sicherheit mit und ohne Netz. Technische und rechtliche Herausforderungen des Web 2.0 (2011) 27.

mittlerweile weithin sichtbare gesellschaftliche Veränderung bewirkt, die sich auch auf den Datenschutz von Nutzern und sogar von Nicht-Nutzern auswirkt“.[29]

Aber nicht nur das Internet, sondern auch das Verhalten der Menschen im Internet veränderte sich in den letzten Jahren stark. Von einem vorsichtigen Umgang mit der eigenen Privatsphäre und dem instinktiven Schutz der Privatheit im realen Leben ist im virtuellen Leben kaum noch etwas übrig. Das virtuelle Entblößen und Zur-Verfügung-Stellen von Informationen über sich selbst oder andere Personen wird immer selbstverständlicher und es wird mittlerweile mit privaten Daten immer freizügiger und nahezu gedankenlos umgegangen.[30]

Die „Nahrung“ und das Lebenselixier von SNP sind Informationen und Daten, welche von möglichst vielen Personen online gestellt werden, um in der Folge verknüpft zu werden. Facebook schreibt: *„Facebook ermöglicht es dir, mit den Menschen in deinem Leben in Verbindung zu treten und Inhalte mit diesen zu teilen.“*[31]

Leissler beschreibt SNP als „globale Plattformen für einen unkomplizierten Informationsaustausch, durch den der Freundeskreis wächst und die Welt zusammenrückt. Nie war es einfacher, mit Freunden zu kommunizieren und Kontakte zu knüpfen. Und nie war es einfacher, Informationen preiszugeben“.[32]

Aber wie funktioniert dieses aktive „Verknüpfen“ und „Suchen und Finden“ bzw das passive „Gefunden werden“ im Internet? Wenn man sich entscheidet, Mitglied einer SNP zu werden, bzw von jemandem per E-Mail eingeladen wird, Mitglied zu werden, dann muss zunächst ein sog „Profil“ angelegt werden. In diesem Profil wird im Grunde eine virtuelle Kopie des Ichs erstellt, indem persönliche Daten angegeben werden und ein Bild online gestellt wird. Je mehr Informationen preisgegeben werden, desto besser und schneller kann ein Nutzer von anderen Nutzern „gefunden und verknüpft“ werden.[33] Alle SNP verfolgen ua das Ziel, einen unkomplizierten, schnellen Informationsaustausch zu gewährleisten und den Nutzern die Möglichkeit zu bieten, sich mit Bekannten, Freunden, Familie etc auf der ganzen Welt zusammenzuschließen bzw zu vernetzen.

---

[29] *Hansen* in *De Meer/Herkenhöner*, Sicherheit mit und ohne Netz. Technische und rechtliche Herausforderungen des Web 2.0 (2011) 23.

[30] *Schaar* spricht idZ treffend von einem „elektronischen Exhibitionismus“ (Symposium „Datenschutz im Zeitalter sozialer Netzwerkdienste“).

[31] http://www.facebook.com

[32] Siehe *Leissler*, Social-networks – Datenschutz in der vernetzten Welt, ecolex 2010, 834.

[33] Vgl *Härting/Schätzle*, Rechtsverletzungen in Social Networks, ITRB 2010, 39 ff.

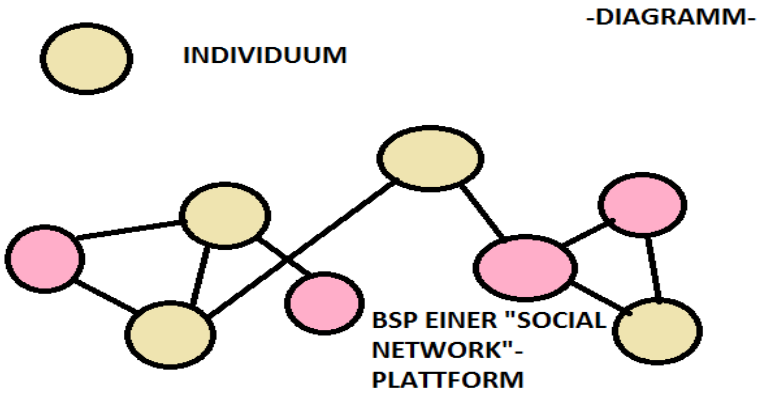

Abbildung 5: Selbst erstelltes Muster-Diagramm einer SNP (Stand: 26.10.2011)[34]

SNP sind eine „Weiterentwicklung“ sog Chatrooms[35], in welchen mit anderen Personen kommuniziert werden konnte. SNP ermöglichen im Unterschied dazu allerdings auch das Hochladen von Fotos, das Abgeben von Kommentaren und das Bilden von Gruppen etc. Chatrooms sind relativ einfach gebaute Möglichkeiten, um mit anderen Personen online zu kommunizieren. Im Unterschied zu diesen Chatrooms sind SNP aber eine Art „kleine virtuelle Welt“ mit virtuellen Kopien der realen Mitglieder.

SNP gibt es in verschiedenen Formen und Ausrichtungen, was die jeweilige Zielgruppe, den Inhalt oder deren Zweck anbelangt. Es gibt Online-Netzwerke für Schüler, Studenten, Arbeitsuchende bzw Arbeitsanbieter, Musikliebhaber, Lehrer uvm.

In der Folge werden einige der bekanntesten SNP dargestellt:

A. BEISPIELE VON SOCIAL NETWORK-PLATTFORMEN

1. Friendster[36]

Friendster wurde im Jahr 2002 von *Jonathan Abrams* gegründet und wird nunmehr durch die Friendster Inc. betrieben. Die meisten Nutzer von Friendster stammen aus dem

[34] Selbsterstelltes Diagramm in Anlehnung an Skizzen aus dem Internet (zB unter Wikipedia).
[35] http://www.businessdictionary.com/definition/chat-room.html, eine Webseite/Forum, in dem mehrere Internetnutzer interaktiv miteinander mittels Eingabe eines Textes (Instant Messaging) kommunizieren können.
[36] http://www.friendster.com

englischsprachigen und asiatischen Raum. In Mitteleuropa hält sich die Popularität bis dato in Grenzen. Bis zum Jahr 2004 galt Friendster als das größte soziale Netzwerk des Internets, wurde aber in der Folge durch das SN MySpace abgelöst. Im Jahr 2003 äußerte Google Interesse daran, die Webseite zu kaufen, doch wurde dieses Angebot ausgeschlagen. Ein großes Problem und ein möglicher Grund, warum Friendster nicht ganz so erfolgreich wurde wie Facebook, sind, dass das Unternehmen mit dem plötzlichen großen Interesse der Nutzer nicht zurechtkam. Außerdem kam es mehrmals zu Serverproblemen bzw -überlastungen, weswegen Friendster viele Nutzer wieder verlor. Speziell in den Jahren 2004 und 2006 verließen viele Nutzer Friendster und wechselten zu den neuen SNP MySpace und Facebook.[37]

2. MySpace[38]

MySpace ist ein speziell für den Musikbereich aufgebautes Online-Netzwerk. MySpace wurde in Los Angeles gegründet und hat im Gegensatz zu fast allen anderen IT-Riesen seinen Firmensitz nicht im Silicon Valley, sondern in Beverly Hills. Die Nutzer von MySpace können kostenlos ein Profil anlegen und Fotos, Videos, Blogs etc erstellen. Im Jahr 2010 hatte MySpace 4 Millionen Mitglieder in Deutschland (zeitgleich hatte Facebook schon 13 Millionen Nutzer).[39]

3. XING[40]

„Xing" steht sowohl für das englische Wort „crossing", sich „kreuzen, begegnen", als auch für das chinesische Zeichen „es klappt, es funktioniert". Der ursprüngliche Name war „openBC" und wurde im Jahr 2006 auf Xing geändert. Xing ist eine webbasierte Online-Plattform, welche es natürlichen Personen ermöglicht, ihre geschäftlichen Kontakte zu verwalten. Xing dient der Selbstvermittlung bzw dem Vermitteln von Arbeit. Gegründet wurde diese Webplattform von *Lars Hinrichs*. Xing erfüllt primär den Zweck, sein Kontaktnetz sichtbar zu machen.

---

[37] Im Detail siehe *Steinschaden*, Phänomen Facebook (2010) 80 ff, insbesondere *Martina Mara*, Narziss im Cyberspace (2009).

[38] http://www.myspace.com, http://de.myspace.com

[39] http://de.wikipedia.org/wiki/myspace

[40] http://fbx.xing.com/?dpt=makhh&ttp=sem&plf=goo&xtr=de11&pid=brte

4. StudiVZ[41]

StudiVZ steht für „Studiverzeichnis“ und ist eine speziell für Studenten konzipierte Online-Plattform, welche im Jahr 2005 gegründet und bis 2009 in mehreren Sprachen angeboten wurde. Ab 2009 lag das Hauptaugenmerk auf dem deutschsprachigen Raum.[42]

5. Twitter[43]

Twitter ist ein im Jahr 2006 von *Dick Costolo* gegründetes Informationsnetzwerk, welches den Nutzern in Echtzeit die neuesten Informationen zu gezielt gewählten Themen durch sog „Tweets“ („to twitter“ heißt so viel wie „zwitschern“) liefert. Man braucht dafür nur nach öffentlichen Streams suchen und der Konversation folgen. Angemeldete Nutzer von Twitter können eigene Textnachrichten, sog „Tweets“, mit maximal 140 Zeichen senden. Diese Nachrichten empfangen die sog „follower“, das sind die dem Verfasser angeschlossenen/„folgenden“ Leser.

Studien aus dem Jahr 2011 zufolge war Twitter zu einem der größten Konkurrenten von Facebook herangewachsen. Twitter hatte im Jahr 2011, fünf Jahre nach der Gründung, bereits 200 Millionen registrierte Nutzer weltweit und soll, einer Studie aus 2011 zufolge, damals täglich 460.000 Nutzer dazugewonnen haben[44]. Der größte Unterschied zu Facebook liegt darin, dass bei Twitter lediglich 140 Zeichen verfasst und gepostet werden können. Auf Twitter gibt es keine Fotos und Videos, es können lediglich Nachrichten gepostet werden. Bei Twitter werden Freunde nicht wie bei Facebook „friends“, sondern „follower“ genannt. Twitter dient daher weniger der privaten Kommunikation als der öffentlichen Diskussion.[45] Dies spiegelt sich in den 20 meistgelesenen Twitter-Seiten wider, bei denen es sich um solche von Journalisten oder Medien handelt.[46]

6. LinkedIn[47]

LinkedIn ist ein webbasiertes soziales Netzwerk zur Pflege bestehender Geschäftskontakte und zum Knüpfen von neuen Verbindungen.

---

41 http://www.studivz.net/Default, ähnlich für Schüler: http://www.schuelervz.net/Default
42 Zur studiVZ Ldt gehören des Weiteren die Portale schülerVZ und meinVZ.
43 http://twitter.com.
44 Das war der Durchschnittswert im Februar 2011: http://blog.twitter.com/2011/03/numbers.html
45 Twitter will das neue Facebook werden, Artikel auf www.futurzone.at, Kurier, 16.6.2011.
46 Stand November 2011.
47 http://www.linkedin.com

7. Flickr[48]

Flickr ist ein Online-Portal, welches seinen Nutzern die Möglichkeit bietet, digitale Bilder und Videos auf die Webseite hoch zu laden. Diese Bilder und Videos können mit Kommentaren versehen und anderen Nutzern zur Verfügung gestellt werden. Die Nutzer von Flickr können die Bilder für jeden sichtbar veröffentlichen oder so hochladen, dass nur sie selbst auf die Bilder zugreifen können. Die Erlaubnis zum Betrachten lässt sich auch auf eine bestimmte Gruppe von anderen Flickr-Nutzern einschränken.

Entwickelt wurde Flickr von einem kanadischen Unternehmen namens Ludicorp[49]. Im Jahr 2005 wurden Flickr und Ludicorp von Yahoo gekauft. Flickr hat nach eigenen Angaben ca. 5.000 Uploads pro Minute und weltweit über 40 Millionen registrierte Benutzer und soll zu den fünfzig am stärksten frequentierten Seiten im Internet gehören.

8. Google+[50]

Google+ ist ein soziales Netzwerk, welches im Juni 2011 von der Google Inc. gegründet wurde. Google+ wird von vielen Seiten als ein „Versuch gesehen, sich in sozialen Netzwerken zu etablieren“.[51] Am Beginn war das Registrieren nur auf Einladung möglich, doch ab September 2011, wenige Monate nach der Gründung, hat Google das Netzwerk geöffnet und man konnte sich ab dann auch ohne vorherige Einladung anmelden. Auch das Mindestalter wurde von ursprünglich 18 Jahren auf 13 Jahre gesenkt. Im März 2012 hatte Google+ 100 Millionen und im Juni 2012 bereits 250 Millionen Nutzer.

[48] http://www.flickr.com
[49] http://www.ludicorp.com
[50] https://accounts.google.com/ServiceLogin?service=oz&continue=https://plus.google.com/?gpsrc%3Dgplp0&hl=d
[51] Siehe http://de.wikipedia.org/wiki/Google%2B (Stand: Oktober 2012).

III. SOCIAL NETWORK-PLATTFORM FACEBOOK[52]

Mit Facebook wurde im Jahr 2004 der Höhepunkt der Gründungen von SNP erreicht. Im August 2008, nur vier Jahre nach der Gründung am 4.2.2004, hatte Facebook bereits 100 Millionen, im Februar 2010 dann 400 Millionen und im Juli 2010 bereits eine halbe Milliarde Mitglieder und Nutzer.[53] *Mark Zuckerberg*, einer der Hauptgründer von Facebook, war im Jahr 2012 mit einem geschätzten Vermögen von 9,4 Milliarden USD an 35. Stelle der 400 reichsten Personen weltweit.[54] Die Webseite von Facebook lag im Jahr 2012 auf 60.000 Servern, welche sich in Palo Alto[55], Kalifornien, USA, befanden. Facebook hat mittlerweile so viele Nutzer, dass – wenn man von einem Staat sprechen würde – Facebook der fünftgrößte Staat weltweit wäre. Facebook hätte 85-mal so viele „Einwohner" wie Österreich[56]. Die Nutzer verbringen weltweit mehr als 8 Milliarden Minuten täglich auf Facebook und pro Monat werden ungefähr zwei Milliarden Fotos und 14 Millionen Videos auf Facebook hochgeladen.[57] 50% aller Facebook-Nutzer loggen sich täglich ein, im Durchschnitt hat ein Nutzer 130 Freunde und 10,2% der Erdbevölkerung haben bereits einen Facebook-Account.[58]

Diese Zahlen zeigen die Bedeutung von SNP und verdeutlichen, was für eine Relevanz sie zwischenzeitlich erlangt haben.

---

[52] http://www.facebook.com

[53] Laut einer Studie von *Denkmayer* und *Bäck* (in *Steinschaden*, Phänomen Facebook [2010] 62 ff) über die Facebook-Nutzer in Österreich und Deutschland ist Facebook keine Teenager-Plattform, sondern unter den 20- bis 40-Jährigen stark verbreitet.

[54] Forbes-Liste abrufbar unter www.forbes.com, http://www.forbes.com/profile/mark-zuckerberg/

[55] Palo Alto ist eine Kleinstadt im Silicon Valley südlich von San Francisco und der Hauptsitz von Facebook. Das Silicon Valley ist das Zentrum der IT-Welt und dort haben Unternehmen wie Google, Intel, Yahoo, Apple, Oracle, eBay, HP, Cisco etc ihren Firmensitz. „Silicon" stammt vom Wort „Silizium", einem wesentlichen Bestandteil von Computer-Chips, vgl auch http://de.wikipedia.org/wiki/Palo_Alto

[56] Facebook hat im November 2011 angegeben, weltweit 721 Mio aktive Nutzer zu haben (https://www.facebook.com/notes/facebook-data-team/anatomy-of-facebook/10150388519243859).

[57] *Staudinger* in *Jaksch-Ratajczak*, Aktuelle Rechtsfragen der Internetnutzung (2010) 248.

[58] Siehe *Beer*, Der große Facebook Ratgeber, 01/2012.

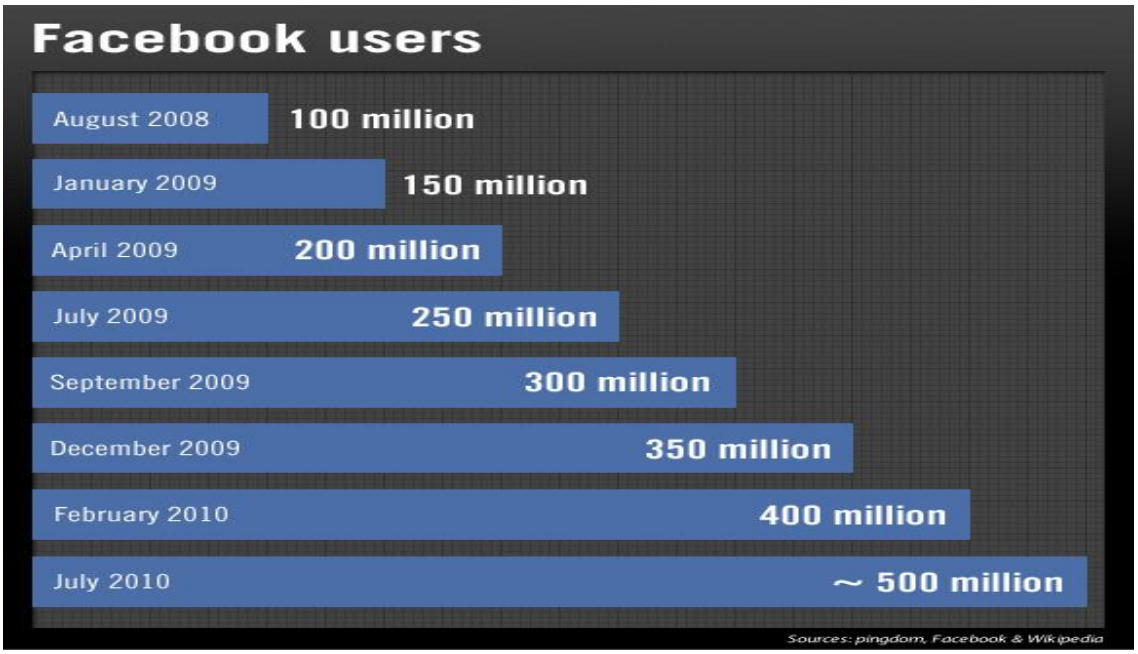

Abbildung 6: Anzahl der Facebook-Nutzer (Stand: 26.10.2011)[59]

Facebook macht sich aber nicht nur unter den Nutzern breit, sondern auch auf anderen Webseiten. Die Entwickler und Programmierer von Facebook entwickeln immer neue Technologien, um die Grenzen der eigenen Webseite zu überschreiten und Teil anderer Internetdienste zu werden.

Die Facebook-Plattform wurde in der Zwischenzeit zu einer neuen Möglichkeit für IT-Entwickler, um Zusatz-Programme, wie insbesondere Apps, zu entwickeln. Es gibt weltweit mehr als eine Million Programmierer und Unternehmer, welche Facebook-spezifische Programme und Anwendungen entwickeln und anbieten.[60]

All diese Entwicklungen sind aber nicht nur aus technischer Sicht interessant zu verfolgen und zu beobachten, sondern auch aus datenschutzrechtlicher Sicht relevant, werden doch mittels Applikationen enorme Datenmengen von Nutzern gewonnen und diese mit anderen Programmen verknüpft.

Die vorliegende Arbeit legt, ob der Größe und Popularität, ein Hauptaugenmerk auf das SN Facebook als eine Online-Plattform, welche innerhalb kürzester Zeit eine derart hohe Akzeptanz gefunden hat, dass es aus dem nur für Studenten zugänglichen Netzwerk

[59] pingdom, facebook und Wikipedia, http://www.rockefeller-news.com und http://www.justsocial.com/facebook-updated-stats.html/

[60] *Steinschaden*, Phänomen Facebook (2010) 28 f.

sukzessive für immer mehr Benutzergruppen geöffnet wurde und nunmehr nahezu weltweit für fast jedermann zugänglich geworden ist.

A. HISTORISCHER ÜBERBLICK

Facebook hieß ursprünglich „TheFacebook.com“ und war als eine Art „Photobuch“ für Studenten der Harvard Universität vom Harvard-Studenten *Mark Zuckerberg*[61] und seinen Kollegen und Mitbegründern, *Chris Hughes*[62], *Dustin Muskovitz*[63] und *Eduardo Saverin*[64], im Jahr 2004 geschaffen worden, um Harvard-Studenten untereinander zu vernetzen. Mit der Zeit wurde das Netzwerk auch für Studenten der US-amerikanischen Universitäten Yale, Stanford und Columbia geöffnet, damit diese ebenfalls ein Profil erstellen und mit ihren Kollegen kommunizieren und sich austauschen konnten. Das Netzwerk ist derart rasant gewachsen und hat unglaublich an Popularität gewonnen, sodass schließlich ein riesiges Unternehmen mit Firmensitz in Palo Alto, Kalifornien, entstanden ist. Der erste große Investor von Facebook war im Jahr 2004 der deutsch-amerikanische Internet-Unternehmer *Peter Thiel*, welcher kolportierte 500.000 USD in das Unternehmen Facebook investierte und dafür rund 10% der Anteile am Unternehmen erhielt.[65]

---

[61] *Mark Elliot Zuckerberg* wurde am 14.5.1984 in White Plains im US-Bundesstaat New York geboren. Er ist Gründer und Vorstandsvorsitzender des Online-Netzwerks Facebook und hält an diesem einen Anteil von 24,7%. Am 15.12.2010 wurde er vom New Yorker Time-Magazin zur „Person des Jahres“ gewählt. Seine erste Webseite „FaceMash.com“, welche Vorreiter von Facebook war, hat *Mark Zuckerberg* am 20.12.2010 um rund 30.000 USD versteigert. *Zuckerberg* hat an der Harvard University ein Informatik-Studium begonnen, hat dieses jedoch ohne Abschluss aufgegeben, nachdem er im Jahr 2004 Facebook gründete. *Zuckerbergs* Vermögen wurde im Jahr 2010 auf rund 6,9 Milliarden USD geschätzt.

[62] *Chris Hughes* war *Zuckerbergs* Zimmerkollege in Harvard. Er gilt als einer der Mitgründer von Facebook. Bis zum Jahr 2008 war er Firmensprecher. *Hughes* gehört knapp 1% vom Unternehmen Facebook (zitiert nach *Steinschaden*, Phänomen Facebook [2010] 40 ff).

[63] *Dustin Muskovitz* war *Zuckerbergs* Zimmerkollege in Harvard. *Muskovitz* zählt zum Gründerteam von Facebook. Er schied im Jahr 2008 aus dem Unternehmen aus. Ihm gehören ca. 6% von Facebook (zitiert nach *Steinschaden*, Phänomen Facebook [2010] 40 ff).

[64] *Eduardo Saverin* ist Mitgründer und erster Finanzier von Facebook. Ihm gehören ca 4% von Facebook.

[65] Ihm gehören ca 3% von Facebook; http://en.wikipedia.org/wiki/Peter_Thiel

Abbildung 7: Screenshot „thefacebook“[66]

Im Jahr 2005 wurde nicht nur das „The“ (von „The Facebook“) gestrichen und hieß das Unternehmen fortan nur noch „facebook“. Es wurde auch der Zugang für andere Nutzer ermöglicht, wodurch die Nutzerzahl auf sagenhafte 5,5 Millionen registrierte Benutzer stieg. 2006 wurde die Funktion der sog „News Feeds“ eingeführt.

Dabei handelt es sich um „abonnierte Informationen aus dem Internet“, die automatisch in den Internetbrowser „eingespeist“ werden[67]. Ab Mai 2007 konnten Fremdentwickler Programme entwickeln und diese Facebook zur Verfügung stellen. Im Jahr 2007 öffnete Facebook seine Plattform für Anwendungen von Drittanbietern, um diesen zu ermöglichen, dass sie eigens programmierte Webdienste auf der Facebook-Seite bereitstellen können. Im selben Jahr kam ein Werbesystem namens „Facebook Ads“ dazu, welches die Investoren ablösen und die Selbsterhaltung der Seite ermöglichen sollte.[68]

Im Jahr 2007 hat Microsoft[69] 240 Millionen USD in das Unternehmen investiert und dafür 1,6% der Anteile am Unternehmen erhalten. Im Jahr 2008 gab es Facebook bereits in den Sprachen Deutsch, Spanisch und Französisch, weitere Sprachen kamen im Laufe der Zeit hinzu. In der Zwischenzeit wurde Facebook in mehr als 70 Sprachen übersetzt. Dadurch stieg

---

66 http://upload.wikimedia.org/wikipedia/en/f/f8/Thefacebook.png (19.11.2014).
67 http://dictionary.reference.com/browse/newsfeed
68 http://www.facebook.com/adsmarketing
69 Microsoft ist ein multinationaler Softwarehersteller mit weltweit ca. 93.000 Mitarbeitern und einem Umsatz von 58,44 Milliarden USD. Siehe auch http://www.microsoft.com/en-us/default.aspx

die Nutzeranzahl auf 100 Millionen. Im Jänner 2009 waren es 150 Millionen, im Februar 175 Millionen, im Juli 250 Millionen, im Juli 2010 bereits eine halbe Milliarde Nutzer und im Oktober 2012 eine Milliarde Mitglieder. Laut socialbakers.com lag Österreich im März 2011 mit 2.385.320 Nutzern an der 48. Stelle weltweit, was ca 29,04% der österreichischen Bevölkerung dargestellt. Die USA liegen mit 152.189.880 Nutzern an erster Stelle der Facebook-Nutzer.[70] 2010 gab es laut socialbakers.com weltweit 7,9 neue Registrierungen pro Sekunde. Facebook hatte im Jahr 2009 weltweit ein geschätztes Jahreseinkommen in der Höhe von 800 Millionen und im Jahr 2011 eines von geschätzten 845 Millionen USD.[71]

Am 18.5.2012 ging Facebook an die Börse, die Gesamtbewertung des Unternehmens lag auf Basis des Ausgabekurses zum damaligen Zeitpunkt bei rund 104 Mrd. USD.[72]

B. FACEBOOK-KONTO ANLEGEN

Um Facebook-Mitglied zu werden, muss ein persönliches (privates oder Unternehmens-) Profil erstellt werden, indem der Nutzer – bei Erstellung eines privaten Profils – seinen (nicht notwendigerweise echten) bürgerlichen Namen, Geburtsdatum, E-Mail-Adresse, Wohnsitz und ein von ihm frei zu wählendes Passwort angibt. In der Folge können weitere Informationen wie Religion, Beruf, Hobbies, Interessen etc angegeben und ein Profilfoto hochgeladen werden.[73] Nach Profilen kann anhand des Namens mithilfe von Kriterien wie Wohnort, Schule, Universität etc gesucht werden. Profile können auch untereinander verknüpft werden, entweder indem angegeben wird, dass ein anderer Nutzer ein „Familienmitglied“ ist, oder indem nach einer positiven Kontaktannahme zwei Mitglieder miteinander verknüpft und dem jeweiligen Freundeskreis hinzugefügt werden. Durch das Verknüpfen entstehen soziale Netzwerke aus Kontakten.[74] Die Registrierung erfolgt in den meisten Fällen kostenlos, je nach Betreiber sind verschiedene Dateneingaben erforderlich.

---

70 http://www.socialbakers.com

71 http://www.facebook.com/press/info.php?factsheet

72 http://de.wikipedia.org/wiki/Facebook_Inc. (Stand Okt 2014).

73 http://www.facebook.com/help/?page=173&hloc=de_DE (6.4.2011): „Wie registriere ich mich für Facebook? Teile uns einfach auf unserer ‚Registrieren‘-Seite deinen vollständigen Namen, deine E-Mail-Adresse, das gewünschte Passwort, dein Geschlecht und dein Geburtsdatum mit. Wenn du aktuell ein Schüler bist, hast du die Möglichkeit, einem unserer Schulnetzwerke beizutreten. Wenn du nicht mehr zur Schule gehst, kannst du einem unserer Hochschul- oder Arbeitsnetzwerke beitreten. Nachdem du das Registrierungsformular ausgefüllt hast, werden wir eine E-Mail an die von dir angegebene Adresse senden. Durch Anklicken des Bestätigungslinks wird die Registrierung abgeschlossen.“

74 Siehe auch *Faber/Schwarz,* Social Networks (2011) 9 f.

Bei Facebook ist die Registrierung weiterhin kostenlos. Im Zuge der Registrierung werden vorab der Name (Vor- und Nachname), E-Mail-Adresse, Geschlecht, Geburtsdatum und ein Passwort verlangt.

Profilnamen dienen primär der leichten Auffindbarkeit einer bestimmten Person oder eines bestimmten Unternehmens. Nicht alle SNP handhaben die Registrierung gleich. Einige Plattformen verlangen im Zuge der Registrierung eine „Versicherung" des Nutzers, dass er korrekte Angaben gemacht und sich nicht mit einer falschen Identität angemeldet hat (zB Facebook und XING).

Facebook schreibt zwar in den „Facebook-Nutzungsbedingungen und Richtlinien", „Erklärung der Rechte und Pflichten" unter dem Punkt „Registrierung" vor, dass alle „Kontoinformationen korrekt und auf dem neuesten Stand" sein müssen, doch gibt es keine wirkliche „Sicherheit" dafür, dass der angegebene Name der richtige Name des Nutzers ist bzw alle Daten tatsächlich stimmen.

Im Unterschied dazu bietet die Plattform Twitter die Möglichkeit einer Art „Verifizierung": Einige Twitter-Konten zeigen ein blau hinterlegtes (aktiviertes) Kontrollfeld hinter dem jeweiligen Namen an, womit gezeigt werden soll, dass das Konto bestimmter „wichtiger Einzelpersonen und Marken" „verifiziert" wurde. Diese Markierung zeigt an, dass Twitter geprüft hat, dass es sich bei der angegebenen Person um die „wahre" handelt. Twitter schreibt dazu auf der Webseite: *„Verifizierung wird im Moment dazu eingesetzt, um Authentizität der Identität wichtiger Einzelpersonen und Marken bei Twitter zu gewährleisten. Das Ziel dieses Features ist es, Verwechslungen bei Twitter zu minimieren und es einfacher zu machen, echte Accounts zu erkennen."*[75] Twitter verifiziert primär Einzelpersonen aus den Bereichen Musik, Film, Mode, Regierung, Politik, Religion, Sport, um ein erleichtertes Auffinden zu ermöglichen.

Abbildung 8: Beispiel „Verified Twitter Account"

[75] http://support.twitter.com/articles/313322-das-neue_twitter-uber-verfizierte-konten

1. Datenangabe

Fakultativ können vom Nutzer ua folgende Daten bzw Informationen online gestellt werden:

- Erstellung einer Kontaktliste bzw eines Adressbuches
- Empfang und Versand von Nachrichten
- Hochladen von Fotos und Videos
- Empfang und Benachrichtigungen über diverse Ereignisse.

Wenn ein Nutzer einer sog Freundesliste hinzugefügt wurde, besteht außerdem die Möglichkeit, regelmäßig über den neuesten Stand und Änderungen in den Profilangaben (verlobt, verheiratet, Single etc) sowie über Postings und Statusmeldungen[76] informiert zu werden. Außerdem gibt es auf Facebook eine sog (virtuelle) „Pinnwand" (engl.: „wall"), auf welcher Nachrichten hinterlassen werden können.

Facebook schreibt in den Nutzungsbedingungen vor, dass Privatkonten nur für private Kommunikation genutzt werden dürfen. Falls ein Konto auch kommerziell genutzt werden soll, muss ein eigenes Unternehmenskonto angelegt werden. Ein Unternehmenskonto besitzt jedoch kein persönliches Profil. „Anfreunden" und Nachrichten schicken sind bei einem Unternehmenskonto nicht möglich.

2. Profileinstellungen

Fast alle SNP bieten die Möglichkeit, mittels sog „Privatsphäre-Einstellungen" den Zugriff anderer Personen bzw Nutzer auf das eigene Profil und damit die Veröffentlichung von online gestellten Daten und Informationen zu beschränken. Der Nutzer kann selbst entscheiden, welche Personen welche Informationen sehen dürfen und können.

Bei der SNP Facebook kann seit dem Jahr 2009 jeder Facebook-Nutzer unter „Account/privacy settings/sharing on facebook" selbst festlegen, ob seine Statusmeldungen, Links und Medien veröffentlicht werden sollen. Damit kann er selbst bestimmen, wer was wie sehen darf und wer nicht. Es kann zwischen den Optionen „Öffentlich, Freunde von Freunden, Freunde, Freunde ohne Bekannte, Benutzerdefiniert und nur ich" hinsichtlich der Einsehbarkeit von Informationen, Bildern udgl gewählt werden.

[76] Als „Statusmeldungen" bezeichnet man Angaben darüber, wo man sich gerade befindet, wie es einem geht, was macht man gerade macht uÄ.

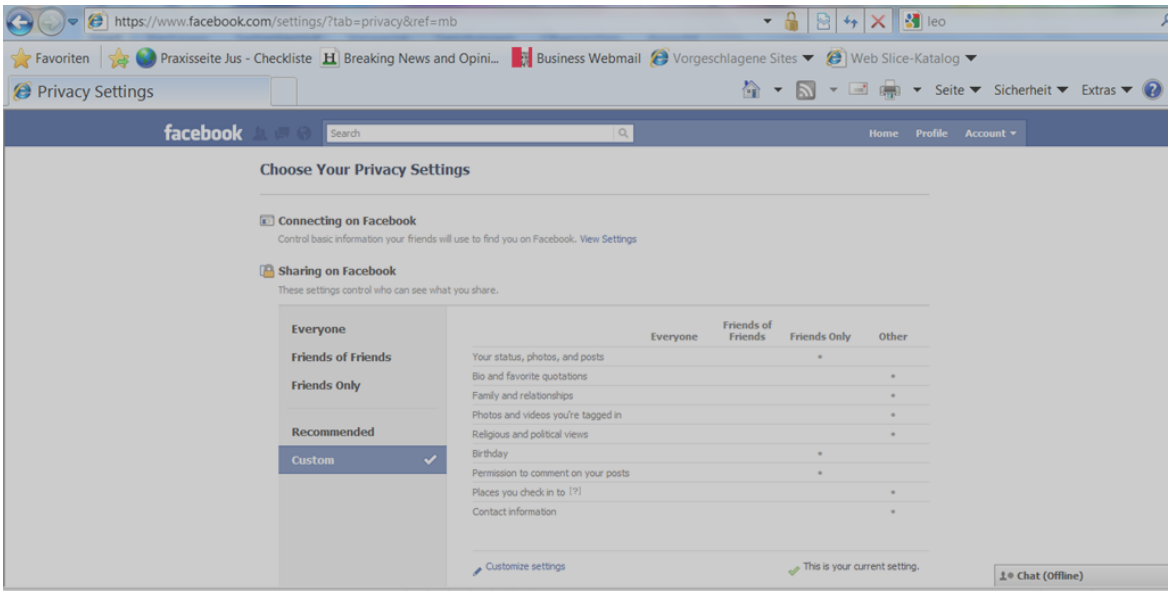

Abbildung 9: Screenshot[77] der Webseite www.facebook.com[78]

3. Facebook-Freundschaft

SNP leben und bestehen aus „Freundesbeziehungen" der Nutzer, welche als Knotenpunkte des jeweiligen Online-Netzwerkes eingegangen werden.[79] Durch diese „Freundschaften" werden Verbindungen und Verknüpfungen zwischen den Nutzern hergestellt.

Nach Erstellung eines Profils wird man in einem nächsten Schritt aufgefordert, „Freunde" zu suchen, indem man einen Namen bei der Suchfunktion eingibt. Nach der Eingabe zusätzlicher Informationen, wie Arbeitsstätte, Ausbildungsort etc, bekommt man außerdem Freunde „vorgeschlagen", welche man möglicherweise kennen könnte.

Zusätzlich entwickelte Facebook den sog „Friendfinder", welcher es den Nutzern „leicht machen" sollte, schnell Freunde auf Facebook „zu finden". Mittels Friendfinder werden Kontakte importiert und mit bereits registrierten Facebook-Mitgliedern abgeglichen, um zu sehen, welche Personen sich möglicherweise kennen könnten, um diese in der Folge zu verknüpfen.

---

[77] Facebook untersagt die ungenehmigte Verwendung von Screenshots und diese dürfen auch nicht mit Anmerkungen versehen werden. Diese Einschränkungen sind mE nur im Zusammenhang mit persönlichen Daten von Mitgliedern, Marken- und Urheberrechten wirksam. Siehe http://www.facebook.com/brandpermissions/screenshots.php (28.6.2011).

[78] http://www.facebook.com

[79] Siehe Kapitel „Freundschaft" in *Steinschaden*, Phänomen Facebook (2010) 14 ff.

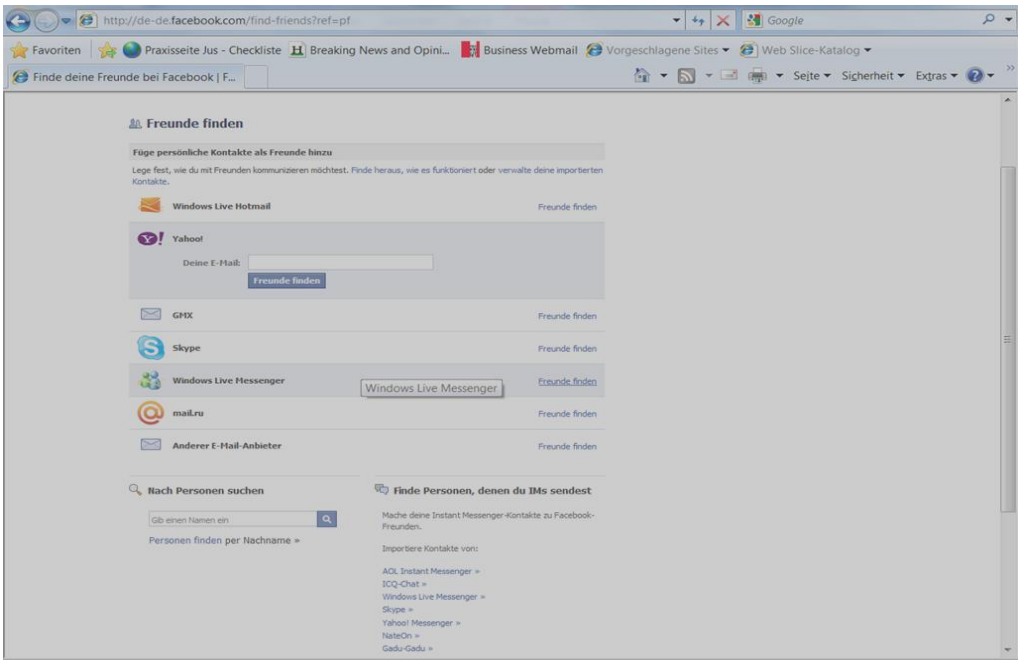

Abbildung 10: Freundefinder von Facebook (Stand: 26.10.2011)

Ich schließe mich der Meinung von *Steinschaden* an, welcher treffend betonte, dass der Begriff „Freund“ von *Mark Zuckerberg* zwar „recht schlau, aber nicht korrekt“ gewählt wurde. Mittlerweile ist der Begriff „Facebook Friend bzw Freund“ jedoch aus dem Sprachgebrauch kaum mehr wegzudenken und es gibt im New Oxford American Dictionary sogar das Verb „to unfriend“: *„To remove someone as a ‚friend‘ on a social networking site such as Facebook.“* Das Verb „to unfriend“ bezeichnet demnach die Tätigkeit, jemanden als Freund in einem Online-Netzwerk wie Facebook (wieder) zu entfernen. Im Jahr 2009 war „to unfriend“ das „New Oxford Dictionary Wort des Jahres“.[80]

In diesem Sinne ist ein Entfreunden gänzlich unkompliziert und „dezent“. Der Entfreundete wird darüber nicht informiert und merkt es zumeist erst, wenn er plötzlich keinen Zugriff mehr auf bestimmte Seiten bzw ein bestimmtes Profil eines „Freundes“ hat.

Statt eines vollkommenen Entfreundens kann die weniger drastische Möglichkeit gewählt werden, bestimmte Freunde in gewissen Unterlisten zusammenzufassen und diesen damit nur gewisse Inhalte des Profils zu zeigen bzw für sie sichtbar zu machen.

[80] http://content.usatoday.com/communities/ondeadline/post/2009/11/unfriend-is-new-oxford-dictionarys-word-of-the-year-/1

4. Facebook-Fanpage

Facebook bietet seinen Nutzern nicht nur die Möglichkeit der Erstellung eines Profils für Privatpersonen, sondern auch sogenannte Facebook-Pages in mehreren Kategorien, wie „lokales Unternehmen oder Ort“, „Unternehmen, Organisation oder Institution“, „Marke oder Produkt“, „Künstler, Band oder öffentliche Person“, „Unterhaltung“ oder „guter Zweck oder Gemeinschaft“ an.

Facebook-Fanpages sind genauso simpel zu erstellen wie private Profilseiten. Sie werden primär von Unternehmen, Künstlern und bekannten Persönlichkeiten als Marketing- und Werbemittel erstellt. Im Unterschied zu „normalen“ Profilen können auf Fanpages Kommentare, Meinungen, Fotos etc auch von Nutzern selbst veröffentlicht werden.

C. AUSGEWÄHLTE FACEBOOK-FUNKTIONEN

In der Folge werden primär die technischen Aspekte einiger ausgewählter Facebook-Funktionen beleuchtet, bevor auf damit in Zusammenhang stehende Rechtsprobleme eingegangen wird.

1. News Feed

Der News Feed ist eine im Jahr 2006 eingeführte Funktion, welche es dem Nutzer von Facebook ermöglicht, permanent über seine „Freunde“ und Bekannte informiert zu sein. Dank News Feed wird ein Nutzer darüber informiert, was seine Freunde den ganzen Tag machen, ohne womöglich auch nur ein Wort mit ihnen gesprochen oder ihnen geschrieben zu haben. News Feed ist ein Algorithmus, welcher in Echtzeit und chronologischer Reihenfolge zusammenfasst, wer was wann als Status-Update veröffentlicht hat.[81]

Beispiele für Statusmeldungen: „XY wurde im Album von Z markiert“, „X gefällt das Foto von Z“, „XY: ich bin arbeiten“.

Die Funktion und die Einführung des News Feed im Jahr 2006 hatten einen großen Aufruhr verursacht. Eine Million Nutzer (das waren im Jahr 2006 ungefähr 10% der Nutzer) forderten, dass der News Feed wieder entfernt werden soll, da die Nutzer plötzlich Angst bekamen, dass

[81] *Steinschaden*, Phänomen Facebook (2010) 17.

aus „Facebook“ ein „StalkerBook“[82] werden könnte. Ein weiteres Problem war die Tatsache, dass dank des Algorithmus Inhalte, welche man veröffentlicht hatte, nicht mehr gelöscht werden konnten, da sie sofort auf hunderte andere Profile verteilt wurden.

Es folgten eine Reaktion von *Mark Zuckerberg* und neue Privatsphäre-Einstellungen, um die „wütende Masse zu beruhigen“.[83]

2. Hochladen von Fotos und Videos

Einleitend möchte ich *Maggiatto* kurz zitieren: *„Geschwindigkeit und Fotos hängen bei Facebook eng zusammen.“*[84]

Facebook setzte sich zum Ziel, auf der ganzen Welt Bilder in Sekundenbruchteilen auf die Monitore der Mitglieder zu bringen und gleichzeitig jedem Nutzer zu erlauben, so viele Fotos wie nur möglich in die Profile zu laden. Ende 2009 waren auf den Facebook-Servern 30 Milliarden digitale Bilder gespeichert. Facebook war eines der größten Foto-Portale im Internet geworden. Ende 2010 waren bei Facebook bereits mehr als 65 Milliarden Schnappschüsse gespeichert.

Facebook führte im Juni 2010 eine Funktion ein, welche die von Nutzern hochgeladenen Fotos und die darauf sichtbaren Gesichter untersuchte bzw durchscannte und diese folglich markierte. Diese Funktion wurde lt Facebook eingeführt, damit nicht jedes einzelne Bild durchforstet und markiert („getagged“) werden muss. Facebook glich die neuen Fotos mit den bereits vorhandenen ab und lieferte, nach der Ermittlung, wer darauf zu sehen ist, Namensvorschläge. Diese Funktion war grundsätzlich standardmäßig aktiviert und musste aktiv in den Privatsphäre-Einstellungen deaktiviert werden.[85]

„Falls du nicht möchtest, dass dein Name vorgeschlagen wird, kannst du das Vorschlagen von Markierungen in deinen Privatsphäre-Einstellungen deaktivieren. Klicke dazu einfach zunächst auf ‚Benutzerdefinierte Einstellungen‘ und dann auf ‚Freunden Fotos von mir vorschlagen‘. Dein Name wird daraufhin nicht mehr in Fotomarkierungsvorschlägen

---

[82] Unter „Stalking“ wird laut Wikipedia „das willentliche und wiederholte (beharrliche) Verfolgen oder Belästigen einer Person verstanden, deren physische oder psychische Unversehrtheit dadurch unmittelbar, mittelbar oder langfristig bedroht und geschädigt werden kann“; http://www.urbandictionary.com/define.php?term=stalkerbook

[83] *Steinschaden*, Phänomen Facebook (2010) 19.

[84] *Rich Maggiatto*, Chef von Zinio.com, im Gespräch mit *Steinschaden*, Mai 2010.

[85] Stand Dezember 2011.

angezeigt. Deine Freunde können dich jedoch auch weiterhin manuell auf Fotos markieren. Weitere Informationen zu dieser Funktion erhältst du in unserem Hilfebereich.“[86]

Flickr ging weiter und führte eine Funktion ein, welche es ermöglichte, anhand des Hintergrundes eines Fotos herauszufinden, wo auf der Welt sich eine Person zum Zeitpunkt des Fotografierens befunden hat. Andere Nutzer konnten dann zusätzlich über die Schlagwortsuchfunktion über die jeweiligen Koordinaten ein Bild (von einer bestimmten Person) suchen und finden.

Auf die rechtlichen Problemfelder iZm dem Hochladen von Fotos wird weiter unten eingegangen.

3. Friendfinder

Der Friendfinder (deutsch: „Freundefinder“) ist eine Software, welche die Kontakte der Nutzer miteinander vergleicht und in der Folge Personen als Freunde vorschlägt, welche mehrmals auf diesen Listen aufscheinen. Diese „Freundschaftsvorschläge“ basieren auf dem Gedanken, dass man Personen, welche mehrmals auf den verglichenen Listen vorkommen, ebenfalls „kennen muss“ und mit diesen daher befreundet sein möchte.

Facebook bietet seinen Mitgliedern die Möglichkeit, durch freiwillige Eingabe der jeweiligen E-Mail-Adresse und des zugehörigen Passwortes des E-Mail-Kontos dieses E-Mail-Konto von Facebook durchsuchen und mit der Facebook-Freundesliste synchronisieren zu lassen.

Für Nutzer von Smartphones[87] bietet Facebook eine kostenlose Software an, welche die Kontakte aus dem jeweiligen Telefonbuch mit den Kontakten von Facebook synchronisieren kann. Dabei werden standardmäßig sämtliche Nach- und Vornamen, Telefonnummern, E-Mail-Adressen und Geburtstage hochgeladen und bei Facebook gespeichert. Ziel von Facebook ist es, dem Nutzer eine möglichst „einfache und für ihn unkomplizierte“ Möglichkeit zur Suche nach Freunden zu bieten, ohne dass dieser die Namen und mögliche weitere Suchkriterien einzeln eingeben muss.[88] Personen, welche zwar einen Account auf

[86] Siehe Auszug auf https://www.facebook.com/notes/facebook-deutschland/leichteres-markieren-von-fotos/225759430770236

[87] Smartphones sind das Resultat aus der Verbindung von einem Mobiltelefon und einem Taschencomputer und besitzen in den überwiegenden Fällen zusätzlich eine Kamera- bzw Videofunktion und einen Organizer. Vgl http://de.wikipedia.org/wiki/Smartphone

[88] http://www.facebook.com/find-friends

Facebook besitzen, aber mit dem jeweiligen Nutzer nicht befreundet sind, werden diesem in der Folge automatisch (per „Freundschaftsanfrage“) „vorgeschlagen“.

Personen, welche nicht bei Facebook registriert sind, werden ebenfalls von Facebook erfasst und gespeichert. Dies wird dadurch belegt, dass an diese in der Folge von Facebook eine Einladungs-E-Mail versandt wird. Wenn sich eine Person aufgrund einer derartigen Einladung bei Facebook registriert, werden dieser wiederum Freunde vorgeschlagen. Dabei handelt es sich um Freunde der Personen, bei welchen diese selbst im jeweiligen E-Mail-Adressbuch aufgeschienen ist. Aber nicht nur E-Mail-Adressen und Namen werden gespeichert. Facebook sendet gemeinsam mit der Einladung auch das Profilfoto des Nutzers, welcher die Einladung versendet hat, damit eine sichere Zuordnung gewährleistet werden kann.[89]

Facebook kann damit alle „durchsuchten“ E-Mail-Adressen der Nicht-Mitglieder und die „Beziehung“ zum jeweiligen Facebook-Nutzer speichern, ohne diese Nicht-Mitglieder vorher gefragt oder informiert zu haben. Die betroffenen Personen wissen damit nicht, ob und wann Facebook ihre E-Mail-Adresse bereits erhalten und gespeichert hat.

Und genau dies wurde bereits im Jahr 2012 vom LG Berlin kritisiert, dass die Mitglieder des sozialen Netzwerks ohne eindeutige Erklärung dazu aufgefordert würden, Namen und E-Mail-Adressen aus ihrem E-Mail-Postfach freizugeben, welche selbst nicht bei Facebook seien, um diesen Personen schließlich ohne vorherige Einwilligung eine Einladung zu senden, neues Mitglied von Facebook zu werden. Laut Urteil des LG Berlin sei der Friendfinder nicht mit dem deutschen Verbraucherrecht vereinbar. Der Nutzer müsse „klar und deutlich darüber informiert werden, wofür er Namen und E-Mail-Adressen aus seinem privaten E-Mail-Postfach freigeben müsse“.[90]

Auf die rechtlichen Probleme iZm dem Friend-Finder wird weiter unten eingegangen.

[89] http://www.heise.de/newsticker/meldung/Facebook-entschaerft-seinen-Freundefinder-1175643.html
[90] Siehe Entscheidung LG Berlin 6.3.2012, 16 O 551/10.

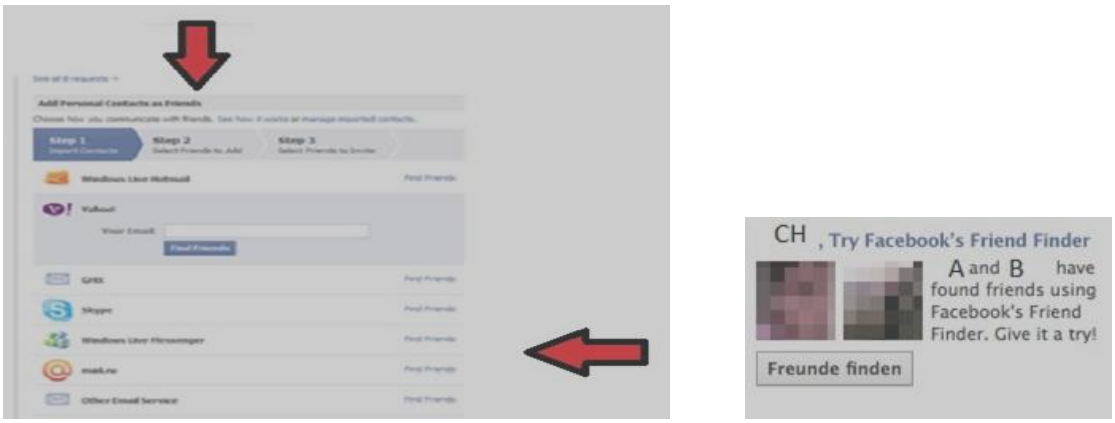

Abbildung 11: Screenshot „FriendFinder“ Facebook (Stand: 26.10.2011)

4. Like-Button

Abbildung 12: Facebook Like-Button

Der Like-Button ist ein Facebook-Spezifikum, welcher die Bewerbung anderer Webseiten zum primären Ziel hat. Webseitenbetreiber können auf ihrer Seite einen Like-Button anbringen, welcher von Facebook-Nutzern angeklickt werden kann. In der Folge wird auf der jeweiligen Facebook-Profilseite angezeigt, dass einem Nutzer der Inhalt einer Webseite gefällt. „Like“ bedeutet im Grunde genommen, dass einem etwas gefällt. Es wird dadurch automatisch ein Link zu dieser Seite angezeigt, damit möglichst viele „Freunde“ des jeweiligen Nutzers auch die Webseite besuchen und möglicherweise ebenfalls „liken“. Facebook-Nutzer werden damit zu effektiven „Werbeträgern“ des jeweiligen Unternehmens. Effektiv, da durch das Anklicken symbolisiert wird, dass man das jeweilige Unternehmen positiv bewertet hat. Eine derartige Werbung ist aber auch deswegen effektiv, da sie nicht mehr völlig „unpersönlich“ erfolgt: Ein „Freund“ macht Werbung, man könnte fast von einer neuen Form der „Mundpropaganda“ sprechen. Für Facebook selbst ist diese Form der

Werbung auch sehr effektiv, weil dadurch noch mehr Personen auf Facebook aufmerksam und möglicherweise neue Mitglieder werden.[91]

Abbildung 13: Screenshot Like-Button (Stand: 26.10.2011)

Technisch betrachtet ist das Anbringen eines Like-Buttons auf einer anderen Webseite relativ einfach und unkompliziert. Der Webseitenbetreiber muss dafür lediglich einen gewissen Programmcode in seine eigene Webseite integrieren und schon wird der Like-Button auf der Startseite angezeigt. Klickt nun ein registrierter Nutzer von Facebook diesen Button an, dann entsteht eine „Kommunikation" zwischen dem Computer des anklickenden Nutzers und dem Server von Facebook, wo dieser Link zum Profil des jeweiligen Nutzers gespeichert wird, indem die URL[92] übermittelt wird. Der Like-Button ist ein sog „Social Plugin"[93], welches Webseiten mit Facebook verbindet.

Plugins verknüpfen Webseiten und Webdienste mit Facebook und können damit Daten von Nutzern, insbesondere deren Vorlieben, Interessen, ihr Verhalten etc, sammeln und analysieren. Facebook selbst nennt diese Art der Recherche „Social Graph"[94].

Eine detaillierte rechtliche Analyse des Like-Buttons erfolgt weiter unten.

---

[91] Siehe auch http://www.thomashelbing.com/de/facebook-social-plugins-datenschutz-bdsg-datenschutz hinweise-privacy-policy-like-button-gefallt-mir, von Rechtsanwalt Dr. *Thomas Helbig* (Stand: 27.4.2011).

[92] URL steht für „Uniform Resource Locator", allgemein bezeichnet man damit eine Internetadresse oder Webadresse.

[93] Weitere Plugins sind die Like Box, Live Stream oder Facebook-Kommentare, siehe http://developers.facebook.com/docs/plugins (Stand: 28.6.2011).

[94] Darunter versteht man „the global mapping of everybody and how they're related", vgl http://en.wikipedia.org/wiki/Social_graph

IV. POTENTIELLE GEFAHREN DES NEUEN INFORMATIONSZEITALTERS, INSBESONDERE IM HINBLICK AUF DEN SCHUTZ DER PERSÖNLICHKEIT

„Kostenlos" ist vielleicht nicht „umsonst", wenn Nutzer vieler sozialer Netzwerke tatsächlich mit der zweckfremden Nutzung ihrer persönlichen Profildaten durch die Diensteanbieter „bezahlen".[95]

Im Hinblick auf die bisherigen Ausführungen kann davon ausgegangen werden, dass der rechtliche Schutz der Privatsphäre und der Schutz der Daten im Internet in der Zwischenzeit zu den größten Herausforderungen für die Rechtsprechung geworden sind.

Aufgrund der neuen technischen Entwicklungen werden immer mehr Daten ausgetauscht, verarbeitet und damit Spuren und virtuelle Fußabdrücke[96] im Internet hinterlassen, welche vor Missbrauch geschützt werden müssen. Die meisten SNP sind zwar grundsätzlich kostenlos, als „Bezahlung" können jedoch die angegebenen Daten angesehen werden.

Ich schließe mich der Meinung von *Härting*[97] an, welcher im Zusammenhang mit der Datenpreisgabe im Netz treffend von einer „Gratiskultur" spricht. Nutzer von SNP bekommen Inhalte zur kostenlosen Nutzung angeboten, als Gegenleistung bietet der Nutzer seine persönlichen Daten an und genau hier gehört ein fairer Ausgleich geschaffen zwischen dem berechtigten Schutz der persönlichen Daten und der Privatsphäre der Nutzer auf der einen Seite und einer sinnvollen und sicheren Datenverwendung von Unternehmen auf der anderen Seite.

A. SCHUTZ DER PRIVATSPHÄRE

Der oberste Wert unserer Rechtsordnung muss der Schutz des Individuums und damit der Persönlichkeit sein. Das Recht muss eine Möglichkeit bieten, eine scharfe Abgrenzung und

---

[95] Siehe Auszug aus dem Bericht und der Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum" – vom 3.– 4.3.2008, Rom (Italien) Pkt 3, 3.

[96] Es wird zwischen „Schleifspuren" als unweigerlich entstandenen maschinenbezogenen Daten, welche lediglich nachvollziehen lassen, wann welche Daten von einem bestimmten Host aus ins Internet gesandt oder empfangen wurden, und „digitalen Fußabdrücken", also jenen Daten über Personen, welche im Internet abgebildet oder abrufbar sind, unterschieden. Siehe *Staudinger* in *Jaksch-Ratajczak* (Hrsg), Aktuelle Rechtsfragen der Internetnutzung (2010) 243.

[97] *Härting*, Internetrecht[4] (1999) Rz 2.

Trennung zwischen dem Schutz der Privatsphäre und dem Recht der Öffentlichkeit auf Information zu ermöglichen.

Doch was ist Privatsphäre? In der österreichischen Rechtsordnung findet sich keine Legaldefinition des Begriffes „Privatsphäre“.[98] Aus der gesamten Rechtsordnung lässt sich lediglich ableiten, welche Bereiche geschützt werden müssen, insbesondere anhand des Grundrechts auf Achtung des Privat- und Familienlebens (Art 8 MRK), des Staatsgrundgesetzes zum Schutz des Hausrechts (Art 9 StGG), des Staatsgrundgesetzes zum Schutz des Brief- und Fernmeldegeheimnisses (Art 10 und 10a StGG) und des Datenschutzgesetzes, all dies sind Bereiche, die auch von SNP „berührt“ werden.

Reischauer erkennt treffend, dass zum Begriff der Privatsphäre auch die Geheimnissphäre des Menschen und Umstände zu zählen sind, die den Werdegang oder die Entwicklung der Person oder bestimmte Ereignisse im Leben betreffen. All diese Informationen können heute automationsunterstützt gespeichert werden.[99]

1. Schutz der Persönlichkeit im Internet

Im nachfolgenden Kapitel wird der zivilrechtliche Persönlichkeitsschutz, insbesondere das „Recht auf Privatsphäre“ (§ 1328 a ABGB), behandelt. Rechtsgebiete wie Datenschutz (DSG 2000), E-Commerce Gesetz (ECG), Bildnisschutz (§ 78 UrhG), Namensrecht (§ 43 ABGB) etc werden an anderen Stellen behandelt.

Die Persönlichkeit ist ein schützenswertes Gut. Im Zusammenhang mit dem Internet kommen die Erschwernis der schnellen weltweiten Verbreitung und, im Gegensatz zu physischen Print- und Funkmedien, die Möglichkeit der permanenten Speicherung und Verfügbarkeit der Daten hinzu. Weiters ist die Anonymität des Verletzers, welcher sich problemlos hinter einem Pseudonym verstecken und in (scheinbarer) Sicherheit wiegen kann, zu nennen. Man kann daher sagen, der Schutz der Persönlichkeit ist mit internetspezifischen Problemen behaftet.

Die Grundregel für den Persönlichkeitsschutz in der neuen Informationsgesellschaft sollte die informationelle Selbstbestimmung des Einzelnen sein, dh das Recht und die Möglichkeit des

[98] *Franz von Zeiller* umschreibt als Redaktor des ABGB das Persönlichkeitsrecht als das „Urrecht, die Würde eines vernünftigen, freihandelnden Wesens […]“, Natürliches Privatrecht (1802) 65.
[99] *Reischauer* in *Rummel*, Kommentar zum ABGB, § 1328 a Rz 3 ff.

einzelnen Nutzers, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[100]

Wie *Brandl* richtig formuliert, besteht im „Offline-Bereich die Möglichkeit, anonym oder pseudonym zu handeln. Im Internet besteht diese Möglichkeit an sich nicht, da mit jeder Handlung Daten generiert und ‚Spuren' hinterlassen werden, die Rückschlüsse auf den Einzelnen zulassen"[101], weshalb dieser Bereich mE strenger Kontrollmechanismen und Abwehrmöglichkeiten bedarf.

B. RECHTLICHE BEWERTUNG DES PERSÖNLICHKEITSSCHUTZES

1. Zivilrechtliche Bewertung des Persönlichkeitsschutzes

Im Privatrecht wird die menschliche Persönlichkeit ua in den §§ 16, 17, 43, 1325, 1328 ff ABGB geschützt, aber auch in Sonderprivatrechtsnormen wie §§ 77 ff UrhG.

Wie *Koziol/Welser* ausführen, ist die Rechtsordnung bei der Annahme von Persönlichkeitsrechten bzw deren Verletzung sehr zurückhaltend, da nicht jede Beeinträchtigung eines Menschen rechtswidrig sein kann. Eine schrankenlose Freiheit könne es nicht geben, weil die Freiheit des einen jeweils eine Einschränkung der Freiheit des anderen bewirke. Normale, selbstverständliche Beeinträchtigungen müssen in Kauf genommen werden, so *Koziol/Welser* weiter.[102]

Das Recht auf eine Privat- bzw Geheimnissphäre gehört neben den Rechten auf Leben, Ehre und Freiheit zu den angeborenen Rechten iSd § 16 ABGB:

„Jeder Mensch hat angeborene, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten. Sklaverei oder Leibeigenschaft, und die Ausübung einer darauf sich beziehenden Macht, wird in diesen Ländern nicht gestattet."

[100] *Brandl,* Datenschutz im Internet, in *Studiengesellschaft für Wirtschaft und Recht, Internet und Recht*, Rechtsfragen von E-Commerce und E-Government (2002) 131.
[101] *Brandl,* Datenschutz im Internet, in *Studiengesellschaft für Wirtschaft und Recht, Internet und Recht*, Rechtsfragen von E-Commerce und E-Government (2002) 131.
[102] *Koziol/Welser*, Bürgerliches Recht I[13] (2006) 83 f.

Obige Norm wird als Zentralnorm der österreichischen Rechtsordnung angesehen, da sie den Menschen als Rechtssubjekt schützt. Sie ist die Grundlage der Persönlichkeitsrechte. Persönlichkeitsrechte können grundsätzlich nicht auf andere Personen übertragen werden.[103]

Aicher stellt mE treffend fest, dass es sich aber nicht um einen bloßen Programmsatz handelt, sondern, dass § 16 ABGB mehrere Funktionen hat, wie die Anerkennung des Menschen als Rechtssubjekt, die Gewährung subjektiver Rechte und die allgemeinen Wertvorstellungen der verfassungsmäßig garantierten Grundrechte.[104]

Dies gilt mE nach auch bzw insbesondere für SNP bzw generell für das Internet, auch sie haben sich an obige Norm zu halten und subjektive Rechte zu gewähren und die verfassungsmäßig garantierten Grundrechte einzuhalten.

In § 1328 a ABGB ist das sog Recht auf Achtung der Privatsphäre normiert, welches in Abs 1 besagt: *„Wer rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet, hat ihm den dadurch entstandenen Schaden zu ersetzen. Bei erheblichen Verletzungen der Privatsphäre, etwa wenn Umstände daraus in einer Weise verwertet werden, die geeignet ist, den Menschen in der Öffentlichkeit bloßzustellen, umfasst der Ersatzanspruch auch eine Entschädigung für die erlittene persönliche Beeinträchtigung."*

In § 1328 a ABGB wird das Recht auf Wahrung der Privatsphäre iSd § 16 ABGB normiert. Die Privatsphäre ist ein absolut geschütztes Rechtsgut, das vor allem natürlichen, aber auch juristischen Personen zusteht.[105] Geschützt wird nicht nur ein möglicher Eingriff in die Privatsphäre, sondern auch ein Verbot entsprechender Veröffentlichung von privaten Informationen wie zB Informationen über Krankheiten etc.

In Kraft getreten ist die Norm erst im Jahr 2004 und hat damit den Unterlassungsanspruch aus § 16 ABGB um einen umfassenden Schadenersatzanspruch ergänzt. Der Schädiger haftet demnach für den Vermögensschaden. Bei einer erheblichen Verletzung der Privatsphäre steht dem Geschädigten auch der Ersatz des immateriellen Schadens zu.

Die Ehrenbeleidigung hingegen ist in § 1330 ABGB geregelt. Ziel der Norm ist es, die Ehre eines Menschen vor rechtswidrigen Eingriffen zu schützen. Als „Ehre" kann die allgemeine Wertschätzung bzw Achtungswürdigkeit eines Menschen verstanden werden.

---

[103] Siehe auch *Welser*, Fachwörterbuch (2005) 388 f.
[104] *Aicher* in *Rummel*, Kommentar zum ABGB, § 16 Rz 3–11.
[105] Siehe auch *Welser*, Fachwörterbuch (2005) 407 f.

Abs 1: „Wenn jemandem durch Ehrenbeleidigung ein wirklicher Schade oder Entgang des Gewinnes verursacht worden ist, so ist er berechtigt, den Ersatz zu fordern."
Abs 2: „Dies gilt auch, wenn jemand Tatsachen verbreitet, die den Kredit, den Erwerb oder das Fortkommen eines anderen gefährden und deren Unwahrheit er kannte oder kennen musste. In diesem Falle kann auch der Widerruf und die Veröffentlichung desselben verlangt werden. Für eine nicht öffentlich vorgebrachte Mitteilung, deren Unwahrheit der Mitteilende nicht kennt, haftet er nicht, wenn er oder der Empfänger der Mitteilung an ihr ein berechtigtes Interesse hatte."

§ 1330 ABGB enthält damit zwei Tatbestände: In Abs 1 die Ehrenbeleidigung und in Abs 2 die Rufschädigung. Die Ehrenbeleidigung in Abs 1 ist als Angriff gegen die Menschenwürde gem § 16 ABGB zu verstehen. *Aicher* stellt fest, dass unter dem Begriff „Ehre" „die allgemeine Wertschätzung einer Person durch die Mitmenschen verstanden wird".[106] Dem Verletzten steht zum Schutz gegen die Ehrenbeleidigung und zur Wahrung seines wirtschaftlichen Rufes bei Vorliegen von Wiederholungsgefahr ein verschuldensunabhängiger Schadenersatzanspruch zu.[107] Im Falle einer Rufschädigung in Verbindung mit einer Ehrenbeleidigung stehen dem Verletzten auch Ansprüche nach § 1330 Abs 2 ABGB zu.

2. Verfassungsrechtlicher Schutz der Privatsphäre

Der Schutz der Privatsphäre wird auch durch das öffentliche Recht verwirklicht. Im Besonderen erfolgt dies durch die Grundrechte, insbesondere Art 5 StGG hinsichtlich des Eigentums, Art 9 StGG hinsichtlich des Schutzes des Hausrechts, Art 10 StGG hinsichtlich des Briefgeheimnisses, Art 12 StGG bezüglich Versammlungs- und Vereinsfreiheit und Art 14 StGG bezüglich Glaubens- und Gewissensfreiheit. Obige Staatsgrundgesetze waren Teil der Verfassung von 1867, das Grundrecht auf Achtung des Privat- und Familienlebens gem Art 8 MRK wurde aufgrund des Beitritts Österreichs zur EMRK[108] im Jahr 1958 Teil des österreichischen Rechtsbestands.

[106] *Aicher* in *Rummel*, ABGB I § 16 Rz 18.
[107] *Aicher* in *Rummel*, ABGB I § 16 Rz 18.
[108] Die Europäische Menschenrechtskonvention (EMRK) bzw Konvention zum Schutze der Menschenrechte und Grundfreiheiten enthält einen Katalog von Grundrechten und Menschenrechten. Der Europäische Gerichtshof für Menschenrechte in Straßburg überwacht die Umsetzung. Die Konvention wurde im Rahmen des Europarats ausgearbeitet, am 4.11.1950 in Rom unterzeichnet und trat am 3.9.1953 allgemein in Kraft.

Grundrechte sollen der einzelnen Person, im Gegensatz zu den Persönlichkeitsrechten des Zivilrechts, einen Schutz gegen den Staat gewähren.

Bei der Betrachtung des verfassungsrechtlichen Schutzes der Persönlichkeit ist wesentlich, dass § 16 ABGB[109] eine Generalklausel für Persönlichkeitsrechte enthält, welche bei Bedarf herangezogen werden kann.

3. Europäische Menschenrechtskonvention

Die Privatsphäre wird nicht nur in innerstaatlichen Normen, sondern auch in der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) unter Schutz gestellt.

Art 8 EMRK besagt:
Abs 1: *„Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."*

Abs 2: *„Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist."*[110]

Art 8 EMRK möchte dem Einzelnen einen privaten Bereich sichern, welcher ihm eine freie Entfaltung seiner Persönlichkeit ermöglicht. Zum persönlichen Bereich gehören ua die körperliche und geistige Befindlichkeit und das private Tun mit Kontakten zu persönlichen Bezugspersonen.[111] Wie *Handler* treffend feststellt, hat *Berka* bereits herausgearbeitet, dass der Schutzbereich des Art 8 EMRK in zwei Bereiche einzuteilen ist. Auf der einen Seite gibt es den sog absoluten Schutz, welcher alle Vorgänge umfasst, welche eine Missachtung des Privatlebens darstellen. Hier kann als Beispiel der Umgang von Medien mit

[109] Siehe § 16 ABGB: „Jeder Mensch hat angeborene, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten. Sklaverei oder Leibeigenschaft, und die Ausübung einer darauf sich beziehenden Macht, wird in diesen Ländern nicht gestattet."

[110] „Beschränkungen der Grundrechte und Eingriffe in ihren Schutzbereich sind nur unter Beachtung des Grundsatzes der Verhältnismäßigkeit zulässig. Der mit einem Grundrechtseingriff verfolgte legitime Zweck darf nicht außer Verhältnis zu dem damit verbundenen Eingriff in die Freiheitssphäre der betroffenen Grundrechtsträger stehen." *Berka*, Die Grundrechte: Grundfreiheiten und Menschenrechte in Österreich (1999) 156, Rz 266.

[111] *Berka*, Verfassungsrecht[3] (2010) Rz 1391 und *ders*, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, GA (2012) 70 ff.

Persönlichkeitsrechten genannt werden. Auf der anderen Seite ist der relative Schutzbereich zu beachten, welcher nicht jede Informationsweitergabe umfasst, sondern nur Berichterstattungen, welche das Privatleben der betroffenen Person entfremden.[112] Dieser Bereich umfasse das Einkommen, das Abbild einer Person, die mediale Berichterstattung, aber nur, wenn Dritten die Möglichkeit geboten werde, den Betroffenen zu identifizieren.

a. Computer-Grundrecht

Die Diskussionen um die Schaffung eines neuen Grundrechts auf Grundversorgung mit Informations- und Kommunikationstechnologien werden immer lauter. Dasselbe gilt für jene Stimmen, die SNP, insbesondere Facebook, als „Förderer und Unterstützer der Menschenrechte" ansehen. Facebook verschafft seinen Mitgliedern nämlich die Möglichkeit, ihre Meinungen auszutauschen und „Gruppen" zu bilden. Amnesty International hat in seinem Report aus 2011 SNP wie Twitter, Facebook und auch Wikileaks gelobt und erklärt, dass all diese neuen Technologien im Kampf um die Menschenrechte eine große Rolle spielen würden, da vor allem in der arabischen Welt Blogger, Journalisten und Menschenrechtsaktivisten verstärkt auf diese setzen würden, um politische Reformen und die Einhaltung der Menschenrechte einzufordern.[113]

C. DER UMGANG MIT DEM SCHUTZ DER PERSÖNLICHKEIT BEI SNP

1. Facebook

Facebook schreibt in seiner „Erklärung der Rechte und Pflichten" unter Punkt 4. „Registrierung und Sicherheit der Konten", dass es ua nicht gestattet ist, ohne Erlaubnis ein Profil für eine andere Person zu erstellen *(„Du wirst keine falschen persönlichen Informationen auf Facebook bereitstellen oder ohne Erlaubnis ein Profil für jemand anderen erstellen.")* und unter Punkt 5. „Schutz der Rechte anderer Personen" reglementiert Facebook, dass ua Handlungen verboten sind, welche in die Rechte anderer Personen eingreifen *(„Du*

[112] *Handler*, Der Schutz von Persönlichkeitsrechten (2008) 481.
[113] Amnesty International Report 2011, http://www.sueddeutsche.de/politik/amnesty-international-report-mit-facebook-zur-freiheit-1.1096193 (Stand: 25.5.2011).

wirst keine Inhalte auf Facebook posten oder Handlungen auf Facebook durchführen, welche die Rechte einer anderen Person oder das Gesetz verletzen.").[114]

2. Twitter

In den Twitter-Regeln wird vorgeschrieben, dass es verboten ist, sich für jemand anderen auszugeben:

Identitätswechsel: *„Es ist verboten, sich auf Twitter für jemand anderes auszugeben, um andere Benutzer zu verwirren, zu betrügen oder zu täuschen. Der Versuch ist ebenfalls verboten."*[115]

Wie bereits festgehalten, normiert § 16 ABGB, dass „jeder Mensch angeborene, schon durch die Vernunft einleuchtende Rechte hat und daher als eine Person zu betrachten ist".[116] Durch § 16 ABGB sollen der Mensch und seine Achtung sowie Unversehrtheit unmittelbar geschützt werden.[117] Die Persönlichkeit wird damit als Grundwert absolut geschützt und muss von jedermann beachtet werden.[118] Im Falle einer Beeinträchtigung muss eine Interessenabwägung zwischen dem Schutz des Einen und der Freiheit des Anderen vorgenommen werden. Im Falle eines unberechtigten, rechtswidrigen Eingriffes gebühren Ansprüche auf Unterlassung, Beseitigung und bei Verschulden auch Schadenersatz.

Erst im Jahr 2004 wurde mit dem ZivRÄG 2004[119] das sog „Recht auf Wahrung der Privatsphäre" ins ABGB eingefügt. § 1328 a Abs 1 ABGB normiert: *„Wer rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingreift oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet, hat ihm den dadurch entstandenen Schaden zu ersetzen. […]"*

Dem Verletzten stehen bei Eingriffen in seine Privatsphäre sowie beim Offenbaren oder Verwerten von Umständen aus seiner Privatsphäre Schadenersatzansprüche bzw Unterlassungs- und Beseitigungsansprüche zu. Im Falle einer erheblichen Verletzung steht dem Verletzten ein Ersatz des immateriellen Schadens zu. Voraussetzung ist ein schuldhafter

[114] http://de-de.facebook.com/legal/terms (Stand: Oktober 2012)
[115] http://support.twitter.com/articles/87137-die-twitter-regeln#
[116] Siehe dazu auch *Zankl*, Bürgerliches Recht[6] (2012) Rz 35.
[117] *Koziol/Welser*, Bürgerliches Recht I[13] (2006) 83 ff.
[118] *Aicher* in *Rummel*, Kommentar zum ABGB, § 16.
[119] Siehe Zivilrechtsänderungsgesetz 2004, BGBl I 91/2003.

und rechtswidriger Eingriff in die Intimsphäre des Einzelnen. Eine Beschränkung dieser Rechte steht nur in gewissen Fällen, wie zB bei einer Überwachung eines Verdächtigen, zu.

§ 1328 a ABGB ist erst am 1.1.2004 in Kraft getreten. Damit wurde die Wahrung der Privatsphäre erstmals ausdrücklich im Gesetz verankert und der Schutz vor der Verletzung der Privatsphäre von Privatpersonen geregelt. § 1328 a ABGB beinhaltet sowohl ein Verbot des Eingriffs in die Privatsphäre als auch ein Verbot entsprechender Veröffentlichungen.[120] Die Verletzung der Privatsphäre durch Medien wird jedoch weiterhin vom MedienG bestimmt.

Es stellt sich nun die Frage, ob § 1328 a ABGB auch bei Verletzungen im Internet, insbesondere durch Preisgabe privater Umstände oder intimer Details einer Person durch Dritte auf einer Webseite, zur Anwendung kommt.

In den Gesetzesmaterialien zu § 1328 a ABGB ist explizit geregelt, dass man sich nicht auf eine Verletzung der Privatsphäre berufen kann, wenn man zuvor private Details oder Lebensumstände selbst öffentlich gemacht hat.[121] Es liegt dann keine Verletzung der Privatsphäre vor, weil der Betroffene die Preisgabe der Informationen selbst veranlasst hat.

Das bedeutet, dass sich eine Person, welche selbst die Informationen über ihr Privat- oder Geschäftsleben veröffentlicht hat, nicht einen Eingriff in die Privatsphäre geltend machen kann. Daraus ergibt sich weiters, dass eine Haftung auch dann nicht besteht, wenn diese Umstände in der Folge weiter erörtert werden, wie zB in einem Online-Forum.

D. JUDIKATUR IZM DEM SCHUTZ DER PRIVATSPHÄRE

Zu den bekanntesten Entscheidungen können die des BVerfG zur Online-Durchsuchung und zur Vorratsdatenspeicherung gezählt werden, durch welche eine wichtige Grundlage des Schutzes der Privatsphäre im Netz gelegt wurde.

In der Entscheidung 4 Ob 150/08 z vom 23.9.2008 hat der OGH ausgesprochen, dass „der Schutz des § 1328 a ABGB auch Personen zukommt, die in der Öffentlichkeit bekannt sind". Die Judikatur schützt damit auch private und familiäre Umstände, welche nicht für die Öffentlichkeit bestimmt sind.

[120] Hier insbesondere Veröffentlichungen über gewisse Krankheiten.
[121] Vgl ErläutRV 173 BlgNR 22. GP 17.

Auszug aus der Entscheidung 4 Ob 150/08 z: „Wenngleich die Verbreitung des Bildnisses einer allgemein bekannten Person deren berechtigte Interessen in aller Regel nicht beeinträchtigt, so ist dennoch eine Verbreitung ihres Bildnisses nicht schrankenlos zulässig. So wird die Verbreitung von Bildern, die öffentlich bekannte Personen im Zusammenhang mit Bildüberschrift oder Begleittext der Neugierde und Sensationslust der Öffentlichkeit preisgibt oder sie mit Vorgängen in Verbindung bringt, mit denen sie nichts zu tun haben, als unzulässig angesehen (stRsp RIS-Justiz RS0077903). Auch eine allgemein bekannte Person, für deren Leben sich die breite Bevölkerung interessiert und die immer wieder Gegenstand von Medienberichten ist, hat Anspruch darauf, dass die Allgemeinheit ihren höchstpersönlichen Lebensbereich respektiert (4 Ob 165/03y = ÖBl 2004, 89 – Pinkelprinz; zuletzt 4 Ob 121/08 k). Die herrschende Auffassung zählt zum höchstpersönlichen Lebensbereich unter anderem das Sexualverhalten eines Menschen und sein Leben in und mit der Familie (*Berka* in *Berka/Hoehne/Noll/Polley*, Mediengesetz[2] § 7 Rz 6, 8 und 9; *Litzka/Strebinger*, Mediengesetz[5] § 7 Rz 3; *Brandstätter/Schmid*, Mediengesetz[2] § 7 Rz 7; *Hanusch*, Mediengesetz § 7 Rz 4; vgl 18 Bs 272/98 = RIS-Justiz RW0000302). […] Dass die Durchsetzung des Rechts auf Wahrung und Achtung der Privatsphäre dem österreichischen Gesetzgeber ein besonderes Anliegen ist, ergibt sich auch aus der durch das ZivRÄG 2004 (BGBl I 91/2003) eingeführten schadenersatzrechtlichen Bestimmung des § 1328 a ABGB. Die Materialien zu dieser Bestimmung zählen zur geschützten ‚Privatsphäre' auch private, das Familienleben betreffende Umstände, die nicht für eine weitere Öffentlichkeit bestimmt sind (RV 173, AB 212 BlgNR 22. GP). Dieser Schutz kommt auch Personen zu, die in der Öffentlichkeit bekannt sind."

V. **RECHTLICHE RAHMENBEDINGUNGEN**

Das Internet ist kein rechtsfreier Raum, auch wenn dies weiterhin von manchen Medien behauptet wird. Auch die modernen und stetig wachsenden Kommunikationsdienste im Internet unterliegen rechtlichen Anforderungen. Ich schließe mich *Zankl* an, der ausführte, *„legal patterns apply to electronic transactions in the same way as they apply to common business"*. Dh Rechtsvorschriften und rechtliche Bestimmungen sollen sowohl für Bereiche des Internets als auch für „nicht-elektronische" bzw digitale Bereiche gleich anwendbar sein und gleich gelten.

Der Staat muss auch in der digitalen Informationsgesellschaft die Rechte und Daten der Bürger schützen und entsprechende Vorkehrungen durch Rechtsvorschriften und rechtliche Bestimmungen treffen.

Solange es keine bzw nicht ausreichend Sondervorschriften für Probleme aus der virtuellen Welt gibt, sollten für Social Media (wie zB Facebook) die „allgemeinen Regeln" gelten, wie bereits *Zankl* ausführte.[122] Im Zuge der fortschreitenden Technisierung sind bereits einige Vorschriften eingeführt und bestehende Rechtsvorschriften, wie insbesondere das Datenschutzrecht, stärker beleuchtet worden.

Wichtig ist, dass bei der Regelung digitaler Rechtsfragen speziell die Eigenheiten der neuen Entwicklungen beachtet werden.

A. EINLEITUNG

SNP, insbesondere die damit zusammenhängende Datenangabe, -preisgabe, -vernetzung und -speicherung, hängen an der Schnittstelle verschiedener Rechtsgebiete bzw -materien (insbesondere dem Schutz der Persönlichkeit und der Privatsphäre, dem Datenschutz, dem allgemeinen Zivilrecht, Arbeitsrecht, E-Commerce Gesetz), weswegen iZm SNP gerne von „Querschnittsmaterie"[123] gesprochen wird und welche erst teilweise durch Sondergesetze geregelt werden und in der Folge aufgezeigt werden sollen.

[122] Siehe *Zankl*, Bürgerliches Recht[6] (2012) Rz 252.
[123] *Zankl*, Bürgerliches Recht[6] (2012) Rz 182.

Nach der Ansicht *Thieles*[124] bietet die Facebook Inc. auf Basis der Definition der Art-29-Gruppe, wonach SNP „Kommunikationsplattformen im Online-Bereich [sind], die es dem Einzelnen ermöglichen, sich Netzwerken von gleich gesinnten Nutzern anzuschließen bzw solche zu schaffen", einen Dienst der Informationsgesellschaft iSd Art 1 Nr 2 Informations-RL an, wodurch sich seiner Ansicht nach auch das Anwendungsfeld der Datenschutz-RL sowie der E-Commerce-RL eröffnet und sollen SNP daher auch im Lichte dieser Richtlinien beleuchtet bzw analysiert werden.

SNP leben einerseits von der freiwilligen Datenpreisgabe auf der Nutzerseite und andererseits von der Sammlung und (teilweise) unerlaubten Verwertung bzw Verwendung von Nutzerdaten auf der Anbieterseite. In diesem Zusammenhang stellen sich rechtliche Probleme mit der unerlaubten Verwendung von Daten bzw deren Löschung durch Löschungs- und Beseitigungsansprüche gegen die Störung geschützter Rechtssphären.

Zwischen dem Nutzer und dem Diensteanbieter können sich aber auch zivilrechtliche Probleme ergeben, wenn die vom Nutzer preisgegebenen Daten weitergegeben, verarbeitet oder vernetzt werden. In diesem Zusammenhang können auch Problemkreise durch die vom Diensteanbieter vorgelegten AGB entstehen.

Die Frage nach dem Schutz persönlicher Informationen stellt sich jedoch nicht nur auf zivilrechtlicher, sondern auch auf verfassungsrechtlicher Ebene, insbesondere im Grundrecht auf Datenschutz (§ 1 DSG), welches personenbezogene Daten und deren Verwendung schützt, dem Hausrecht (Art 8 StGG) und dem Recht auf Meinungsfreiheit (Art 13 StGG).

In der Folge sollen einige der durch SNP betroffenen Rechtsgebiete aufgezeigt und einige Probleme analysiert werden:

B. ZIVILRECHT

1. E-Commerce Gesetz

Das Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden, BGBl I 152/2001 (in der Folge: ECG) wurde vom

[124] Siehe *Thiele*, Persönlichkeitsschutz in Neuen Medien – Facebook, Google & Co, AnwBl 2013, 11.

österreichischen Gesetzgeber als Umsetzung der E-Commerce-Richtlinie[125] geschaffen, um Tatbestände mit Internetbezug bestmöglich lösen und behandeln zu können und es ist am 1.1.2002 in Kraft getreten.

Das ECG verfolgt maW das Ziel, den Nutzer vor dem Diensteanbieter[126] zu schützen, indem bestimmte Informationen über den Diensteanbieter für den Nutzer leicht und unmittelbar zugänglich sein müssen. Durch diese Informationspflichten soll ein Mindestmaß an Transparenz kommerzieller Aktivitäten erreicht werden.[127]

In diesem Zusammenhang interessant ist die Entscheidung des deutschen Amtsgerichts Aschaffenburg, welches im August 2011 ein Unternehmen verurteilte, weil dieses bei seinem Facebook-Auftritt, dh bei seiner Facebook-Unternehmensseite, kein ordnungsgemäßes Impressum anführte.[128] Das Gericht sprach aus, dass die notwendigen Pflichtangaben „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar" gehalten werden müssen.

---

[125] RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Rechtsverkehrs, im Binnenmarkt (RL über den elektronischen Rechtsverkehr), ABl L 178 vom 17.7.2000. Ziel der Richtlinie war es, „einen rechtlichen Rahmen zur Sicherstellung des freien Verkehrs von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten zu schaffen, nicht aber, den Bereich des Strafrechts als solchen zu harmonisieren". Die Kommission der Europäischen Gemeinschaft wollte mit dieser Richtlinie rechtliche Hindernisse beseitigen, welche der Erbringung von Dienstleistungen entgegenstehen. Das Gemeinschaftsrecht und die gemeinschaftliche Rechtsordnung sind nach Ansicht der Kommission wichtige Instrumente, um den EU-Bürgern eine uneingeschränkte Möglichkeit der Nutzung des Internets zu ermöglichen. Ziel war es auch, ein hohes Schutzniveau für die dem Allgemeininteresse dienlichen Ziele, wie Jugendschutz, Schutz der Menschenwürde, Verbraucherschutz etc, zu schaffen, um damit einen sicheren Rechtsrahmen herzustellen, welcher einer Weiterentwicklung der Informations- und Kommunikationstechniken, worunter neue Internetdienste wie Facebook fallen, nicht im Wege stehen solle. Die Richtlinie sollte aber nur jene Bereiche regeln, welche nicht den nationalen Rechtsordnungen überlassen werden können. So soll die Richtlinie nur bereits bestehendes Gemeinschaftsrecht ergänzen, bereits bestehende Regelungen zum Schutz der Verbraucher bleiben unberührt.
Sowohl die RL 93/13/EG vom 5.4.1993 über missbräuchliche Klauseln in Verbraucherverträgen (RL 93/13/EG vom 5.4.1993 über missbräuchliche Klauseln in Verbraucherverträgen, ABl L 95 vom 21.4.1993) als auch die RL 97/7/EG des Europäischen Parlaments und des Rates vom 20.5.1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz gelten zur Gänze für den Bereich der Informationsgesellschaft.
Ausgenommen sind jedoch Regelungen über Bereiche, die von der RL 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 95/46/EG, ABl L 281 vom 23.11.1995) und von der RL 97/66/EG des Europäischen Parlaments und des Rates vom 15.12.1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (RL 97/66/EG vom 15.12.1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikationn, ABl L 24 vom 30.1.1998) abgedeckt werden.

[126] Diensteanbieter sind natürliche oder juristische Personen oder sonstige Rechtssubjekte, die einen Dienst der Informationsgesellschaft (§ 3 Z 1 ECG) anbieten. Dazu gehören neben allen Arten von Providern und Suchmaschinenbetreibern auch Betreiber von Webseiten, Foren etc.

[127] Siehe ua *Zankl*, Zivilrecht und E-Commerce, ÖJZ 2001 (542).

[128] Siehe Entscheidung LG Aschaffenburg 19.8.2011, 2 HK O 54/11.

Diensteanbieter im Sinne des ECG sind natürliche oder juristische Personen oder sonstige Rechtssubjekte, die einen Dienst der Informationsgesellschaft (§ 3 Z 1 ECG) anbieten. Dh grundsätzlich Unternehmen, welche ua einen Online-Vertrieb von Waren, einen Online-Vertrieb von Dienstleistungen, Online-Informationsangebote, elektronische Suchmaschinen, Datenabfragemöglichkeiten, SMS-Dienste, aber auch Betreiber von Webseiten und Foren etc anbieten.

Gemäß § 5 ECG hat ein Diensteanbieter allgemeine Informationen wie seinen Namen, seine Anschrift etc leicht und unmittelbar zugänglich zu machen. Vor Vertragsabschluss hat ein Diensteanbieter gem § 9 ECG den Nutzer über die einzelnen technischen Schritte, die zu einer Vertragserklärung und zum Vertragsabschluss führen, den Umstand, ob der Vertragstext nach Vertragsabschluss vom Diensteanbieter gespeichert wird, sowie gegebenenfalls den Zugang zu einem solchen Vertragstext sowie die Sprachen, in denen der Vertrag abgeschlossen werden kann, klar, verständlich und eindeutig zu informieren bzw seine AGB in einer speicher- und ausdruckbaren Version zur Verfügung zu stellen.

a. Sind SNP Diensteanbieter?

Es stellt sich nun die Frage, ob auch SNP unter den Begriff eines Diensteanbieters iSd ECG fallen und damit den darin normierten Informationspflichten und Haftungsbestimmungen unterliegen.

Gemäß § 3 Z 2 ECG ist ein Diensteanbieter „eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die einen Dienst der Informationsgesellschaft bereitstellt". Ein Dienst der Informationsgesellschaft ist ein „(...) elektronisch im Fernabsatz auf individuellen Abruf des Empfängers bereitgestellter Dienst, (...) Online-Informationsangebote, die Online-Werbung, elektronische Suchmaschinen und Datenabfragemöglichkeiten sowie Dienste, die Informationen über ein elektronisches Netz übermitteln, die den Zugang zu einem solchen vermitteln oder die Informationen eines Nutzers speichern". § 16 Abs 1 ECG normiert: *„Ein Diensteanbieter, der von einem Nutzer eingegebene Informationen speichert, […]."* Es lässt sich festhalten, dass Betreiber von SNP mehrere der erforderlichen Charakteristika eines Diensteanbieters iSd ECG erfüllen und damit den Bestimmungen des ECG unterliegen.

Diensteanbieter, aus dem Englischen „Provider“, werden je nach ihrer konkreten Tätigkeit in Access-[129], Host- oder Content[130]-Provider eingeteilt.

SNP leben von und durch nutzergenerierte Inhalte, das sind Inhalte, die der Netznutzer selbst erstellt, indem sie der Betreiber der Plattform speichert.

Als Host-Provider werden Anbieter im Internet bezeichnet, welche fremde Inhalte auf ihren Webseiten für andere Nutzer bereithalten. Das bedeutet, dass SNP grundsätzlich als Host-Provider anzusehen sind.

b. Host-Provider

Host-Provider haben die Aufgabe, fremde Inhalte zu speichern. Primäres Ziel einer SNP ist es, viele Informationen online zu sammeln und abzuspeichern. Sie handeln somit als Host-Provider iSd ECG.

Das ECG knüpft bei der Beurteilung, um welche Art Provider (Access-, Host- oder Content-Provider) es sich handelt, an funktionelle Kriterien an, das bedeutet, die konkret ausgeübte Tätigkeit ist relevant und nicht deren Bezeichnung bzw die Bezeichnung des Providers.[131]

Content-Provider haften nach den jeweils in Betracht kommenden allgemeinen rechtlichen Regeln des Zivil-, Wettbewerbs-, Urheber-, Marken- und Strafrechts.

Bei Host-Providern kommen hingegen Haftungsbefreiungen zum Tragen, da diese lediglich „hosten“ bzw, grob gesagt, „Speicherplatz“ zur Verfügung stellen. Es stellt sich nun die Frage, ob ein Betreiber einer SNP, welcher als Host-Provider seinen Nutzern die Möglichkeit eröffnet, von diesen online gestellte Daten auf seiner Plattform abzuspeichern, für den Inhalt verantwortlich gemacht werden kann oder ob es bestimmte Haftungsbeschränkungen gibt.

[129] Ein Access-Provider hat die Aufgabe, Signale zu übertragen und/oder diese auf einem Kommunikationsnetz weiterzuleiten. Der Access-Provider versorgt also den Nutzer mit dem Zugang zu einem elektronischen Kommunikationsnetz (zB Internet, aber auch SMS-, WAP- oder UMTS-Dienste), indem er sich mit anderen Access-Providern verknüpft, um eine weltweite Anbindung zu anderen bestehenden Netzen zu ermöglichen. Der Access-Provider stellt den Zugang zur Verfügung oder übermittelt vom oder in dasselbe Netz. Siehe *Welser*, Fachwörterbuch (2005) 9.

[130] Content-Provider bieten hingegen eigene Inhalte an bzw kommunizieren eigene Inhalte.

[131] Vgl *Zankl*, E-Commerce-Gesetz, Kommentar und Handbuch (2002) Rz 184.

c. Haftung eines Host-Providers

§ 16 ECG beinhaltet einen Haftungsbefreiungstatbestand. In § 16 ECG ist geregelt, dass ein Host-Provider, welcher Speicherplatz für fremde Inhalte zur Verfügung stellt, für diese Informationen nicht verantwortlich ist, „wenn er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hatte und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst war, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erhalten hat, unverzüglich tätig wurde, um die Information zu entfernen oder den Zugang zu sperren". Ein Host-Provider ist demnach grundsätzlich von jeglicher Verantwortung befreit, solange er keine Kenntnis von der Rechtswidrigkeit eines fremden Inhalts hatte oder nach Kenntnis unverzüglich tätig wurde.

Eine allgemeine Überwachung durch den Host-Provider sieht das ECG jedoch nicht vor (siehe § 18 Abs 1 ECG), wenn der Host-Provider aber von einem rechtswidrigen Inhalt Kenntnis erlangt, dann muss er diesen unverzüglich löschen.[132]

Es stellt sich die Frage, ob einen Host-Provider eine allgemeine Überwachungspflicht hinsichtlich der von ihm gehosteten Seiten trifft, und wenn ja, wie dieser Verpflichtung am besten nachgekommen werden kann. Es besteht gem § 18 ECG grundsätzlich keine Verpflichtung, fremde Inhalte und Postings zu überwachen, um Kenntnis von rechtswidrigen Inhalten und Aktivitäten zu erhalten.

Viele Unternehmen verwenden jedoch trotzdem freiwillig sog Screening Programme, das sind Programme, welche gewisse Wörter aus Dateien und Dokumenten filtern, um rechtswidrige Inhalte ausfindig machen zu können.[133]

In der EC-RL wurde in Art 15 Abs 1 bzw § 18 Abs 1 ECG normiert, dass Diensteanbieter nicht verpflichtet sind, die von ihnen gespeicherten, übermittelten oder zugänglich gemachten Informationen allgemein zu überwachen oder von sich aus nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Davon sind aber zielgerichtete Überwachungsmaßnahmen, wie etwa solche von der Polizei oder den Justizbehörden, nicht

[132] Siehe *Ghazal* in *Jaksch-Ratajczak* (2010) 67 ff.
[133] Vgl ECG, BGBl I 152/2001 idgF.

betroffen.[134] Dh Art 15 der RL bzw § 18 ECG enthalten bei einer wortwörtlichen Betrachtung keine Verpflichtung zur Überwachung.

Brenn ist hingegen der Ansicht, dass trotz Art 15 Abs 1 der RL bzw § 18 ECG die Provider generell dazu verpflichtet sein sollten, nach dem „Stand der Technik verfügbare Filtersoftware einzusetzen"[135] und damit generell eine Überwachung durchzuführen.

Der OGH geht trotz Art 15 der RL und § 18 ECG – wie ich für richtig erachte – ebenfalls von einer Überwachungspflicht aus, wenn Hinweise auf eine Rechtswidrigkeit gegeben sind, so bereits im Verfahren OGH 6 Ob 178/04 a vom 21.12.2006 („Gästebuch-Entscheidung"[136], siehe weiter unten im Detail). Nach Ansicht des OGH schließt das Haftungsprivileg des § 16 Abs 2 ECG lediglich eine allgemeine Schadenersatzhaftung bzw strafrechtliche Verantwortlichkeit aus, nicht jedoch einen allfälligen verschuldensunabhängigen zivilrechtlichen Unterlassungsanspruch (siehe dazu gleich unterhalb).[137]

Entscheidend für die Verantwortlichkeit eines Providers sind dessen Wissen und Kontrollmöglichkeiten.

Auch beim Access-Provider gibt es Haftungsbefreiungsvoraussetzungen, welche in § 13 ECG geregelt sind und vorsehen, dass der Access-Provider von jeglicher Verantwortung für die über das Kommunikationsnetz beförderten Informationen befreit wird. Falls diese Haftungsbefreiungen nicht gegeben sind, muss eine mögliche Verantwortlichkeit nach dem jeweiligen Rechtsgebiet (zivilrechtliche, strafrechtliche Haftung) gesondert geprüft werden.[138]

(1) Exkurs: Haftung eines Host-Providers aus materiell-rechtlicher Sicht

Kommt man nach Prüfung der Haftungsbefreiung iSd § 16 Abs 1 iVm § 18 Abs 1 ECG zum Ergebnis, dass der Host-Provider – im Zusammenhang mit SNP: der Betreiber einer Facebook-Seite – für den rechtswidrigen Inhalt, aufgrund der Nicht-Anwendbarkeit der

---

[134] *Brenn*, Der elektronische Geschäftsverkehr, ÖJZ 1999, 481.
[135] *Brenn*, Der elektronische Geschäftsverkehr, ÖJZ 1999, 481.
[136] In dieser oberstgerichtlichen Entscheidung lag eine rufschädigende Tatsachenbehauptung iSd § 1330 Abs 2 ABGB vor, welche gleichzeitig eine Ehrenbeleidigung iSd § 1330 Abs 1 ABGB darstellte. Die Klage war auf Unterlassung gegen den Betreiber gerichtet und auf § 1330 ABGB gestützt. Dem Betreiber der verfahrensgegenständlichen Plattform war bereits eine Rechtsverletzung bekannt, weswegen der OGH erkannte, dass im Falle des Bekanntwerdens einer solchen der Betreiber verpflichtet sei, die Beiträge in seinem Online-Forum regelmäßig zu überwachen. Erst bei Verletzung dieser Pflicht stehe dem Betroffenen ein Unterlassungsanspruch gegen den Betreiber zu.
[137] OGH 21.12.2006, 6 Ob 178/04a; 19.2.2004, 6 Ob 190/03i, 11.12.2003, 6 Ob 274/03t.
[138] *Zankl*, E-Commerce-Gesetz (2002) Rz 180 ff.

gegenständlichen Haftungsbefreiung, verantwortlich ist, ist seine Haftung nach den materiell-rechtlichen (zivil- und strafrechtlichen) Vorschriften zu prüfen.

In den überwiegenden Fällen wird es sich bei den rechtswidrigen Inhalten auf SNP um Inhalte handeln, welche im zivilrechtlichen Sinn eine Verletzung an der Ehre der betroffenen Person iSd § 1330 ABGB zur Folge haben. Gemäß § 1330 ABGB wird die zivilrechtliche Ehrenbeleidigung und Kreditschädigung geschützt. In Abs 1 wird das Recht des Menschen auf Ehre und in Abs 2 die Gefährdung des wirtschaftlichen Rufes durch die Verbreitung von (unwahren) Tatsachen geschützt.

Die neuen technischen Gegebenheiten strahlen auch auf den zivilrechtlichen Ehrenschutz aus. Dies ist insbesondere im Zusammenhang mit Diskussionsforen oder den sog „walls“, wie jenen von Facebook, der Fall.

Äußerungen, welche auf einer Webseite sichtbar sind, gelten ebenso als verbreitet wie schriftliche Beiträge, welche sich in einem Online-Archiv befinden. Der OGH hat bereits in mehreren Entscheidungen ausgesprochen, „dass eine Mitteilung als verbreitet gilt, wenn diese gegenüber einer vom Verletzten verschiedenen Person geäußert wurde“[139] und bezeichnet dies als „Mindestpublizität“, welche sowohl bei Ehrenbeleidigungen nach § 1330 Abs 1 ABGB als auch bei kreditschädigenden Behauptungen nach Abs 2 heranzuziehen ist.[140]

Wenn eine die Ehre beleidigende Äußerung auf der „wall“ eines Facebook-Profils getätigt wird, ist das Erfordernis, dass auch Dritte davon Kenntnis erlangen können, mE gegeben, da es lediglich die Einstellung gibt, eine „wall“ zu aktivieren bzw zu deaktivieren. Dies ist durch die Erstellung von sog Freundeslisten mit verschiedenen Befugnissen möglich.

Es muss aber grundsätzlich eine Interessenabwägung zwischen dem Schutz der Persönlichkeit und der Meinungsfreiheit vorgenommen werden. Im Falle eines Zuwiderhandelns können Unterlassung und Schadenersatz begehrt werden. Im Internet wäre wohl die Konsequenz das Löschen der betreffenden Stelle, weswegen sich nun die Frage stellt, ob es zu einer Verpflichtung kommen kann, derartige ehrenbeleidigende Inhalte, wie zB Kommentare auf fremden Facebook-Seiten, löschen zu müssen:

Sofern eine materiell-rechtliche Verletzung vorliegt (zB gem § 1330 Abs 1 ABGB), kann der Betreiber einer Facebook-Seite bei Vorliegen der gesetzlichen Voraussetzungen (§ 381 Z 2

[139] Siehe ua OGH 11.6.1952, 3 Ob 295/52; 14.6.1977, 4 Ob 320/77; 14.12.2000, 6 Ob 291/00 p.
[140] OGH 25.1.1995, 6 Ob 37/95.

EO) mit einstweiliger Verfügung zur Sperre bzw Löschung der Kommentare angehalten werden.

Strafrechtlich betrachtet, könnte durch ein (rechtswidriges) Posting auf einer SNP die Ehre eines Menschen oder sein Ansehen verletzt und damit der Tatbestand der üblen Nachrede iSd § 111 StGB erfüllt werden. Das Delikt der üblen Nachrede iSd § 111 StGB begeht nämlich, „wer einen anderen in einer für einen Dritten wahrnehmbaren Weise einer verächtlichen Eigenschaft oder Gesinnung zeiht oder eines unehrenhaften Verhaltens […] beschuldigt, […]".

(2) § 1330 ABGB versus Meinungsäußerung

Eine Einschränkung erfährt § 1330 ABGB durch Art 10 MRK und Art 13 StGG, welche die freie Meinungsäußerung garantieren sollen. Grundsätzlich ist auch nicht jede Äußerung, welche zwar von der betroffenen Person subjektiv als negativ und schädigend empfunden wird, automatisch als Ehrenbeleidigung anzusehen. Die Beurteilung, ob eine Ehrenbeleidigung vorliegt, sollte daher streng und nicht zu „locker" vorgenommen werden.

Damit eine Ehrenbeleidigung strafrechtlich relevant wird, muss, in Ergänzung zur schädigenden Handlung an sich, diese dergestalt erfolgen, dass sie für Dritte wahrnehmbar ist.

Die österreichischen Gerichte hatten sich bereits mit Ehrenbeleidigungen im Internet zu befassen, konkret bei Internet-Meinungsforen.[141] Die Gerichte hatten jeweils zu klären, ob tatsächlich Ehrenbeleidigungen vorlagen.

In der bereits weiter oben erwähnten Entscheidung des OGH, 6 Ob 178/04 a, hatte dieser die Überwachungspflicht des Betreibers eines Online-Gästebuches[142] eines Tourismusbüros zu prüfen bzw zu bewerten, auf dessen Seite Nutzer ihre Meinung zu Restaurants, Lokalen und grundsätzlich zum besuchten Ort äußern konnten. Im vorliegenden Fall gab ein Nutzer recht deutlich seinen Ärger über einen Wirt zu verstehen, weswegen der Betroffene den Betreiber des Gästebuches aufforderte, den Beitrag zu löschen (zB „Der schlechteste Wirt von

[141] Auf Internetforen kann man seine Meinung und Gedanken zu bestimmten Themen und Gebieten veröffentlichen und sich mit anderen Personen austauschen.
[142] OGH 21.12.2006, 6 Ob 178/04 a. Siehe auch *Thiele*, Internet4Jurists, Zusammenfassung zu 6 Ob 178/04 a, http://www.internet4jurists.at/entscheidungen/ogh6_178_04a.htm (Stand: 18.5.2011).

Österreich“). Der Betreiber hatte aber nur Teile gelöscht, weswegen es zum Gerichtsverfahren mit dem Antrag auf Unterlassung kam.

Der OGH hat schließlich ausgesprochen, dass der Betreiber des Gästebuches als Host-Provider iSd § 16 ECG anzusehen[143] und die Rechtswidrigkeit des Verhaltens des Host-Providers nicht aus den Bestimmungen des ECG abzuleiten sei. Dies sei vielmehr nach den materiell-rechtlichen Bestimmungen zu beurteilen. In § 18 ECG ist normiert, dass eine allgemeine Überwachungspflicht für Host-Provider grundsätzlich nicht besteht.

Der OGH sprach damit aus, dass ein Host-Provider nicht für die im Auftrag des Nutzers gespeicherten Informationen verantwortlich ist, wenn er von diesen keine tatsächliche Kenntnis über die rechtswidrige Tätigkeit oder Information hatte oder er nicht unverzüglich nach Kenntnis durch Löschen oder Sperren tätig geworden ist.

Gemäß § 1330 ABGB reicht ein „technisches Verbreiten“ aus, um auf Unterlassung in Anspruch genommen werden zu können. Die Aufnahme von Informationen auf eine Internet-Webseite stellt nach Ansicht des OGH ein derartiges Verbreiten von Informationen dar[144]. In dieser Entscheidung hat der OGH zum ersten Mal ausdrücklich ausgesprochen, dass aus der Bestimmung des § 19 Abs 1 ECG abzuleiten sei, dass die Haftungsprivilegierung des § 16 ECG lediglich eine Schadenersatzpflicht (und eine strafrechtliche Verantwortlichkeit) ausschließt, aber keinesfalls eine Verantwortlichkeit für verschuldensunabhängige Unterlassungsansprüche.

Den Host-Provider treffe demnach zwar keine allgemeine Überwachungspflicht, aber eine besondere Überprüfungspflicht, was bedeutet, dass ein Host-Provider bei Bekanntwerden offensichtlich rechtswidriger Inhalte diese zu entfernen hat. In obiger Entscheidung hat der OGH dem Unterlassungsanspruch für den rufschädigenden Gästebucheintrag stattgegeben. Dem Betreiber eines Online-Forums, mE können SNP zu solchen gezählt werden, sind rechtswidrige Beiträge ihrer Nutzer damit nicht zuzurechnen.

Diese Judikaturlinie ist mE nach begrüßenswert, da im Falle von nicht moderierten Online-Diskussionsforen für jeden Teilnehmer die Möglichkeit besteht, Beiträge über das Internet zu veröffentlichen, die – je nach Einstellung – von anderen Personen eingesehen und damit wahrgenommen werden können. Außerdem kann es den Betreibern nicht zugemutet werden, eine permanente Vorabkontrolle vorzunehmen.

---

[143] *Zankl*, E-Commerce-Gesetz (2002) Rz 222.
[144] Siehe *Ghazal* in *Jaksch-Ratajczak* (2010) 56 ff.

Das deutsche LG Hamburg hat in einer Entscheidung ausgesprochen, dass einen Host-Provider, in diesem Fall war es YouTube, die Pflicht treffe, einen konkreten Inhalt zu sperren bzw „die im zumutbaren Rahmen geeigneten Maßnahmen zu ergreifen“, wenn er über eine Urheberrechtsverletzung informiert wurde, um weiteren Urheberrechtsverletzungen vorbeugen zu können. Das LG Hamburg führte weiters aus, dass zwar keine Verpflichtung zur Kontrolle bestehe, aber im Falle einer Kenntnis sehr wohl reagiert werden müsse. Falls es zu einer Verletzung dieser Kontrollpflichten komme, dann würde YouTube als Störer haften und nicht als Täter.[145]

d. Haftung für fremde Postings auf einer Social network-Plattform

Zivilrechtlich interessant ist die Frage, ob einen Host-Provider gem § 18 ECG grundsätzlich die Verpflichtung trifft, aktiv fremde Inhalte und Postings zu überwachen, um Kenntnis von rechtswidrigen Inhalten und Aktivitäten zu erhalten.

Wenn es aber Hinweise auf eine Rechtswidrigkeit gibt, dann geht die Judikatur von einer Überwachungspflicht aus, so im Verfahren OGH 21.12.2006, 6 Ob 178/04a. Auch das OLG München hat in einem ähnlich gelagerten Verfahren (21.9.2011, 6 W 1551/11) entschieden, dass ein Host-Provider auf Unterlassung haftet, wenn er von einer Rechtsverletzung Kenntnis hatte und die rechtsverletzenden Inhalte nicht beseitigt.[146]

Dh der Provider wäre dann verpflichtet, das rechtsverletzende Posting umgehend zu beseitigen, sowie die ihm möglichen und zumutbaren Maßnahmen zur Verhinderung weiterer gleichartiger Verletzungen zu treffen. Kommt der Betreiber dem nicht nach oder kommt es zu neuerlichen Verstößen, so kann er selbst als mithaftender Störer in Anspruch genommen werden.

Die Judikatur des EuGH hingegen geht hinsichtlich Host-Providern in eine andere Richtung, welche besagt, dass Host-Provider nicht präventiv verpflichtet sind, auf eigene Kosten und

[145] LG Hamburg 20.4.2012, 310 O 461/10.

[146] Inhalt des Verfahrens war ein Meinungsforum, welches der Beklagte hostete. Es wurden auf diesem Forum ehrverletzende Äußerungen über den Kläger getätigt und auch Urheberrechte von diesem verletzt. Der Betreiber des Forums hat den Hostprovider (Beklagten) schließlich darauf hingewiesen, doch hat dieser keine entsprechenden Schritte gesetzt, weswegen es zum Verfahren kam. Siehe OLG München 21.9.2011, 6 W 1551/11.

zeitlich unbegrenzt Filtersysteme zu verwenden, um dadurch (mögliche) Urheberrechtsverletzungen zu verhindern.[147]

Wie kann eine betroffene Person ihre Ansprüche geltend machen, hat der Host-Provider und damit der Betreiber der SNP eine Auskunftspflicht hinsichtlich Identitätsdaten? Grundsätzlich normiert § 18 ECG, welcher den Umfang der Pflichten des Diensteanbieters regelt, eine Auskunftspflicht ua des Host-Providers hinsichtlich inländischer Gerichte (Abs 2) bzw dritter Personen (Abs 4), wenn dies der Feststellung eines rechtswidrigen Sachverhalts bzw zur Rechtsverfolgung dienlich ist. Allerdings bietet das keine Gewähr dafür, dass der Betreiber einer SNP über die (wahren) Identitätsdaten verfügt.

Zusätzlich stellt sich die Frage, ob sich ein Betreiber einer SNP genauso wie ein Betreiber eines moderierten Onlineforums auf das Redaktionsgeheimnis iSd MedienG berufen und damit die Auskunft verweigern kann. Der OGH hat in der Entscheidung 6 Ob 133/13x ausgesprochen, dass Postings in Online-Foren von Zeitungen nicht dem Redaktionsgeheimnis unterliegen, wenn diese in keinerlei Zusammenhang mit einer journalistischen Tätigkeit stehen. Ein Dritter habe demnach im Falle der Glaubhaftmachung eines „überwiegenden rechtlichen Interesses das Recht, die Identität des Nutzers zu erfahren“. Im konkreten Fall ging es um Beleidigungen in einem Online-Forum einer österreichischen Zeitung. Der Entscheidung des OGH zufolge müssten die Betreiber der Foren E-Mail-Adressen und Namen der Nutzer preisgegeben, auch wenn sie – wie hier erfolgt – die betreffenden Postings bereits gelöscht haben.

Das ECG normiert, dass Betreiber nicht-moderierter Foren bei entsprechender Glaubhaftmachung des rechtlichen Interesses Dritter die Identitäten herausgeben müssen.

Das Redaktionsgeheimnis soll lediglich dann greifen, wenn ein direkter Zusammenhang mit einer journalistischen Tätigkeit gegeben ist, was bei Postings in der überwiegenden Zahl der Fälle nicht gegeben ist.

Im Falle von SNP ist die Ausgangslage mE gleich gelagert. Wenn es sich bei einem beleidigenden Posting auf einer Facebook-Wall nicht um eine konkrete juristische Tätigkeit handelt, welche in den wenigsten Fallkonstellationen möglich sein wird, wird der Betreiber bei Erfüllung der weiteren Voraussetzungen zu einer Offenlegung der Identitätsdaten verpflichtet sein.

[147] Siehe EuGH 19.2.2012, C-360/10.

Ist der Anspruchsgegner identifiziert, richtet sich das primäre Interesse darauf, dass das verletzende Posting aus dem Internet gelöscht wird. Dazu stehen Unterlassungs- und Beseitigungsansprüche zur Verfügung. Darüber hinaus ist es oft geboten, den durch das Posting hervorgerufenen unwahren Eindruck gegenüber dem Publikum richtigzustellen. Insofern stehen auch Widerrufs- bzw. Urteilsveröffentlichungsansprüche und unter bestimmten Umständen auch ein Anspruch auf Gegendarstellung zu.

Je nach Anspruchsgrundlage kann bei Rufschädigung ein Ersatzanspruch für einen eingetretenen Vermögensschaden oder, bei besonderen Umständen, für die erlittene Kränkung oder andere persönliche Nachteile geltend gemacht werden. Schließlich wären auch medienrechtliche Entschädigungsansprüche denkbar.

e. Haftung für Tweets

Bei der SNP Twitter ist die Haftungsfrage ein wenig anders gelagert: Der Follower eines Tweets erhält eine Nachricht zugeordnet. Für den Inhalt der Meldung verantwortlich ist aber der Content-Provider, als derjenige, der die Nachricht verfasst hat.

Das OLG Bremen sprach am 14.1.2011 in seiner Entscheidung 2 U 115/10 aus, dass der Content-Provider für den Inhalt der Meldung verantwortlich ist und dafür einzustehen hat.

Auch das LG Frankfurt/Main sprach in seiner Entscheidung vom 20.4.2010[148] aus, dass man, ähnlich wie beim Einbinden von Links auf einer Webseite, auch als Nutzer von Twitter für Links in einem Tweet haftbar gemacht werden kann. Das LG Frankfurt belangte einen Twitter-Nutzer dafür, dass er trotz Kenntnis der Rechtwidrigkeit einen Link über Twitter postete. Die Kenntnis der Rechtswidrigkeit sei aus dem Tweet hervorgegangen. Ein Twitter-Nutzer könne somit rechtlich belangt werden, wenn er Links über Twitter postet und damit eventuelle Fehlinformationen über Dritte sogar bewusst im Internet streut.

f. Sind Facebook-Nutzer Host-Provider bei einer Facebook-Fanpage?

Wie weiter oben beschrieben, können auf Fanpages Nachrichten und Kommentare hinterlassen bzw Fotos hochgeladen und veröffentlich werden.

[148] Siehe LG Frankfurt/Main, 20.4.2010, 3-08 O 46/10.

Es stellt sich nun die Frage, wer für ehrenbeleidigende, rufschädigende, herabwürdigende etc Kommentare von Facebook-Nutzern auf derartigen Fanpages zu haften hat. Kommt es zu einer Haftung des Fanpage-Betreibers oder haftet der Betreiber von Facebook? Wer ist bei Fanpages als Host-Provider iSd ECG anzusehen?

In Anlehnung an die oberstgerichtliche Entscheidung 6 Ob 178/04a können meiner Ansicht nach Facebook-Fanpages den in dieser Entscheidung thematisierten Online-Gästebüchern gleichgesetzt werden, da sowohl bei Fanpages als auch Online-Gästebuchern Kommentare hinterlassen und auch regelmässig Fotos hochgeladen: Der OGH verstand als „Online-Gästebuch“, Webseiten, auf denen Nachrichten und Kommentare hinterlassen werden können. Bei Fanpages ist es wie erwähnt ähnlich, der Betreiber der Fanpage kann selbst wählen und festlegen, unter welchen Voraussetzungen Nachrichten und Kommentare auf der Fanpage hinterlassen werden können bzw selbst entscheiden, wann und ob die Seite wieder geschlossen werden soll. Durch diese „Eigenständigkeit bzw Eigenverantwortung“ sind Betreiber derartiger Fanpages mE als Host-Provider anzusehen und deren Haftung ist nach dem ECG, insbesondere §§ 16 und 18 ECG, zu beurteilen.

Genauso wie beim Host-Provider von privaten Profilseiten kommt es auch beim Host-Provider einer Fanpage darauf an, ob die in § 16 ECG angeführten Voraussetzungen zum Ausschluss der Haftung vorliegen. Denn nur wenn diese nicht vorliegen, ist die Verantwortung des Host-Providers auf Grundlage des materiellen Rechts weiter zu prüfen.

Den Host-Provider trifft auch bei einer Fanpage gem § 18 Abs 1 ECG keine allgemeine Kontrollpflicht. Solange der Host-Provider keine Kenntnis von rechtswidrigen Informationen hat, kommt das Haftungsprivileg des § 16 Abs 1 ECG zur Anwendung.

2. Allgemeine Geschäftsbedingungen im Zusammenhang mit Social network-Plattformen, insbesondere am Beispiel Facebook

Für einen Vertragsabschluss im Internet gelten grundsätzlich dieselben Regelungen und Vorschriften wie bei einem Vertragsabschluss außerhalb des elektronischen Bereichs, insbesondere gilt das Prinzip der Vertragsfreiheit, welches die Abschlussfreiheit, Formfreiheit, Gestaltungsfreiheit und Beendigungsfreiheit beinhaltet[149]. Zusätzlich zu den „normalen" Auslegungsgrundsätzen des ABGB treten im Internet spezielle Regelungen hinzu, deren Grundlage insbesondere die E-Commerce-Richtlinie bildet, welche durch das ECG umgesetzt wurde, wobei speziell die §§ 9, 10, 11 und 12 ECG den Vertragsabschluss regeln. Für Konsumenten sind außerdem die Bestimmungen des KSchG relevant, welche bei Verbrauchergeschäften anzuwenden sind.

Zur Form- und Gestaltungsfreiheit zählt ua die Möglichkeit, einen Vertrag unter Zugrundelegung von Allgemeinen Geschäftsbedingungen abzuschließen, weswegen in der Folge auf mögliche Probleme iZm Allgemeinen Geschäftsbedingungen bei SNP – insbesondere im Lichte des ECG und KSchG – eingegangen werden soll:

Allgemeine Geschäftsbedingungen sind in unserem Leben allgegenwärtig. Fast täglich stehen wir ihnen gegenüber, sei es bei einem Kaufvertrag, bei einem Mietvertrag, bei einer Bestellung etc oder eben iZm SNP. Auch SNP weisen in der Regel AGB auf, unter welchen die jeweiligen Plattformbetreiber kontrahieren wollen und ist es daher unerlässlich, diese näher zu betrachten und sich rechtlich mit ihnen auseinanderzusetzen.

Insbesondere sind deren Wirkungen (anwendbares Recht, datenschutzrechtliche Verantwortlichkeit, Einwilligung etc.) näher zu betrachten.

a. Allgemeines

Im österreichischen Recht ist eine genaue Definition des Begriffs „Allgemeine Geschäftsbedingungen" (AGB) nicht auffindbar. Die Regelungen für die rechtliche

[149] Vgl *Koziol/Welser*, Bürgerliches Recht II[13] (2007) 13 ff.

Beurteilung finden sich in verschiedenen Gesetzen wie dem Allgemeinen Bürgerlichen Gesetzbuch (ABGB), Konsumentenschutzgesetz (KSchG), Unternehmensgesetzbuch (UGB), E-Commerce Gesetz (ECG)[150] etc. In Deutschland hingegen sind AGB ein Grundtatbestand des dt AGBG[151]. Ich schließe mich der Meinung von *Ellenhuber*[152] an, welche davon ausgeht, dass es „gerechtfertigt erscheint, sich (in Österreich) an dem in Deutschland entwickelten Begriff der AGB zu orientieren".[153]

„Allgemeine Geschäftsbedingungen sind alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrages stellt. Gleichgültig ist, ob die Bestimmungen einen äußerlich gesonderten Bestandteil des Vertrages bilden oder in die Vertragsurkunde selbst aufgenommen werden, welchen Umfang sie haben, in welcher Schriftart sie verfasst sind und welche Form der Vertrag hat. Allgemeine Geschäftsbedingungen liegen nicht vor, soweit die Vertragsbedingungen zwischen den Vertragsparteien im Einzelnen ausgehandelt sind."[154]

In den österreichischen Gesetzen wird zwar von „Allgemeinen Geschäftsbedingungen" und „Vertragsformblättern" gesprochen, doch erscheint eine genaue Differenzierung der Begriffe nicht notwendig, da sowohl in § 864 a als auch in § 879 Abs 3 ABGB in Verbindung mit den AGB stets auch von Vertragsformblättern gesprochen wird. Laut *Krejci* kommt es bei der Frage, ob AGB als solche zu qualifizieren sind oder nicht, nicht auf ihre formale Ausgestaltung an.[155]

AGB dienen einer Vielzahl von Verträgen als Gestaltungsmodell, um im Geschäftsverkehr die zivilrechtliche Position von Unternehmen gegenüber den Kunden zu verbessern.

---

[150] Vgl § 11 ECG, welcher nur auf Rechtsgeschäfte im E-Commerce und M-Commerce anwendbar ist und daher bei Webseiten, welche lediglich der Werbung dienen, keine Anwendung findet.

[151] § 1 Abs 1 dt AGBG: Allgemeine Geschäftsbedingungen sind alle für eine Vielzahl von Verträgen vorformulierten Vertragsbedingungen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrages stellt. Gleichgültig ist, ob die Bestimmungen einen äußerlich gesonderten Bestandteil des Vertrages bilden oder in die Vertragsurkunde selbst aufgenommen werden, welchen Umfang sie haben, in welcher Schriftart sie verfasst sind und welche Form der Vertrag hat […].

[152] *Ellenhuber*, Rechtliche Probleme des Vertragsabschlusses im Internet unter besonderer Berücksichtigung der Allgemeinen Geschäftsbedingungen (2001) 116 ff.

[153] *Rummel* in *Rummel*, ABGB § 864 a.

[154] Legaldefinition des § 305 Abs 1 dt BGB, Einbeziehung Allgemeiner Geschäftsbedingungen in den Vertrag, dt Bürgerliches Gesetzbuch idF der Bekanntmachung vom 2.1.2002, BGBl. I S 42, ber. S 2909, 2003 I S 738, idgF.

[155] Die überwiegende Ansicht geht von einer Geltungs- und Inhaltskontrolle aus: vgl *Koziol/Welser*, Bürgerliches Recht I[13] (2006) 130 ff; *Rummel* in *Rummel*, ABGB § 864 a; *Zankl*, Bürgerliches Recht[6] (2012) Rz 57 ff; anders *P. Bydlinski* in *Apathy* (Hrsg), Bürgerliches Recht I, AT, welcher von einer Einbeziehungs-, Geltungs- und Inhaltskontrolle ausgeht.

b. Allgemeine Geschäftsbedingungen im Internet und deren Prüfung

Für den schlichten Besuch einer Webseite, wie zB der Webseite einer SNP, ist das Abgeben einer rechtsgeschäftlichen Erklärung an sich noch nicht nötig.

Ich schließe mich der Meinung von *Härting* an, dass ein Betreiber einer Plattform ein „virtuelles Hausrecht" an seiner Plattform hat und daher Bedingungen für ihre Benützung aufstellen kann.[156] Ich gehe davon aus, dass *Härting* damit ausdrücken möchte, dass jeder Betreiber, egal ob Betreiber eines virtuellen oder eines realen Unternehmens, die Möglichkeit haben soll, selbst über die Nutzungsbedingungen bzw über sein Hausrecht entscheiden zu dürfen (solange er sich im rechtlichen Rahmen bewegt).

Probleme im Zusammenhang mit AGB ergeben sich jedoch zumeist schon bei der Frage nach deren Einbeziehung bzw ob diese überhaupt Vertragsbestandteil wurden und in der Folge, welcher Teil der AGB gültig bestehen bleibt, wenn einzelne Klauseln unwirksam werden bzw unwirksam sind.[157]

Zunächst ist daher zu prüfen, ob zwischen der SNP Facebook und ihren Nutzern AGB überhaupt wirksam vereinbart werden, denn erst wenn die AGB in den Vertrag einbezogen wurden, ist sowohl eine Geltungskontrolle nach § 864a ABGB als auch eine Inhaltskontrolle, auch Angemessenheitskontrolle genannt, nach § 879 Abs 3 ABGB vorzunehmen. Im Verbrauchergeschäft sind überdies § 6 Abs 1 und 2 KSchG sowie das Transparenzgebot (§ 6 Abs 3 KSchG) zu beachten. Sowohl Geltungs- als auch Inhaltskontrolle dienen der Überprüfung, ob einerseits ein Vertrag unter Anwendung von AGB zustande gekommen ist und andererseits, ob diese angewendeten AGB möglicherweise sittenwidrig sind.

Generell lässt sich sagen, dass „unter dem Gesichtspunkt der Geltungskontrolle geprüft wird, ob sich der Vertragspartner mit den AGB überhaupt einverstanden erklärt hat", dh ob ihm die AGB vor Vertragsabschluss erkennbar waren oder er zumindest die Möglichkeit zur Kenntnisnahme der AGB hatte[158]. Unter Inhaltskontrolle wird „eine Kontrolle der AGB unter dem Aspekt der Sittenwidrigkeit" iSd § 879 ABGB verstanden[159].

Selbst im Falle des Vertragsabschlusses mit einem Konsumenten ist weiters zu prüfen, ob in diesen AGB Bestimmungen enthalten sind, welche mit Verbrauchern gar nicht vereinbart

---

156 *Härting*, Internetrecht[4] Rz 1127.
157 *Höss*, Die Einbeziehung von AGB beim Vertragsabschluss im Internet (2007) 74 ff.
158 *Zankl*, Bürgerliches Recht[6] (2012) Rz 57 ff.
159 *Zankl*, Bürgerliches Recht[6] (2012) Rz 57 ff.

werden dürfen und ob unklare oder unverständliche Regeln enthalten sind. Verbraucher genießen einen ganz besonderen „stärkeren“ Schutz und das Gesetz schreibt vor, dass mit einem Verbraucher gewisse AGB gar nicht wirksam vereinbart werden können, um die „Überrumpelungsgefahr“, wie *Zankl* treffend formuliert[160], zu reduzieren.

Ein Webseitenbetreiber kann zwar Bedingungen für die Nutzung seiner Webseite aufstellen, er muss jedoch klar und deutlich seinen Willen zum Ausdruck bringen, rechtsgeschäftlich bindende Regelungen gegenüber dem Nutzer wirksam werden zu lassen.

Ein Unternehmen hat allerdings nicht die Möglichkeit, in den „Benützungsverträgen“ ein für seine Vertragspartner geltendes Recht einseitig zu schaffen.

(1) Wirksame Einbeziehung der AGB bei der SNP Facebook?

Fraglich ist, ob und in welchem Umfang die AGB von Facebook in den Nutzungsvertrag mit den Nutzern einbezogen werden, dh ob bereits bei Vertragsabschluss ein ausdrücklicher Hinweis auf die bzw eine zumutbare Kenntnisnahme der AGB erfolgt, um schließlich eine Geltungs- und Inhaltskontrolle vornehmen zu können.

Nach der herrschenden Ansicht reicht nämlich für die Einbeziehung von AGB bei online abgeschlossenen Verträgen ein „deutlicher Hinweis auf der Webseite mit der übrigen Bestellinformation“.[161] *Zankl* schließt aus dem Umstand, dass bei Vertragsabschlüssen in der analogen Welt die Möglichkeit zur Kenntnisnahme der AGB ausreicht, da in dem Fall von einer konkludenten Annahme ausgegangen werden kann, dass die Abrufbarkeit an einer deutlich sichtbaren Stelle vor Vertragsabschluss ausreicht, um die AGB zu einem Vertragsteil zu machen.[162]

Im konkreten Fall ist eine Registrierung – und damit ein Vertragsabschluss mit – Facebook lediglich „nach Bestätigung des Lesens und der Zustimmung der Nutzungsbedingungen und Datenschutzrichtlinien“ möglich, welche sowohl über einen Link direkt unterhalb des Registrierungs-Buttons als auch auf der Startseite rechts unten über dem Icon[163] „Impressum/Nutzungsbedingungen“[164] bzw „Terms (of Service)“ abrufbar sind:[165]

---

[160] *Zankl*, Bürgerliches Recht[6] (2012) Rz 56.
[161] *Tangl*, Leitfaden für die Einbeziehung elektronischer AGB, ecolex 2001, 896 (896).
[162] *Zankl*, Zur Umsetzung vertragsrechtlicher Bestimmungen der E-Commerce RL, NZ 2001, 288; *Madl*, ecolex 1996, 79
[163] Icon ist ein kleines Bildsymbol, über das ein bestimmter Bedeutungsgehalt transportiert werden soll.
[164] http://de-de.facebook.com

„Erklärung der Rechte und Pflichten

Die vorliegende Erklärung der Rechte und Pflichten (‚Erklärung') beruht auf den Facebook-Grundsätzen und reguliert unsere Beziehung zu den Nutzern und anderen, die mit Facebook interagieren. Mit deiner Nutzung von Facebook oder dem Zugriff darauf stimmst du dieser Erklärung zu.“[166]

Abbildung 14: Screenshot, Registrierungsfeld

Facebook spricht zwar von „Nutzungsbedingungen“, doch kann einerseits unterstellt werden, dass es sich um „Allgemeine Geschäftsbedingungen“ handelt, welche zur Vereinheitlichung von einer Vielzahl abzuschließender Geschäfte (mit dem Ziel, neue Nutzer zu gewinnen) vorformuliert wurden und auf deren Basis die Verträge zustande kommen sollen, und auf der anderen Seite ist eine (Fehl-)Bezeichnung grundsätzlich irrelevant, wenn klar erkennbar ist, was eigentlich gemeint ist.

Wie bereits erwähnt wurde, ist im österreichischen Recht eine genaue Erklärung des Begriffs der Allgemeinen Geschäftsbedingungen (AGB) nicht auffindbar. Es wird sowohl von „Vertragsbestimmungen“ als auch von „Allgemeinen Geschäftsbedingungen“ gesprochen, weswegen eine Bezeichnung als „Nutzungsbedingungen“ nicht schadet. In weiterer Folge sollen alle drei Begriffe gemeint sein, wenn über „Allgemeine Geschäftsbedingungen“ (AGB) iZm SNP gesprochen wird.

---

[165] http://www.facebook.com

[166] Auszug aus den Nutzungsbedingungen von Facebook, http://www.facebook.com/#!/terms.php (Stand: Oktober 2012).

Es findet sich auf der Startseite von Facebook[167] rechts unten das Icon[168] „Impressum/Nutzungsbedingungen“[169] bzw „Terms (of Service)“.[170]

Facebook erklärt zwar, dass man durch das Nutzen, Zugreifen und Registrieren bei Facebook den Nutzungsbedingungen von Facebook zustimmt, doch ist zweifelhaft, ob sich der Hinweis an der richtigen Stelle befindet, um bei „Vertragsabschluss“ vom Nutzer bemerkt zu werden. Des Weiteren muss der Hinweis auf die AGB so klar und übersichtlich platziert sein, dass beim Nutzer keine Zweifel über den Inhalt aufkommen können.

Wie alle anderen Vereinbarungen eines Vertrages haben auch AGB den allgemeinen Geltungsgrund, sodass sie nur kraft beiderseitigem[171] Einverständnis Geltung erlangen.

AGB gelten gem § 863 ABGB kraft ausdrücklicher oder stillschweigender Parteienvereinbarung, wobei bei einer stillschweigenden Annahme die Maßstäbe naturgemäß strenger zu beurteilen sind und nur als gegeben angenommen werden dürfen, wenn deutlich erkennbar ist, dass der Unternehmer nur aufgrund seiner AGB den Vertrag abschließen möchte und der Kunde die Möglichkeit hat, sich vor Vertragsabschluss vom Inhalt Kenntnis zu verschaffen.[172]

Fehlt ein deutlicher Hinweis auf die AGB[173] oder kann der Kunde (Vertragspartner) nicht auf zumutbare Weise Einsicht nehmen, dann werden die AGB von vornherein nicht Vertragsbestandteil. AGB werden somit nur dann verbindlich, wenn der Kunde diese kennen musste oder aus eigenem, grob fahrlässigem Verschulden diese nicht kannte.[174]

Die Facebook-AGB sind sowohl rechts unten auf der Facebook-Webseite als auch oberhalb des Registrierungs-Buttons, mit welchem man nach Eingabe von Namen, E-Mail-Adresse, Geschlecht, Geburtsdatum und Passwort seine Registrierung bestätigt, abrufbar.

---

[167] Siehe https://de-de.facebook.com/ (Stand Oktober 2014).
[168] Icon ist ein kleines Bildsymbol, über das ein bestimmter Bedeutungsgehalt transportiert werden soll.
[169] http://de-de.facebook.com
[170] http://www.facebook.com
[171] Es gibt Ausnahmen, wo AGB kraft objektiven Rechts gelten und sich der Vertragspartner unterwerfen muss. Derartige AGB werden vom Gesetzgeber selbst erlassen und durch eine Behörde in Kraft gesetzt, zB Beförderungsbedingungen der Post und Bundesbahn, welche durch Gesetz erlassen wurden (siehe ua Bundesgesetz über die Regulierung des Postmarktes [Postmarktgesetz-PMG] StF: BGBl I 123/2009).
[172] *Madl*, Vertragsabschluss im Internet, ecolex 1996, 79.
[173] OGH 3.2.1966, 1 Ob 24/66; 30.4.1987, 7 Ob 535/87. Es gibt jedoch Fälle, wo ein „deutlicher Anschlag“ der AGB in den jeweiligen Geschäftsräumlichkeiten genügt, zB Putzereien.
[174] *Rummel* in *Rummel*, ABGB[2] § 864a Rz 2.

Facebook gibt mE damit klar zu verstehen, dass eine Registrierung als neuer Nutzer nur aufgrund bzw unter Zugrundelegung der Nutzungsbedingungen von Facebook stattfinden kann.

Der Hinweis darauf findet sich mE an einer präsenten Position, die Nutzungsbedingungen sind direkt oberhalb des Registrierungs-Buttons zu finden und mittels Link zu öffnen. Eine Kenntnisnahme ist damit möglich und durch den Klick auf das „Registrieren" erklärt der Kunde unzweifelhaft, dass er mit der Einbeziehung der AGB beim Abschluss des Nutzungsvertrags einverstanden ist.

c. Allgemeine Geschäftsbedingungen im Lichte des ECG und KSchG

Da es sich bei SNP um Internetdienste handelt, ist bei der Prüfung der AGB auch ein Blick in das ECG[175] zu werfen. Das ECG regelt zwar nicht die Modalitäten des Vertragsabschlusses, so *Zankl*[176], diese richten sich nach dem allgemeinen Zivilrecht, das ECG enthält jedoch Bestimmungen hinsichtlich Vertragsbestimmungen und Allgemeine Geschäftsbedingungen:

In § 11 ECG ist normiert, dass „ein Diensteanbieter[177] (siehe weiter oben) die Vertragsbestimmungen und die Allgemeinen Geschäftsbedingungen dem Nutzer so zur Verfügung zu stellen hat, dass er sie speichern und wiedergeben kann. Diese Verpflichtung kann nicht zum Nachteil des Nutzers abbedungen werden". § 11 ECG[178] regelt somit, dass der Diensteanbieter seine Vertragsbestimmungen und Allgemeinen Geschäftsbedingungen seinen Nutzern so zur Verfügung zu stellen hat, dass diese sie speichern und wiedergeben können. Regelungen bzgl. aktiven Lesens und Verstehens sind nicht enthalten.

Über die Art und Weise des Zugangs zu den AGB finden sich in § 11 ECG keine Regelungen.

Außerdem besteht für den Diensteanbieter keine Verpflichtung, sicherzustellen, dass der Nutzer das jeweilige Format (.pdf, .doc etc[179]) auch tatsächlich öffnen kann.[180]

---

[175] Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden (E-Commerce-Gesetz-ECG), BGBl I 152/2001.
[176] Siehe *Zankl*, Bürgerliches Recht[5], Kurzlehrbuch 265.
[177] Der Begriff „Diensteanbieter" wird in § 3 ECG definiert als eine natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die einen Dienst der Informationsgesellschaft bereitstellt.
[178] RL 2000/31/EG des Europäischen Parlaments und des Rates vom 8.6.2000, ABl L 178/1.
[179] AGB dürfen nicht in ungewöhnlichen Formaten abgespeichert sein, vgl *Redeker*, IT-Recht[4] (2007) Rz 885.
[180] *Höss*, Die Einbeziehung von AGB beim Vertragsabschluss im Internet (2007) 78.

(1) Hinweispflicht des Diensteanbieters und Kenntnisnahme des Nutzers

Allgemeine Geschäftsbedingungen müssen in Entsprechung der allgemeinen zivilrechtlichen Grundsätze wirksam vereinbart werden, um Vertragsinhalt zu werden. Dies gilt auch für den E-Commerce-Bereich.

Wenn der Nutzer Verbraucher (Konsument) ist, dann sind (zusätzlich) die Maßstäbe des KSchG[181], insbesondere § 6 KSchG, anzuwenden, welcher unzulässige Vertragsbestandteile aufzählt und normiert, dass gewisse Bestimmungen für einen Verbraucher nicht verbindlich vereinbart werden können:[182]

Unzulässige Vertragsbestandteile

§ 6 Abs 1 KSchG: *Für den Verbraucher sind besonders solche Vertragsbestimmungen im Sinn des § 879 ABGB jedenfalls nicht verbindlich, nach denen*

1. sich der Unternehmer eine unangemessen lange oder nicht hinreichend bestimmte Frist ausbedingt, während deren er einen Vertragsantrag des Verbrauchers annehmen oder ablehnen kann oder während deren der Verbraucher an den Vertrag gebunden ist;

2. ein bestimmtes Verhalten des Verbrauchers als Abgabe oder Nichtabgabe einer Erklärung gilt, es sei denn, der Verbraucher wird bei Beginn der hiefür vorgesehenen Frist auf die Bedeutung seines Verhaltens besonders hingewiesen und hat zur Abgabe einer ausdrücklichen Erklärung eine angemessene Frist; […].

(2) Möglichkeit der Kenntnisnahme

Wie bereits ausgeführt, muss ein Unternehmer bzw Diensteanbieter einer SNP auf seine AGB deutlich hinweisen und dem Nutzer die Möglichkeit bieten, sich vom Inhalt in zumutbarer Weise Kenntnis verschaffen zu können. Durch die Speicher- bzw Ausdruckbarkeit der AGB soll dem Nutzer die Möglichkeit eingeräumt werden, sich diese durchzulesen, um in der Folge zu entscheiden, ob er mit dem Anbieter in eine „Vertragsbeziehung“ treten will und Mitglied einer SNP werden möchte.

Die Übermittlung der AGB ist dabei grundsätzlich nicht nötig. Es muss jedoch ein deutlicher Hinweis darauf existieren, dass nur unter Zugrundelegung der AGB (im Falle von Facebook die „Nutzungsbedingungen“) kontrahiert werden soll. Art und Intensität des Hinweises sind im ECG nicht geregelt.

[181] Konsumentenschutzgesetz, BGBl 140/1979, zuletzt geändert durch BGBl I 91/2003.
[182] Siehe § 6 KSchG.

Facebook weist mE deutlich auf seine AGB hin, denn es findet sich direkt oberhalb des Registrierungs-Buttons ein Link zu den AGB. Außerdem befinden sich rechts unten auf der Webseite[183] Links zu „Datenschutz“, „Impressum/Nutzungsbedingungen“ etc.

(3) Abstufung der Geltungskontrolle?

Beim Verfassen dieses Kapitels ist die Frage aufgetaucht, ob es eigentlich je nach Vertragstyp Unterschiede in der Art des Hinweisens bzw Einbeziehens von AGB geben sollte bzw ob AGB bei SNP möglicherweise anderen (Geltungs-)Kontrollen unterworfen werden sollten als zB bei einem Kaufvertrag?

Nach der Judikatur hat die Geltungskontrolle grundsätzlich nach der Art des jeweiligen Rechtsgeschäfts sowie nach den Umständen des Einzelfalls zu erfolgen. In der E sprach der OGH aus, dass es im Hinblick auf die Ungewöhnlichkeit einer AGB-Klausel auf die „Branchenüblichkeit und den Erwartungshorizont der angesprochenen Kreise ankommt“.[184]

Doch was sind die typischen Vertragsbestimmungen einer SNP, womit sollte bzw kann ein Durchschnittsnutzer einer SNP im Hinblick auf AGB bei SNP rechnen und kann aus dieser „Einzelfall-Prüfung“ geschlossen werden, dass es eine gewisse Abstufung bzw Unterschiede bei der Einbeziehung von AGB geben soll?

Meines Erachtens, ja. SNP gibt es mittlerweile seit mehreren Jahren und es haben sich damit gewisse „übliche Bestimmungen“ herauskristallisiert, welche zwischenzeitig zu einer gewissen „Branchenüblichkeit“ geführt und damit die Geltungskontrolle in eine gewisse Richtung gewiesen haben.

(4) Hinweis bei Online-Vertragsabschlüssen bzw Deutlichkeit des Hinweises

Facebook weist im Zuge des Registrierens auf seine AGB und damit inhaltlich unmissverständlich auf die Einbeziehung dieser hin. Fraglich ist, ob dieser Hinweis an einer hinreichend übersichtlichen Stelle platziert ist.

Der Hinweis muss an einer Stelle platziert sein, an welcher „üblicherweise“ damit gerechnet werden kann. Laut *Zankl* ist ein Hinweis auf AGB unzureichend, der erst „durch Scrollen[185]

[183] Stand Oktober 2014.
[184] Siehe OGH 22.9.1988, 7 Ob 649/88 (RIS-Justiz RS0014646).
[185] Scrollen ist das horizontale und vertikale Bewegen, das „Rollen“ von Programmfenstern, Listenfeldern etc.

auf einer Webseite erkennbar wird und sich nicht im selben Zusammenhang wie die Vertragserklärung befindet“[186]. *Höss* sieht dies jedoch anders und erklärt, dass, solange in der Vertragserklärung unmissverständlich auf die Einbeziehung von AGB hingewiesen wird und der Link zu den AGB auch nicht versteckt auf einer Unterseite an einer Stelle angebracht ist, an der man nicht erkennen kann, dass sich dort AGB befinden, die AGB gültiger Vertragsbestandteil werden. Seiner Ansicht nach ist ein Scrollen an das untere Ende einer Webseite zumutbar.[187]

Es wird jedoch von der hM weiterhin als unzulässig angesehen, dass sich ein Neukunde durch zahlreiche Links durchklicken muss, um zu den AGB zu gelangen.[188] Ich schließe mich der Meinung von *Zankl* an. AGB sollten mE schnell und deutlich auffindbar sein und sollten nicht erst nach langem Scrollen an das Ende einer Webseite „sichtbar“ werden.

Facebook hat den Hinweis zwar unterhalb, aber doch in unmittelbarer Nähe des Registrieren-Buttons platziert. Dh selbst bei flüchtiger Betrachtung ist nicht zu übersehen, dass Facebook seine AGB einbezogen haben möchte. Die Platzierung findet sich mE daher an einer geeigneten Stelle für einen erforderlichen Hinweis.

(5) Einverständnis des Nutzers

§ 863 Abs 1 ABGB bezieht sich auf das Einverständnis einer Person und normiert, dass man nicht nur ausdrücklich durch Worte, sondern auch stillschweigend sein Einverständnis für etwas erklären kann:
Abs 1: *„Man kann seinen Willen nicht nur ausdrücklich durch Worte und allgemein angenommene Zeichen, sondern auch stillschweigend durch solche Handlungen erklären, welche mit Überlegung aller Umstände keinen vernünftigen Grund, daran zu zweifeln, übrig lassen.“*

Abs 2: *„In Bezug auf die Bedeutung und Wirkung von Handlungen und Unterlassungen ist auf die im redlichen Verkehr geltenden Gewohnheiten und Gebräuche Rücksicht zu nehmen.“*

In § 863 ABGB ist geregelt, dass man seinen Willen, und damit das Akzeptieren von AGB, auch ohne Worte und Zeichen, also stillschweigend, erklären kann, es darf jedoch mit Überlegung aller Umstände kein vernünftiger Grund, daran zu zweifeln, existieren.

---

[186] *Zankl*, E-Commerce-Gesetz Rz 163.
[187] *Höss*, Die Einbeziehung von AGB beim Vertragsabschluss im Internet (2007) 79.
[188] *Härting*, Internetrecht Rz 370 bzw *Redeker*, IT-Recht[4] (2007) Rz 885.

Facebook entspricht dieser Bestimmung, indem der zukünftige Nutzer auf die AGB hingewiesen wird. Es ist sodann die Wahl des Nutzers, ob und wie er sich die AGB durchliest. Der Bindungswille von Facebook wird jedoch ausdrücklich geäußert. Es wird mit dem Abschluss des Registrierungsvorganges ein Vertrag über die Nutzung der SNP wirksam abgeschlossen.[189] Andere SNP verlangen die Aktivierung einer sog Kontrollbox bei der Anmeldung zur Plattform.

(6) Transparenzgebot und Inhaltskontrolle

Das sog „Transparenzgebot" setzt Art 5 der Vertragsklausel-RL um und ist in § 6 Abs 3 KSchG normiert:

„Eine in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern enthaltene Vertragsbestimmung ist unwirksam, wenn sie unklar oder unverständlich abgefasst ist."

Die AGB müssen demnach verständlich sein und einen gewissen Umfang an Struktur vorweisen.

§ 879 ABGB normiert in Abs 1: *„Ein Vertrag, der gegen ein gesetzliches Verbot oder gegen die guten Sitten verstößt, ist nichtig."* und in Abs 3: *„Eine in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern enthaltene Vertragsbestimmung, die nicht eine der beiderseitigen Hauptleistungen festlegt, ist jedenfalls nichtig, wenn sie unter Berücksichtigung aller Umstände des Falles einen Teil gröblich benachteiligt."*

Im Gegensatz zu § 879 Abs 3 ABGB, welcher sich auf Vertragsbestimmungen beschränkt, erfasst § 6 Abs 3 KSchG auch Hauptbestimmungen eines Vertrags, soweit diese im Rahmen Allgemeiner Geschäftsbedingungen festgelegt werden können.

AGB sind in der Regel dann „unverständlich" oder „unklar" formuliert, wenn dem Nutzer das Einsehen und Lesen unmöglich gemacht wird oder wenn der Text unvollständig, unleserlich (Größe der Schrift) oder unverhältnismäßig lang ist, womit ein Weiterlesen verhindert werden soll. Aber auch die Sprachwahl kann zu einer Unverständlichkeit führen, wenn die AGB nur in bestimmten Sprachen aufrufbar und daher nicht für jeden möglichen neuen Nutzer verständlich sind.[190]

[189] *Härting/Schätzle*, Nutzungsbedingungen in Social Networks, ITRB 2011, 40.
[190] Vgl *Berger*, Die Vereinbarung von AGB im Internet (2000) 40 f, zur Frage nach der Sprache der AGB im Internet.

Sowohl Schriftgröße als auch Sprache der Facebook-Nutzungsbedingungen unterfallen nicht dieser Norm, da Facebook sein Webportal mittlerweile in sehr viele Sprachen übersetzt hat. Mir erscheint auch die Schriftgröße als „normal groß“ gewählt.

Auszug aus der Facebook-Webseite:

„Du kannst auf die Erklärung der Rechte und Pflichten in verschiedenen Sprachen zugreifen, indem du die Spracheinstellung für Facebook änderst. Klicke dazu auf den Sprache-Link links unten auf einer beliebigen Seite. Falls die Erklärung in der von dir ausgewählten Sprache nicht zur Verfügung steht, wird dir die englische Version angezeigt.“[191]

In dieser Passage weist Facebook darauf hin, dass der Nutzer zwischen mehreren Sprachen wählen kann, um die AGB in einer für ihn verständlichen Sprache lesen zu können.

Gemäß § 864 a ABGB werden:

„Bestimmungen ungewöhnlichen Inhaltes in Allgemeinen Geschäftsbedingungen oder Vertragsformblättern, die ein Vertragsteil verwendet hat, nicht Vertragsbestandteil, wenn sie dem anderen Teil nachteilig sind und er mit ihnen auch nach den Umständen, vor allem nach dem äußeren Erscheinungsbild der Urkunde, nicht zu rechnen brauchte; es sei denn, der eine Vertragsteil hat den anderen besonders darauf hingewiesen.“

Das bedeutet, dass Bestimmungen, welche zwar alle Voraussetzungen zur Einbeziehung erfüllt haben, dann trotzdem nicht Vertragsbestandteil werden, wenn sie überraschend und nachteilig sind. So zB, wenn der zukünftige Nutzer einer SNP den Eindruck erhält, die Mitgliedschaft bei einer von ihm gewählten SNP sei gratis, in den Nutzungsbedingungen aber dann plötzlich eine Entgeltpflicht zu finden ist.

(7) Exkurs: Geltung von Allgemeinen Geschäftsbedingungen bei Betrachtung auf mobilen Endgeräten

Der Zugang zum Internet und damit zu SNP hat sich in den letzten Jahren stark verändert. War noch vor einigen Jahren der Zugang über einen Stand-PC üblich, folgte bald der Zugang über ein mobiles Notebook und nunmehr über sog Smartphones.[192]

Die meisten Smartphones bieten die sog „Facebook-Applikation“ bereits vorinstalliert an. Mit dieser kann man über das Mobiltelefon in einer für Smartphones angepassten Sondergröße auf

[191] http://de-de.facebook.com/terms.php?ref=pf (Stand: 3.3.2011).
[192] Smartphones sind eine Mischung aus Mobiltelefon und Mini-Computer.

Facebook einsteigen. „Die Anzahl an Nutzern, die fast täglich Social-Media-Inhalte mobil aufrufen, stieg in den letzten 12 Monaten um 67% (blog.adobe-solutions.de)“, so aus dem Social-Media-Rechtskonzept des e-center Wien.

Nun stellt sich jedoch die Frage, ob AGB bei beschränkter Bildschirmoberfläche und auch bei kleinerer Schriftgröße dem Nutzer überhaupt zugemutet werden können. Denn mit der kleineren Bildschirmoberfläche geht auch eine kleinere Schriftgröße einher, welche ein Scrollen durch den Nutzer zur Folge hat.

Härting vertritt die Ansicht, dass „ein langes und häufiges Scrollen dem Nutzer nicht zugemutet werden kann“.[193]

(8) Zwischenfazit

Wie dargelegt, regelt das Zivilrecht in § 869 ABGB, dass unverständliche rechtsgeschäftliche Willenserklärungen unwirksam sind und Ersatzpflichten gegenüber dem anderen Vertragspartner auslösen.

Überraschende Klauseln sind vom Geschäftswillen nicht erfasst und gem § 864 a ABGB daher unwirksam. § 879 Abs 3 ABGB erklärt gröblich benachteiligende AGB-Bestimmungen für nichtig.

SNP müssen somit einen ausdrücklichen Hinweis auf ihre AGB enthalten und der Nutzer muss die Möglichkeit erhalten, sich vom Inhalt Kenntnis zu verschaffen, bevor er seine Zustimmung erteilt.

Direkt auf der Startseite von Facebook befindet sich rechts unten ein Link mit der Bezeichnung „Impressum/Nutzungsbedingungen“. Ein Neukunde kann sich damit, vor der Registrierung und ohne das Setzen weiterer Schritte, einen Überblick über die Nutzungsbedingungen verschaffen und diese auch abspeichern.

d. Änderungen von Allgemeinen Geschäftsbedingungen nach Vertragsabschluss

Grundsätzlich gilt, dass Änderungen von AGB jederzeit (im rechtlichen Rahmen) möglich sind, dh ein Unternehmen kann seine AGB grundsätzlich jederzeit ändern bzw anpassen.

[193] *Härting/Schätzle,* Rechtsverletzungen in Social Networks, ITRB 2011, 41f.

Werden diese Änderungen jedoch nach Vertragsabschluss vorgenommen, wird für deren Änderung grundsätzlich die Zustimmung beider Vertragsteile benötigt, denn die Vertragsteile haben unter Zugrundelegung von bestimmten AGB einen Vertrag abgeschlossen und die beiderseitigen Willenserklärungen waren auf ganz bestimmte Vertragsbestimmungen gegründet.[194]

Der Vertragspartner muss schließlich die Möglichkeit haben, von den geänderten Klauseln Kenntnis zu erlangen.

(1) Möglichkeit der Kenntnisnahme

Falls eine SNP ihre AGB ändern möchte, bedeutet dies für die bestehenden Nutzer, dass diese über die geplanten Änderungen informiert werden und auch die Möglichkeit eingeräumt bekommen müssen, sich über die Änderungen Kenntnis verschaffen zu können.

Für neue Nutzer gelten die jeweiligen (in der Zwischenzeit geänderten neuen) AGB, falls deren Anmeldung erst nach einer AGB-Änderung erfolgt. Dies kann grundsätzlich dazu führen, dass gegenüber verschiedenen Nutzern verschiedene Fassungen der AGB gültig sind.

Viele Unternehmen haben daher „Änderungsvorbehalte“, welche nachträgliche Änderungen der Nutzungsbedingungen (AGB) erleichtern und keine explizite Zustimmung der Betroffenen verlangen. Derartige Änderungsvorbehalte sind aufgrund der Vertragsfreiheit grundsätzlich zulässig. Die Parteien müssen die entsprechenden Voraussetzungen jedoch vorab regeln.

In Deutschland hat der BGH in einem Verfahren betreffend die einseitige Änderung von AGB eines Versicherungsunternehmens nachfolgend ausgesprochen:[195]

„Die Anpassung durch neue, allein vom Versicherer aufgestellte Regelungen stellt einen Eingriff in ein bestehendes Vertragsverhältnis dar. Dieser lässt sich nach berücksichtigenden Interessen beider Vertragsparteien nur rechtfertigen, wenn durch unvorhersehbare Änderungen, die der Versicherer nicht veranlasst und auf die er auch keinen Einfluss hat, das bei Vertragsschluss vorhandene Äquivalenzverhältnis in nicht unbedeutendem Maße gestört wurde. Bei Versicherungsverträgen mit einer nicht nur kurzen Laufzeit kann die Störung des

[194] Vgl auch *Berger*, Die Vereinbarung von AGB im Internet (2000) 46, zur Frage nach der einseitigen AGB-Änderung.

[195] BGH 17.3.1999, IV ZR 218/97, siehe http://www.rechtzweinull.de/index.php?/archives/91-Facebook-aendert-seine-Terms-of-Service-Zulaessigkeit-der-nachtraeglichen-AEnderung-von-Allgemeinen-Geschaeftsbedingungen-AGB.html von RA Dr. *Carsten Ulbricht*.

Äquivalenzverhältnisses eine Anpassung erforderlich machen, wenn die Parteien ohne sie nicht oder nur mit Schwierigkeiten in der Lage sind, den Vertrag fortzusetzen und durchzuführen. Ebenso kann eine im Regelungswerk entstandene Lücke – etwa wenn die Rechtsprechung eine Klausel für unwirksam erklärt – Schwierigkeiten bei der Durchführung des Vertrags entstehen lassen, die nur durch Anpassung oder Ergänzung zu beseitigen sind. Nur unter diesen Voraussetzungen der Vertragslücke und der Störung des Äquivalenzverhältnisses ist eine nachträgliche Anpassung des Vertragsinhalts gerechtfertigt, die durch eine Anpassungsklausel geregelt werden kann."

Aus dieser Entscheidung kann abgeleitet werden, dass für einen rechtswirksamen Änderungsvorbehalt die Gründe, unter denen eine AGB-Änderung zulässig sein soll, ausdrücklich genannt werden sollen. Der Kunde muss über die möglichen Gründe einer AGB-Änderung ausreichend informiert werden.

Das notwendige Einverständnis des Kunden kann durch eine sog Erklärungsfiktion ersetzt werden. Dh dass die Zustimmung nicht ausdrücklich erklärt werden muss, sondern unter bestimmten weiteren Voraussetzungen durch eine „vermutete" Zustimmung ersetzt werden kann, wenn der Nutzer eine angemessene Frist zur Abgabe einer ausdrücklichen Erklärung eingeräumt bekommen und der Betreiber sich verpflichtet hat, den Vertragspartner bei Beginn der Frist auf die vorgesehene Bedeutung seines Verhaltens besonders hinzuweisen.

(2) Zustimmung durch Schweigen

Oftmals werden neue AGB mit den Worten eingeführt, dass „diese gelten sollen, wenn nicht innerhalb einer bestimmten Frist widersprochen wird". Eine derartige Zustimmung gilt jedoch nur, wenn der Betroffene auf diese fingierte Zustimmung (vorab) hingewiesen wurde bzw hingewiesen wird und ihm eine angemessene Frist gesetzt worden ist, darauf zu reagieren.

Bei Facebook wurden schon mehrmals einseitige Anpassungen bzw Änderungen der AGB vorgenommen. Facebook hat dazu beispielsweise in seiner „Erklärung der Rechte und Pflichten"[196] hinsichtlich ABG-Änderungen im Oktober 2012 geschrieben:

Änderungen[197]

1. *Wir können diese Erklärung ändern, wenn wir dich über die „Facebook Site Governance"-Seite (Seite zur Regelung der Nutzung von Facebook) darüber*

[196] Stand Oktober 2012.
[197] Siehe Aktualisierungen der Erklärung der Rechte und Pflichten, Facebook Site Governance.

informieren (indem wir die Änderung dort posten) und dir die Möglichkeit zur Reaktion auf die entsprechenden Änderungen geben. Um Informationen zu künftigen Änderungen an dieser Erklärung zu erhalten, besuche unsere „Facebook Site Governance"-Seite und klicke auf der Seite auf „Gefällt mir".

2. *[…]*
3. *Wenn mehr als 7.000 Nutzer einen inhaltlichen Kommentar zu einer bestimmten geplanten Änderung hinterlassen, erhältst du außerdem die Gelegenheit, an einer Abstimmung teilzunehmen, bei der Alternativen vorgeschlagen werden. Das Ergebnis ist verbindlich für uns, wenn sich mehr als 30 % der aktiven registrierten Nutzer (ab dem Benachrichtigungsdatum) an der Abstimmung beteiligen.*
4. *Wenn wir Änderungen an den in dieser Erklärung erwähnten bzw. dargestellten Richtlinien vornehmen, können wir dies auf der „Facebook Site Governance"-Seite mitteilen.*
5. *Wir dürfen Änderungen aus rechtlichen oder administrativen Gründen oder zur Berichtigung einer falschen Aussage nach Benachrichtigung auch ohne die Möglichkeit von Kommentaren vornehmen.*
6. *Deine weitere Nutzung von Facebook nach Änderungen an unseren Bedingungen bedeutet gleichzeitig dein Akzeptieren unserer geänderten Bedingungen.*

Insbesondere Punkt 6, *„Deine weitere Nutzung von Facebook nach Änderungen an unseren Bedingungen bedeutet gleichzeitig dein Akzeptieren unserer geänderten Bedingungen"*, verdeutlicht, dass Facebook seinen Nutzern vorschreibt, dass sie – nach einer Änderung der AGB – mit der weiteren Nutzung des Portals auch automatisch den neuen AGB zustimmen.

Aber ist obige Bestimmung (Zustimmung zu den AGB durch Weiterbenützung der Plattform) überhaupt rechtlich möglich und zulässig bzw ist es zulässig, Änderungen auf einer anderen Seite (konkret der Facebook Site Governance-Seite) bekanntzugeben?

Im Dezember 2012 folgte nachstehender Text in der Erklärung der Rechte und Pflichten von Facebook (Stand 11.12.2012), mit welchem Facebook nunmehr lediglich die Möglichkeit einer Kommentierung der Änderungen zuließ:

14. Änderungen

1. *Sofern wir eine Änderung nicht aus rechtlichen oder administrativen Gründen oder zur Korrektur einer ungenauen Erklärung vornehmen, geben wir dir eine* ***Frist*** *von* ***sieben (7) Tagen*** *(beispielsweise durch Posten der Änderung auf der „Facebook Site Governance"-Seite) sowie die Gelegenheit, die Änderungen zu dieser Erklärung zu kommentieren. Du kannst auch unsere „Facebook Site Governance"-Seite besuchen und auf „Gefällt mir" klicken, um die Aktualisierungen über die Änderungen an dieser Erklärung zu erhalten.*
2. *Wenn wir Änderungen an den in dieser Erklärung erwähnten bzw. dargestellten Richtlinien vornehmen, können wir dies auf der „Facebook Site Governance"-Seite* ***mitteilen****.*
3. *Deine* ***weitere Nutzung*** *von Facebook nach Änderungen an unseren Bedingungen* ***bedeutet gleichzeitig dein Akzeptieren*** *unserer geänderten Bedingungen.*

Facebook räumte damit seinen Nutzer einen Zeitraum von sieben Tagen ein, um die damals neuen Geschäftsbedingungen zu lesen und zu kommentieren. Aber es gab keine Möglichkeit mehr, die Änderungen abzulehnen, wie es bis dahin (theoretisch) möglich war. Davor gab es eine Art Mitbestimmungssystem. Wenn 7.000 Nutzer in ihrem Kommentaren zu einer AGB-Änderung übereinstimmend eine Abstimmung darüber forderten, wurde diese auch abgehalten. Stimmten dann 30 % aller Nutzer gegen die Änderungspläne, musste Facebook neue vorschlagen, auch wenn dies in der Praxis eigentlich nie erreicht wurde.

Gleichgeblieben war lediglich die Art der Bekanntgabe von Änderungen der Nutzungsbedingungen, nämlich über die Facebook Site Governance-Seite.

Abbildung 15: Screenshot Facebook Site Governance-Seite (Stand: 5.2.2013)

Um zu dieser Facebook Site Governance-Seite zu gelangen, musste man sich als Nutzer durch einige Seiten durchklicken.

Es stellt sich nun die Frage, ob obige Bestimmung (Zustimmung zu den AGB durch Weiterbenützung der Plattform bzw Änderungsvorbehalte) in der Form rechtlich möglich sowie ob die Vorgehensweise von Facebook überhaupt rechtlich zulässig ist und ob es zulässig ist, Änderungen auf einer anderen Seite (der Facebook Site Governance-Seite) bekanntzugeben?

Grundsätzlich werden und bleiben ABG nur Vertragsbestandteil in der Form, wie sie im Zeitpunkt des Vertragsabschlusses bestanden haben, dh die Einbeziehung geänderter AGB setzt eine neuerliche Einigung der Vertragsparteien voraus.

Abweichend davon kann bereits in den AGB ein Änderungsvorbehalt enthalten sein. Dieser ist jedoch an strenge Anforderungen gebunden und muss stets eine sachliche Rechtfertigung bzw Transparenz vorweisen, damit der Vertragspartner vorhersehen kann, unter welchen konkreten Umständen und in welchen Bereichen mögliche Änderungen bzw Adaptierungen möglich sind.

Keinesfalls möglich sind Änderungsvorbehalte, die den Nutzer schlechter stellen bzw das Ausmaß möglicher Änderungen komplett offen lassen.

Facebook versuchte zwar regelmäßig, Änderungsvorbehalte in seinen AGB zu formulieren und gab seinen Nutzern auch die Möglichkeit zur Kommentierung, doch verlangte Facebook niemals eine explizite Zustimmung der Nutzer. Auch waren Zweck und Reichweite durch obige Änderungsvorbehalte weder begrenzt, noch ist eine sachliche Rechtfertigung ableitbar, weswegen diese mE nach jedes Mal unwirksam waren. Hier sind einige Beispiele:

Version 23.9.2008: „[…] We deserve the right, at our sole discretion, to change, modify, add, or delete portions of these Terms of Use at any time without further notice. […]“

Version 1.5.2009: „[…] We can change this Statement so long as we provide notice through Facebook. […]“

Version 23.9.2009: „We can change this Statement if we provide you notice [...] and an opportunity to comment. […]“

Version 22.4.2010: „[….] We can make changes for legal or administrative reasons, or to correct an inaccurate statement, upon notice without opportunity to comment. […]“

Im Dezember 2014 gab Facebook erneut seinen Nutzern bekannt, dass diese eine Woche Zeit hätten, um die mit 1.1.2015 geplanten AGB-Änderungen zu kommentieren. Auch dieses Mal wurde lediglich von Kommentierung gesprochen, aber keine Zustimmung verlangt. Diese Vorgehensweise ist jedoch keinesfalls rechtsgültig. Entweder muss der Nutzer explizit zustimmen, etwa durch eine Opt-In Funktion, oder es muss ein wirksamer Änderungsvorbehalt vorliegen, welcher genau darlegen muss, unter welchen Umständen mit Änderungen gerechnet werden muss. Aus den obigen Auszügen ist ersichtlich, dass Facebook

regelmäßig pauschale Formulierungen verwendet, welche damit zu keiner rechtswirksamen Änderung der Nutzungsbedingungen führen.

(a) Sittenwidrigkeit als Grenze

Sittenwidrig sind in AGB solche Klauseln, in welchen sich der Betreiber einer Plattform vorbehaltlos ganz generell das Recht einräumt, seine AGB auch mit Wirkung für bestehende Verträge zu ändern.

In jedem Fall unzulässig und damit unwirksam ist es auch, die Gültigkeit „in ihrer jeweils geltenden Fassung" zu vereinbaren und dem Vertragspartner die Möglichkeit zur Kenntnisnahme und Reaktion darauf zu gewähren. Siehe dazu die Entscheidung des BGH vom 17.3.1999, IV ZR 218/97, in welcher dieser ausgesprochen hat, dass „die Anpassung durch neue, allein vom Versicherer aufgestellte Regelungen einen Eingriff in ein bestehendes Vertragsverhältnis darstellt".[198]

e. Einwilligung Minderjähriger: Zustimmungsfähigkeit Minderjähriger in die Verwendung ihrer Daten im Zuge des Abschlusses eines SNP-Nutzungsvertrages?

SNP sind nicht nur für Erwachsene interessant, sondern auch für Minderjährige. Im Zuge der Registrierung werden nicht selten Zustimmungserklärungen zur Verwendung personenbezogener Daten eingeholt, in den meisten Fällen, ohne zwischen (mündigen, unmündigen) Minderjährigen und Erwachsenen zu unterscheiden.

Ein Sonderproblem stellt daher die Frage dar, ob Minderjährige einer Verwendung ihrer Daten derart selbst zustimmen können bzw ob eine Datenverwendung, welche aufgrund mangelnder Urteils- und Einsichtsfähigkeit abgegeben wurde, mangels Rechtsgrundlage unzulässig sein soll. Der Grundgedanke des DSG ist der Anspruch auf Geheimhaltung personenbezogener Daten, welcher nach dem Gesetzeswortlaut jedermann, dh unabhängig von Alter, Herkunft oder Geschlecht, zusteht. Eine Verarbeitung und/oder Übermittlung personenbezogener Daten ist demgegenüber nur bei Vorliegen einer besonderen Rechtsgrundlage – wie insbesondere einer entsprechenden Zustimmungserklärung – zulässig.

[198] BGH 17.3.1999, IV ZR 218/97, siehe http://www.rechtzweinull.de/index.php?/archives/91-Facebook-aendert-seine-Terms-of-Service-Zulaessigkeit-der-nachtraeglichen-AEnderung-von-Allgemeinen-Geschaeftsbedingungen-AGB.html von RA Dr. *Carsten Ulbricht*.

Das DSG schreibt lediglich vor, dass das Recht auf Erteilung einer Zustimmungserklärung dem Betroffenen zusteht. Betroffener ist gem § 4 Z 3 DSG jede vom Auftraggeber (§ 4 Z 4 DSG) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (§ 4 Z 8 DSG) werden.

Als Zwischenfazit kann festgehalten werden, dass aus § 4 Z 3 und 14 DSG weder der Anspruch auf Geheimhaltung personenbezogener Daten noch das Recht auf Erteilung einer Zustimmungserklärung an bestimmte Altersgrenzen gebunden ist.

Lediglich aus § 4 Z 14 DSG ließe sich eine gewisse Altersbegrenzung ableiten, wonach zur Erteilung einer rechtsgültigen Willenserklärung Handlungsfähigkeit notwendig ist, was somit bedeuten würde, dass die Zustimmungsfähigkeit im Datenschutzrecht Handlungsfähigkeit erfordert. Offen ist jedoch die Frage, welche Form der Handlungsfähigkeit im Datenschutzrecht anzuwenden sein soll.

Handlungsfähigkeit ist die Fähigkeit, durch eigenes Verhalten Rechte und Pflichten zu begründen. Erst mit der Vollendung des 18. Lebensjahres erreicht man die volle Handlungsfähigkeit. Innerhalb der Handlungsfähigkeit wird weiter in Geschäftsfähigkeit und Deliktsfähigkeit unterschieden. Aus § 170 ABGB ergibt sich, dass hinsichtlich des Abschlusses von Rechtsgeschäften zwischen geschäftsunfähigen Kindern (bis sieben Jahre), unmündigen Minderjährigen (bis 14 Jahre) und mündigen Minderjährigen unterschieden wird.

Bei Anwendung dieses Systems auf die notwendige datenschutzrechtliche Zustimmungserklärung kommt man schließlich zum Ergebnis, dass Kinder generell aufgrund ihres zu geringen Alters von der Abgabe einer Zustimmungserklärung ausgeschlossen sind. Das bedeutet, dass Kinder keinesfalls einer Datenverwendung selbst zustimmen können. Diese kann lediglich durch vertretungsbefugte Personen erfolgen.

Für Zustimmungserklärungen mündiger Minderjähriger ist deren Einsichts- und Urteilsfähigkeit relevant. Wenn diese gegeben ist, sollte von einer Verfügungsmöglichkeit über die eigenen personenbezogenen Daten ausgegangen werden.

Während bei der Verwendung nicht-sensibler Daten die alleinige Zustimmung des einsichts- und urteilsfähigen Minderjährigen ausreichend ist, bedarf die Zustimmung zur Verwendung sensibler Daten zu ihrer Rechtswirksamkeit zusätzlich der Genehmigung des gesetzlichen Vertreters.

Wurde schließlich eine Zustimmungserklärung nicht gültig erteilt oder eine gültige Zustimmung widerrufen, so dürfen die Daten nicht verwendet werden. Dem Betroffenen steht das Recht auf Löschung nach § 27 DSG sowie ein Anspruch auf Unterlassung und Beseitigung nach § 32 Abs 2 DSG zu. Diese Rechte sind gegenüber einem privaten Auftraggeber gem § 32 DSG gerichtlich geltend zu machen.

Zusammengefasst bedeutet dies, dass die Frage, ob und wann ein Minderjähriger eine datenschutzrechtliche Zustimmungserklärung rechtswirksam abgeben kann, nach dem DSG nicht konkret geregelt ist. Als Anhaltspunkte sind somit die individuelle Einsichts- und Urteilsfähigkeit des Minderjährigen heranzuziehen.

Sonntag zieht eine Analogie zu § 146 c ABGB, welcher bestimmt, dass Minderjährige ihre Zustimmung zu einer medizinischen Behandlung selbst abgeben können, soweit Einsichts- und Urteilsfähigkeit gegeben ist, und erklärt, dass Minderjährige ab sieben Jahren selbst einer Datenverwendung zustimmen können, wenn Einsichts- und Urteilsfähigkeit gegeben ist, was von Gesetzes wegen ab 14 Jahren vermutet wird. Für *Sonntag* müssen Informationen daher umso klarer und eindeutiger sein und Belastungen durch die Zustimmung umso geringer, je jünger die betroffene Person ist. Für ihn ist daher eine alleinige Zustimmung hinsichtlich sensibler oder bonitätsrelevanter Daten unter 14 Jahren nicht möglich.[199]

Trotz allem sollte die Schutzbedürftigkeit der Minderjährigen im Vordergrund stehen und sollten SNP daher technische Möglichkeiten anbieten, um dem Schutzbedürfnis zu entsprechen und übereilte Einwilligungen bzw Zustimmungen zu vermeiden.

f. Rechtliche Analyse von Auszügen der Allgemeinen Geschäftsbedingungen/ Facebook-Datenschutzrichtlinien[200]

(1) Ad Vertragliche Zustimmung zur Verwendung von Daten, „IP-Lizenz von Facebook“

Facebook statuiert in seinen Nutzungsbedingungen hinsichtlich der Inhalte und Informationen seiner Nutzer, dass diese Facebook eine „nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz zur Nutzung jeglicher IP-Inhalte, die [du] auf oder im Zusammenhang mit Facebook postest (IP-Lizenz)“ einräumen.

[199] *Sonntag*, Einführung in das Internetrecht (2009) 239.
[200] http://www.facebook.com/policy.php (Stand: 22.12.2010).

Dh Facebook räumt sich mit dieser Klausel eine generelle unentgeltliche Befugnis ein, alle von den Facebook-Mitgliedern eingestellten urheberrechtlich geschützten Werke (insbesondere Fotos und Videos) weltweit verwenden zu dürfen.

Grundsätzlich lässt sich festhalten, dass Datenverwendungsklauseln aufgrund der Privatautonomie und Vertragsfreiheit solange zulässig sind, als sie nicht der Privatsphäre Dritter widersprechen, Regeln des Daten- und Konsumentenschutzes gerecht werden und ausreichend konkret bestimmen, um welche Daten es sich handelt und zu welchem Zweck diese verwendet werden sollen.

Obige Bestimmungen führen jedoch zu enormen Unklarheiten, insbesondere betreffend die Frage, welche konkreten Rechte sich Facebook dadurch an den von Nutzern hochgeladenen Fotos etc einräumen möchte.

Auch können Probleme dort entstehen, wo Facebook – die für einen bestimmten Zweck erlaubten – Daten für einen anderen Zweck verwendet oder verknüpft. Zu dieser zweiten Frage gleich weiter unten.

Das LG Berlin hat obige Klausel bereits für unwirksam erklärt mit der Begründung, dass die Klausel gegen die Generalklausel des § 307 Abs 2 Nr. 1 BGB verstoße. § 307 Abs 2 BGB ist dem österreichischen § 879 Abs 3 ABGB vergleichbar[201] und bestimmt, dass Bestimmungen in Allgemeinen Geschäftsbedingungen dann unwirksam sind, wenn sie den Vertragspartner des Verwenders entgegen den Geboten Treu und Glauben unangemessen benachteiligen, indem sie entweder mit wesentlichen Grundgedanken der gesetzlichen Regelung unvereinbar sind oder wesentliche Rechte und Pflichten, die sich aus der Natur des Vertrages ergeben, derart einschränken, dass die Erreichung des Vertragszwecks gefährdet ist.
Im konkreten Fall beanstandete das LG Berlin, dass aus obiger Klausel nicht zum Ausdruck komme, welche konkreten urheberrechtlichen Nutzungsrechte an Facebook übertragen werden sollen, obwohl der Umfang der einzuräumenden Rechte bestimmt sein müsse.

Das LG Berlin sprach in obiger Entscheidung 16 O 551/10 auch aus, dass sich Facebook kein umfassendes weltweites und kostenloses Nutzungsrecht an Inhalten von Nutzern einräumen

[201] § 879 ABGB bestimmt, dass ein Vertrag, der gegen ein gesetzliches Verbot oder gegen die guten Sitten verstößt, nichtig ist.

dürfe. Nach Ansicht des Gerichts seien die Nutzer Urheber ihrer Bilder oder selbst komponierten Musiktitel, weswegen Facebook diese Werke nur nach ausdrücklicher Genehmigung der Urheber/Nutzer verwenden dürfe.[202]

Hinsichtlich der zweiten Frage, was die Folgen wären, wenn Facebook Daten, welche – erlaubterweise für einen bestimmten Zweck verwendet werden dürfen – für einen anderen Zweck verwendet bzw verknüpft und ob durch die Zustimmung des Betroffenen die Verwendung von Datensätzen, die durch Verknüpfung entstanden sind, noch gedeckt ist, was ich persönlich ablehne.

Fall ein Facebook-Nutzer seine Erlaubnis zur Datenverwendung für einen ganz bestimmten Zweck erteilt, dann ist mE die Weitergabe von Daten an einen Dritten bzw ein anderes Unternehmen zu einem anderen Zweck, der mit dem ursprünglichen in keinem Zusammenhang steht, nicht mehr vom Willen des betroffenen Nutzers umfasst, was folglich zu einem zivilrechtlichen Willensmangel führen muss.

(2) Sicherungskopien

Unter dem Punkt „Sicherungskopien" führte Facebook in seiner Datenschutzrichtlinie[203] aus: *„Entfernte oder gelöschte Daten können für eine Dauer von max. 90 Tagen noch in Sicherungskopien vorhanden sein, stehen jedoch anderen nicht mehr zur Verfügung."*

Facebook schrieb damit vor, dass von Nutzern gelöschte bzw entfernte Daten bis zu einer „maximalen Dauer von 90 Tagen als Sicherungskopien" gespeichert bleiben.

Das Grundrecht auf Datenschutz regelt, dass „jedermann ein Geheimhaltungsinteresse hinsichtlich seiner personenbezogenen Daten" hat bzw dass jedermann das Recht auf Löschung unzulässigerweise verarbeiteter Daten hat. Facebook verstößt mit seinen AGB daher gegen diese Bestimmung, da vom Nutzer entfernte bzw gelöschte Daten unzulässig verarbeitet werden, indem Facebook Sicherungskopien dieser Daten aufbewahrt.

Diese Bestimmung der Datenschutzrichtlinie ist daher mE rechtswidrig.

[202] Siehe LG Berlin 6.3.2012, 16 O 551/10; derzeit noch anhängig am KG Berlin 5 U 42/12.
[203] Siehe Facebook Datenschutzrichtlinie, Punkt „Sicherungskopien" (Stand: 29.10.2009).

Mittlerweile wurden die Datenverwendungsrichtlinien umgeschrieben und steht nunmehr unter dem Punkt „Löschung“: *„Wenn du ein Konto löscht, wird es dauerhaft von Facebook gelöscht. Normalerweise dauert es ungefähr einen Monat bis eine Kontolöschung vollzogen ist. Manche Daten sind jedoch noch bis zu 90 Tage in Sicherungskopien und Protokolldateien vorhanden. […]“*[204]

[204] Facebook Datenverwendungsrichtlinien (Stand: 9.10.2012).

3. Das virtuelle Leben nach dem Tod

Für immer mehr Menschen sind SNP wichtiger Bestandteil ihres realen Lebens, aber was passiert im Falle des Todes eines Nutzers mit seiner „digitalen Verlassenschaft"? Ist die Ansicht des Salzburger Richters und Internet-Rechtsexperten *Schmidbauer* richtig, dass „Nutzungsprofile in Netzwerken höchstpersönliche Rechte sind, welche somit mit dem Tod enden"?[205]

Auf der einen Seite stellt sich – sowohl auf Betreiber- als auch auf Hinterbliebenenseite – die Frage, ob mit dem Tod eines Nutzers ipso iure ein Offline-Status des Profils eintritt bzw ob der Betreiber der SNP den Account automatisch löschen darf/muss, und auf der anderen Seite ist zu hinterfragen, wie mit den Daten des verstorbenen Nutzers umzugehen ist, ob diese automatisch gelöscht werden bzw wer das Recht haben soll, die entsprechenden Passwörter zu erfahren, um das Profil einer verstorbenen Person zu löschen?

Der Gesetzgeber hat sich dem Themenkomplex der virtuellen Verlassenschaft noch nicht konkret gewidmet, auch wurde die Frage, ob es sich bei einer SNP um ein „typisches" höchstpersönliches Recht handelt, noch nicht konkret beantwortet.

In der Folge sollen die damit verbundenen Probleme im Lichte der Persönlichkeits-, Datenschutz- und Urheberrechte sowie des Erbrechts beleuchtet werden.

a. Das virtuelle Leben nach dem Tod im Sinne von Facebook

(1) Facebook-Konten im Gedenkzustand

Facebook war eine der ersten SNP, welche sich mit dem Thema „Tod eines Nutzers" beschäftigte und versuchte, eine „passende" Lösung zu finden, seinen Nutzern bzw deren Hinterbliebenen eine Möglichkeit anzubieten, ein Konto eines verstorbenen Nutzers in einer gewissen Art und Weise weiterzuführen oder dieses zu schließen.

Als Anstoß dazu kann das Massaker an der Virginia Tech[206] angesehen werden, wo unzählige Nutzer Nachrichten auf den Pinnwänden Verstorbener hinterließen und die Pinnwand damit als eine Art „Kondolenzbuch" verwendeten. Facebook wollte eine Möglichkeit schaffen, dass

[205] *Schmidbauer*, Profile in Social Networks vererben, e-center law survey, http://www.e-center.co.at/static/files/e-center%20law%20survey% 2010-2010.pdf (Stand: 22.6.2010).
[206] Am 16.4.2007 hat ein Amoklauf an der Virginia Tech, USA, stattgefunden, bei welchem 32 Menschen getötet und 29 weitere verletzt wurden.

das Konto eines verstorbenen Nutzers von einem Verwandten oder Freund in eine Art „Gedenkbuch“ umgewandelt und damit grds aufrechterhalten werden kann. Facebook verlangt dafür lediglich einen Nachweis über das Versterben eines Nutzers. Das Profil wird sodann in eine „virtuelle Gedenkstätte“ umgewandelt. Danach ist ein weiteres Einloggen unmöglich, Kontaktinformationen und Status-Updates werden gelöscht, das Profil wird aus allen Gruppen entfernt, denen der verstorbene Nutzer angehörte, und die restlichen Inhalte sind nur noch für bereits bestätigte Freunde sichtbar.

Facebook schrieb im Jahr 2011 in seiner Datenschutzrichtlinie „Konten im Gedenkzustand“[207]: *„Wird Facebook über den Tod eines Nutzers benachrichtigt, kann das Unternehmen das Konto des Nutzers zu seinem Gedenken aufrechterhalten. In diesen Fällen schränkt Facebook den Profilzugriff auf bestätigte Freunde ein, damit Freunde und Verwandte im Gedenken an den verstorbenen Nutzer an seine Pinnwand schreiben können.“*

Facebook erklärte weiters, *„Auf entsprechende, förmliche Anfrage der nächsten Angehörigen des verstorbenen Nutzers oder einen anderen rechtmäßigen Antrag kann Facebook das Konto schließen.“*[208]

Zur Identifikation des Profils verlangt Facebook den vollständigen Namen, das Geburtsdatum sowie die E-Mail-Adresse des Verstorbenen, welche zur Anmeldung verwendet wurden. Als Todesnachweis muss eine Todesanzeige oder eine Kopie eines Nachrichtenartikels vorgelegt werden.

Aus obiger Formulierung ergibt sich jedoch, dass sich Facebook grundsätzlich nicht verpflichten wollte, ein Konto schließen zu müssen: „[…] kann Facebook das Konto schließen […]“. Vielmehr behielt sich Facebook die Entscheidung vor, erst nach Überprüfung und Feststellung des Versterbens eines Nutzers das Konto zu schließen bzw in einen Gedenkzustand zu versetzen.

---

[207] Facebook, Datenschutzrichtlinien Facebook, http://www.facebook.com/policy.php, Punkt 5 (Stand: 28.6.2011).

[208] Facebook hat eine Änderung der Datenverwendungsrichtlinien vorgenommen und den Text folgendermaßen adaptiert (Facebook, Datenverwendungsrichtlinien Facebook, http://de-de.facebook.com/full_data_use_policy, Punkt 6 (Stand: 11.12.2012): „Wir können das Konto einer verstorbenen Person in den Gedenkzustand versetzen. Wenn wir ein Konto in den Gedenkzustand versetzen, bleibt die betreffende Chronik auf Facebook bestehen; allerdings schränken wir den Zugriff und einige Funktionen ein. Du kannst die Chronik eines verstorbenen Nutzers hier melden: https://www.facebook.com/help/contact.php?show_form=deceased
Wir können ein Konto auch schließen, wenn wir eine formelle Aufforderung erhalten, die bestimmte Kriterien erfüllt.“

(2) „Testament-Funktion“ bei Facebook

Im Februar 2015 führte Facebook schließlich eine neue Funktion zur „Nachlassverwaltung“ eines Facebook-Profils ein: Diese Funktion soll die Möglichkeit eröffnen, eine bestimmte Person als Kontaktperson im Todesfall anzugeben, damit sich diese im Falle des Ablebens – im Sinne der erteilten Berechtigungen durch den Verstorbenen – um die Seite des Verstorbenen und damit um seinen digitalen Nachlass (weiter) kümmern kann.

Bisher gab es eben nur die sehr eingeschränkte Möglichkeit, das Facebook-Profil einer verstorbenen Person als simple „Gedenkstätte“ weiterzuführen, indem Angehörige oder Freunde Facebook auf das Ableben hinwiesen und Facebook schließlich das Profil in eine Art digitale Gedenkstätte umwandelte. Veränderungen hinsichtlich bereits hochgeladener Fotos etc können in diesem Zusammenhang aber nicht vorgenommen werden.

Mit der neuen Funktion kann nun vom Facebook-Nutzer vorab bestimmt werden, wer das Profil nach dem Ableben verwalten soll. Facebook wandelt zwar weiterhin das Profil des Verstorbenen in eine Gedenkstätte um, doch haben Angehörige nun viel mehr Möglichkeiten, wenn ein Nachlassverwalter bestimmt wurde. Der mit der Aufgabe Betraute kann etwa das Profilbild ändern und eine Status-Meldung posten, etwa zu Details der Trauerfeierlichkeiten oder eine Abschiedsnachricht. Zudem kann er im Namen des Profils auf Pinnwand-Einträge antworten. Auch Freundschaftsanfragen bisher nicht verknüpfter Angehöriger können angenommen werden.

Ausgenommen sind persönliche Nachrichten, diese werden dem „Nachlassverwalter“, wie ihn Facebook nennt, nicht zur Verfügung gestellt. Die Privatsphäre des Verstorbenen soll nach Angaben von Facebook auf jeden Fall erhalten bleiben: Der Verwalter erhält nicht den vollen Zugriff auf das Profil. So ist es eben nicht möglich, persönliche Nachrichten zu lesen. Auch Änderungen der Einstellungen des Accounts bleiben dem Verwalter verwehrt.

Der Nachlassverwalter tritt wie ein Fanpage-Manager auf, dh er kann sich nicht mit dem Namen des Verstorbenen einloggen. Durch den Zusatz „Remembering“ (In Erinnerung) beim Namen wird darauf hingewiesen, dass es sich um die Gedenkstätte der verstorbenen Person handelt.

Der Nachlassverwalter muss im Falle des Todes des Nutzers Facebook das Ableben melden. In dem entsprechenden Kontaktformular muss ein Beweis für das Ableben des Betreffenden erbracht werden.

Diese neue Funktion wurde zunächst nur für die USA eröffnet. Es sollen aber auch andere Länder hinzukommen.

Eine weitere Neuigkeit war, dass jeder Nutzer festlegen kann, ob das eigene Profil nach dem Tod gelöscht werden soll.

b. Das virtuelle Leben nach dem Tod im Lichte des Erbrechts

Abgesehen von der von Facebook angebotenen „Testament-Funktion" ist vorab zu klären, ob Nutzerprofile zu den vermögenswerten Rechten zählen, welche vererblich sind, oder zu höchstpersönlichen Rechten, die idR nach dem Tod enden (*Welser* in *Rummel*[3] § 531 ABGB Rz 6).

(1) Vererbung eines SNP-Profils mittels Testament

Unter Nachlass werden alle Vermögensrechte und Verbindlichkeiten des Verstorbenen verstanden, welche im Wege der Gesamtrechtsnachfolge auf den Erben übergehen sollen.

Wesentlich ist daher, dass einem SNP-Profil ein gewisser Vermögenswert zuerkannt werden muss, um überhaupt in den Nachlass fallen zu können. Doch welche Faktoren führen zu einem Vermögenswert, sind es die Datenmengen bzw Kontakte, die ein Profil „kostbar" machen? Und ist ein Profil, welches lediglich als Zeitvertreib dienen soll und auf welchem kaum Fotos oder Videos hochgeladen wurden, automatisch vermögenslos?

Ich vertrete die Ansicht, dass SNP-Profile einen Vermögenswert haben und damit in den Nachlass fallen. Eine Vererbung ist damit mE möglich, in Betracht käme auch eine Vererbung unter Auftrag:

§ 709 ABGB normiert, dass der Erblasser „jemandem einen Nachlass unter einem Auftrage zuwenden kann […]", dh der Erbe muss zuerst den vom Erblasser bestimmten Auftrag erfüllen, um in den Genuss des Nachlasses zu kommen. Das Erbe steht in dem Fall unter einer auflösenden Bedingung.

Nutzer von SNP können mE ihren Account mittels Auflage iSd § 709 ABGB vererben. „Bei einer Auflage muss der Bedachte ein bestimmtes Verhalten setzen“, so *Zankl*,[209] zB durch Nennung der Zugangsdaten zu einem Account uÄ.

Zankl ist der Ansicht, dass die „Weiternutzung von Sozialen Netzwerkprofilen in der Tat in den Bereich des höchstpersönlichen Lebensbereiches fällt“. Im Wege einer Universalsukzession (Gesamtrechtsnachfolge) könnten seiner Ansicht nach Profile gelöscht werden, da derartige „Profile sonst ewig weiterbestehen können“, was seiner Ansicht nach widersinnig wäre.[210]

(2) Kein Testament

Wenn man davon ausgeht, dass SNP-Profile einen Vermögenswert haben, stellt sich die Frage, was mit diesen passiert/passieren soll, wenn kein Testament vorliegt. Vermögensrechtliche Rechte und Pflichten sind ja nach hM vererblich[211].

Wenn ein Angehöriger trotz fehlendem Testament oder einer sonstigen Vorkehrung Zugriff auf das Konto eines Verstorbenen erhalten möchte, dann müssten die gesetzlichen Erben im Rahmen einer Gesamtrechtsnachfolge, so *Zankl*[212], das Profil des Verstorbenen jedenfalls löschen lassen. Gemäß *Zankl* bleibt es aber unklar, was passieren soll, wenn die Angehörigen den Account des Verstorbenen weiterführen möchten, dieser aber keine diesbezüglichen Regelungen getroffen hat.[213]

Ich schließe mich dem an und bin grundsätzlich der Ansicht, dass ein SNP-Profil einen Vermögenswert haben kann und damit vererblich ist. Wenn nun vom verstorbenen Nutzer keine Vorkehrung, sei es in Form eines Testaments oder direkt über die Plattform, getroffen wurde, dann sollte mE der Account per gesetzlicher Erbfolge an die Erben übertragen werden, damit diese das Profil – jedoch nur noch in Form einer Gedenkstätte – weiterführen können.

---

[209] *Zankl*, Bürgerliches Recht[6] (2012) Rz 498.
[210] *Zankl* mit Verweis auf *Schmidbauer*, unter e-center law survey, http://www.e-center.co.at/static/files/e-center%20law%20survey%2010-2010.pdf (Stand: 22.6.2010).
[211] *Koziol/Welser*, Bürgerliches Recht II[13] (2007) 446 ff; siehe auch *Zankl*, Bürgerliches Recht[6] (2012) Rz 474.
[212] ao. Univ.-Prof. Dr. *Wolfgang Zankl* (Rechtswissenschaftliche Fakultät der Universität Wien, E-center law survey team), e-center law survey 10-2010, Profile in Social Networks vererben, Punkt 2, http://www.e-center.co.at/static/files/e-center%20law%20survey%2010-2010.pdf (Stand: 26.7.2011).
[213] E-center law survey team, e-center law survey 10-2010, Profile in Social Networks vererben, Punkt 2, http://www.e-center.co.at/static/files/e-center%20law%20survey%2010-2010.pdf (Stand: 26.7.2011).

(3) Passwort-Vererben bzw -Erben

In diesem Kapitel soll näher auf die Problematik des Passwort-Vererbens bzw -Erbens eingegangen und die Frage behandelt werden, ob computerbezogene bzw computergestützte Güter hinterlassen werden können und ob es möglich ist, digitale Güter zu vererben?

§ 531 ABGB normiert, dass „alle Rechte und Verbindlichkeiten eines Verstorbenen, sofern sie nicht in bloß persönlichen Verhältnissen begründet sind, die Verlassenschaft oder der Nachlass einer Person sind“.[214]

Es stellt sich nun die Frage, ob auch digitale Rechte unter den Begriff „Rechte“ und damit in den Nachlass bzw in eine Verlassenschaft fallen? Grundsätzlich fallen alle vererblichen, vermögenswerten Rechte und Pflichten im Todeszeitpunkt des Verstorbenen in den Nachlass gem § 531 ABGB. Es muss daher eine Abgrenzung danach erfolgen, ob es sich bei den digitalen Gütern um solche handelt, die „private Vermögensrechte und Verbindlichkeiten“ darstellen. Eine Erbschaft wird durch deren Einantwortung und damit der Übergabe in den rechtlichen Besitz erworben.

Unter der Universalsukzession versteht man, dass man als Erbe in die Rechtsstellung des Erblassers tritt. Damit gehen alle Rechte und Pflichten mit Drittwirkung auf den Erben über. Es kommt zu einer Art Personenidentität zwischen Erblasser und Erben.[215]

§ 547 ABGB schreibt vor, dass „der Erbe, sobald er die Erbschaft angenommen hat, in Rücksicht auf dieselbe den Erblasser vorsteht. Beide werden in Beziehung auf einen Dritten für eine Person gehalten. Vor der Annahme des Erben wird die Verlassenschaft so betrachtet, als wenn sie noch von dem Verstorbenen besessen würde. […]“

Können Rechte von SNP auf einen Erben übertragen werden? Sind höchstpersönliche Rechte[216] an einem „digitalen bzw Online-Account“ grundsätzlich auch vererbbar?

Vererblich sind gem § 1448 ABGB grundsätzlich nur vermögensrechtliche Rechte und Verbindlichkeiten. § 1448 ABGB normiert, dass durch den Tod eines Menschen Rechte und Verbindlichkeiten erlöschen, „welche auf die Person eingeschränkt sind, oder die bloß persönliche Handlungen des Verstorbenen betreffen“. Daraus kann geschlossen werden, dass grundsätzlich höchstpersönliche Rechte und Verbindlichkeiten nicht vererbbar sein sollen.

[214] Siehe dazu *Zankl*, Bürgerliches Recht[6] (2012) Rz 473.
[215] Siehe dazu *Zankl*, Bürgerliches Recht[6] (2012) Rz 472.
[216] Siehe § 531 ABGB.

Bydlinski hat sich mit der Problematik des Vererbens höchstpersönlicher Rechte (ohne konkret auf SNP einzugehen) auseinandergesetzt und festgestellt, dass eine Vererbung höchstpersönlicher Rechte, die mit der Person und deren immateriellen Gütern unmittelbar verbunden sind, nicht in Betracht kommt. Nahe Angehörige des Verstorbenen kämen für die Wahrnehmung des Schutzes der persönlichen Rechte des Verstorbenen in Frage. *Bydlinski* führt weiters aus, dass dieser Grundsatz aus dem StGB bzw UrhG per analogiam abzuleiten sei, da diese Gesetze ausdrückliche Regeln zum Schutz der persönlichen Interessen nach dem Tod des Trägers enthalten.[217]

(4) Passwort-Aufbewahrungs-Services

Es gibt mittlerweile Online-Portale (Webseiten)[218], welche die Übergabe von Passwörtern an zuvor bestimmte Personen nach dem Todesfall anbieten. Dieser Service erfolgt idR gegen eine monatliche oder jährliche Gebühr. Die Übergabe des Passworts erfolgt üblicherweise gegen Vorlage einer Todesanzeige.

Diese „Passwort-Aufbewahrungs-Unternehmen" haben sich darauf spezialisiert, das virtuelle Leben eines Verstorbenen zu „regeln", indem sie den „Online-Freundeskreis" des Verstorbenen über dessen Ableben informieren und seine „Online-Verlassenschaft" organisieren.

Beispiel Deathswitch[219]:

Deathswitch ist ein Internet-Portal, auf welchem Daten und persönliche Nachrichten „hinterlegt" werden können. Bei Deathswitch muss auf E-Mails des Unternehmens geantwortet werden, um zu bestätigen, dass kein Todesfall eingetreten ist. Bleiben wiederholt Antworten aus, dann wird von einem Todesfall ausgegangen und die hinterlegten Informationen werden an zuvor bestimmte Personen ausgehändigt.

Beispiel My Webwill[220]:

---

[217] *Bydlinski*, Paradoxer Geheimnisschutz post mortem? JBl 1999 (553) und *Handler*, Der Schutz von Persönlichkeitsrechten (2008) 69 ff.

[218] Lastmessage.de, legacylocker.com, deathswitch.com ua bieten derartige Services an.

[219] http://deathswitch.com, *„A deathswitch is information insurance. Don't die with secrets that need to be free"*. Eingangszitat auf der Webseite (Stand: 26.10.2011).

[220] https://www.mywebwill.com (Stand: 26.10.2011).

My Webwill ist ein schwedisches Online-Unternehmen, welches seinen Kunden die Möglichkeit bietet, Verfügungen über das „Online-Leben“ nach dem Tod zu treffen. Man kann zwischen „Deaktivieren, Ändern oder Übertragen“ der Online-Accounts wählen.

c. Das virtuelle Leben nach dem Tod im Lichte des Datenschutzrechts

Das Grundrecht auf Datenschutz besagt in § 1 DSG, dass *„Jedermann, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat, soweit ein schutzwürdiges Interesse daran besteht.“* Es handelt sich damit um ein sog „höchstpersönliches Recht“, welches an eine bestimmte Person *(„… der ihn betreffenden Daten …“)* gebunden ist und damit grundsätzlich weder übertragbar, noch vererblich ist. *Jahnel* spricht von einem „Menschenrecht“ und bezieht sich dabei auf den Teil der Gesetzesbestimmung „Jedermann hat“. Er führt aus, dass es sich gemäß bisheriger Judikatur und Literatur um ein „höchstpersönliches Recht handelt, das mit dem Tod des Betroffenen erlischt und nicht auf Rechtsnachfolger übergeht“.[221] Von dieser Höchstpersönlichkeit ausgehend kann nur eine lebende Person Träger des Grundrechts sein. Aufgrund dieser Höchstpersönlichkeit kann argumentiert werden, dass das Grundrecht auf Datenschutz mit dem Tod eines Nutzers einer SNP „erlischt“, da höchstpersönliche Rechte nicht übertrag- bzw vererbbar sind.

Wenn man diesen Gedanken weiter verfolgt, so muss davon ausgegangen werden, dass der Datenschutz und damit der Schutz der personenbezogenen Daten auch nur bis zum Tod einer Person gegeben ist. Dementsprechend stellt sich die Frage, ob gespeicherte „personenbezogene“ Daten auf einer SNP nach dem Ableben des Nutzers nicht mehr geschützt sind.

Wenn man hingegen der Sichtweise folgt, dass auch nach dem Tod eines Nutzers ein mittelbarer Schutz gegeben ist, wenn die Daten eines verstorbenen Nutzers auch personenbezogene Daten über eine andere Person enthalten, dann könnte wiederum ein Konnex zu einem lebenden Grundrechtsträger hergestellt und ein Schutz gebildet werden.[222]

Ich folge der Sichtweise bezüglich des mittelbaren Schutzes nach dem Tod eines Nutzers, denn nur so kann mE auch gewährleistet werden, dass Daten eines verstorbenen Nutzers auch nach seinem Tod weiterhin unter Schutz stehen.

---

[221] *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Heinz Schäffer (2006) 315.
[222] Vgl *Thiele*, Der digitale Nachlass – Erbrechtliches zum Internet und seinen Diensten, jusIT 2010, 167 f.

d. Das virtuelle Leben nach dem Tod im Lichte der Persönlichkeitsrechte

In § 16 ABGB ist bestimmt, dass *„Jeder Mensch angeborene, schon durch die Vernunft einleuchtende Rechte hat, und daher als eine Person zu betrachten ist. [...]"* Lediglich der Wortwahl folgend müsste daraus geschlossen werden, dass nur ein „Mensch" Inhaber von Persönlichkeitsrechten sein kann und dass mit dem Tod auch die Persönlichkeit des Menschen erlischt. Dies würde bedeuten, dass die daran angeknüpften Persönlichkeitsrechte, das sind subjektive Rechte nicht vermögensrechtlicher Natur, welche untrennbar mit der physischen oder juristischen Person verbunden, unübertragbar und verzichtbar sind, aufgrund ihrer Höchstpersönlichkeit unvererblich sind.

Wie *Rest* betont, steht aber die Unvererblichkeit eines Persönlichkeitsrechts nach herrschender Judikatur einem „postmortalen Persönlichkeitsschutz nicht entgegen, denn Persönlichkeitsrechte haben den Zweck, die freie Entfaltung der Persönlichkeit möglichst weitgehend zu gewährleisten" und dafür diene ein postmortales Persönlichkeitsrecht.[223]

Nach stRsp wird daher ein „nach dem Tod bestehendes Persönlichkeitsrecht" als fortbestehendes Abwehrrecht zum Schutz von Verstorbenen zum Teil anerkannt. Der rechtliche Schutz und die Geltendmachung von Ansprüchen iZm §§ 16, 43, 1330 ABGB und § 78 UrhG enden daher nicht mit dem Tod. Der Verstorbene kann seine Persönlichkeitsrechte aber nicht mehr selbst ausüben, sodass seine Interessen von seinen Erben wahrgenommen werden müssen, auch wenn sich deren Interessen, wie *Handler* treffend feststellte, von jenen des Verstorbenen unterscheiden können. Er führt weiter aus, dass sich das „Eigeninteresse der Angehörigen wohl des Öfteren mit den Interessen des Verstorbenen nicht decken wird".[224]

Der OGH hat zB in seiner Entscheidung vom 25.5.2000, 1 Ob 341/99 z, von einem „fortwirkenden Persönlichkeitsrecht" gesprochen. Der Angehörige eines Verstorbenen behauptete, er habe das Recht auf Einsichtnahme in die Krankengeschichte eines Verstorbenen. Der OGH lehnte dieses Recht auf Einsicht jedoch mit der Begründung ab, es bestehe ein postmortales Persönlichkeitsrecht und es sei eine Einsicht in die Unterlagen daher abzulehnen.

In einer anderen Entscheidung geht der OGH noch weiter und erkennt:

---

[223] *Rest*, Postmortaler Persönlichkeitsschutz – ein Überblick, medien und recht 2012, 113 f.
[224] *Handler*, Der Schutz von Persönlichkeitsrechten (2008) 63.

„Persönlichkeitsrechte haben insgesamt den Zweck, die freie Entfaltung der Persönlichkeit möglichst weitgehend zu gewährleisten. Dieses Ziel kann nur verwirklicht werden, wenn auch nach dem Tod ein gewisser Schutz bestehen bleibt. Dies gilt insbesondere für den Schutz der Ehre und der Privatsphäre des Verstorbenen. Nahe Angehörige sind nur befugt, die Rechte des Verstorbenen wahrzunehmen. Ihnen und Erben kann insoweit, als die Wahrung der Geheimsphäre gerade ihnen gegenüber erfolgen sollte, ein Verzicht darauf nicht zustehen."[225]

Die Judikatur anerkennt mE richtigerweise das Fortwirken der Persönlichkeitsrechte des Menschen über seinen Tod hinaus, damit insbesondere die Persönlichkeitsrechte des Verstorbenen einen fortwährenden Schutz genießen können.

In Anlehnung an die bereits gefestigte deutsche Judikatur hat sich auch in Österreich unter Zugrundelegung der §§ 16, 43 und 1130 Abs 1 und 2 ABGB und § 78 UrhG eine Rechtsprechung zur Geltendmachung des Persönlichkeitsrechts Ehre durch nahe Angehörige entwickelt, so *Rest*.[226] In der Entscheidung 6 Ob 283/01 p hat der OGH ausgesprochen, dass „eine zeitliche Begrenzung des umfassenden Schutzes der Menschenwürde auf das Leben nicht zu erkennen und die Unantastbarkeit der Menschenwürde für den österreichischen Rechtsbereich in § 16 ABGB festgeschrieben sei. So sei das fortwirkende Lebensbild eines Verstorbenen wenigstens gegen grob ehrverletzende Beeinträchtigungen geschützt".[227]

Gemäß herrschender Judikatur[228] erlöschen höchstpersönliche Rechte, wie insbesondere das Recht auf Ehre, nach dem Tod nicht und bestehen in einem gewissen Umfang weiter.

Ich bin derselben Ansicht, da mE die Menschenwürde mit dem Tod nicht verloren geht oder einfach erlischt, sondern über den Tod hinaus wirkt. Persönlichkeitsrechte sollten daher mE fortdauern.

e. Das virtuelle Leben nach dem Tod im Lichte des Urheberrechts

In den Sonderbestimmungen des UrhG, im Speziellen dem Brief- und Bildnisschutz nach den §§ 77 und 78 UrhG, ist geregelt, dass „auch nahe Angehörige bei Verletzungen berechtigter

[225] OGH 23.5.1984, 1 Ob 550/84.
[226] *Rest*, Postmortaler Persönlichkeitsschutz – ein Überblick, medien und recht 2012, 113.
[227] OGH 29.8.2002, 6 Ob 283/01p: Das Lebensbild des Verstorbenen *Omofuma* sei dadurch entstellt worden, dass behauptet wurde, er sei Drogendealer gewesen und habe Kinderleben ruiniert.
[228] Die Rechtsprechung in Deutschland anerkennt bereits seit der Entscheidung BGHZ 15, 249 (259–262), *Cosima Wagner*, ein allgemeines postmortales Persönlichkeitsrecht.

Interessen des Abgebildeten bzw des Verfassers oder Adressaten Unterlassungs-, Beseitigungs- und Schadenersatzansprüche haben".

§ 77 UrhG normiert in Abs 1, dass *„Briefe, Tagebücher und ähnliche vertrauliche Aufzeichnungen weder öffentlich vorgelesen, noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden dürfen, wenn dadurch berechtigte Interessen des Verfassers oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden."*

Abs 2: *„Nahe Angehörige im Sinn des Abs 1 sind die Verwandten in auf- und absteigender Linie sowie der überlebende Ehegatte oder Lebensgefährte. Die mit dem Verfasser im ersten Grade Verwandten und der überlebende Ehegatte oder Lebensgefährte genießen diesen Schutz Zeit ihres Lebens, andere Angehörige nur, wenn seit dem Ablauf des Todesjahres des Verfassers zehn Jahre noch nicht verstrichen sind."*

Es kann daher aus § 77 UrhG geschlossen werden, dass urheberrechtlich geschützte Werke, wie Briefe, Tagebücher etc., nur mit Zustimmung des Verfassers und, wenn dieser bereits verstorben ist, mit der Zustimmung seiner nahen Verwandten veröffentlicht werden dürfen, dh das UrhG räumt auch nahen Angehörigen Rechte iZm einem Verstorbenen und dessen urheberrechtlich geschützten Werken ein.

f. Fazit

Das Thema des virtuellen Lebens nach dem Tod lässt sich von vielen Seiten beleuchten und wurde noch nicht abschließend geklärt. Für *Jahnel* können nur lebende Personen Grundrechtsträger von Daten sein und sind folglich Daten von Nutzern nach deren Ableben aus datenschutzrechtlicher Sicht nicht mehr direkt geschützt.

Aus der Sicht des Schutzes der Privatsphäre ist es zweifelhaft, ob die Möglichkeit besteht, dass gespeicherte Daten die Privatsphäre von Angehörigen betreffen könnten und folglich aufgrund der Zuordnung zu einem lebenden Grundrechtsträger datenschutzrechtlich geschützt wären.

Darüber hinaus hat die zivilrechtliche Rechtsprechung ein „postmortales Persönlichkeitsrecht" als fortbestehendes Abwehrrecht zum Schutz des Lebensbildes des Betroffenen nach § 1330 ABGB anerkannt.

Das Urheberrecht hingegen regelt ganz genau den Übergang des Bildnisschutzes auf Angehörige und erkennt in § 78 UrhG, dass Bildnisse von Personen weder öffentlich ausgestellt, noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden dürfen, wenn dadurch berechtigte Interessen des Abgebildeten oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden.

ME müssen personenbezogene Daten (welche sich in der Regel in großen Mengen auf SNP befinden) über den Tod des Nutzers hinaus Schutz genießen und soll daher eine Vererbung von SNP-Profilen bzw dazugehörigen Zugangsdaten möglich sein, sowohl per Testament als auch im Wege der normalen gesetzlichen Erbfolge.

4. Datenschutzgesetz

Im DSG 2000 ist normiert, dass jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat […], dh das Datenschutzgesetz dient, grob formuliert, dem Schutz der Daten. Das DSG 2000 verpflichtet alle Auftraggeber und Dienstleister zum Schutz personenbezogener Daten[229], konkret zum Schutz der Betroffenen vor der Ermittlung ihrer Daten sowie deren Weitergabe.[230] Personenbezogene Daten iSd Legaldefinition des § 3 Abs 1 DSG sind „auf einem Datenträger festgehaltene Angaben über bestimmte oder mit hoher Wahrscheinlichkeit bestimmbare Betroffene". Es handelt sich somit um Angaben über Betroffene (natürliche Personen, juristische Personen oder Personengemeinschaften), deren Identität bestimmt oder bestimmbar[231] ist.

Das primäre Ziel von SNP ist das Sammeln von Daten, und es werden daher in der Folge Bestimmungen des DSG mit den Einstellungen und Vorgehensweisen von SNP verglichen.

a. Allgemeines

Das österreichische Datenschutzrecht war bis zum Inkrafttreten des DSG 2000 durch das Datenschutzgesetz 1978[232] geregelt. Das DSG ist aufgrund der Verpflichtung zur Umsetzung der Europäischen Datenschutzrichtlinie aus dem Jahr 1995[233] entstanden und durch die DSG-Novelle 2010[234] aktualisiert worden.

Die RL hatte zum Ziel, alle Datenflüsse im Binnenmarkt zu vereinfachen[235] und Datenanwendungen grundsätzlich zu schützen. Es wurden Informationspflichten, Auskunftsrechte und die Befugnisse der Datenschutzkommission bzw die Rechtsstellung der Betroffenen durch die RL verstärkt bzw verbessert. Des Weiteren finden sich in der RL

---

[229] *Brandl*, Datenschutz im Internet, in *Studiengesellschaft für Wirtschaft und Recht, Internet und Recht*, Rechtsfragen von E-Commerce und E-Government (2002) 118.

[230] *Jahnel*, Das Grundrecht auf Datenschutz nach dem DSG 2000, in FS Heinz Schäffer (2006) 320 ff.

[231] Gemäß Erwägungsgrund 26 zur DS-RL 95/46/EG und ErläutRV 1613 BlgNR 20. GP 37 soll man unter „Bestimmbarkeit" „mit vernünftigen Mitteln bestimmbar" verstehen.

[232] Bundesgesetz vom 18.10.1978 über den Schutz personenbezogener Daten (Datenschutzgesetz-DSG), BGBl 565/1978.

[233] Datenschutzrichtlinie, RL 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995.

[234] Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010).

[235] *Knyrim* (Datenschutzrecht [2003] 5) führt aus, dass es ursprünglich geplant war, das Datenschutzrecht durch die Datenschutzrichtlinie europaweit zu harmonisieren, doch sei dies nur teilweise geglückt.

gewisse Schutzbestimmungen, welche im Falle unzureichender innerstaatlicher Umsetzung Anwendungsvorrang genießen sollen.[236]

b. Data Breach Notification

Mit der DSG-Novelle 2010[237] wurde ua auch die Data Breach Notification eingeführt. Dabei handelt es sich um eine Informationspflicht des Auftraggebers, mit der dieser verpflichtet wird, einen Betroffenen unverzüglich von einer schwerwiegenden, unrechtmäßigen Datenanwendung zu informieren, wenn dem Betroffenen ein Schaden droht.[238]

Die Data Breach Notification beschreibt den Vorgang, welcher in § 24 Abs 2 a DSG normiert ist: Auftraggeber haben die Betroffenen nach Bekanntwerden einer systematischen und schwerwiegenden unrechtmäßigen Verwendung der Datenanwendungen zu informieren, sofern den Betroffenen dadurch ein Schaden droht. Lediglich im Falle eines geringfügigen Schadens oder wenn mit der Verständigung ein unverhältnismäßig hoher Aufwand verbunden wäre, kann auf die Information verzichtet werden.

(1) Verständigung über eine Datenanwendung

Informationspflicht des Auftraggebers
§ 24 Abs 1 DSG:
Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise

---

[236] Die EU hat versucht, mit der RL 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 vom 23.11.1995 (DS-RL), den Schutz personenbezogener Daten EU-weit zu gewährleisten, indem eine unbedingte Pflicht des Datenverarbeiters vorgesehen wird, alle Betroffenen über die Tatsache einer Datenverarbeitung zu informieren. Die DS-RL ist durch das DSG 2000 umgesetzt worden und am 1.1.2000 in Kraft getreten. Das Hauptproblem des Datenschutzrechts und der Europäischen Union ist ganz grundsätzlich, dass die nationalen datenschutzrechtlichen Beschränkungen an den jeweiligen Staatsgrenzen enden – Grenzen, welche es im Internet aber in der Art nicht gibt. Das Internet ist grenzenlos und viele Länder haben keine oder nur sehr abgeschwächte Datenschutznormen. Die USA haben zB noch kein umfassendes, das gesamte Staatsgebiet abdeckendes Datenschutzrecht. Es soll gemäß der RL das nationalstaatliche Gesetz zur Anwendung kommen, in welchem der Verantwortliche zur Datenverarbeitung eine Niederlassung unterhält. Liegt die Niederlassung jedoch in einem Drittstaat, so kommt das Recht jenes Mitgliedstaats zur Anwendung, in dem sich die für die betreffenden Verarbeitungen verwendeten Mittel befinden, sofern diese in einem Mitgliedstaat belegen sind. Diese Bestimmung zeigt mE ganz deutlich, dass die DS-RL das Ziel hat, personenbezogene Daten ausreichend zu schützen.

[237] Siehe das Bundesgesetz, mit dem das Bundes-Verfassungsgesetz, das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010).

[238] Eine weitere wichtige Neuerung war die Regelung über die Videoüberwachung im Abschnitt 9 a. Im Entwurf war außerdem die Einführung eines betrieblichen Datenschutzbeauftragten vorgesehen, doch wurde die verpflichtende Bestellung nicht umgesetzt. Siehe ua http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062/index.shtml (Stand: 17.10.2011).

1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und
2. über Namen und Adresse des Auftraggebers
zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen. […]

Nach dem Wortlaut des Gesetzes könnte eine Information auch über eine SNP erfolgen, sofern sichergestellt ist, dass alle Betroffenen verständigt werden.

In § 1 DSG ist das Grundrecht auf Datenschutz geregelt, welches aus mehreren unterschiedlichen Rechten besteht. Es handelt sich dabei um das Recht auf Geheimhaltung personenbezogener Daten (§ 1 Abs 1 DSG), das Recht auf Auskunft (§ 1 Abs 3 Z 1 DSG), das Recht auf Richtigstellung unrichtiger Daten (§ 1 Abs 3 Z 2 DSG) und das Recht auf Löschung unzulässigerweise verarbeiteter Daten (§ 1 Abs 3 Z 2 DSG), wobei die Ziffern 1 und 2 von Abs 3 allgemein als sog „Begleitrechte" bzw „Betroffenenrechte" bezeichnet werden.[239] Sie werden deswegen als Betroffenenrechte bezeichnet, da sie dem Betroffenen Instrumente geben, seine Rechte durchsetzen zu können.

(2) Data breach notification iZm SNP

Es stellt sich nun die Frage, ob SNP Auftraggeber iSd § 4 Z 4 DSG sind. Das Gesetz normiert, dass ein Auftraggeber ua eine natürliche bzw juristische Person oder Personengesellschaft sein kann, wenn diese alleine oder mit anderen die Entscheidung getroffen hat, Daten zu verwenden, unabhängig davon, ob sie die Daten dann selbst verwenden oder damit einen Dienstleister beauftragen.

Betreiber einer SNP sind zumeist juristische Personen, welche primär das Ziel verfolgen, Daten zu sammeln und zu verwenden. Als Verwendung wird grob gesagt das Verarbeiten, Übermitteln, Verknüpfen, Speichern etc von Daten verstanden. Und genau das machen SNP, sie speichern und verknüpfen Daten.

Ich bin somit der Ansicht, dass SNP der Informationspflicht eines Auftraggebers unterliegen und ihre Nutzer im Falle einer schwerwiegenden, unrechtmäßigen Datenverwendung zu informieren haben.

[239] Siehe Lexikon Datenschutzrecht, http://www.bka.gv.at/site/5811/default.aspx (Stand: 17.10.2011).

c. Datenschutz im Web 2.0

Obige Ausführungen zeigen, dass das Datenschutzrecht grundsätzlich von der Konstellation ausgeht, dass professionelle Datenverarbeiter, also „Stellen, welche Daten verarbeiten", personenbezogene Daten von natürlichen Personen, also „Betroffenen", verarbeiten. Im Web 2.0 ist die Situation aber eine andere, denn dort wird der Nutzer selbst zum Datenverarbeiter, da er seine Daten zur Verfügung stellt und diese selbst verarbeitet. Im Unterschied zum „normalen Nutzer" müssen aber verarbeitende Stellen gesetzliche Verpflichtungen zum Schutz personenbezogener Daten erfüllen.

Hansen stellt richtigerweise fest, dass Privatpersonen für ihre eigenen Datenverarbeitungen bislang von der Anwendung des Datenschutzgesetzes ausgenommen sind, obwohl die zunehmende Datenverarbeitung im Web 2.0 die Privatsphäre von zahlreichen Menschen bedroht, indem bereitgestellte personenbezogene Inhalte global im Netz abrufbar und faktisch für beliebige Zwecke nutzbar sind und seiner Ansicht nach für einmal veröffentlichte Daten „rückstandsfreies Löschen nicht garantiert werden kann"[240].

Wie zu Beginn in diesem Kapitel ausgeführt, versucht das europäische Datenschutzrecht durch Erlass von Richtlinien eine Harmonisierung in ganz Europa herbeizuführen und für die Betroffenen einen einheitlichen Schutz zu schaffen bzw zu gewährleisten. Es ergibt sich allerdings die Problematik, dass sich viele Anbieter von Web 2.0-Anwendungen im außereuropäischen Raum befinden. Diesen sind die europäischen datenschutzrechtlichen Vorgaben bzw Prinzipien wenig geläufig, weshalb diese wegen Unkenntnis ignoriert und nicht angewendet werden.

McNealy hat bereits im Jahr 2006 ausgesprochen, dass ein notwendiges Maß an Datenschutz und Datensicherheit über eine Kombination aus Technik und sozialen und gesetzlichen Regeln zu erreichen ist: *„It is going to get scarier if we don't come up with the technology and rules to protect appropriately privacy and secure the data, and the most important asset we have is obviously the data on people – our customers and employees and partners. And if we can't protect that, people are not going to go online."*[241]

---

[240] *Hansen* in *De Meer/Herkenhöner*, Sicherheit mit und ohne Netz. Technische und rechtliche Herausforderungen des Web 2.0 (2011) 23 f.

[241] *Scott McNealy*, ehemaliger CEO von Sun Microsystems, in *Robert Lemos*, Private identities become a corporate focus, SecurityFocus, 20.2.2006, San Jose, California, USA. Siehe auch *Hansen* in *De Meer/Herkenhöner*, Sicherheit mit und ohne Netz. Technische und rechtliche Herausforderungen des Web 2.0 (2011) 24.

Ich schließe mich dem an. Es müssen Möglichkeiten geschaffen werden, die Privatsphäre der Nutzer zu sichern und deren Daten zu schützen, da die Menschheit sich (hoffentlich) früher oder später der Gefahren bewusst werden wird und in der Folge, als letzte Konsequenz, möglicherweise auch nicht mehr online gehen wird.

d. Anwendbarkeit des DSG auf Social network-Plattformen[242]

§ 3 Abs 1 DSG, welcher den räumlichen Anwendungsbereich des DSG regelt, normiert, dass das DSG zur Anwendung kommt, wenn personenbezogene Daten im Inland „verwendet" werden. Die Anwendbarkeit des DSG wird damit durch den Ort der Datenverwendung bestimmt. Erfolgt eine Datenverwendung in Österreich, kommt das DSG auch zur Anwendung. Außerdem ist das DSG auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der EU für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung eines Auftraggebers geschieht.[243]

In § 4 DSG, welcher Begriffsdefinitionen[244] vornimmt, wird als „Datenverwendung" jede Art der Handhabung von Daten, konkret das Verarbeiten und Übermitteln von Daten, definiert.[245] Datenverarbeitung ist wiederum jede Form der Handhabung von Daten, so zB das Speichern, Verändern, Verknüpfen, Überlassen, Vervielfältigen oder Vernichten von Daten, aber auch deren Ermittlung.[246]

Es stellt sich nun die Frage, ob das Erfassen von Nutzer- bzw Mitgliedsdaten durch den Betreiber einer SNP eine derartige „Ermittlung" iSd § 4 Z 9 DSG *(„Verarbeiten von Daten: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen [Z 11], Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten mit Ausnahme des Übermittelns [Z 12] von Daten")* darstellt.

ME fällt das Erfassen von Nutzer- bzw Mitgliedsdaten in den Begriff der „Ermittlung" des § 4 Z 9 DSG. Es werden die Nutzerdaten auf einer SNP „gespeichert", weswegen die Tatbestandsmerkmale des § 4 DSG – und damit die „Daten-Verwendung" – meiner Ansicht

---

[242] Datenschutzgesetz 2000, BGBl 165/1999 idgF.
[243] *Jahnel/Siegwart/Fercher*, Aktuelle Fragen des Datenschutzrechts (2007) 23 f.
[244] *Lehner* in *Bauer/Reimer*, Handbuch Datenschutzrecht (2009) 123: In § 4 DSG werden eine Reihe von Begriffen definiert, deren Bedeutung sogar über das DSG hinausreicht.
[245] Vgl § 4 Z 8 DSG und *Pollirer/Weiss/Knyrim*, DSG (2010) § 4 Z 8.
[246] Vgl § 4 Z 9 DSG und *Pollirer/Weiss/Knyrim*, DSG (2010) § 4 Z 9.

nach als gegeben erscheinen. Regelmäßig werden die Daten von den Betreibern einer SNP auch weiter „verarbeitet“ bzw weiter verwendet, zB durch das Löschen.

Technisch betrachtet stellt sich aber die Frage, ob diese „Verwendung“ der Daten tatsächlich in Österreich erfolgt. Bei vielen IT-Unternehmen sind der Sitz und der Standort ihrer Server getrennt. Woran misst man dann den Bezugspunkt? Ist der Bezugspunkt der Sitz, der Serverstandort oder der Ort, wo sich der Nutzer, dessen Daten in der Folge verarbeitet, verwendet und gespeichert werden, aufhält?

Die Art 29-Datenschutzgruppe hat sich bereits im Jahr 2002 dazu geäußert. Die Art 29-Datenschutzgruppe[247] ist ein unabhängiges Beratungsgremium der Europäischen Kommission in Datenschutzfragen, welches aus Vertretern der jeweiligen nationalen Datenschutzbehörden, dem Europäischen Datenschutzbeauftragten und einem Vertreter der Europäischen Kommission besteht. Die Art 29-Datenschutzgruppe hat primär beratende Funktion. Sie kann aber auch Empfehlungen und Stellungnahmen zu allen Fragen abgeben[248], die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Union betreffen.

Im Jahr 2002 hat die Art 29-Datenschutzgruppe das Arbeitspapier WP 56[249] in Brüssel verabschiedet und festgestellt, dass schon die Erhebung personenbezogener Daten eines (in der EU ansässigen) Nutzers die Anwendbarkeit des nationalen Datenschutzrechts des Mitgliedstaats des Nutzers begründen kann. Wenn man dieser Ansicht folgt, wird eine Anwendbarkeit des DSG auf SNP anzunehmen sein, auch wenn diese von einem in einem Drittstaat ansässigen Plattformbetreiber betrieben und in Österreich abrufbar sind.[250]

Auch der *Verein für Konsumenteninformation* hat hinsichtlich der Frage, ob das österreichische Recht, insbesondere das Datenschutzgesetz, überhaupt zur Anwendung kommt, ausgeführt, dass es aufgrund der Tatsache, dass die Dateneingabe auf einem

[247] http://ec.europa.eu/justice/policies/privacy/index_en.htm (Stand: 20.4.2011).

[248] Die Datenschutzgruppe wurde durch Art 29 RL 95/46/EG eingesetzt. Sie ist das unabhängige EU-Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Art 30 RL 95/46/EG sowie in Art 14 RL 97/66/EG festgelegt. Siehe http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_de.pdf

[249] Siehe „Arbeitspapier über die Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU“ – „WP 56“ der Art 29-Datenschutzgruppe, 5035/01/DE/endg., hinsichtlich der Frage der internationalen Anwendbarkeit des EU-Datenschutzrechts bei der Verarbeitung personenbezogener Daten im Internet durch Websites außerhalb der EU, angenommen am 30.5.2002.

[250] Anders ist es zu beurteilen, wenn der Plattformbetreiber jedoch über eine Niederlassung in einem anderen Mitgliedstaat verfügt, dann könnte das Herkunftslandprinzip des § 3 Abs 2 DSG greifen und würde dann die Anwendbarkeit des Datenschutzrechts dieses Mitgliedstaats bewirken.

Computer mit Standort in Österreich erfolgt, kein Fehler sein kann, sich auf das österreichische Datenschutzgesetz zu berufen.[251]

Obiges gilt für das anwendbare Recht, auf den Gerichtsstand wird an anderer Stelle noch näher einzugehen sein.

e. Ausblick

Die digitalen Entwicklungen der letzten Jahre haben nicht nur zu Erleichterungen geführt und neue Märkte, Programme und Möglichkeiten eröffnet, sondern auch neuartige Gefährdungen mit sich gebracht. Der österreichische Gesetzgeber wollte seinerzeit mit dem Grundrecht auf Datenschutz auf die Entwicklungen der Jahre davor reagieren. Die Intention des Datenschutzgesetzes 1978[252] war der „Schutz vor der Ermittlung und Weitergabe entsprechender Daten, um den gläsernen Menschen nicht Wirklichkeit werden zu lassen", wie *Handler* treffend formuliert.[253]

Der Gesetzgeber wollte auf die „neuen Gefährdungen der menschlichen Persönlichkeit durch die Möglichkeiten der elektronischen Datenverarbeitung reagieren und einem neuen Missbrauchspotenzial entgegentreten". Mit dem Erlass des DSG 1978 sollte eine „Art informationelles Selbstbestimmungsrecht verwirklicht werden", indem das DSG 1978 „die automationsunterstützte Ermittlung, Verarbeitung und Übermittlung von Daten im öffentlichen und privaten Bereich an enge Zulässigkeitsgrenzen bindet und entsprechende Rechtsschutzmöglichkeiten schafft". Wie *Berka* betont, hat der Gesetzgeber an die „Spitze des DSG 1978 ein Grundrecht gestellt, nämlich das in der Verfassungsbestimmung des § 1 DSG verankerte Grundrecht auf Datenschutz, welches die einfachgesetzlichen Bestimmungen des DSG verfassungsrechtlich absichert, das zugleich aber auch einen über das DSG hinausgehenden Anwendungsbereich hat und einen allgemeinen Geheimhaltungsschutz verbürgt".[254] Das bedeutet, dass alle einfachen Gesetze mit dieser Norm in Einklang zu stehen haben. Das DSG möchte nicht nur die Daten schützen, sondern auch die dahinterstehenden Interessen der Menschen, indem der im Vordergrund stehende Anspruch auf Geheimhaltung von persönlichen Daten von den Ansprüchen auf Auskunft über die Art der Datenverarbeitung, auf Richtigstellung von falschen Informationen und Löschung von unzulässigerweise verarbeiteten Daten begleitet wird.

---

[251] *Verein für Konsumenteninformation,* Ihr Recht im Internet (2011) 100.
[252] Bundesgesetz vom 18.10.1978 über den Schutz personenbezogener Daten BGBl 565.
[253] *Handler*, Der Schutz von Persönlichkeitsrechten (2008) 490.
[254] *Berka*, Die Grundrechte: Grundfreiheiten und Menschenrechte in Österreich (1999) 273, Rz 480.

Ausblick:

Es gab zwar in den letzten Jahren zahlreiche Änderungen und Erweiterungen der rechtlichen Rahmenbedingungen im Bereich des Datenschutzes, doch denke ich, dass das Recht all den neuen Herausforderungen des neuen virtuellen Lebens und all der technischen Neuerungen kaum mehr gewachsen ist. Es gibt kaum internetspezifische Regelungen zum Persönlichkeitsschutz, zum Schutz von Transaktionen personenbezogener Daten im Internet etc.

Auf der einen Seite gibt es die Anforderung an den Gesetzgeber, die erforderlichen gesetzlichen Rahmenbedingungen zu schaffen, welche all den neuen technischen Errungenschaften entsprechen, um eine ausreichende Datensicherheit des Nutzers zu gewähren, und auf der anderen Seite gibt es Anforderungen an die Diensteanbieter von SNP, die gesetzlichen Vorgaben umzusetzen. Nur wenn beide Seiten zusammenarbeiten, können die Nutzer vor einem missbräuchlichen und schädigenden Umgang mit ihren Daten geschützt werden. Ziel sollte ein Zusammenspiel von Technik und Recht sein, damit die rechtlichen Rahmenbedingungen auch technisch umgesetzt werden können.

Wesentliche Fragen sind in diesem Zusammenhang, welche Gesetze bei einer Datenschutzverletzung eingreifen, welche Verpflichtungen des Diensteanbieters daraus resultieren und welche Rechte einem Nutzer zustehen, damit dieser seine Daten schützen und eine missbräuchliche Verwendung oder Weitergabe vermeiden kann?

VI. AUSGEWÄHLTE RECHTSPROBLEME IM ZUSAMMENHANG MIT SOCIAL NETWORK-PLATTFORMEN

A. RECHT AM EIGENEN NAMEN

Jedem SNP-Profil wird durch den Nutzer ein Name zugeordnet, weswegen in der Folge kurz auf das Recht am eigenen Namen eingegangen werden sollte:

§ 43 ABGB normiert, dass derjenige, der in seinem Recht zur Führung seines Namens verletzt wird, indem eine dritte Person sich unbefugt seines Namens bedient oder seinen Namen bestreitet, auf Unterlassung und bei Verschulden auf Schadenersatz klagen kann.[255]

Der Name soll schließlich als Identifikationsmerkmal als auch als Kennzeichnung einer Person dienen. § 43 ABGB schützt aber nicht nur den Familiennamen, sondern jegliche Pseudonyme, wie sie auch gerne auf SNP benützt werden, oftmals mit dem Argument, die komplette Zuordnung zu einer Person zu erschweren.

Der Schutz bei natürlichen Personen beinhaltet den Familiennamen, Decknamen oder ein Pseudonym (Künstlername, Kryptonym) und die Firma bei Unternehmern. Bei juristischen Personen sind Personen- und Kapitalgesellschaften, Abkürzungen und Bestandteile von Firmen, politische Parteien und juristische Personen des öffentlichen Rechts geschützt.

Das Namensrecht ist nach hL und österreichischer Rechtsprechung[256] ein Persönlichkeitsrecht, da dem Namen an sich Kennzeichnungs- sowie Ordnungsfunktion zukommt und die mit dem Namen identifizierte Person geschützt ist.

Im Falle eines unbefugten Namensgebrauches kann sich der Verletzte mittels Unterlassungs- oder Beseitigungsanspruch wehren und bei Verschulden zusätzlich Schadenersatz begehren. Unbefugt ist der Gebrauch eines Namens, wenn weder eine Berechtigung noch ein Recht zur Verwendung besteht. Es ist irrelevant, ob nur ein Teil des Namens oder der gesamte Name verwendet wird.[257]

---

[255] Vgl § 43 ABGB.
[256] Siehe ua OGH 24.2.1998, 4 Ob 368/97i und 23.11.2000, 6 Ob 109/00y.
[257] Siehe ua OGH 22.11.1977, 4 Ob 377/77.

Wenn der Berechtigte den Namensgebrauch jedoch gestattet, wird dies als Verzicht auf seine möglichen Unterlassungsansprüche gewertet.

Verwendet aber ein Dritter ohne Berechtigung bzw Einverständnis einen Namen auf Facebook, so hat der Berechtigte Beseitigungsansprüche sowie bei Verschulden[258] Schadenersatzansprüche gegen den berechtigungslosen Verwender.

Die SNP Facebook zB erklärt unter Punkt 5.1. der Nutzungsbedingungen, dass Handlungen auf Facebook untersagt sind, die die Rechte anderer Personen bzw das Gesetz verletzen. Dies kann zB durch den Inhalt eines Postings verwirklicht werden. Im Falle eines Verstoßes schreibt Facebook unter Punkt 5.2. vor, dass Facebook Inhalte löschen kann, wenn diese Punkt 5.1. widersprechen.

Twitter hingegen erklärt in den Nutzungsbedingungen, dass die Vergabe von Profilnamen „einmalig und exklusiv" sein soll wie bei Domains unter einer Top Level Domain. XING verbietet die Nutzung von Pseudonymen und Künstlernamen. Facebook hingegen lässt mehrere Profile mit demselben Profilnamen zu.

Twitter hat für das Problem der falschen Identität dergestalt eine Lösung gefunden, als es die sog „verifizierten Accounts" geschaffen hat (siehe dazu weiter oben im Detail).

1. Judikatur im Zusammenhang mit dem Recht am eigenen Namen

In der Entscheidung 4 Ob 377/77 vom 22.11.1977 hatte der OGH zu beurteilen, ob auch der Name einer juristischen Person geschützt gehört, um damit dem Schutzbereich des Namensrechts zu unterliegen, und der OGH hat anerkannt, dass auch die Firma eines Unternehmens unter den Schutz des § 43 ABGB fällt. Dh auch eine juristische Person kann den Namensschutz nach § 43 ABGB geltend machen. Mithilfe dieser Rechte kann verhindert werden, dass sich jemand eines Namens bzw einer Identität bedient, welche nicht die eigene ist. Aus der Entscheidung: „Unbefugt ist jeder Gebrauch des Namens oder eines wesentlichen Namensbestandteiles, der weder auf eigenem Recht beruht, noch vom berechtigten Namensträger gestattet wurde."

[258] Eine subjektive Vorwerfbarkeit ist erforderlich.

2. Exkurs: Erstellung einer Facebook-Unternehmens-Webseite durch unternehmensfremde Personen

Hierbei geht es um die Frage, ob es iZm § 43 ABGB erlaubt ist, als unternehmensfremde Person eine Facebook-Webseite zu erstellen, welche den Namen eines Unternehmens in der Webseiten-Bezeichnung beinhaltet. Der OGH hatte bereits im Jahr 2009 in einem Verfahren[259] eine ähnliche Frage zu beurteilen: Ausgangspunkt dieses Verfahrens war es, dass ein offensichtlich unzufriedener Kunde des Unternehmens „Aquapol GmbH", welches im Bereich der Gebäude- bzw Mauertrockenlegung tätig war, eine Domain mit dem Namen „www.aquapol-unzufriedene.at" registrierte, um sich mit anderen Personen kritisch über das Unternehmen Aquapol auszutauschen. Das Unternehmen hatte sich jedoch nicht nur den Firmenwortlaut „Aquapol" als Gemeinschaftsmarke registrieren lassen, sondern war Berechtigte der Domain „www.aquapol.at".

Aquapol hat daraufhin auf Unterlassung der Verwendung der Bezeichnung „aquapol" als Bestandteil der Domain geklagt, da sich das Unternehmen in seinem Namensrecht verletzt sah. Die beklagte Partei brachte hingegen vor, dass es sich bei der Domain „aquapol-unzufriendene.at" lediglich um einen beschreibenden Zusatz handle, der auf das Thema der Webseite verweisen solle. Die Webseite sei nach Ansicht des Beklagten nur ein Meinungsforum für Personen, welche bereits Erfahrungen mit Aquapol gemacht haben, und die Leser des Meinungsforums würden lediglich aufgefordert, „möglichst sachlich" über ihre Erfahrungen mit der Trockenlegung von Mauern mittels Aquapol oder ähnlichen Verfahren zu schreiben. Außerdem liege nach Ansicht des Beklagten schon ein aus Gründen der Meinungsfreiheit gerechtfertigter Fall einer notwendigen und damit zulässigen Namensnennung vor.

Der OGH hat schließlich ausgesprochen, dass die Verwendung einer kritisierenden Domain nicht das Persönlichkeitsrecht des Namensträgers verletzt, da das Interesse des Beklagten, Kritik zu üben, gegenüber dem Interesse der Klägerin überwogen habe. Der Gebrauch des Namens bzw der Firma als bloßes Signal, um andere Personen auf Kritik aufmerksam zu machen, sei demnach zulässig, wenn dieser Umstand den Besuchern der Webseite unmittelbar erkennbar ist. Der Beklagte habe nämlich weder das Recht der Klägerin, unter ihrem Firmenschlagwort aufzutreten, bestritten, noch sei er Dritten gegenüber unter ihrem Firmenschlagwort aufgetreten.

[259] Siehe OGH 24.2.2009, 17 Ob 2/09g.

Fazit

Obige Entscheidung behandelt zwar grundsätzlich „normale“ Webseiten, doch kann der Tenor der Entscheidung mE sinngemäß auch auf Social network-Plattformen übertragen werden, wenn dort eine unternehmensfremde Person in der Profilbezeichnung einen Teil eines Unternehmensnamens verwendet.

B. RECHT AM EIGENEN WORT

Das Recht am eigenen Wort gehört zum Schutz der Persönlichkeit und gewährleistet die Selbstbestimmung über die eigene Darstellung in der Kommunikation mit anderen und schützt die geschriebene und gesprochene Kommunikation. Genauso wie es ein Recht am eigenen Bild gibt, sollte es auch ein Recht am eigenen Wort geben. Dessen Schutzbereich sollte auch im Bereich von SNP wirken, da die Initiative zum Kommentieren und Preisgeben von Informationen (zB auf einer Facebook „wall“) primär vom Seitenbetreiber ausgeht, der dadurch seine Seite attraktiver und spannender gestalten möchte. Es sollte daher auch hier der Seitenbetreiber verpflichtet werden, den Nutzer vor der Veröffentlichung von Informationen auf die Risiken hinzuweisen.

Sowohl das StGG als auch die EMRK beinhalten Rechte zum Schutze der Kommunikation bzw Meinungsfreiheit. Art 13 StGG normiert: *„Jedermann hat das Recht, durch Wort, Schrift, Druck oder durch bildliche Darstellung seine Meinung innerhalb der gesetzlichen Schranken frei zu äußern. Die Presse darf weder unter Censur gestellt, noch durch das Concessions-System beschränkt werden. Administrative Postverbote finden auf inländische Druckschriften keine Anwendung.“*

Art 10 EMRK beinhaltet die Freiheit der Meinungsäußerung. Durch Art 10 EMRK wird die Meinungsfreiheit in ihren unterschiedlichen Ausprägungen und Formen geschützt: Abs 1: *„Jede Person hat das Recht auf freie Meinungsäußerung. Dieses Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Dieser Artikel hindert die Staaten nicht, für Hörfunk-, Fernseh- oder Kinounternehmen eine Genehmigung vorzuschreiben.“*

In Art 13 Abs 1 StGG ist normiert: *„Jedermann hat das Recht, durch Wort, Schrift, Druck oder durch bildliche Darstellung seine Meinung innerhalb der gesetzlichen Schranken frei zu äußern."*

Art 13 Staatsgrundgesetz, welcher durch Art 49 Bundesverfassungsgesetz in Verfassungsrang steht, normiert das Recht auf Meinungs- und Pressefreiheit:

„Jedermann hat das Recht, durch Wort, Schrift, Druck oder durch bildliche Darstellung seine Meinung innerhalb der gesetzlichen Schranken frei zu äußern. Die Presse darf weder unter Zensur gestellt, noch durch das Konzessionssystem beschränkt werden. […]"

Art 10 Menschenrechtskonvention geht noch weiter und erklärt, dass alle „Mitteilungen von Nachrichten oder Ideen, unabhängig von der dazu verwendeten Art menschlicher Sinnvermittlung, geschützt werden sollen". Informationsaufnahme und Informationspreisgabe sollen gleichgestellt und geschützt werden.

In Art 10 Abs 2 MRK ist normiert, dass gewisse Eingriffe erlaubt sein sollen. So ua, wenn der Eingriff im „Interesse der nationalen Sicherheit, der Aufrechterhaltung der Ordnung, Verbrechensverhütung, um die Unparteilichkeit der Rechtsprechung zu gewährleisten […]" ist. Das Datenschutzgesetz erklärt in § 1 Abs 1 DSG, dass Daten „geheim zu halten sind, soweit der Betroffene daran ein schutzwürdiges Interesse hat".

Es stellt sich nun die Frage, ob obige Regelungen für Inhalte von SNP und die von den Nutzern online gestellten Inhalte gelten (sollen) und ob es nicht (bereits) einfach bundesgesetzliche Beschränkungen gibt.

Deutsche Gerichte hatten bereits in einigen Verfahren zu beurteilen, ob eine auf einer SNP getätigte Äußerung vom Grundrecht der Meinungsfreiheit gedeckt war:

Im Verfahren 12 C 12.264 zB hatte der Bayrische Verwaltungsgerichtshof die Frage zu beantworten, ob eine Kündigung wegen eines Facebook-Postings gerechtfertigt war. Eine Arbeitnehmerin hatte sich auf Facebook negativ über einen Geschäftspartner ihres Arbeitgebers geäußert, weswegen dieser die Arbeitnehmerin gekündigt hat. Die negative Äußerung betraf den Ärger der Arbeitnehmerin über ihren privaten Mobilfunkvertrag mit dem Geschäftspartner ihres Arbeitgebers. Der VGH Bayern hat mE zu Recht ausgesprochen, dass die Äußerung an sich nicht schwer war und vom Grundrecht der Meinungsfreiheit gedeckt

war, da sie im privaten Bereich von Facebook lag und die Klage auf Zulassung der Kündigung daher nur geringe Erfolgsaussichten habe.[260]

In einer weiteren Entscheidung des deutschen Gerichts, ArbG Bochum, 3 Ca 1203/11, und LAG Hamm, 5 Sa 451/12 als Rechtsmittelentscheidung, hatte das ArbG Bochum darüber zu entscheiden, ob Äußerungen einer ehemaligen Arbeitnehmerin über ihren Arbeitgeber auf Facebook wie „Pfanne von Chef", „die Pfeife" und „mit diesem Drecksladen" von der Meinungsfreiheit gedeckt und damit zulässig waren, und das Gericht hat ausgesprochen, dass die Äußerungen im konkreten Fall zulässig waren, da der Dialog nicht öffentlich geführt wurde und nur von den Facebook-Freunden der ehemaligen Arbeitnehmerin verfolgt werden konnte. Das Berufungsverfahren vor dem LAG Hamm wurde mittels Vergleich beendet.[261]

C. RECHTSPROBLEME IM ZUSAMMENHANG MIT DEM HOCHLADEN VON FOTOS

Wie im Kapitel Hochladen von Fotos und Videos bereits kurz angesprochen, machen es SNP den jeweiligen Nutzern sehr einfach, Bilder, Grafiken etc auf das jeweilige Profil hochzuladen, indem Bilder in sogenannte „Galerien" hochgeladen und in Status-Updates oder Kommentaren eingebunden werden können.

Grundsätzlich unproblematisch ist in diesem Zusammenhang das Hochladen bzw Verwenden selbstgenerierter Inhalte. Probleme können sich aber dann ergeben, wenn nicht selbstgenerierte Inhalte verwendet werden, dh wenn Inhalte Dritter gepostet, auf einer Facebook-Seite eingepflegt oder gar vervielfältigt werden, ohne dass der jeweilige Rechteinhaber dem vorher zugestimmt hat.

Zuerst soll auf den besonderen Bildnisschutz des § 78 UrhG eingegangen werden, bevor das Vervielfältigungs- bzw Zurverfügungstellungsrecht iSd UrhG betrachtet wird.

1. Recht am eigenen Bild – Bildnisschutz gemäß § 78 UrhG

Es ist wenigen Nutzern bewusst, dass sie beim Hochladen von Bildern auch Rechte Dritter verletzen können, wenn sie ein „fremdes" Bild auf ihr Profil hochladen. Rechtlich ist ua zu

[260] VGH Bayern 29.2.2012, 12 C 12.264.
[261] ArbG Bochum 9.2.2012, 3 Ca 1203/11 und LAG Hamm 5 Sa 451/12.

beachten, dass das Urheberrechtsgesetz (UrhG) „Werke der Literatur und der Kunst“ unter Schutz stellt. Bilder zählen zu „Lichtbildwerken“ und sind vor unerlaubtem Gebrauch geschützt, dh sie dürfen ohne Einverständnis des Urhebers nicht benützt werden.

Die auf einem Bild abgebildete Person wird durch § 78 UrhG geschützt, welcher das Recht am eigenen Bild normiert. Darin ist normiert, dass *„Bildnisse von Personen weder öffentlich ausgestellt, noch auf eine andere Art, wodurch sie der Öffentlichkeit zugänglich gemacht werden, verbreitet werden, wenn dadurch berechtigte Interessen des Abgebildeten oder, falls er gestorben ist, ohne die Veröffentlichung gestattet oder angeordnet zu haben, eines nahen Angehörigen verletzt würden“.*

Laut *Welser* soll der Abgebildete davor geschützt werden, dass er durch die Verbreitung seines Bildnisses bloßgestellt, sein Privatleben der Öffentlichkeit preisgegeben oder sein Bildnis auf eine Art benützt wird, welche zu Missdeutungen Anlass geben könnte bzw die Verbreitung entwürdigend oder herabsetzend wirkt.[262]

Zweck dieses Persönlichkeitsrechts ist somit der Schutz der abgebildeten Person in jeglicher Form. Nicht in den Schutzbereich fallen hingegen nach hM unbefugte Bildaufnahmen.[263] Nach österreichischem Recht gibt es kein allgemeines Fotografier- bzw Abbildungsverbot. Das bedeutet, dass sich der Abgebildete zwar nicht gegen das Fotografieren seiner Person wehren kann, er kann sich aber unter bestimmten Voraussetzungen vor einer ungenehmigten Verbreitung bzw Veröffentlichung seines Bildnisses schützen.

Gem § 78 UrhG dürfen persönliche Bildnisse nicht öffentlich ausgestellt oder verbreitet werden, wenn dadurch berechtigte Interessen des Abgebildeten verletzt werden.[264] Der Abgebildete soll damit vor einer Bloßstellung durch Verbreitung, die Preisgabe seines Privatlebens gegenüber der Öffentlichkeit oder einer Benützung, die zu Missdeutungen führen kann, geschützt werden.[265] Zu beachten ist, dass § 78 UrhG zwar vor der Veröffentlichung von Bildern schützt, nicht jedoch die Bildaufnahme unter Schutz stellt.[266]

Nicht in den Schutzbereich des § 78 UrhG fallen auch Tatbestände, wo die abgebildete Person hingegen der Veröffentlichung ausdrücklich oder stillschweigend zugestimmt hat.

---

[262] *Welser*, Fachwörterbuch (2005) 424.
[263] *Thiele*, Eurolawyer, Unbefugte Bandaufnahme und ihre Verbreitung im Internet – Braucht Österreich einen eigenen Paparazzi-Paragrafen? http://www.eurolawyer.at/pdf/paparazzi_paragraf.pdf (Stand: 18.5.2011).
[264] Eine Ausnahme besteht nur für Rechtspflege.
[265] *Koziol*, Haftpflichtrecht II^2 (1984) 11 f.
[266] *Frick*, Persönlichkeitsrechte (1991) 106.

Gemäß der EMRK unterliegt auch eine „bildliche Kommunikation“ der Meinungsfreiheit nach Art 10 MRK.[267] Im Bereich von SNP ergibt sich das Hauptproblem daraus, dass der Nutzer grundsätzlich freiwillig Bilder von sich oder aus seinem privaten Bereich in das Internet stellt. Probleme können sich in diesem Bereich insbesondere dann ergeben, wenn diese Fotos von anderen Personen heruntergeladen und in der Folge auf einer anderen Webseite wieder online gestellt, verlinkt oder mit Suchmaschinen verknüpft werden. Bei Suchmaschinen werden in den meisten Fällen auch veraltete „Ansichten“ im sog Cache gespeichert.[268] Durch ein ungewolltes Hochladen eines Fotos kann es für den Abgebildeten aber auch zu Missdeutungen kommen. Dies ist zB im folgenden Fall geschehen[269]:

In einer Zeitung wurde eine Weinwerbung unter dem Titel „Zum Wohl ein guter Tropfen“ mit dem Bild des Klägers verwendet, auf welchem dieser bei einem Heurigenbesuch zu sehen war. Im Text neben dem Bild stand: „Kaum ein Weinliebhaber, der sich bis ins hohe Alter sein tägliches Tröpferl Wein nehmen ließe. Und bei Gesunden haben die Ärzte nichts dagegen“.

Durch die Veröffentlichung dieses Bildes wurde nicht nur in die Privatsphäre des Klägers eingegriffen, sondern es war auch ein Anlass zu Missdeutungen gegeben, nämlich dass der Kläger Heurigenbesucher und damit Weinkonsument sei. Die Klage war auf Unterlassung und Urteilsveröffentlichung gestützt. Dieser wurde stattgegeben, das Begehren auf Zuspruch einer Entschädigung wurde jedoch gemeinsam mit dem Begehren auf Herausgabe des Films bzw der Negative abgewiesen. Der OGH begründete seine Entscheidung im Grunde damit, dass die Bildveröffentlichung bei einem unbestimmten Personenkreis eine falsche Vorstellung erwecken könnte und der Kläger sein Bildnis für Werbezwecke entgeltlich zur Verfügung gestellt hatte. Dies sei ein „Musterbeispiel einer herabsetzenden Bildnisveröffentlichung“.

Diese Entscheidung ist mE auch auf diverse Sachverhalte im Zusammenhang mit SNP anwendbar. Dies ist zB der Fall, wenn eine Person ein Bild einer anderen Person unerlaubterweise veröffentlicht und dieses durch den Ort der Aufnahme, die Personen im Bild etc zu falschen Vorstellungen führt und damit einen falschen Eindruck vom Betroffenen erwecken könnte.

---

[267] Zum Bildnisschutz im Internet siehe *Haller/Limberger* in *Schweighofer* et al., IRIS 2005, 479 ff.

[268] Es gibt Vorschläge und Ideen, das Internet „vergesslicher“ zu machen, zB durch einen „digitalen Radiergummi“ oder ein „Verfallsdatum“, nach welchem sich Daten automatisch löschen. Siehe dazu Rede des dt Innenministers *Thomas de Maizieres* zum Thema Netzpolitik vom 22.6.2010 (siehe http://www.bmi.bund.de/cln_165/SharedDocs/Pressemitteilungen/DE/2010/mitMarginalspalte/06/netzpolitik.html, zuletzt 8.8.2011).

[269] OGH 29.6.1971, 4 Ob 330/71 SZ 44/104.

Wenn ein Nutzer aber nun in das Hochladen des Bildes einwilligt, so verzichtet er im Rahmen seiner Einwilligung auf seinen Rechtsschutz.[270] Ohne Einwilligung ist eine Veröffentlichung nur zulässig, wenn das Veröffentlichungsinteresse die Interessen des Abgebildeten überwiegt.

Der Betreiber einer Webseite hat mE klar und deutlich auf obige Risiken hinzuweisen, da sich der Betroffene nur dann bewusst und freiwillig für eine Veröffentlichung seiner Fotos entscheiden kann.[271]

Zusammenfassend kann festgehalten werden, dass das Aufnehmen von Fotos urheberrechtlich grundsätzlich erlaubt ist, das Verarbeiten, das Onlinestellen etc könnte aber möglicherweise zu Datenschutz- oder Persönlichkeitsrechtsverletzungen führen.

a. Ansprüche

Es gibt verschiedene Ansprüche aus der Verletzung am Recht am eigenen Bild iSd § 78 UrhG:

Im Urheberrechtsgesetz (UrhG) sind der Unterlassungsanspruch (§ 81), der Beseitigungsanspruch (§ 82), der Anspruch auf Urteilsveröffentlichung (§ 85) sowie bei Verschulden ein Anspruch auf Schadenersatz (§ 87) geregelt:

Das Gesetz sieht damit für den Inhaber eines „Ausschließungsrechts“ (einen Urheberrechtsinhaber) bestimmte Ansprüche vor, falls dieser in seinen Rechten verletzt wurde. Dh der Urheber eines Bildes kann ua die Unterlassung der Verwendung seines Bildes begehren und damit Fremde von der Verwendung etc ausschließen.

Im ABGB ist der Verwendungsanspruch in § 1041 ABGB[272] geregelt, welcher normiert, dass derjenige, dessen Sache (das Bild) ohne Erlaubnis des Eigentümers verwendet wurde, den Wert verlangen darf, den die Sache zur Zeit der Verwendung gehabt hat. Es wird somit ein Betrag errechnet, der dem Eigentümer dafür zustehen soll, weil sein Bild von einer dritten Person unerlaubterweise verwendet wurde.

---

[270] Siehe auch OGH 16.12.2003, 4 Ob 211/03p zum Widerruf bei unwiderruflicher Veröffentlichungsermächtigung.

[271] Siehe auch § 13 Abs 1 dt TMG, der das Erfordernis der „Einwilligung“ des Betroffenen bestimmt und *Iraschko-Luscher/Kiekenbeck*, Datenschutz im Internet – Widerspruch oder Herausforderung? RDV 2010, 263.

[272] Ein Verwendungsanspruch kann zB im Hinblick auf die Ausnützung des geldwerten Bekanntheitsgrades des Abgebildeten bestehen.

Das bedeutet iZm SNP, dass im Falle der unerlaubten Verwendung eines Bildes auf einem SNP-Profil der Urheberrechtsinhaber einen Anspruch auf Schadenersatz gegen den Verwender begehren kann.

b. Judikatur

In der Entscheidung betreffend die Veröffentlichung von Privatfotos von Caroline von Hannover[273] hat bereits der EGMR ausgesprochen, dass „das Recht auf Achtung des Privat- und Familienlebens nach Art 8 MRK eine Einschränkung nur toleriere, wenn diese notwendig und der öffentlichen Sicherheit dienlich sei […] und die Rechte und Freiheiten Dritter als höherwertig angesehen werden können".[274]

In der Entscheidung 8 ObA 136/00 h[275] war das Problem, dass ein Arbeitgeber (Beklagter) auf seiner Firmenwebseite ein Foto einer Arbeitnehmerin (Klägerin) online gestellt hatte. Der OGH sieht im Abrufbarhalten eines Fotos gegen den Willen des Arbeitnehmers eine Bildnisschutzverletzung. Das Veröffentlichen eines Bildes des Dienstnehmers im Internet stellt ohne vorherige Zustimmung des abgebildeten Arbeitnehmers einen Verstoß gegen den Bildnisschutz des § 78 UrhG dar, der nicht mit der Treuepflicht des Dienstnehmers gerechtfertigt werden kann.

Zu einer Verletzung des Rechts am eigenen Bild kommt es häufig auch dann, wenn ein Unternehmen auf einer Veranstaltung Privatpersonen fotografiert und die Fotos in der Folge auf der eigenen Webseite online stellt. Wenn die betroffenen Personen dem Ablichten und Hochladen nicht zugestimmt haben und es den Anschein hat, dass die betroffenen Personen für die Abbildungen ein Entgelt erhalten haben, sind deren berechtigte Interessen verletzt.[276]

Das OLG München hat in der Entscheidung 18 U 2067/07 ausgesprochen, „dass ohne Einwilligung des Betroffenen Bildnisse aus dem privaten Bereich im Internet nicht veröffentlicht werden dürfen".[277]

In den Entscheidungen 10 Cg 115/10 g und 39 Cg 75/10 p hat das HG Wien die Beklagten zur Urteilsveröffentlichung auf ihren SNP gem UWG verpflichtet. Das Gericht wollte dem

---

[273] EGMR 24.6.2004, 59320/00, *Hannover gegen Deutschland*, MR 2004, 246.
[274] Siehe auch *Ghazal* in *Jaksch-Ratajczak* (2010) 59.
[275] Siehe OGH 5.10.2000, 8 ObA 136/00 h.
[276] Eine Bildnisveröffentlichung zu Werbezwecken ist bei Prominenten unzulässig.
[277] Siehe OLG München 26.6.2007, 18 U 2067/07. Dies gilt auch für Personen der Zeitgeschichte, siehe *„Caroline-von-Monaco-Urteil II"* (BVerfG 1 BvR 653/96).

Talionsprinzip folgend ein Gleichgewicht zwischen dem Schaden, welcher dem Kläger zugefügt wurde, und dem Schaden, welcher dem Beklagten zugefügt werden sollte, schaffen, indem es die Beklagten zur Urteilsveröffentlichung auf der social media-Seite verpflichtete, denn der Schaden wurde durch eine Rechtsverletzung durch eine Grafik verursacht.

Nach stRsp des OGH sind alle Rechtsfolgen bei Verletzung des Rechts am eigenen Bild durch das UrhG abschließend und ausreichend geregelt.

c. **Verlinken von Bildern**

Beim Verlinken von Bildern werden Links auf ein Foto „gesetzt", um durch das Anklicken des Links auf eine andere Webseite zu gelangen.

Wie der VKI – Europäisches Verbraucher Zentrum mE richtig zusammenfasst, ist es grundsätzlich dann erlaubt, fremde Inhalte durch einen Link in einem Posting oder auf der Pinnwand online zu stellen, wenn diese Inhalte mit einer Einwilligung des Rechteinhabers ohnehin für jeden ohne Anmeldung frei zugänglich sind. In diesem Fall wird lediglich der Zugang zu einem Inhalt eröffnet, den dessen Rechteinhaber ohnedies jedem zur Verfügung stellt. Nicht erlaubt ist hingegen eine Linksetzung zu Inhalten, welche gegen den Willen des Rechteinhabers im Internet veröffentlicht wurden.[278] Falls der Sinn des Verlinkens jedoch darin liegt, sich mit dem rechtswidrigen Inhalt der Zielseite zu identifizieren und der Link nur deswegen gesetzt wurde, kann der Linksetzer nach Ansicht des VKI genauso wie der „Seiteninhaber" haften[279].

Das OLG Köln beschäftigte sich im Verfahren 15 U 107/09 mit dem Einstellen von persönlichen Fotos auf Facebook und entschied mit Urteil vom 9.2.2010, dass durch das Einstellen von persönlichen Fotos auf einer SNP eine stillschweigende Einwilligung für die Verwertung auf Personensuchmaschinen abgegeben wird. Das Gericht ging sogar so weit, auszusprechen, dass im Falle eines „ungeschützten Einstellens" eines Bildes zugleich eine „konkludente Einwilligung" abgegeben wird, dass Personen-Suchmaschinen wie 123people die Bilder in der Folge verwenden dürfen. Für das OLG Köln ist somit eine konkludente Zustimmung zur Verwendung von Fotos durch Dritte gegeben, wenn ein Nutzer Bilder „offen" und damit für jedermann zugänglich online stellt.

[278] Vgl *Verein für Konsumenteninformation,* Ihr Recht im Internet (2011) 102.
[279] Vgl *Verein für Konsumenteninformation,* Ihr Recht im Internet (2011) 118 f.

Ich teile die Ansicht des OLG Köln nicht. Meiner Ansicht nach muss unterschieden werden, ob und wofür eine Einwilligung zur Verwendung von online gestellten Bildern erteilt wurde. Ich denke nicht, dass ein Nutzer im Falle eines „ungeschützten Einstellens“ eines Bildes eine generelle Einwilligung zur Veröffentlichung auf jeder beliebigen Webseite erteilen möchte. Vielmehr wäre eine (erneute) Zustimmung des Urhebers notwendig.

2. Zurverfügungstellungsrecht iSd § 18a UrhG

Wie bereits weiter oben festgehalten, hat sich durch die Digitalisierung eine große Vereinfachung von Vervielfältigungs- und Verbreitungsmöglichkeiten ergeben. Die urheberrechtlichen Fragen im Zusammenhang mit SNP stellen sich primär in Bezug auf das Hochladen von Fotos bzw. Film- oder Musikwerken Dritter, die ein Nutzer in seinem Profil anderen Nutzern zur Verfügung stellt und nicht selbst hergestellt hat.

Es stellen sich in diesem Zusammenhang die Fragen, ob dadurch bereits das „öffentliche Zugänglichmachen“ iSd UrhG erfüllt ist bzw ob dadurch Unterlassungs- und Schadenersatzansprüche ausgelöst werden? Beim Hochladen von Inhalten auf eine SNP werden grundsätzlich zwei Verwertungsrechte berührt, das Vervielfältigungsrecht und das Zurverfügungstellungsrecht, Rechte, welche grundsätzlich alleine dem Urheber zustehen. Demnach ist dessen Zustimmung zu solchen Handlungen grundsätzlich erforderlich.

Ziel des Urheberrechts ist der Schutz der „eigentümlichen geistigen Schöpfungen“[280] der Literatur, Tonkunst, bildenden Künste und Filmkunst.[281] Das Urheberrecht hat damit die Aufgabe, der Schutzmechanismus des geistigen Eigentums zu sein und dem Urheber die Urheberrechtspersönlichkeitsrechte und Verwertungsrechte an seinem Werk zu gewährleisten.

Das Verwertungsrecht ist ein ausschließliches Recht, ein Werk gem §§ 14 bis 18 UrhG und den vom Gesetz bestimmten Beschränkungen zu verwerten. Der Urheber eines Werkes hat somit das ausschließliche Recht, über sein Werk zu walten, zu verfügen und dieses zu verändern oder zu zerstören.

[280] § 1 Abs 1 UrhG.
[281] Siehe BG über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), BGBl 111/1936 idgF.

„Eigentümlichkeit“ iZm einem Werk bedeutet eine Unterscheidbarkeit von anderen Werken und verdankt seine Eigenart der Persönlichkeit des Schöpfers.[282] Das Urheberrecht ist zeitlich beschränkt, dh die jeweiligen Verwertungsrechte enden nach Ablauf einer gesetzlich vorgeschriebenen Zeitspanne.[283]

a. Vervielfältigungsrecht

In § 42 UrhG ist normiert, dass eine „Vervielfältigung von einem Werk zum eigenen und privaten Gebrauch grundsätzlich gestattet ist, wenn dies aus nicht kommerziellen Zwecken geschieht“.[284]

Vervielfältigungen auf einer SNP sind damit aber nur legitim, wenn sie zum privaten Gebrauch und weder für unmittelbare noch mittelbare kommerzielle Zwecke geschehen.

Kommerziell ist eine Nutzung zB, wenn ein Fotograf Fotos hochladet, um damit seine Arbeit zu bewerben. In einem solchen Fall kann davon ausgegangen werden, dass zumindest „mittelbar“ ein für den Fotografen kommerzieller Zweck verfolgt werden soll. Demnach wäre eine Vervielfältigung, ohne diesen Fotografen davor um Genehmigung zu bitten, unzulässig.

b. Zurverfügungstellungsrecht

In § 18 a UrhG ist normiert, dass der „Urheber das ausschließliche Recht hat, sein Werk […] zur Verfügung zu stellen, dass es [….] öffentlich zugänglich gemacht wird“. Das Zurverfügungstellungsrecht behandelt damit die Frage, ob ein Nutzer einer SNP überhaupt etwas hochladen darf oder nicht, wenn es dadurch zu einer „öffentlichen Zugänglichmachung“ kommt.

Bei Facebook gibt es aber verschiedene Einstellungsmöglichkeiten, um den „Zugriff“ einzuschränken und nur bestimmten Personenkreisen Zugriff auf bestimmte Inhalte zu gewähren. Ein Nutzer kann einstellen, dass Fotos nur „Familienmitgliedern, bestimmten Freunden und davor erstellten ‚Gruppen‘ etc“ angezeigt werden dürfen und kann somit gewisse Personen oder ganze Personengruppen vom Zugriff ausschließen.

---

[282] *Hauser/Thomasser*, Wettbewerbs- und Immaterialgüterrecht (1998) Rz 880.
[283] § 60 UrhG, BGBl 111/1936 idgF.
[284] § 42 UrhG, BGBl 111/1936 idgF.

Ob eine „Gruppe“ bereits eine „Öffentlichkeit im Sinne des Zurverfügungstellungsrechts“ darstellt, wurde bereits auf Ebene der EU in Art 8 WCT[285], durch welchen die RL 2001/29/EG des Europäischen Parlaments und des Rates vom 22.5.2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (kurz Info-RL) umgesetzt wurde, geklärt, indem der EuGH klarstellte, dass „ihm die Auslegung des Begriffs der Öffentlichkeit obliegt“.[286]

Nach dessen Rechtsprechung sei unter „öffentlich“ zb eine „unbestimmte Zahl möglicher Fernsehzuschauer“ zu verstehen bzw seien „recht viele Personen“ davon erfasst, ohne jedoch eine konkrete numerische Größenordnung anzudeuten.

In der Rechtssache „SGAE“[287] ging es vor dem EuGH um den Begriff der öffentlichen Wiedergabe urheberrechtlich geschützter Werke iSv Art 3 Abs 1 der RL 2001/29/EG im Falle der Wiedergabe über in Hotelzimmern aufgestellte Fernsehgeräte. Der EuGH hatte zunächst die Frage zu beurteilen, wann eine „öffentliche Wiedergabe“ vorliegt.

Ob eine Gruppe öffentlich ist oder nicht, sei primär an der Anzahl der Gruppenmitglieder und einer Gewinnerzielungsabsicht zu bemessen. Die Rechtsprechung hat Öffentlichkeit als „eine unbestimmte Zahl möglicher Fernsehzuschauer“ definiert bzw „dass es um recht viele Personen gehen müsse“. Eine konkrete numerische Größe wurde jedoch nicht genannt. Eine Abgrenzung hat der EuGH am Begriff „privater Bereich“ gezogen. Für den EuGH ist weiters das Erfordernis der Gewinnerzielungsabsicht für das Erfordernis einer öffentlichen Wiedergabe maßgeblich.

In § 18 a Abs 1 UrhG, durch den die Info-RL umgesetzt wurde, wird der Begriff der Öffentlichkeit nicht definiert. Die österreichische Rechtsprechung definiert „Öffentlichkeit“ sehr unterschiedlich: beim Verbreiten liegt „Öffentlichkeit“ vor, wenn das Werk der Allgemeinheit oder einem breiten Publikum zugänglich gemacht wird, bei der öffentlichen Wiedergabe dann, wenn der Kreis der Teilnehmer durch ein „reales persönliches Band verbunden und durch wechselseitige Beziehungen untereinander oder zum Veranstalter nach außen hin abgegrenzt ist“.

---

[285] WCT, WIPO-Urheberrechtsvertrag, 20.12.1996 ist ein von der Weltorganisation für geistiges Eigentum (WIPO) verabschiedetes Sonderabkommen iSd Art 20 der Berner Übereinkunft. Er bildet den Rahmen für die Anpassung der nationalen Urheberrechtsgesetze an die Anforderungen digitaler Netzmedien, siehe http://de.wikipedia.org/wiki/WIPO-Urheberrechtsvertrag

[286] Siehe EuGH 7.12.2006, C-306/05, *Societad General de Autores y Editores de Espana (SGAE)/Rafael Hotels SL*.

[287] Siehe EuGH 7.12.2006, C-306/05, *Societad General de Autores y Editores de Espana (SGAE)/Rafael Hotels SL*.

c. Rechtsverletzungen

Fast alle SNP bieten ihren Nutzern die Möglichkeit, mögliche Urheberrechtsverletzungen (im Zusammenhang mit Bildern etc) zu melden, damit diese Bilder, welche ein Urheberrecht eines Nutzers verletzen, gegebenenfalls aus dem Suchindex wieder entfernt werden können. Diese Meldemöglichkeit soll eine „erste Hilfsmaßnahme" für die in ihren Rechten verletzten Personen darstellen.

Facebook schreibt unter Punkt 5.5. seiner Nutzungsbedingungen[288]: „Bei wiederholten Verletzungen von Rechten am geistigem Eigentum anderer droht Facebook auch mit einer Sperre des Kontos."

Twitter behält sich gem Punkt 9 seiner Nutzungsbedingungen[289] das Recht vor, Inhalte von Nutzern ohne vorherige Ankündigung zu löschen, wenn Twitter der Auffassung ist, dass diese das Urheberrecht anderer Nutzer verletzen. Twitter droht sogar an, bei wiederholten Verstößen das Konto zu löschen.

d. Entstehung des Urheberrechts und Geltendmachung von Rechtsverletzungen

Das Urheberrecht entsteht grundsätzlich zeitgleich mit der Schaffung eines Werkes, dh die Entstehung und der Beginn des Schutzes bedarf keiner weiteren Maßnahmen, wie es zB bei einer Marke durch deren Registrierung nötig ist. Das bedeutet aber, dass auch dann Urheberrechtsverletzungen vorliegen können, wenn dem Verletzer der Urheber womöglich gar nicht bekannt ist. Rechtsverletzungen können somit auch dann eintreten, wenn es dem Verletzer mangels Kenntnis des Urhebers gar nicht möglich war, eine entsprechende Zustimmung zur Nutzung, Verpflichtung oder Vervielfältigung des Werkes einzuholen.

[288] Stand 30.10.2012.
[289] Stand 30.10.2012.

e. Rechtsverletzung durch die Nutzung, das Posten oder das Teilen eines fremden Werkes auf einer Social network-Plattform

Verwendet ein Nutzer einer SNP ein urheberrechtlich geschütztes Werk, beispielsweise als Profilbild, kann es sich dabei um eine Verletzung des Urheberrechts handeln, wenn dadurch das Werk der Öffentlichkeit zugänglich gemacht wird.

Ähnlich verhält es sich, wenn ein fremdes Werk gepostet oder auf einer SNP „geteilt" wird, und dadurch ein fremdes Werk der Öffentlichkeit zugänglich gemacht wird.

Es gibt jedoch zwei Ausnahmefälle, bei welchen es zu keiner Urheberrechtsverletzung kommt, obwohl ein fremdes Werk benutzt wird:

● Verwendung in Form einer Privatkopie iSd § 42 UrhG:

Eine Privatkopie iSd § 42 UrhG liegt dann vor, wenn eine – grundsätzlich dem Urheber vorbehaltene – Vervielfältigung lediglich für private Zwecke oder nur für einen engen privaten Kreis erfolgt und – eingeschränkt – auf einem SNP-Profil verwendet wird. Wobei die Einschränkung mE streng zu beurteilen ist, da auch bei einer Einschränkung normalerweise viele Nutzer Zugriff auf online gestellte Werke eines anderen Nutzers haben. Dies ist wohl immer iZm der Freundesanzahl des jeweiligen Nutzers zu beurteilen. Der private Gebrauch ist dann gegeben, wenn ein Werk lediglich dafür vervielfältigt wird, um dieses dann selbst zu privaten Zwecken zu nutzen, wenn die einzelnen Vervielfältigungsstücke auf Papier oder einem ähnlichen Träger hergestellt werden und die Privatkopie darf nicht der Öffentlichkeit zugänglich gemacht werden. Es hängt somit grundsätzlich von der Größe der Gruppe ab, um eine Zurverfügungstellung anzunehmen.

Bei digitalen Werken ist wesentlich, dass von diesen lediglich von natürlichen Personen zu nicht kommerziellen Zwecken Privatkopien angefertigt werden dürfen. Dh von Fotos, welche auf einer SNP veröffentlicht wurden, dürfen nur Privatkopien hergestellt werden, wenn diese zu nicht kommerziellen Zwecken erfolgen. Bei Profilbildern auf einer SNP ist weiters zu beachten, dass diese grundsätzlich für die Allgemeinsicht sind, falls nicht eine entsprechende Einstellung getroffen wurde, und demnach liegt eine Urheberrechtsverletzung vor, wenn ein Bild als Profilbild verwendet wird, zu dessen Nutzung der Urheber keine Zustimmung erteilt hat.

● Verwendung in Form eines Zitats iSd § 46 UrhG

Die zweite Ausnahmeregelung ist das Zitat gem § 46 UrhG. Als Zitat wird die Übernahme eines fremden, geistigen Gutes, sei es wörtlich oder zumindest dem Sinne nach, verstanden. Kleine Zitate sind solche, bei welchen einzelne Stellen eines bereits veröffentlichten Sprachwerks unter Nennung des Autors angeführt werden und eine Belegfunktion erfüllt wird. Bei großen Zitaten werden umfangreichere Stellen zitiert.

(1) Rechtsfolgen im Falle einer Urheberrechtsverletzung

Im Falle einer Urheberrechtsverletzung besteht einerseits ein zivilrechtlicher Anspruch auf Unterlassung, Beseitigung, Urteilsveröffentlichung, ein angemessenes Entgelt, Schadenersatz und Herausgabe des Gewinnes und andererseits besteht die Möglichkeit einer strafrechtlichen Verfolgung bei vorsätzlich begangenen Eingriffen in Verwertungsrechte gem § 91 UrhG.

Es liegt jedoch dann keine Strafbarkeit vor, wenn es sich um eine Vervielfältigung oder um ein Festhalten eines Vortrages oder einer Aufführung jeweils zum eigenen Gebrauch handelt.

(2) Fazit

Es kann somit festgehalten werden, dass bei einer kommerziellen Nutzung von SNP auch eine geschlossene Gruppe grundsätzlich eine „Öffentlichkeit“ darstellen kann. Im Falle einer nicht kommerziellen Nutzung ist die Frage der Öffentlichkeit, anhand der Größe des Teilnehmerkreises bzw der Gruppe zu beantworten. Denn auch wenn eine „Einschränkung“ getroffen wurde, kann zumeist eine große Anzahl von Personen die Veröffentlichungen einsehen.

D. RECHTSPROBLEME IM ZUSAMMENHANG MIT DEM FRIENDFINDER

Wie bereits weiter oben beschrieben, ist der Friendfinder („Freundefinder“) eine von Facebook entwickelte Software, welche die Kontakte der Nutzer miteinander vergleicht und in der Folge den Nutzern Personen als Freunde vorschlägt, welche mehrmals auf diesen Listen aufscheinen, dh der Friendfinder schreibt Nicht-Nutzer an und schlägt ihnen vor, neue Nutzer von Facebook zu werden.

Der Friendfinder ist primär in Deutschland auf heftige Kritik gestoßen, weswegen in der Folge vor allem anhand der deutschen Rechtslage versucht wird, einige Problembereiche idZ aufzuzeigen.

Beim Datenschutzbeauftragten für Hamburg, *Johannes Caspar*, gingen unzählige Beschwerden von Nicht-Nutzern ein, da sich diese durch „unfreiwillige" Freundschaftsanfragen „gestört" fühlten, da sie, ohne aktiv ein Profil anlegen zu wollen, mittels E-Mail (teilweise samt Bildern der Nutzer) gefragt wurden, ob sie nicht Mitglieder von Facebook werden wollen.[290] Die Daten stammten aus den E-Mail- und Adressbüchern bereits bestehender Facebook-Nutzer.

Die Vorwürfe deutscher Datenschützer gründeten sich primär darauf, dass Facebook die zuvor bei Nutzern gesammelten Daten von Nichtmitgliedern speicherte und ohne Einverständnis zur Vermarktung weiter nützte. Die Nutzer wurden nicht informiert, welche Auswirkungen ihre Datenpreisgabe in diesem Zusammenhang hatte.

Für *Caspar* dürfen nur solche Kontakte zu Facebook eingeladen werden, die der Nutzer persönlich kennt und auch tatsächlich einladen möchte und eingeladene Nicht-Mitglieder müssen ebenfalls informiert werden, warum sie diese E-Mail erhalten. Anschließend sollen sie verfügen können, dass sie keine weiteren E-Mails von Facebook bekommen wollen, und ihre Adresse sperren, denn nur so könne dem Recht auf informationelle Selbstbestimmung entsprochen werden.

1. Das Recht auf informationelle Selbstbestimmung

Jeder habe das Recht, selber zu bestimmen, wer seine Daten bekommt, und vor allem ein Recht darauf, zu wissen, wie sie dort verwendet werden. Diese informationelle Selbstbestimmung ist seit dem Volkszählungsurteil 1983 als Grundrecht fest verankert. Auf diesem Recht sind auch große Teile des deutschen Datenschutzgesetzes aufgebaut.

Das deutsche Bundesverfassungsgericht hat im deutschen Volkszählungsurteil vom 15.12.1983[291] erstmals anerkannt, dass es ein Grundrecht auf die sogenannte informationelle

[290] http://jgoldfarb.wordpress.com/2011/01/24/facebook-andert-friend-finder-aber-nur-ein-bischen

[291] Siehe BVerfG 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83. In diesem Urteil hat das BundesVerfG auf die Verfassungsbeschwerden gegen die damalige Volkszählung 1983 wesentliche Grundsätze des verfassungskonformen Umgangs mit Daten festgeschrieben und wurde mit diesem Urteil das „informationelle Selbstbestimmungsrecht" entwickelt (*Ehmann/Kramer*, Datenschutz-Glossar [2005] 173).

Selbstbestimmung gibt und hat dazu Folgendes ausgeführt: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig." Es soll demnach ein „Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" bestehen. Das Grundrecht auf informationelle Selbstbestimmung ist eine Art Weiterführung des grundrechtlich geschützten allgemeinen Persönlichkeitsrechts und beide werden verfassungsrechtlich aus Art 2 Abs 1 GG (sog allgemeine Handlungsfreiheit) in Verbindung mit Art 1 Abs 1 GG (Menschenwürde-Garantie) hergeleitet.[292]

Der Friendfinder wurde als Widerspruch zur informationellen Selbstbestimmung angesehen, da Mitglieder von Facebook ohne eindeutige Erklärung dazu aufgefordert wurden, Daten über Personen freizugeben, die selbst nicht bei Facebook waren, was heftige Kritik zur Folge hatte.

2. Judikatur

Heftige Kritik war die Folge der Einführung des Friendfinder. Bereits im Jahr 2009 kritisierte die Art 29-Datenschutzgruppe[293] die Erhebung und Verwendung von E-Mail-Adressen und Namen von Nicht-Mitgliedern durch SNP stark und hielt fest, dass ein Verstoß gegen datenschutzrechtliche Grundsätze vorliege, wenn Beziehungsprofile von Nicht-Mitgliedern gespeichert werden, da eine derartige Erhebung jeglicher rechtlicher Grundlagen entbehre:

Facebook sah dies anders und formulierte die Erhebung von Daten von Nicht-Mitgliedern auf seiner Webseite folgendermaßen:
Processing data of non-members

[292] Das Grundgesetz ist das Gegenstück zum B-VG. Die Menschenwürde ist in keinem österreichischen Gesetz niedergeschrieben. Das Persönlichkeitsrecht wird aber aus § 16 ABGB abgeleitet.

[293] „Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt. Die Gruppe ist unabhängig und hat beratende Funktion". Beschreibung der Datenschutzgruppe in Art 29 Abs 1 DatenschutzRL. Die Art 29-Datenschutzgruppe hat zwar nur beratende Funktion, doch übt sie großen Einfluss auf die Datenschutzdiskussion in der EU aus. Vgl *Ehmann/Kramer*, Datenschutz-Glossar (2005) Praxislexikon 57. Der Art 29-Datenschutzgruppe obliegt gem Art 30 DatenschutzRL die Überprüfung der Umsetzung der DatenschutzRL in die nationalen Rechtsordnungen. Sie kann zu allen Fragen Stellungnahmen abgeben, wenn diese den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen. Die Art 29-Datenschutzgruppe schreibt jährlich Berichte, welche der Kommission, dem Parlament und dem Rat vorgelegt werden. Ihre Empfehlungen haben keine bindende Wirkung, sind aber dennoch von großer praktischer Bedeutung.

„However, the processing of such data about non-members by the SNS may only be performed if one of the criteria laid down in Article 7 of the Data Protection Directive is fulfilled. In addition, the creation of pre-built profiles of non-members through the aggregation of data that is independently contributed by SNS users, including relationship data inferred from uploaded address books, lacks a legal basis.“[294]

Auch der deutsche Verbraucherzentrale Bundesverband (vzbv)[295] kritisierte das Vorgehen von Facebook in diesem Zusammenhang stark und mahnte Facebook Ireland mit einem Schreiben vom 28.7.2010 wegen des Friendfinder und des Adressbuchimports sowie unzulässiger Nutzungsbedingungen und Datenschutzbestimmungen ab. Nachdem Facebook nicht darauf reagierte und auch keine Unterlassungserklärung abgab, reichte der vzbv gegen Facebook eine Klage vor dem LG Berlin ein.

Der vzbv gründete seine Klage darauf, dass Facebook seiner Ansicht nach mit dem „Adressbuch-Import“ und der „Einladung von Nicht-Mitgliedern (sog Freundefinder)“ gegen geltende Verbraucherrechte verstoße, indem der Freundefinder Facebook-Nutzern die Möglichkeit biete, den gesamten Datenbestand von Personen, inklusive deren E-Mail-Adressen und Namen, welche keine Facebook-Nutzer sind, auf die Facebook-Seite zu importieren. Hauptkritikpunkt war somit, dass Mitglieder von Facebook ohne eindeutige Erklärung dazu aufgefordert wurden, Namen und E-Mail-Adressen aus ihrem E-Mail-Postfach freizugeben, die selbst nicht bei Facebook waren. Diesen Personen wurde in der Folge ohne vorherige Einwilligung eine Einladung zu Facebook gesandt, was verbraucherrechtlich höchst bedenklich ist.

Facebook erklärte daraufhin, dass die „Daten lediglich zur Einladung benützt werden und ein leichteres Registrieren ermöglichen sollen“.

Mit Urteil vom 6.3.2012 sprach das LG Berlin aus, dass es unlauter iSd § 7 Abs 2 und 3 dt UWG sei, Einladungs-E-Mails an Personen zu versenden, welche nicht bei Facebook registriert sind. Facebook-Mitglieder, welche die E-Mail-Adressen auf Facebook hochgeladen haben, seien hingegen als Mittäter iSd § 830 Abs 1 Satz 1 BGB zu qualifizieren.

---

[294] http://www.scribd.com/doc/16736099/ARTICLE-29-DATA-PROTECTION-WORKING-PARTY-Opinion-52009-on-online-social-networking#outer_page_8

[295] Der vzbv vertritt die Interessen der Verbraucher gegenüber Politik, Wirtschaft und Zivilgesellschaft. Hier finden sich aktuelle Informationen zu Verbraucherschutz, Verbraucherpolitik und Verbraucherrecht. Der vzbv trägt die Anliegen der Verbraucher in die Öffentlichkeit und wirkt auf die Politik ein, Spielregeln für einen fairen und transparenten Markt zu schaffen. Er weist auf Missstände hin und setzt Verbraucherrechte notfalls vor Gericht durch. Der vzbv schafft die Grundlagen, damit ihre Mitglieder seriöse und unabhängige Verbraucherberatung leisten können. Siehe auch: http://www.vzbv.de/go/

Facebook Irland legte Berufung beim Kammergericht Berlin ein, welche am 24.1.2014, 5U 42/12, zurückgewiesen wurde, da der Friendfinder gegen deutsches Recht verstoße.[296]

a. Friendfinder und die Anwendung deutschen Bundesdatenschutzrechts

Das Kammergericht Berlin sprach hinsichtlich des Friendfinder und des anwendbaren (Datenschutz-)Rechts aus, dass deswegen deutsches Datenschutzrecht anzuwenden ist, weil „Facebook jedenfalls auch in Deutschland Daten iSd deutschen Datenschutzrechts ‚erhebt und verarbeitet'".[297] Durch die Tochtergesellschaft in Irland (siehe weiter unten im Detail) werden nämlich Cookies auf den Computern der Nutzer (ua) in Deutschland gesetzt und dadurch „Mittel" zur Datenverarbeitung geschaffen. Diese Daten werden schließlich „erhoben" und „verarbeitet" im Sinne des Bundesdatenschutzgesetzes (BDSG), weswegen deutsches Datenschutzrecht zur Anwendung kommt.

3. Fazit

Aus obigen Ausführungen ergibt sich, dass der Friendfinder einen Verstoß gegen Datenschutzrecht darstellte. Nach Betätigen des Buttons „Freunde finden" durch den Nutzer verarbeitet und nutzt Facebook personenbezogene Daten zu Werbezwecken ohne Informationen und die gesetzlich vorgegebene Einwilligung seiner Nutzer eingeholt zu haben und mangelte es daher an einer datenschutzrechtlich notwendigen Einwilligung.

Aus dem Urteil des KG Berlin[298] geht hervor, dass das deutsche Datenschutzrecht sowie die EU-Datenschutzrichtlinie den einzelnen Verbraucher nicht nur in seinem Persönlichkeitsrecht schützen sollen, sondern sei vielmehr ebenso Teil des allgemeinen Persönlichkeitsrechts der Schutz des Verbrauchers im Zusammenhang mit einer Datenverarbeitung durch Unternehmen.

Schließlich reglementiere das BDSG wie auch die EG-Datenschutzrichtlinie nicht nur eine Datenverarbeitung im persönlichen Lebensbereich der Bürger, sondern auch in ihrer wirtschaftlichen Betätigung als Verbraucher.

[296] Siehe LG Berlin 6.3.2012, 16 O 551/10 und KG Berlin 24.1.2014, 5 U 42/12.
[297] Siehe KG Berlin 24.1.2014, 5 U 42/12.
[298] Siehe KG Berlin 24.1.2014, 5 U 42/12.

E. RECHTSPROBLEME IM ZUSAMMENHANG MIT DEM LIKE-BUTTON

Wie bereits weiter oben ausgeführt wurde, handelt es sich beim Like-Button um ein Social Plugin, welches auf fremden Webseiten angezeigt wird. Durch Anklicken können Facebook-Nutzer zeigen, dass sie an einer bestimmten Webseite Gefallen finden.

Facebook kann damit aber über seine Nutzer Daten verfolgen und sammeln. Sobald ein Like-Button auf einer Webseite implementiert wurde, können von Facebook personenbezogene Daten der Besucher-Webseite erhoben und ausgewertet werden.

Aus datenschutzrechtlicher Sicht handelt es sich noch dazu um personenbezogene Daten iSd § 4 Z 1 DSG, da die „Webseite-besuchende" Person über das Profil und den Facebook-Account eindeutig identifizierbar ist. Problematisch ist weiters, dass üblicherweise auch keine Zustimmung des Nutzers erfolgte und auch keine rechtliche Verpflichtung zur Übermittlung dieser Daten an Facebook besteht. Dies wären jedoch die Voraussetzungen für eine Übermittlung personenbezogener Daten iSd Datenschutzgesetzes.

Die deutschen Aufsichtsbehörden („Düsseldorfer Kreis[299]"), die sich dazu bereits geäußert haben, sind daher – mE zu Recht – der Ansicht, dass die Verwendung des Like-Buttons datenschutzrechtlich problematisch ist[300].

Facebook verstoße ihrer Ansicht nach gegen deutsches und europäisches Datenschutzrecht, weil Nutzer nicht hinreichend informiert würden, welche Verkehrs- und Inhaltsdaten in die USA übermittelt und wie sie dort genutzt werden. Konkret geht es dabei um Daten, die Facebook auf Fanseiten und auf Websites von Drittanbietern sammelt, die den sogenannten Like-Button einbinden und damit den Code von Facebook nachladen.

Der Betreiber einer SNP darf personenbezogene Daten grundsätzlich nur zur Verwaltung des Benutzerkontos, für eine Kontaktaufnahme und zur Verfolgung von Rechtsverstößen verwenden. Für andere Zwecke braucht der Betreiber die ausdrückliche Zustimmung des Nutzers. Der Betreiber darf Daten an Dritte nicht weitergeben, wenn keine explizite

[299] Der sog Düsseldorfer Kreis ist ein verwaltungsinternes Gremium bestehend aus den Datenschutzbehörden für die Privatwirtschaft. Der Düsseldorfer Kreis gibt Stellungnahmen zu strittigen Rechtsfragen iZm dem Datenschutzrecht ab. Mittlerweile behandelt die Art 29-Gruppe viele (ähnliche) Fragen wie der Düsseldorfer Kreis, siehe *Ehmann/Kramer*, Datenschutz-Glossar (2005) 70.

[300] Beschluss vom 8.12.2011. Entschließung des Düsseldorfer Kreises (das ist die Oberste Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich) zum Thema „Datenschutz in sozialen Netzwerken", siehe http://www.bfdi.bund.de/DE/Entschliessungen/DuesseldorferKreis/DKreis_node.html

Zustimmung vorliegt. Die österreichische Rechtsprechung stellt an Zustimmungserklärungen sehr hohe Ansprüche. Da man nach dem DSG nur „in Kenntnis der Sachlage für den konkreten Fall“ zustimmen kann, muss die Zustimmungserklärung entsprechend verständlich und transparent sein.

1. Der Like-Button im Lichte des DSG

Rechtlich betrachtet sind mit dem Like-Button nicht nur Vorteile verbunden, da personenbezogene Daten (siehe § 4 Z 1 DSG) der Webseitenbesucher von Facebook erhoben und gesammelt werden[301]. Personenbezogen sind die Daten iSd DSG[302] deswegen, weil die betroffene Person über das Facebook-Profil bzw den -Account eindeutig zuordenbar ist.

Des Weiteren könnte dadurch auch die IP-Adresse des Nutzers erhoben werden. IP-Adressen sind die Grundlage einer Kommunikation im Internet. IP-Adressen sind Zahlencodes, welche der Adressierung einzelner Rechner in einem Netzwerk dienen, dh eine IP-Adresse sorgt dafür, dass ein Rechner identifiziert werden kann.[303]

Dank einer sehr komplexen Cookie- und Tracking-Technik[304] kann Facebook Daten „sammeln“, sogar ohne dass es der betroffene Nutzer merkt. Dh Facebook kann durch den Like-Button zahlreiche Informationen wie Vorlieben, Interessen etc seiner Nutzer sammeln.

Ein Tracking-Cookie ist eine kleine Textdatei, die beim Besuch einer Webseite auf dem Rechner gespeichert wird, und damit soll der Internetnutzer beim nächsten Besuch wiedererkannt und gleich mit seinem Benutzernamen oder den ihn interessierenden Produkten durch gezielte Werbeeinschaltungen angesprochen werden, so *Dassler*[305]. Dadurch können Informationen darüber gesammelt werden, welche Seiten ein Nutzer wie lange und wie oft

---

[301] *Pollirer/Weiss/Knyrim*, DSG (2010) § 4; Name, Geburtsdatum, Adresse, Geschlecht, Einkommen, Vermögen, Lebensgewohnheiten, Umsatz, Werturteile, Fingerabdruck, Bild, Stimme stellen idR personenbezogene Daten dar.

[302] Personenbezogene Daten sind Angaben, mit deren Hilfe man ohne unverhältnismäßigen Aufwand eine Person finden und zurückverfolgen kann. Nach hM gehören dazu Name, E-Mail-Adresse und mittlerweile auch IP-Adressen.

[303] Vgl *Lechner* in *Bauer/Reimer*, Handbuch Datenschutzrecht (2009) 213 ff und RL 2006/24/EG, Vorratsdatenspeicherungsrichtlinie. Der Anschlussinhaber eines PC ist aber nicht automatisch auch der Rechtsverletzer.

[304] Gemäß Computerlexikon (www.computerlexikon.com) ist ein Tracking Cookie oder verfolgendes Cookie eine kleine Textdatei, die bei einem Besuch einer Webseite auf dem Rechner gespeichert wird. Im Gegensatz zu normalen Cookies werden die verfolgenden Cookies ausgelesen, um Einblicke in das Surfverhalten des Benutzers zu erlangen. Damit kann dann der User gezielt mit Werbung etc bombardiert werden. Um dieser Art von Cookies vorzubeugen, kann man in den Optionen des Browsers einstellen, ob alle oder nur bestimmte Textdateien angenommen werden.

[305] *Dassler*, Datenschutz in der Informationsgesellschaft (2007) 91.

besucht hat. Als problematisch erweist sich, dass dadurch auch Informationen von Nicht-Mitgliedern gesammelt werden.

§ 10 DSG normiert, dass „Auftraggeber“ bei ihren Datenanwendungen Dienstleister in Anspruch nehmen dürfen, […], notwendige Vereinbarungen darüber aber getroffen werden müssen und damit eine Auftragsdatenverarbeitung vorliegen muss, welche in diesem Fall aber nicht gegeben ist, da weder eine Einwilligung vom Nutzer zur Übermittlung der Daten erfolgt, noch eine rechtliche Grundlage dafür besteht. Es liegt damit keine „Auftragsdatenverarbeitung“ iSd § 10 DSG vor, da es sich auch um zwei unterschiedliche Stellen handelt, zwischen welchen keine Weisungsgebundenheit besteht.

Es kann festgehalten werden, dass personenbezogene Daten nur übermittelt werden dürfen, wenn entweder der Nutzer selbst zuvor zugestimmt hat oder eine Rechtsgrundlage oder eine rechtliche Verpflichtung zur Übermittlung besteht. Im Falle von Facebook kann der Nutzer aber gar nicht wirklich zustimmen, da ihm nicht mitgeteilt wird, wofür, wo, wie lange etc die Daten gespeichert, verarbeitet oder weitergegeben werden. Auch liegt keine rechtliche Verpflichtung vor.

Webseitenbetreiber, welche sog Social Plugins (wie den Like-Button) benützen, sollten daher einen entsprechenden Datenschutzhinweis in der Datenschutzerklärung vorsehen, der die Besucher ihrer Webseite zumindest einmal über die jeweilige Funktion sowie den Empfänger und den Inhalt einer Datenübermittlung informiert. Es muss in der Datenschutzerklärung klar darauf hingewiesen werden, dass sich Social Plugins auf der Webseite befinden und wer die Betreiber bzw Empfänger der Plugins sind. Alternativ kann das Social Plugin so ausgestaltet sein, dass es nur Nutzern angeboten wird, welche dessen Einbindung davor ausdrücklich zugestimmt hatten, um damit die Transparenz ausreichend zu gewährleisten.

Das tatsächliche Erfordernis eines Like-Buttons wird von den Webseitenbetreibern damit begründet, dass damit die Besucherzahlen gesteigert und das Geschäft und die Internetpräsenz verstärkt werden können.

Ein Unternehmer bzw Webseitenbetreiber wird eher für die Notwendigkeit eines Like-Buttons argumentieren. Anders sehen es jedoch Datenschutz-Verfechter. Diese argumentieren, dass es nicht nötig ist, Daten von Nicht-Mitgliedern zu sammeln, um eine Webseite betreiben zu können. Es sei auf keinen Fall nötig, IP-Adressen von Nicht-Mitgliedern zu erheben, um eine Webseite betreiben zu können.

Ob der letzte Punkt tatsächlich schlagend wird bzw ist, bleibt abzuwarten, da die Pflicht der Datenschutzerklärung grundsätzlich nicht als Marktverhaltensvorschrift konzipiert wurde und daher kein „richtiger" wettbewerbsrechtlicher Verstoß darin gesehen werden kann, wenn in einer Datenschutzerklärung nicht explizit auf den Like-Button hingewiesen wird.

2. Judikatur im Zusammenhang mit dem Like-Button

Das LG Berlin hat mit Beschluss vom 14.3.2011[306] den Antrag der Antragstellerin, eine einstweilige Verfügung gegen die Nutzung eines „Gefällt mir"-Buttons zu erlassen, mit der Begründung zurückgewiesen, dass § 13 dt TMG[307] nicht „als Marktverhaltensvorschrift zu qualifizieren ist",[308] denn im Kern ist die Aufgabe des § 13 dt TMG der Persönlichkeitsschutz des Betroffenen und nicht die Kontrolle eines lauteren Verhaltens am Markt.

Ausgangspunkt der obigen Entscheidung war ein Streit zwischen zwei Online-Händlern, welche beide ua „Sterntaufen" anboten. Einer der beiden Händler hatte auf seiner Webseite einen Like-Button installiert und, wie der andere Händler vorbrachte, die Besucher nicht über Art, Umfang und Zweck der erhobenen personenbezogenen Daten unterrichtet und daher hat dieser beim LG Berlin beantragt, dass eine einstweilige Verfügung gegen den Beklagten zu erlassen sei, da ein derartiges Verhalten einen Verstoß gegen das Wettbewerbsrecht darstelle. Wie bereits weiter oben in diesem Kapitel ausgeführt, werden nämlich nicht nur beim Aktivieren des Like-Buttons, sondern bereits beim Aufrufen der Webseite, welche den Like-Button enthält, potenziell personenbezogene Daten an Facebook übertragen und gespeichert, ohne dass der Betroffene darüber entsprechend den gesetzlichen Vorgaben informiert wird. Dies hat nach Ansicht des Mitbewerbers eine Wettbewerbsverletzung aufgrund der Missachtung gesetzlicher Vorgaben dargestellt.[309]

Das LG Berlin hatte sich also mit der Frage zu beschäftigen, ob der Like-Button im Verhältnis zwischen Konkurrenten eine Wettbewerbswidrigkeit darstellt, und hat schließlich ausgesprochen, dass durch die Nutzung des Buttons kein Verstoß gegen das

[306] Siehe LG Berlin 14.3.2011, 91 O 25/11.

[307] Siehe § 13 Abs 1 dt TMG. Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der RL 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl L 281, 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist.

[308] Siehe Leitsatz unter http://www.telemedicus.info/urteile/Wettbewerbsrecht/Abmahnungen/1241-LG-Berlin-Az-91-O-2511-Facebook-Like-Button.html (Stand: 24.9.2011); LG Berlin 14.3.2011, 91 O 25/11 und KG Berlin 29.4.2011, 5 W 88/11.

[309] Siehe auch ecolex 2011, 898.

Wettbewerbsrecht vorliege. Grundsätzlich seien die hier relevanten datenschutzrechtlichen Pflichten des Anbieters einer Webseite durch § 13 dt TMG geregelt. Diese Regelung sei jedoch nicht als „Marktverhaltensvorschrift“ iSd deutschen Wettbewerbsrechts zu bewerten[310]. Solche Vorschriften seien dadurch bestimmt, das Marktverhalten im Interesse der Marktteilnehmer zu regeln und gleiche Voraussetzungen für die auf einem Markt tätigen Wettbewerber zu schaffen. Dies gelte jedoch nicht für § 13 dt TMG. Die Vorschriften zum Datenschutz dienten jedoch, anders als Verbraucherschutzvorschriften zum Internethandel, dem Persönlichkeitsschutz der Betroffenen und nicht dazu, für ein lauteres Verhalten am Markt zu sorgen. Insofern komme es nicht mehr darauf an, ob die Verwendung des Buttons überhaupt geeignet ist, den Wettbewerb iSd Wettbewerbsrechts mehr als nur unerheblich zu beeinträchtigen.

Diese Entscheidung betrifft aber lediglich das Verhältnis Wettbewerber – Wettbewerber. Die Frage, ob und inwieweit die Nutzung des Like-Buttons im Verhältnis von Nutzer und Webseitenbetreiber einen Datenschutzkonflikt darstellt, musste vom LG Berlin nicht behandelt und entschieden werden.[311]

Im Rechtsmittelverfahren hat das KG Berlin am 29.4.2011 einen Beschluss (5 W 88/11[312]) gefasst, mit welchem die Beschwerde der Antragstellerin vom 31.3.2011 gegen den Beschluss der Kammer für Handelssachen des LG Berlin vom 14.3.2011 zurückgewiesen wurde. Es wurde erneut ausgesprochen, dass der „Einsatz des Like-Buttons“ von Facebook nicht wettbewerbswidrig sei. Somit wurde der Antrag des Mitbewerbers auf Erlass einer einstweiligen Verfügung gegen einen Webseitenbetreiber, welcher den Like-Button verwendet hatte, erneut abgewiesen.

Der Grund des Streits war, dass sich ein Marktteilnehmer von einem Konkurrenten, welcher auf seiner Webseite einen Like-Button integriert hatte, gestört und aus wettbewerbsrechtlicher Sicht benachteiligt fühlte. Das Gericht hat seine Entscheidung primär darauf gestützt, dass

---

[310] Siehe § 4 Nr. 11 dt UWG: *„Nach § 4 Nr. 11 UWG handelt aber nur derjenige unlauter, der einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln. Als Marktverhalten ist jede Tätigkeit auf dem Markt zu sehen, durch die ein Unternehmer auf die Mitbewerber, Verbraucher und sonstigen Marktteilnehmer einwirkt. Dazu gehören nicht nur das Angebot und die Nachfrage von Waren und Dienstleistungen, sondern auch die Werbung und der Abschluss und die Durchführung von Verträgen (vgl Köhler in: Köhler/Bornkamm, UWG, 29. Aufl., § 4, Rn 11.34; Schaffert in: Münchener Kommentar, Lauterkeitsrecht, § 4 Nr. 11, Rn 54).“*, siehe http://www.telemedicus.info/ urteile/Wettbewerbsrecht/Abmahnungen/1281-KG-Berlin-Az-5-W-8811-Wettbewerbsrechtliche-Zulaessigkeit-des-Like-Buttons-von-Facebook.html

[311] Vgl *Heidrich*, http://www.heise.de/newsticker/meldung/Gefaellt-mir-Button-von-Facebook-verstoesst-nicht-gegen-Wettbewerbsrecht-1230632 (Stand: 23.9.2011).

[312] KG Berlin 29.4.2011, 5 W 88/11, http://openjur.de/u/164627.html (Stand: 24.5.2011).

kein Verstoß gegen Marktverhaltensvorschriften vorliege. Man darf jedoch nicht außer Acht lassen, dass obige Entscheidung lediglich den wettbewerbsrechtlichen Aspekt untersucht hat, nicht jedoch den datenschutzrechtlichen. Außerdem ist bei einer Abmahnung wegen eines möglichen Verstoßes gegen das Datenschutzrecht eine – rechtlich – spannendere Entscheidung[313] zu erwarten.

3. Fazit

Wie in diesem Kapitel weiter oben erwähnt, betreffen die Entscheidungen lediglich das Verhältnis Wettbewerber – Wettbewerber. Auf die Frage, ob und inwieweit die Nutzung des Like-Buttons einen Datenschutzkonflikt im Verhältnis von Nutzer und Webseitenbetreiber darstellt, wird nicht eingegangen, da diese vom LG Berlin nicht behandelt und entschieden werden musste.

Grundsätzlich ist die Entscheidung des LG Berlin zu begrüßen, da sie im Hinblick auf die Frage der Einbindung derartiger Plugins zu ein wenig mehr Rechtssicherheit geführt hat. Es bleibt jedoch die Frage offen, ob dadurch ein datenschutzrechtliches Problem entstehen könnte, bzw bleibt die Frage nach den Anforderungen bei der Einbindung derartiger Plugins weiterhin ungeklärt.

Ich bin der Ansicht, dass sich aufgrund der stetig wachsenden Bedeutung von SNP die Spruchpraxis im Zusammenhang mit dem Like-Button in den nächsten Jahren intensivieren wird. Es bleibt also abzuwarten, wie sich die Rechtsprechung entwickeln wird.

F. LÖSCHEN DER DATEN

1. Deaktivierung/Löschung eines Facebook-Accounts

In diesem Kapitel soll auf die Frage eingegangen werden, ob ein vollständiges Löschen (bzw eine Deaktivierung) eines Facebook-Accounts möglich und wie vollständig ein Löschen tatsächlich ist.

[313] Bis dato ist noch keine höchstgerichtliche Entscheidung ergangen (Stand: 18.10.2012).

Facebook bietet seinen Nutzern grundsätzlich sowohl eine „Deaktivierung“ als auch eine „Löschung“ des Facebook-Accounts an, wobei bei einer Deaktivierung das Konto lediglich nicht mehr angezeigt wird und Facebook die Profilinformationen weiterhin speichert, um dem Benutzer die Möglichkeit zu bewahren, das deaktivierte Konto zu einem späteren Zeitpunkt wieder zu aktivieren. Bei einer Löschung sollen hingegen alle Inhalte dauerhaft gelöscht werden.

Bis vor kurzem fand sich nachfolgender Text auf der Facebook-Webseite in den Datenschutzrichtlinien iZm dem Löschen eines Accounts (Stand 2010):

„Nach dem Entfernen von Daten oder dem Löschen eines Kontos werden Kopien der Daten unter Umständen an anderer Stelle angezeigt, sofern sie mit anderen Benutzern ausgetauscht, übermittelt oder von anderen Benutzern kopiert oder gespeichert wurden. Der Benutzername wird nicht mehr mit diesen Daten verknüpft. Bestimmte Informationen werden zur Vermeidung von Identitätsbetrug oder anderem missbräuchlichen Verhalten gespeichert, selbst wenn sie gelöscht worden sein sollten.“

Mit obigem Text wies Facebook darauf hin, dass sie zwar ein Löschen anbieten, jedoch nicht garantieren können (wollen?), dass im Falle eines Löschens oder Entfernens von Daten diese Daten auch definitiv nicht mehr auffindbar sind, denn Facebook kann nicht verhindern, dass ein anderer Nutzer die gelöschten oder entfernten Daten nicht bereits abgespeichert hat. Denn das Entfernen und Löschen betreffe nur das eigene Facebook-Profil, nicht jedoch auch die Profile von Freunden und Bekannten.

In der Zwischenzeit änderte Facebook seine Datenverwendungsrichtlinien (mehrfach) und steht nun folgender Text unter dem Punkt Löschung/Deaktivierung deines Kontos (Stand 2013):

„Wenn du ein Konto löschst, wird es dauerhaft von Facebook gelöscht. Normalerweise dauert es ungefähr einen Monat, bis eine Kontolöschung vollzogen ist. Manche Daten sind jedoch noch bis zu 90 Tage in Sicherungskopien und Protokolldateien vorhanden. Du solltest dein Konto nur löschen, wenn du dir sicher bist, dass du es nicht mehr reaktivieren möchtest. Du kannst Dein Konto hier löschen: https://www.facebook.com/help/contact.php?show_form=delete_account
Erfahre mehr dazu unter: https://www.facebook.com/help/?faq=356107851084108

Bestimmte Informationen sind erforderlich, um dir Dienste anzubieten. Deshalb löschen wir solche Informationen erst, nachdem du dein Konto gelöscht hast. Einige Dinge, die du auf Facebook machst, werden nicht in deinem Konto gespeichert, wie beispielsweise in einer Gruppe gepostete Beiträge oder das Senden einer Nachricht an jemanden (dein/e FreundIn kann eine von dir gesendete Nachricht eventuell sogar noch nach deiner Kontolöschung haben). Solche Informationen bleiben auch noch nach der Löschung deines Kontos erhalten."

Ein Löschen bedeutet nunmehr aufgrund einer Systemumstellung tatsächlich ein Gelöschtsein. Wenn man sich nach dem Löschen 14 Tage nicht mehr einloggt, wird der Löschvorgang gestartet, ansonsten gilt die Löschung als widerrufen. Danach dauert es weitere 90 Tage, bis die Daten tatsächlich gelöscht sind und vom Server entfernt werden. Facebook reagierte damit auf die vielen Beschwerden von Datenschützern.

2. Recht auf Löschung des Accounts

In der Folge soll geklärt werden, ob ein Nutzer einen durchsetzbaren Anspruch auf sofortige Löschung seines Profils und aller damit zusammenhängenden Daten hat, und wenn ja, wie er eine Löschung bewirken kann. Schließlich soll darauf eingegangen werden, welche „Hilfsmöglichkeiten" ein Nutzer hat, wenn seinem Löschungswunsch nicht nachgekommen wird.

§ 1 Abs 3 Z 2 DSG 2000 normiert das Recht des Betroffenen auf „Richtigstellung unrichtiger Daten" und das „Recht auf Löschung" unzulässigerweise verarbeiteter Daten nach Maßgabe gesetzlicher Bestimmungen. Wenn nun ein Nutzer seinen Facebook-Account löschen möchte, werden seine damit in Zusammenhang stehenden personenbezogenen Daten nicht mehr benötigt. Dies hat zur Folge, dass diese ab dem Löschen als „unzulässig verarbeitete Daten" iSd § 27 Abs 1 Z 2 DSG anzusehen sind. Eine Archivierung bzw Speicherung ist nur noch dann gestattet, wenn diese rechtlich zulässig bzw der Zugang zu diesen Daten besonders geschützt ist. § 27 DSG sieht weiters vor, dass ein Auftraggeber, das ist der Betreiber einer SNP, solcherart unzulässig verarbeitete Daten richtigzustellen oder zu löschen hat und zwar entweder aus eigenem Antrieb, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder auf begründeten Antrag des Betroffenen.

In Abs 4 ist schließlich geregelt, dass „innerhalb von 8 Wochen nach Einlangen eines Antrages auf Richtigstellung oder Löschung dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen ist […]".

Das bedeutet konkret, dass ein Betreiber einer SNP gemäß obiger datenschutzrechtlicher Bestimmungen Daten von einem Nutzer zu entfernen hat, wenn dieser sie löschen möchte bzw gelöscht hat, es sei denn, es liegt ein rechtlich zulässiger Grund vor, der eine Speicherung weiterhin gestattet.

3. Rechtsschutz

a. Beschwerde bei der Datenschutzkommission

Ein detailliertes Eingehen auf die Beschwerdemöglichkeit bei der Datenschutzkommission würde den Rahmen der Arbeit sprengen, daher wird nur in der Fußnote kurz darauf eingegangen.[314]

b. Geltendmachung auf dem Zivilrechtsweg

In § 32 DSG 2000 ist die Anrufung der Gerichte zur „Durchsetzung von Ansprüchen wegen Verletzung der Rechte einer Person oder Personengemeinschaft auf Geheimhaltung, auf Richtigstellung oder auf Löschung gegenüber natürlichen Personen, Personengemeinschaften oder Rechtsträgern, die privatrechtlicher Natur sind und soweit diese bei der behaupteten Verletzung nicht in Vollziehung der Gesetze tätig geworden sind" geregelt.

Das Gesetz sieht damit für den Nutzer einer SNP die Möglichkeit vor, sich an die Gerichte zu wenden, wenn seinem Anspruch auf Löschung seiner Daten nicht entsprochen wird.

[314] Kurz zusammengefasst sei jedoch angemerkt, dass die österreichische Datenschutzkommission (DSK) eine Behörde ist, welche für die Einhaltung der Bestimmungen des Datenschutzgesetzes zuständig ist. Ihre Zuständigkeit umfasst „alle Verletzungen des Auskunftsrechts sowie alle sonstigen Verletzungen durch Auftraggeber des öffentlichen Bereichs". Wenn Handlungen vorliegen, welche der Gerichtsbarkeit bzw Gesetzgebung zuzuordnen sind, dann ist die Datenschutzkommission unzuständig, siehe *Sonntag*, Einführung in das Internetrecht (2009) 263. Die DSK kann einstweilige Verfügungen treffen, dass eine weitere Verwendung von Daten untersagt wird oder ein Bestreitungsvermerk anzubringen ist. Sie kann berichtigen oder löschen bzw überprüfen. Bei der sog Beschwerde an die DSK gem § 31 DSG hat die DSK eine „quasi-richterliche Entscheidungsfunktion", wobei bei der Anregung einer Kontrolle gem § 30 DSG eine amtswegige Überprüfung ohne Anspruch auf Durchführung oder ein bestimmtes Ergebnis vorgeschlagen wird, siehe *Sonntag*, Einführung in das Internetrecht (2009) 264.

4. „Recht auf Vergessen“

Der Schutz der Privatsphäre muss auch bestehen bleiben, wenn der Nutzer einer SNP diesen möglicherweise aufgibt. Das Veröffentlichen von Daten auf einer SNP sollte nicht dazu führen, dass dem Nutzer überhaupt kein Rechtsanspruch mehr gebührt. Es ist zwischenzeitig bekannt, dass nicht alle Daten vollkommen gelöscht sind, wenn man einen Account gelöscht hat, und wird deshalb ein „Recht auf Vergessen“ gefordert. Im Internet gibt es grundsätzlich kein Vergessen, einmal publizierte Daten können ewig gespeichert bleiben, selbst dann, wenn sie vom Betroffenen von der Ursprungsseite gelöscht wurden. Denn Kopien der Daten, welche bei Dritten oder in sog „Cache“-Speichern oder Archivdiensten, wie zB der „Wayback Machine“[315], gespeichert sind, können vom Betroffenen kaum gelöscht werden. Entfernt man eine Datei von einem Server, kann nicht ausgeschlossen werden, dass Kopien auf einem anderen Server oder irgendwelchen Client-Rechnern bereits gespeichert sind.

Siehe dazu im Detail weiter unten.

a. Facebook: Datenverwendung von nicht registrierten Personen

Facebook hat für Personen, die kein Konto auf Facebook besitzen, deren Daten (Fotos, kundgetane Meinungen) jedoch auf Facebook von anderen veröffentlicht wurden, die Möglichkeit eingeräumt, mittels Antrag die Löschung dieser Daten zu verlangen:

Abbildung 16: Screenshot Löschen des Facebook-Accounts (Stand: 26.10.2011)[316]

[315] http://www.archive.org/web/web.php (Stand: 7.11.2011).
[316] http://www.facebook.com/help/contact.php?show_form=database_removal (Stand: 22.7.2011).

Wenn eine Person ein Bild einer dritten Person veröffentlichen möchte, dann muss diese Person über die nötigen Rechte verfügen. Eine Angabe der Quelle reicht nicht aus,[317] es muss eine Einwilligung des Rechteinhabers gegeben sein.

[317] *Verein für Konsumenteninformation,* Ihr Recht im Internet (2011) 102.

VII. GERICHTSSTAND UND ANWENDUNG DES ÖSTERREICHISCHEN UND EUROPÄISCHEN RECHTES

A. PROBLEMSTELLUNG

In diesem Kapitel soll auf die Frage eingegangen werden, ob eine Rechtssache mit Auslandsbezug, welche SNP betrifft, von einem inländischen Gericht entschieden werden darf bzw welches Recht iZm SNP zur Anwendung kommen soll.[318]

Der betroffene Nutzer wird ein Interesse daran haben, einen Rechtsstreit vor einem für ihn heimischen Gericht zu führen, wo er die Rechtslage und das Rechtssystem kennt und wo das Verfahren in seiner Muttersprache abgehalten wird. Auch Anreise- und Gerichtskosten werden eine Rolle spielen.

Die meisten SNP werden von Unternehmen betrieben, welche ihren Firmensitz im (EU-)Ausland haben. Viele dieser SNP versuchen, ihre Nutzer dem Recht des Niederlassungsortes zu unterwerfen.

Es muss in diesem Zusammenhang zwischen SNP im Allgemeinen und Facebook im Speziellen unterschieden werden. Hinter der Plattform Facebook steht für den US-amerikanischen und kanadischen Bereich als Betreiber die „Facebook Inc." mit Sitz in Kalifornien, USA. Hinter „facebook.de", welche grundsätzlich den gesamten deutschsprachigen Raum erfasst, steht eine Tochtergesellschaft mit Sitz in Irland, „Facebook Ireland Ltd". Seit 2009 gibt es auch eine „Facebook Germany GmbH" mit Sitz in Deutschland, welche primär der Vermarktung des Unternehmens dienen soll.

Es stellt sich nun die Frage, welches konkrete Recht bei der Benutzung von SNP zur Anwendung kommt und welches Gericht zuständig ist.

B. GERICHTSSTAND

Grundsätzlich ist eine Rechtssache von einem österreichischen Gericht zu entscheiden, wenn dies durch völkerrechtliche (zB EuGVÜ), gemeinschaftsrechtliche (zB EuGVVO) oder nationale Norm ausdrücklich angeordnet ist oder die Voraussetzungen für die örtliche

[318] *Rechberger/Simotta*, Zivilprozessrecht[7] (2009) Rz 64.

Zuständigkeit eines österreichischen Gerichtes vorliegen bzw sich die Parteien durch eine Gerichtsstandsvereinbarung darauf geeinigt haben, dass ein österreichisches Gericht örtlich zuständig sein soll.

Außerhalb der EU, zB im Verhältnis zu den USA, gelten die Bestimmungen der österreichischen Jurisdiktionsnorm (JN) über die örtliche Zuständigkeit, die auch für die internationale Zuständigkeit entsprechend zu berücksichtigen sind.

§ 27 a JN regelt die inländische Gerichtsbarkeit:

Abs 1: *„Sind für eine bürgerliche Rechtssache die Voraussetzungen für die örtliche Zuständigkeit eines Gerichts gegeben, so besteht die inländische Gerichtsbarkeit, ohne daß eine sonstige Voraussetzung erfüllt sein muß."*

Abs 2: *„Der Abs. 1 gilt nicht, soweit nach Völkerrecht zur Gänze oder zum Teil ausdrücklich anderes bestimmt ist."*

1. Internationale Zuständigkeit

Zunächst möchte ich kurz auf die allgemeinen Bestimmungen der internationalen Zuständigkeit eingehen, bevor die Frage der Zuständigkeit iZm SNP geklärt werden soll.

Österreichische Gerichte haben gem § 42 JN von Amts wegen ihre Zuständigkeit zu prüfen.

In § 42 Abs 1 JN ist normiert:
„Sobald eine Rechtssache der streitigen oder freiwilligen Gerichtsbarkeit bei einem Gerichte anhängig wird, hat dasselbe seine Zuständigkeit zu prüfen."[319]

a. Generelle Zuständigkeitsregeln

(1) Anwendung der EuGVVO bzw des EuGVÜ

Seit 1.3.2002 gilt die VO (EG) Nr. 44/2001 des Rates vom 22.12.2000 über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen, welche durch die seit dem 10.1.2015 geltende VO (EU) Nr. 1215/2012 vom 12.12.2012 (EuGVVO nF) ersetzt wurde.

[319] § 41 JN, Gesetz über die Ausübung der Gerichtsbarkeit und die Zuständigkeit der ordentlichen Gerichte in bürgerlichen Rechtssachen (Jurisdiktionsnorm – JN), RGBl 111/1895.

Durch die EuGVVO wurde das bis dahin geltende EuGVÜ, Übereinkommen von Brüssel über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen (mit Ausnahme von Dänemark), welches seit 1968 zwischen den EG-Mitgliedstaaten für die EG-Mitgliedstaaten galt, abgelöst. Im Verhältnis zu Dänemark gilt weiterhin die Brüssel I-Verordnung.[320]

Gemäß Art 5 EuGVVO nF können Personen, die ihren Wohnsitz im Hoheitsgebiet eines Mitgliedstaats haben, vor den Gerichten eines anderen Mitgliedstaats nur gemäß den Vorschriften der Abschnitte 2 bis 7 des Kapitels II der EuGVVO geklagt werden.

Art 5 EuGVVO nF:
Abs 1: *„Personen, die ihren Wohnsitz im Hoheitsgebiet eines Mitgliedstaats haben, können vor den Gerichten eines anderen Mitgliedstaats nur gemäß den Vorschriften der Abschnitte 2 bis 7 dieses Kapitels verklagt werden."*

Abs 2: *„Gegen diese Personen können insbesondere nicht die in Anhang I aufgeführten innerstaatlichen Zuständigkeitsvorschriften geltend gemacht werden."*

Es sollen die innerstaatlichen Zuständigkeitsvorschriften (insbesondere diejenigen der ZPO) nicht angewendet werden.

(2) Anwendung der ZPO

Wenn die beklagte Partei keinen Wohnsitz in einem EU-Mitgliedstaat hat, sind die Art 24 und 25 EuGVVO nF über die ausschließlichen Gerichtsstände und Gerichtsstandsvereinbarungen heranzuziehen, ansonsten ist Art 6 Abs 1 EuGVVO nF maßgebend, welcher die Zuständigkeit der Gerichte eines jeden Mitgliedstaats nach dessen eigenen Gesetzen bestimmt.

Art 6 Abs 1 EuGVVO nF normiert:
„Hat der Beklagte keinen Wohnsitz im Hoheitsgebiet eines Mitgliedstaats, so bestimmt sich vorbehaltlich […] und der Art 24 und 25 die Zuständigkeit der Gerichte eines jeden Mitgliedstaats nach dessen eigenen Gesetzen. […]"[321]

[320] *Welser*, Fachwörterbuch (2005) 89.
[321] Siehe VO (EG) 44/2001 sowie VO (EU) Nr. 1215/2012 des Rates über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen, ABl L 2001/12 sowie ABl L 351/1.

Unter Anwendung der Zuständigkeitsvorschriften ist sodann festzustellen, ob ein inländischer Gerichtsstand besteht oder nicht.

(3) Gerichtsstand für deliktische Ansprüche

Gemäß Art 7 Z 3 EuGVVO nF (Besondere Zuständigkeiten) kann eine Person, die ihren Wohnsitz im Hoheitsgebiet eines Vertragsstaats hat, in einem anderen Vertragsstaat vor dem Gericht des Ortes verklagt werden, an dem das schädigende Ereignis eingetreten ist, wenn eine unerlaubte Handlung oder eine Handlung, die einer unerlaubten Handlung gleichsteht, oder Ansprüche aus einer solchen Handlung den Gegenstand des Verfahrens bilden.

Art 7 Z 3 EuGVVO nF regelt die besonderen Zuständigkeiten:
„[…] wenn eine unerlaubte Handlung oder eine Handlung, die einer unerlaubten Handlung gleichgestellt ist, oder wenn Ansprüche aus einer solchen Handlung den Gegenstand des Verfahrens bilden, vor dem Gericht des Ortes, an dem das schädigende Ereignis eingetreten ist oder einzutreten droht.“[322]

Diese Regelung deckt sich mit der in § 92 a ZPO für solche Fälle vorgesehenen:

„Streitigkeiten über den Ersatz des Schadens, der aus der Tötung oder Verletzung einer oder mehrerer Personen, aus einer Freiheitsberaubung oder aus der Beschädigung einer körperlichen Sache entstanden ist, können auch bei dem Gericht angebracht werden, in dessen Sprengel das den Schaden verursachende Verhalten gesetzt worden ist.“

Der Ort des schädigenden Ereignisses ist neben dem Handlungsort auch der Erfolgsort, dh der Ort, an dem das schädigende Ereignis eingetreten ist.

(4) Verbraucher

Für Verbraucher, die in einem Mitgliedstaat der Europäischen Union ihren Wohnsitz oder gewöhnlichen Aufenthalt haben, regelt die EuGVVO nF[323] in den Art 17 und 18 die Gerichtszuständigkeit in Zivil- und Handelssachen.

In Art 17 Abs 2 EuGVVO nF ist geregelt:

[322] Art 7 Nr. 3 EuGVVO nF.
[323] VO 44/2001/EG, ABl L 2001/12, 1.

„[…] Hat der Vertragspartner des Verbrauchers im Hoheitsgebiet eines Mitgliedstaats keinen Wohnsitz, besitzt er aber in einem Mitgliedstaat eine Zweigniederlassung, Agentur oder sonstige Niederlassung, so wird er für Streitigkeiten aus ihrem Betrieb so behandelt, wie wenn er seinen Wohnsitz im Hoheitsgebiet dieses Staates hätte. […]"

Facebook hat eine Zweigniederlassung in einem Mitgliedstaat der Europäischen Union, konkret die Facebook Ireland Limited, Hanover Reach, 5–7 Hanover Quay, Dublin 2 Ireland.[324] Daher kommt die Regelung des Art 17 Abs 2 EuGVVO nF zur Anwendung.

Aus Art 18 EuGVVO nF geht hervor:

Abs 1: *„Die Klage eines Verbrauchers gegen den anderen Vertragspartner kann entweder vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet dieser Vertragspartner seinen Wohnsitz hat, oder vor dem Gericht des Ortes, an dem der Verbraucher seinen Wohnsitz hat."*

Abs 2: *„Die Klage des anderen Vertragspartners gegen den Verbraucher kann nur vor den Gerichten des Mitgliedstaats erhoben werden, in dessen Hoheitsgebiet der Verbraucher seinen Wohnsitz hat. […]"*[325]

b. Fazit

Es kann daher aus Art 18 EuGVVO nF gefolgert werden, dass die Klage eines Verbrauchers gegen eine SNP entweder vor den Gerichten des Mitgliedstaats, in dessen Hoheitsgebiet der Vertragspartner (die SNP) seinen Wohnsitz hat, oder vor dem Gericht des Ortes, wo der Verbraucher seinen Wohnsitz hat, eingebracht werden muss. Umgekehrt kann der SN-Betreiber einen Verbraucher nur vor den Gerichten des Mitgliedstaats klagen, in dem der Verbraucher seinen Wohnsitz hat.

Diese Bestimmungen haben zur Folge, dass die von Facebook in den „Erklärungen der Rechte und Pflichten" normierte Zuständigkeit unbeachtlich ist. Der Gerichtsstand für den österreichischen Verbraucher ist allein nach der EuGVVO zu beurteilen, im gegenständlichen Fall bedeutet dies die Gerichtszuständigkeit der österreichischen Gerichte.

---

[324] Gemäß http://www.facebook.com/press/info.php?factsheet: „Headquartered in Palo Alto, Calif. U.S., offices: Atlanta; Birmingham, Michigan; Chicago; Dallas; Detroit; New York; Venice Beach, Calif.; Washington, DC; Austin International offices: Dublin; Hamburg; Hong Kong; Hyderabad; London; Madrid; Milan; Paris; Selangor; Singapore; Stockholm; Sydney; Tokyo; Toronto".

[325] VO 44/2001/EG, ABl L 2001/12, 1.

C. FACEBOOK – ANWENDBARES RECHT

Auszug aus den Nutzungsbedingungen von Facebook:

„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 einverstanden, dich bei einem Prozess über alle derartigen Ansprüche der personenbezogenen Zuständigkeit der Gerichte in Santa Clara County, Kalifornien, zu unterwerfen. […]"[326]

bzw aus den englischen Nutzungsbedingungen:

„Disputes: You will resolve any claim, cause of action or dispute (claim) you have with us arising out of or relating to this Statement or Facebook exclusively in a state or federal court located in Santa Clara County. The laws of the State of California will govern this Statement, as well as any claim that might arise between you and us, without regard to conflict of law provisions. You agree to submit to the personal jurisdiction of the courts located in Santa Clara County, California for the purpose of litigating all such claims. […]"[327]

Facebook unterscheidet außerdem auf seinen Webseiten (facebook.com und facebook.de), welches Tochterunternehmen von Facebook Vertragspartner eines Nutzers werden soll, je nachdem, wo der Nutzer ortsansässig ist:

„Sonstiges: Wenn du in den USA oder Kanada ortsansässig bist oder dort deinen Hauptgeschäftssitz hast, stellt diese Erklärung eine Vereinbarung zwischen dir und Facebook, Inc. dar. Anderenfalls stellt diese Erklärung eine Vereinbarung zwischen dir und Facebook Ireland Limited dar. Die Begriffe ‚uns', ‚wir' und ‚unser' verweisen jeweils entweder auf Facebook, Inc. oder Facebook Ireland Limited."[328]

Zunächst ist zu prüfen, ob diese Unterwerfung überhaupt rechtmäßig zustande kommt, insbesondere im Hinblick auf verbraucherschutzrechtliche Normen und andere

[326] http://de-de.facebook.com/terms.php?ref=pf (Stand: 8.3.2011).
[327] http://www.facebook.com/terms.php?ref=pf (Stand: 26.10.2011).
[328] http://www.facebook.com/terms.php?ref=pf (Stand: 26.10.2011).

Rechtsvorschriften des österreichischen Rechts, und schließlich, welches Recht bei der Benutzung von SNP, insbesondere bei Facebook, zur Anwendung gelangt.

Jahnel führt aus, dass die anzuwendenden datenschutzrechtlichen Normen auf drei Rechtsebenen verteilt sind, auf einer einfachgesetzlichen, einer verfassungsrechtlichen und einer unionsrechtlichen Ebene.[329]

Das österreichische Datenschutzrecht ist im DSG 2000 normiert:

In § 3 DSG, welcher den räumlichen Anwendungsbereich des DSG regelt, steht zwar:

Abs 1: *„Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht."*

Doch ist in Abs 2, als lex specialis, die Ausnahme für den Fall geregelt, dass die Datenverwendung im Inland von einem Auftraggeber des privaten Bereichs mit Sitz in einem anderen Mitgliedstaat der EU zu einem Zweck erfolgt, der keiner in Österreich gelegenen Niederlassung des Auftraggebers zuzurechnen ist. In diesem Fall soll das Recht des Sitzstaates gelten:

Abs 2: *„Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist. […]"*

Das bedeutet, dass das Recht des Unternehmenssitzes anzuwenden ist, wenn sich dieser oder eine Niederlassung in einem EU-Mitgliedstaat befindet und die Datenverwendung nicht in Österreich erfolgt.

Wenn sich hingegen die Niederlassung in einem Drittland befindet, soll das Recht des Mitgliedstaates zur Anwendung kommen, in dem sich die für die betreffenden Verarbeitungen verwendeten Mittel befinden, sofern diese in einem Mitgliedstaat gelegen sind, es sei denn, diese werden nur zur Durchfuhr der Daten verwendet, weswegen *Jahnel* ausführte, dass seiner

[329] *Jahnel*, Dreifacher Datenschutz? in *Bergauer/Staudegger* (Hrsg), Recht und IT (2009) 33.

Ansicht nach „die bloße Durchführung von personenbezogenen Daten durch Österreich“ nicht vom DSG umfasst ist und daher für ihn kein österreichisches DSG zur Anwendung kommen soll, wenn Daten lediglich durch Österreich „durchgeschleust“ werden.[330]

1. Die Safe Harbor-Richtlinie

Wenn man den Medien glauben möchte, stehen die meisten Server von Facebook in den USA und damit außerhalb der Europäischen Union. Es kommt damit zu einer Datenübermittlung in einen Drittstaat gem Art 25 DatenschutzRL.

Genau für solche Konstellationen, nämlich die Datenübermittlung an Orte außerhalb der EU, wurde das Safe Harbor-Abkommen zwischen dem US-Handelsministerium und der EU abgeschlossen, um einen Mindestschutzstandard und ungehinderten Datenverkehr zu garantieren[331]. Die Vereinigten Staaten haben sich in diesem Abkommen bereit erklärt, anzuerkennen, dass personenbezogene Daten nur an solche amerikanische Unternehmen übermittelt werden dürfen, welche sich im Wege einer Selbstverpflichtung bereit erklärt haben, essenzielle Datenschutzgrundsätze auch bei Online-Transaktionen zu beachten. Diese Grundsätze sind zB die Information der Nutzer über den jeweiligen Zweck und Umfang der Verarbeitung ihrer Daten, das Widerspruchsrecht der Nutzer gegen die Zweckentfremdung ihrer Daten etc. Weitergegeben werden dürfen diese Daten von US-amerikanischen Unternehmen nur an Unternehmen, die wiederum die Safe Harbor-Bestimmungen anerkannt haben.[332] Im Jahr 2000 wurde das Safe Harbor-Abkommen von der EU offiziell anerkannt.[333]

a. Safe Harbor

Die Initiative kam vom US-Handelsministerium im Jahr 1998 in Form eines Rundbriefes an unzählige US-Unternehmen, in dem diesen eine „Safe Harbor-Lösung“ vorgeschlagen wurde.

[330] *Jahnel/Siegwart/Fercher*, Aktuelle Fragen des Datenschutzrechts (2007) 24.
[331] *Westphal* in *Bauer/Reimer*, Grundbuch Datenschutzrecht (2009) 74 ff.
[332] *Dix* in *Bäumler*, E-Privacy (2000) 98 ff.
[333] Entscheidung der Kommission vom 26.7.2000, ABl L 215/1, siehe http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF (29.4.2011).

Am 31.5.2000, nach zweijährigen Verhandlungen zwischen der EU-Kommission und dem US-Handelsministerium, wurde das Safe Harbor-Abkommen schließlich von allen Mitgliedstaaten der EU einstimmig angenommen.[334]

„Safe Harbor" kommt aus dem Englischen und bedeutet „sicherer Hafen". Diese Bezeichnung wurde gewählt, um zu symbolisieren, dass eine Datenübermittlung nur durch „einen sicheren Hafen" erfolgen soll bzw darf. Mit der Safe Harbor-Vereinbarung, welche zwischen den USA und der Europäischen Union abgeschlossen wurde, wird es europäischen Unternehmen gestattet, personenbezogene Daten legal in die USA zu übermitteln. Hintergrund des Safe Harbor-Abkommens ist, dass die Datenschutzrichtlinie (RL 95/46/EG) grundsätzlich ein Verbot der Übermittlung personenbezogener Daten aus EG-Mitgliedstaaten in Staaten, welche über kein „dem EG-Recht vergleichbares Datenschutzniveau" verfügen[335], vorsieht. Das ist bei den USA grundsätzlich der Fall, da diese über keine umfassenden gesetzlichen datenschutzrechtlichen Bestimmungen verfügen.

Das Safe Harbor-Abkommen soll dem entgegen wirken und gibt US-Unternehmen die Möglichkeit, diesem durch Annahme und Befolgung der sog „Safe Harbor Principles"[336] beizutreten. Immer mehr US-Unternehmen, wie zB Microsoft, Google oder Facebook, treten dem Safe Harbor bei.[337]

Grundsätzlich normiert Art 25 Abs 1 der RL nämlich, dass eine Übermittlung personenbezogener Daten in ein Drittland lediglich dann möglich ist, wenn vom Drittland ein ausreichendes Datenschutzniveau gewährleistet wird. In Art 26 sind schließlich Ausnahmefälle[338] genannt, in welchen eine Datenübermittlung ausnahmsweise in ein Drittland erfolgen darf, obwohl dieses die Voraussetzungen grundsätzlich nicht erfüllt.[339]

---

[334] *Holzhausen*, Die Safe-Harbor-Vereinbarung als Methode zur Sicherung eines „angemessenen Datenschutzniveaus" im Sinne der EG-Datenschutzrichtlinie (2002) 35 f.

[335] *Westphal* in *Bauer/Reimer*, Grundbuch Datenschutzrecht (2009) 73.

[336] Siehe im Detail http://www.export.gov/safeharbor/eu/eg_main_018365.asp (Stand: 29.4.2011).

[337] Allgemeine Datenschutzrichtlinie EWR/CH-USA, Safe Harbor Richtlinie, http://de-de.facebook.com/safeharbor.php (29.4.2011); laut ArgeDaten Privacy Service haben aber bloß 194 Unternehmen (Stand: Mai 2002) die Vereinbarung akzeptiert. Neben vielen eher kleineren Unternehmen finden sich auch einige bekannte IT- und Pharmafirmen, Hotelketten und Finanzdienstleister: Agilent Technologies, Baxter International Inc., Compaq Computer Corporation, Eastman Kodak Company, Hewlett Packard, Microsoft Corporation, Marriott International, Inc., Oracle Corporation, Procter & Gamble Company, Dun & Bradstreet Corporation. Deutlich unterrepräsentiert seien laut ArgeDaten jedoch die Bereiche: Internetdienstleistungen, EDV-Ausstattung, Telekommunikation, Informationsdienste ua (siehe http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=89651273; Stand: 3.5.2011).

[338] *Westphal* in *Bauer/Reimer*, Grundbuch Datenschutzrecht (2009) 73.

[339] RL 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 vom 23.11.1995.

Facebook hat im Zuge der Safe Harbor-Anerkennung („Safe Harbor-Rechtshinweis“) akzeptiert, dass die Europäische Gemeinschaft Datenschutzrichtlinien besitzt, welche Wirkung für den gesamten EWR haben[340]. Hinsichtlich der Schweiz hat Facebook anerkannt, dass diese eine Datenschutzrichtlinie nach dem Bundesgesetz über den Datenschutz entwickelt hat:

ALLGEMEINE DATENSCHUTZRICHTLINIE EWR/CH-USA – SAFE HARBOR-RECHTSHINWEIS GELTUNGSBEREICH DER SAFE HARBOR-ZERTIFIZIERUNG:

Facebook, Inc. (im Folgenden „Facebook“ oder „wir“ genannt) erkennt an, dass die Europäische Gemeinschaft eine europäische Datenschutzrichtlinie nach Richtlinie 95/46/EG (die „Richtlinie“) entwickelt hat, die für den Europäischen Wirtschaftsraum („EWR“) gilt, und dass die Schweiz eine Datenschutzrichtlinie nach dem Bundesgesetz über den Datenschutz („BSG“) entwickelt hat. Facebook erkennt weiterhin an, dass durch diese Richtlinien die Übermittlung von personenbezogenen Daten aus dem EWR und der Schweiz (gemeinschaftlich als „EWR/CH“ bezeichnet) in die USA durch Unternehmen und andere Organisationen eingeschränkt wird, wenn kein „angemessener Schutz“ für diese personenbezogenen Daten besteht, wenn sie in den USA empfangen werden. Um einen solchen „angemessenen Schutz“ sowie die Einhaltung der durch die Richtlinie und das BSG festgelegten Einschränkungen zur internationalen Datenübertragung zu gewährleisten, befolgt Facebook in Bezug auf die Übermittlung bestimmter Daten in die USA die vom US-Handelsministerium herausgegebenen Safe Harbor-Grundsätze („Safe Harbor-Grundsätze“): Hierzu zählen personenbezogene Daten von Mitarbeitern oder sonstigen Vertretern von bestimmten Unternehmenskunden, Lieferanten, Händlern, Werbekunden und anderen Geschäftspartnern von Facebook oder einer Tochter- bzw. Schwestergesellschaft der Facebook-Gruppe im Raum EWR/CH („EWR/CH-Daten“). [...]

Facebook hat anerkannt, dass die Übermittlung personenbezogener Daten aus dem EWR und der Schweiz in die USA durch Unternehmen und andere Organisationen eingeschränkt werden muss, wenn kein „angemessener Schutz“ für diese besteht.[341]

Als EWR/CH-Bürger hat man aber nichtsdestotrotz die Möglichkeit, festzulegen, dass man keine Werbe-E-Mails von Facebook mehr erhält, und braucht dafür nur ein E-Mail an die Safe Harbor-Datenschutzkontaktperson zu senden oder die Anweisungen zum Ablehnen, welche mit einer Werbe-E-Mail mitgeschickt werden, annehmen.

Außerdem hat man die Möglichkeit, einen Antrag auf Zugang, Aktualisierung und Korrektur von aufbewahrten EWR/CH-Daten an Facebook zu richten.

Dh Facebook muss neben einem gewissen Mindestniveau an Datenschutz auch gewisse Informationspflichten einhalten. Konkret muss Facebook über den Zweck einer

[340] *Westphal* in *Bauer/Reimer*, Grundbuch Datenschutzrecht (2009) 56 f.
[341] Allgemeine Datenschutzrichtlinie EWR/CH-USA, Safe Harbor Richtlinie, http://de-de.facebook.com/safeharbor.php 2. Absatz (29.4.2011).

Datenerhebung und Datenverwendung informieren.[342] Der betroffenen Person muss ganz klar erkennbar sein, zu welchem Zweck Daten über sie erhoben und verwendet worden sind, wie die datenerhebende Organisation kontaktiert werden kann und welche Möglichkeiten es für die betroffene Person gibt, die Weitergabe der Daten einzuschränken.[343]

b. Einhaltung des Safe Harbor durch Facebook

Facebook bekennt sich zwar auf seiner Webseite zur Einhaltung des Safe Harbor-Abkommens, doch werden Personen nicht darüber informiert[344], wenn ihre Daten verwendet und übermittelt werden. Auch der Zweck der Erhebung wird nicht genannt. Nicht-Mitglieder von Facebook haben überhaupt keine Möglichkeit, zu erfahren, wann und ob ihre Daten übermittelt und/oder gespeichert werden. Eine Stelle, an die man sich wenden kann, wird auch nicht genannt.[345] Der betroffenen Person ist es daher kaum möglich, ihre vorgesehenen Rechte durchzusetzen.

Wie weiter oben bereits ausgeführt wurde, brachte der Hamburger Datenschutzbeauftragte Prof. Dr. *Johannes Caspar*[346] bereits im Oktober 2010 eine Beschwerde gegen Facebook ein, da die monatelangen Verhandlungen mit dem Unternehmen darüber, das Safe Harbor-Abkommen korrekt zu befolgen, offensichtlich wenig erfolgreich waren. Für *Caspar* liege ein „klarer Verstoß gegen das Transparenzgebot des Safe Harbor-Abkommens vor" und er fände es „fast schon unverschämt, dass sich die Firma dazu nicht äußert". Dies sei auch ein Zeichen dafür, „dass Datenschutz (für Facebook, Anm) nicht an erster Stelle stehe".

In einer Pressemitteilung vom 24.1.2011 fügte Prof. Dr. *Caspar* noch hinzu: „Wir erwarten nun eine zeitnahe Umsetzung unserer Vereinbarung und werden diese kritisch begleiten. Insoweit hoffen wir, dass Facebook die gezeigte Bereitschaft zur kooperativen Zusammenarbeit beibehält und die detaillierten Ergebnisse unserer Verhandlungen im

[342] *Holzhausen*, Die Safe-Harbor-Vereinbarung als Methode zur Sicherung eines „angemessenen Datenschutzniveaus" im Sinne der EG-Datenschutzrichtlinie (2002) 51 ff.
[343] Entscheidung der Kommission vom 26.7.2000 gemäß der RL 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des sicheren Hafens und der diesbezüglichen häufig gestellten Fragen (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA.
[344] Eine Information könnte zB über eine FB-Nachricht erfolgen.
[345] Stand: 2.5.2011.
[346] Prof. Dr. *Johannes Caspar* ist Datenschutzbeauftragter für Hamburg, Deutschland. Er ist primär für die US-amerikanischen Unternehmen Google und Facebook zuständig.

Interesse der Nichtnutzer wie auch der Nutzer tatsächlich in transparenter Weise verwirklicht."[347]

c. Kritik an Safe Harbor

Am 29.4.2010 wurde vom Düsseldorfer Kreis[348] ein Beschluss mit dem Inhalt, dass deutsche Datenexporteure das datenimportierende Unternehmen eigenständig zu „überprüfen" haben und sich damit nicht auf die Behauptung einer Safe Harbor-Zertifizierung verlassen dürften, gefasst. Deutsche Unternehmen sollen damit verpflichtet werden, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

2. TRUSTe-Datenschutzprogramm

Facebook verweist direkt am Beginn der Facebook-Datenschutzrichtlinien auf das TRUSTe-Datenschutzprogramm (TRUSTe Privacy Seal Program)[349] und weist darauf hin, dass die Datenschutzrichtlinien bzw das Datenschutzverfahren anhand der Programmanforderung von TRUSTe geprüft wurden.

a. USA

Gründe, warum die USA im Gegensatz zu Europa keine bzw unzureichend ausgestaltete Datenschutzgesetze haben, könnten ua in der höheren gesellschaftlichen Akzeptanz von Datenzugriffen bzw Dateneingriffen liegen. In den USA wird vor Beginn eines Arbeitsverhältnisses oder im Zuge der Anmietung einer Wohnung oder eines Hauses sofort eine Bonitätsprüfung durchgeführt. Dabei werden personenbezogene Daten „durchforstet". Informationen über die Bonität und den finanziellen Hintergrund einer Person sind offensichtlich wichtiger als der Schutz der Daten des Einzelnen.[350]

---

[347] Presseerklärung von *Caspar* vom 24.1.2011.

[348] Als oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich in Hannover, Deutschland.

[349] Einer von mehreren US-amerikanischen Anbietern (BBBonline, WebTrust etc), welche „Gütesiegel im Internet" vergeben. Diese Anbieter vereinbaren mit Anbietern kommerzieller Webseiten, dass sich diese zur Einhaltung von Datenschutzprinzipien verpflichten und regelmäßig durch den Gütesiegelanbieter kontrolliert werden.

[350] Seit den Terroranschlägen am 11.9.2001 sind die Kontrollen der Daten und die nationale Sicherheit noch mehr angestiegen.

VIII. **CONCLUSIO UND AUSBLICK**

Das geltende österreichische Datenschutzgesetz ist am 1.1.2000 in Kraft getreten. Es ist zu einer Zeit geplant worden bzw entstanden, in der es noch keine SNP wie Facebook, Twitter etc gab. Das DSG sollte den Erfordernissen der 1990er Jahre Rechnung tragen und insbesondere verhindern, dass aufgrund der damals neu entwickelten Technologien und Methoden immer mehr Daten leichter erfasst, bearbeitet bzw gespeichert werden und dadurch womöglich „gläserne" Bürger entstehen. Das DSG wollte primär den Bürger vor dem Staat bzw das Verhältnis der Privaten untereinander schützen.

In der Zeit von SNP sind die Schutz-Notwendigkeiten aber anders gelagert. Vorrangig sammelt nicht der Staat die Daten Privater, vielmehr geben viele Bürger Informationen freiwillig preis.

Es stellt sich nun die Frage, ob Probleme, die aus diesem „freiwilligen Preisgeben" resultieren, trotzdem noch vom Datenschutzrecht geregelt werden können oder ob es eines (neuen oder novellierten?) Maßnahmengesetzes bedarf, welches speziell für all die neuen technischen Entwicklungen geeignet ist bzw es schafft, auf die neuen technischen Gegebenheiten ausreichend zu reagieren?

Die EU-Kommission sprach mehrfach aus, dass eine einheitliche (datenschutzrechtliche) Regelung für alle EU-Mitgliedstaaten erzielt werden müsse, dass die Sanktionen ganz Europa gleichermaßen durchdringen sollten und dass versucht werden müsse, die gravierendsten Unterschiede in der Datenschutzkontrolle zu entfernen.[351]

Das größte Problem ist jedoch dabei, dass die Nutzungsbedingungen der meisten SNP ua den österreichischen Datenschutzrichtlinien keinesfalls gerecht werden.

In den USA gibt es nur die Safe Harbor-Richtlinie, welche zwar versucht, eine einheitliche Regelung für das gesamte Staatsgebiet zu schaffen, doch fehlen eine eigene „amerikanische" Datenschutzkommission sowie Bestimmungen, die den Umgang mit weltweiten Datenverletzungen regeln. Safe Harbor kann mE keinesfalls als ausreichender Schutz angesehen werden, im Gegenteil spiegelt diese „Institution" lediglich die noch immer vorherrschende Ansicht der meisten US-Unternehmen im Hinblick auf Selbstregulierung und

[351] ZB *Viviane Reding*, Vizepräsidentin der Europäischen Kommission, EU-Justizkommissarin beim Vortrag zum Thema „Die neue EU-Datenschutzverordnung. Eine Chance für effektiven Datenschutz in Europa" bei der 83. Datenschutzkonferenz in Potsdam, 21.3.2012.

Selbstzertifizierung wider, was bis dato eine verbindliche und überprüfbare Festlegung durch ein Gesetz verhindert hat.

Es mangelt mE noch immer an effektiven Durchsetzungsmechanismen und Kontrollorganen, welche die Einhaltung der Bestimmungen kontrollieren, damit für den Nutzer, wie *Stix* gesagt hat, sichergestellt werden kann, dass „der sichere Hafen nicht zu einer Piratenbucht wird".[352]

Ein weiteres sehr großes Problem ist in diesem Zusammenhang die Tatsache, dass im Falle des SN Facebook ein einziges Unternehmen alle unsere Daten sammelt und hortet. Es ist damit ein Unternehmen im Besitz unserer Daten, welche auf ca. 60.000 Servern nahezu unverschlüsselt verteilt werden[353].

Was Facebook mit all diesen gesammelten Daten tatsächlich macht, ist mE nach weiterhin ein ungelöstes Mysterium.

A. „RECHT AUF VERGESSEN" ODER EWIGE DIGITALE ERINNERUNG?

In seinem Buch Delete – Die Tugend des Vergessens in digitalen Zeiten beschreibt *Mayer-Schönberger* die Geschichte von Stacy Snyder, welche Lehrerin werden wollte: „... Stacy dachte daran, das Foto zu löschen, aber der Schaden war nicht ungeschehen zu machen: Die Seite war bereits von Suchmaschinen erfasst, das Foto von Webcrawlern archiviert worden. Das Internet erinnerte sich an etwas, von dem Stacy wollte, dass die Welt es vergisst."[354]

Ein vielfach unterschätztes Risiko liegt im endlosen „Gedächtnis" des Internets und der zwischenzeitig existierenden digitalen Speicherkapazitäten. Einmal online gestellt Fotos, Beiträge, Kommentare etc können nur sehr schwer oder gar nicht mehr gelöscht werden, dies insbesondere dann, wenn derartige Inhalte von anderen Nutzern gespeichert und erneut veröffentlicht werden.

Mayer-Schönberger[355] erzählt ua im oben erwähnten Buch die Geschichte einer jungen Frau, welche Lehrerin werden wollte, aber aufgrund eines privaten Fotos, welches sie ins Internet hochgeladen hatte, keine Lehrbefugnis erhielt. Auf dem Foto war Stacy verkleidet und mit

[352] *Dix* in *Bäumler*, E-Privacy (2000) 99 ff.
[353] Zur „Unverschlüsseltheit" von Daten ein Beispiel von *Sokol* in *Gehrke*, Datenschutz und -sicherheit im Internet (2005) 95: „Eine unverschlüsselte E-Mail ist einer maschinengeschriebenen Postkarte vergleichbar, die von allen gelesen und sogar verwendet werden kann, ohne dass der Absender zustimmen muss."
[354] Siehe *Mayer-Schönberger* (Hrsg), Delete – Die Tugend des Vergessens im digitalen Zeitalter (2010) 10 ff.
[355] *Mayer-Schönberger*, Delete – Die Tugend des Vergessens im digitalen Zeitalter (2009) 10.

einem Plastikbecher mit der Beschriftung „Betrunkener Pirat“ zu sehen. Dieses Bild wurde von ihrer Universität veröffentlicht, weswegen Stacy die Universität verklagte und verlor.

Mayer-Schönberger möchte damit die Wichtigkeit des Vergessens mit den treffenden Worten hervorheben: „Seit Beginn der Menschheitsgeschichte war das Vergessen für uns Menschen die Regel und das Erinnern die Ausnahme. Durch die Digitaltechnologie und die globale Vernetzung hat sich das Verhältnis aber verschoben, […] das Vergessen ist heute zur Ausnahme und das Erinnern zur Regel geworden.“[356]

Das Problem dabei ist jedoch, dass dem ursprünglichen Anbieter die Verfügungsgewalt über die von ihm online gestellten Inhalte durch die nahezu schrankenlosen Speichermöglichkeiten anderer Internetnutzer (zB Archivieren auf Servern, Spiegeln auf anderen Festplatten etc) entzogen wurde. Außerdem gibt es dank des Programms „Take me back“[357] die Möglichkeit, auf den früheren Inhalt einer gelöschten Webseite zu gelangen und diesen zu betrachten. Die Speicherkapazitäten und Verarbeitungsleistungen wachsen stetig an und es kommt zu einer steigenden Vernetzung der Computer. Schließlich werden immer bessere mobile Geräte entwickelt, welche es erlauben, sich von fast jedem Ort ins Internet einzuloggen und Informationen online zu stellen, abzurufen oder zu verarbeiten.

1. Verfallsdatum für Informationen

Ein digitales Verfallsdatum würde bewirken, dass gewisse Informationen gelöscht werden, wenn diese ihre „Aufbewahrungsdauer erreicht bzw überschritten haben“.[358] Die Idee wäre es, Dateien zB mit einem „Verfallsdatum“ auszustatten, welche sich nach Ablauf der Frist einfach „selbst löschen“ und damit vergessen werden. *Mayer-Schönberger* nennt als Lösungsansatz die Möglichkeit, dass bei Anlegung bzw Speicherung eines Dokuments auf dem Computer ein frei wählbares Verfallsdatum eingegeben wird. Dieses soll jederzeit verlängert oder verkürzt werden können.

Mayer-Schönberger erklärt, dass mit Hilfe eines Verfallsdatums nicht ein Vergessen erzwungen werden soll, sondern ein Problembewusstsein entstehen soll. Die Menschen sollen selbst entscheiden und wählen können, wann ein Dokument „verfällt“.[359]

---

[356] *Mayer-Schönberger*, Delete – Die Tugend des Vergessens im digitalen Zeitalter (2009) 11.
[357] Ein im Jahr 1996 in San Francisco gegründetes Internetarchiv, www.archive.org, welches ua „take me back“ anbietet.
[358] *Mayer-Schönberger*, Delete – Die Tugend des Vergessens im digitalen Zeitalter (2009) 201 ff.
[359] *Mayer-Schönberger*, Delete – Die Tugend des Vergessens im digitalen Zeitalter (2009) 203.

a. Technische Umsetzbarkeit

Verfallsdaten könnten in Form von sog „Metainformationen" gespeichert werden. Sie werden im Falle eines Kopierens, Speicherns oder Veränderns einfach mitkopiert. So wäre lediglich eine Art Zusatzprogramm nötig, welches im Hintergrund läuft und die abgelaufenen Informationen regelmäßig löscht.

Mayer-Schönberger beschreibt, dass ein Verfallsdatum aber lediglich dann durchsetzbar wäre und Allgemeingültigkeit erreichen kann, wenn der Gesetzgeber bestimmt, dass Softwarehersteller verpflichtet werden, auf allen Geräten zur Speicherung digitaler Informationen einen bestimmten Softwarecode implementieren zu müssen, welcher das jeweilige Verfallsdatum der Informationen verwaltet und veraltete Dateien automatisch löscht.[360]

Ein weiteres großes Problem ist auch die Funktion des „Like-Buttons". Anhand des Like-Buttons bzw der Platzierung eines Like-Buttons auf einer Webseite kann Facebook dokumentieren und mitverfolgen, von welcher IP-Adresse aus eine Webseite besucht wird. Eine Verknüpfung des Namens mit der Uhrzeit ist damit leicht möglich.

Der Plan der EU-Kommission war, dass die Internetnutzer eine bessere Kontrolle über ihre Daten erhalten und wollte sogar ein „right to be forgotten" einführen. Ein Nutzer sollte selbst bestimmen können, ob er seine einmal online gestellten Daten wieder korrigieren bzw löschen möchte.

Die für Grundrechte zuständige EU-Kommissarin *Viviane Reding* ging sogar noch weiter und wollte, dass „privacy by default" üblich werden soll, dh die „Erst-Einstellungen" von SNP sollten nicht – wie grundsätzlich üblich – offen, sondern verschlüsselt sein und der Nutzer sollte selbst bestimmen können, wie viele Informationen er preisgeben möchte.

Das Ziel von EU-Justizkommissarin *Reding* war, dass jeder Bürger „jederzeit und selbstbestimmt seine persönlichen Daten löschen kann"[361] und Unternehmen sollten ebenfalls von außerhalb der EU in Hinblick auf den Datenschutz in die Pflicht genommen werden.

Als Ziel der Reform der EU-Datenschutzrichtlinie wurde immer wieder genannt, dass Verbrauchern mehr Rechte und eine bessere Kontrolle über ihre Daten eingeräumt bzw deren

---

[360] *Mayer-Schönberger*, Delete – Die Tugend des Vergessens im digitalen Zeitalter (2009) 205.

[361] http://futurezone.at/netzpolitik/5823-eu-will-recht-auf-vergessen-im-internet.php (APA-Meldung vom 8.11.2011).

Daten gesichert werden sollen. *Reding* wollte außerdem, dass „Unternehmen, die ihre Dienste an europäische Verbraucher richten, direkt dem europäischen Datenschutzrecht unterliegen sollen“.[362] *Reding* weiter: „Netzwerke sollen sich an EU-Recht halten und europäisches Recht sollte auch angewendet werden, wenn die Anbieter sich außerhalb der EU befinden“.[363]

Meiner Ansicht nach wäre das „Recht auf Vergessen“ ein guter Ansatz, wenn damit tatsächlich die Möglichkeit geschaffen wird, ganz alleine und selbst zu entscheiden, ob und wie Informationen über sich selbst im Internet gespeichert bleiben sollen und Dateien mit einem Verfallsdatum auszustatten. Doch denke ich, dass ein derartiges „Verfallsdatum“ und eine „Selbstzerstörung“ technisch (noch) nicht möglich sind und somit an ihre Grenzen stoßen.

Die Denkrichtung ist mE aber die richtige, die Menschheit soll sich Gedanken machen darüber, wie das fundamentale Recht auf Schutz der persönlichen Daten digital in Zukunft am besten geschützt werden kann. Die von der EU-Kommission Anfang 2012 vorgeschlagene Datenschutzreform war ein großer Schritt. Die EU-Kommission möchte einen Weg finden, die bestehenden Regeln aus den 90er Jahren an die neue, digitale Ära anzupassen.

Eine technisch umsetzbare Lösung wäre mE nach zB eine Kooperation mit Suchmaschinen und zwar, dass „zu vergessende“ Daten herausgefiltert werden und mit Hilfe von Suchmaschinen nicht mehr angezeigt werden.

B. PERSÖNLICHES FAZIT

Für mich können SNP als eine der größten technischen Errungenschaften der letzten Jahre angesehen werden. Sie sind ein Spiegelbild unserer schnelllebigen, pulsierenden und vernetzten Welt und eine technisch neue Möglichkeit des weltweiten Verknüpfens und Kommunizierens im Internet.

Technische Entwicklungen gehören mE gefördert und unterstützt, doch sollten dabei auch immer Werte wie Privatsphäre, Datenschutz und Persönlichkeitsrechte ge- bzw beschützt werden.

[362] http://futurezone.at/netzpolitik/5823-eu-will-recht-auf-vergessen-im-internet.php (APA-Meldung vom 8.11.2011).
[363] http://www.golem.de/1111/87466.html, EU will „Recht auf Vergessen“ im Internet.

Es muss eine Balance zwischen der Forschung bzw der Zulassung neuer Technologien und dem Schutz und der Selbstbestimmung der Daten bestehen. Wie *Leissler* schon geschrieben hat, stellen SNP „höchste Anforderungen an die informationelle Selbstbestimmung des Einzelnen“[364]. Mit Disziplin, Aufmerksamkeit und dem Eigenschutz der Daten kann diese Balance hergestellt werden.

Ich halte es mit dem Ausblick von *Häger*, dass „es die schwierige Aufgabe der nächsten Jahre sein wird, Interessen des Datenschutzes, der Strafverfolgungsbehörden, der Internetwirtschaft und natürlich auch der Internetnutzer gegeneinander sinnvoll abzuwägen und die Technik dem entsprechend weiter zu entwickeln sein wird“.[365]

Datenschutz ist und war immer schon eine notwendige Anforderung bei der Gestaltung unserer Gesellschaft, doch entsprechen viele datenschutzrechtliche Bestimmungen nicht mehr den neuen technischen Errungenschaften. Sie müssen weiterentwickelt und in technischen Realisierungen integriert und diesen auch angepasst werden.

Abschließend möchte ich zwei Zitate zum Nach- bzw Überdenken anführen. Beide stammen von *Steve Jobs*, Mitbegründer und ehemaliger CEO von Apple Inc. und wohl eine der bekanntesten Persönlichkeiten der Computerindustrie:

„Again, you can’t connect the dots looking forward; you can only connect them looking backwards. – Wer nach vorne blickt, weiß nie, was wirklich Sinn ergibt. Nur rückblickend erscheint etwas logisch.“ (2005)[366]
„Technology alone is not enough. It’s technology, married with liberal arts, married with the humanities, that yields us the result that makes our hearts sing.“ (2011)[367]

[364] *Leissler*, Social-Networks – Datenschutz in der vernetzten Welt, ecolex, 2010, 834.
[365] Siehe *Häger* in *Gehrke*, Datenschutz und -sicherheit im Internet (2005) 43.
[366] *Steve Jobs*, Commencement Speech for Stanford University (2005). Siehe ua http://blinksoflife.tumblr.com/post/779983497/steve-jobs-commencement-speech-for-stanford (Stand: 7.11.2011).
[367] Zitat aus einer Rede von *Steve Jobs* am 29.8.2011 zur Einführung des iPad 2 in den USA.

IX. LITERATURVERZEICHNIS

Apathy (Hrsg), Bürgerliches Recht I, AT (2010) Wien, Springer

Bauer/*Reimer* (Hrsg), Handbuch Datenschutzrecht (2009) Wien, facultas

Bäumler (Hrsg), E-Privacy, Datenschutz im Internet (2000) Braunschweig, Vieweg

Beer, Der große Facebook Ratgeber. Für Einsteiger und Power-User, 01/2012

Berger, Die Vereinbarung von AGB im Internet (2000) Diplomarbeit

Berka (Hrsg), Verfassungsrecht[3], Grundzüge des österreichischen Verfassungsrechts für das juristische Studium (2010) Wien, Springer

–, Die Grundrechte: Grundfreiheiten und Menschenrechte in Österreich (1999) Wien, Springer

–, Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit, Gutachten (2012) Wien, Manz

Brenn, Der elektronische Geschäftsverkehr, ÖJZ 1999, 481

Bydlinski, Paradoxer Geheimnisschutz post mortem? JBl 1999, 553

Dassler (Hrsg), Datenschutz in der modernen Informationsgesellschaft (2007) Berlin, wvb

De Meer/Herkenhöner (Hrsg), Sicherheit mit und ohne Netz. Technische und rechtliche Herausforderungen des Web 2.0, Management Convent der Universität Passau, Heft 2 (2011) Passau, Verlag Karl Stutz

Dohr/Pollirer/Weiss/Knyrim (Hrsg), DSG 2010, 12. Erg.-Lfg., Kommentar (2011) Wien, Manz

Ehmann/Kramer (Hrsg), Datenschutz Glossar, Die wichtigsten Begriffe zum Datenschutz leicht verständlich erklärt, Praxislexikon (2005) Berlin, Interest Verlag

Ellenhuber, Rechtliche Probleme des Vertragsabschlusses im Internet unter besonderer Berücksichtigung der Allgemeinen Geschäftsbedingungen (2002) Universität Innsbruck, Dissertation

Emich, Internet – ein rechtsfreier Raum? (1999) Universität Salzburg, Diplomarbeit

Faber/Schwarz (Hrsg), Social Networks, So funktionieren Facebook, Xing & Co., Digital lifeguide (2011) Krugzell, Kösel

Frick (Hrsg), Persönlichkeitsrechte, Rechtsvergleichende Studie über den Stand des Persönlichkeitsschutzes in Österreich, Deutschland, der Schweiz und Liechtenstein (1991) Schaan, Österreichische Staatsdruckerei

Gehrke (Hrsg), Datenschutz und -sicherheit im Internet, Handlungsvorschläge und Gestaltungsmöglichkeiten (2005) Düsseldorf, kopaed verlagsgmbh

Handler (Hrsg), Der Schutz von Persönlichkeitsrechten mit besonderer Berücksichtigung des UWG und UrhG (2008) Wien, Verlag Österreich

Härting (Hrsg), Internetrecht[4] (1999) Köln, OVS

Härting/Schätzle, Rechtsverletzungen in Social Networks, ITRB 2010, 39

–, Nutzungsbedingungen in Social Networks, Transparenzgebot und Inhaltskontrolle für soziale Netzwerke, ITRB 2011, 40

Hauser/Thomasser (Hrsg), Wettbewerbs- und Immaterialgüterrecht (1998) Wien, Verlag Österreich

Hofer (Hrsg), datenschutz@internet, Die Privatsphäre im Informationszeitalter (2002) Wien/Graz, NWV Verlag

Höhne/Koukal (Hrsg), Ihr Recht im Internet (2011) Wien, Verein für Konsumenteninformation

Holzhausen, Die Safe-Harbor-Vereinbarung als Methode zur Sicherung eines „angemessenen Datenschutzniveaus“ im Sinne der EG-Datenschutzrichtlinie (2002) Abschlussarbeit im Ergänzungsstudiengang Rechtsinformatik der Universität Hannover

Höss (Hrsg), Die Einbeziehung von AGB beim Vertragsabschluss im Internet, Grundlagen für den österreichisch-deutschen Online-Rechtsverkehr (2007) Saarbrücken, VDM Verlag Müller

Iraschko-Luscher/Kiekenbeck, Datenschutz im Internet – Widerspruch oder Herausforderung? RDV 2010, 261

Jahnel (Hrsg), Handbuch Datenschutzrecht (2010) Wien, Jan Sramek Verlag

–, Dreifacher Datenschutz?, in *Bergauer/Staudegger* (Hrsg), Recht und IT, Zehn Studien, Jan Sramek Verlag (2009)

–, Das Grundrecht auf Datenschutz nach dem DSG 2000, in *Akyürek/Baumgartner/Jahnel/Lienbacher/Stolzlechner* (Hrsg), Staat und Recht in europäischer Perspektive, Festschrift für Heinz Schäffer (2006) Wien, Manz

Jahnel/Siegwart/Fercher (Hrsg), Aktuelle Fragen des Datenschutzrechts (2007) Wien, facultas

Jaksch-Ratajczak (Hrsg), Aktuelle Rechtsfragen der Internetnutzung (2010) Wien, facultas

Knyrim (Hrsg), Datenschutzrecht, Leitfaden für richtiges Registrieren, Verarbeiten, Übermitteln, Zustimmen, Outsourcen, Werben uvm (2003) Wien, Manz

Koziol (Hrsg), Haftpflichtrecht II^{2} (1984) Wien, Manz

Koziol/Welser (Hrsg), Grundriss des Bürgerlichen Rechts I^{13} (2007) Wien, Manz

–, Grundriss des Bürgerlichen Rechts II^{13} (2007) Wien, Manz

Leissler, Social-Networks – Datenschutz in der vernetzten Welt, ecolex 2010, 834

Madl, Vertragsabschluss im Internet, ecolex 1996, 79

Mayer-Schönberger (Hrsg), Delete – Die Tugend des Vergessens im digitalen Zeitalter (2010) Berlin, Dittebrandt Verlagsservice

Pollirer/Weiss/Knyrim (Hrsg), DSG (2010) Wien, Manz

Rechberger/Simotta (Hrsg), Grundriss des österreichischen Zivilprozessrechts, Erkenntnisverfahren[7] (2009) Wien, Manz

Redeker (Hrsg), IT-Recht[4] (2007) München, C.H. Beck

Rest, Postmortaler Persönlichkeitsschutz – Ein Überblick, medien und recht 2012, 113

Rummel (Hrsg), Kommentar zum ABGB (2004) Wien, Manz

Schaar, Soziale Netzwerke: Abschied von der Privatsphäre? Symposium „Datenschutz im Zeitalter sozialer Netzwerkdienste", 13.10.2008, Strasbourg (France)

Schmidbauer, Profile in Social Networks vererben, e-center law survey, http://www.e-center.co.at/static/files/e-center%20law%20survey% 2010-2010.pdf

Schweighofer/Liebwald/Augeneder/Menzel (Hrsg), Effizienz von e-Lösungen in Staat und Gesellschaft – Aktuelle Fragen der Rechtsinformatik, Tagungsband des 8. Internationalen Rechtsinformatik-Symposions IRIS 2005 (2005) Stuttgart, Richard Boorberg Verlag

Sonntag (Hrsg), Einführung in das Internetrecht, Rechtsgrundlagen für Informatiker (2009) Linz, Linde

Steinschaden (Hrsg), Phänomen Facebook, Wie eine Webseite unser Leben auf den Kopf stellt (2010) Wien, Verlag Carl Ueberreuter

Studiengesellschaft für Wirtschaft und Recht (Hrsg), Internet und Recht, Rechtsfragen von E-Commerce und E-Government (2002) Wien, Linde Verlag

Tangl, Leitfaden für die Einbeziehung elektronischer AGB, ecolex 2001, 896

Thiele, Persönlichkeitsschutz in Neuen Medien – Facebook, Google & Co, AnwBl 2013/11 (2013)

–, Der digitale Nachlass – Erbrechtliches zum Internet und seinen Diensten, jusIT 2010/79 (2010)

–, Eurolawyer, Unbefugte Bandaufnahme und ihre Verbreitung im Internet – Braucht Österreich einen eigenen Paparazzi-Paragrafen?, www.eurolawyer.at

Welser (Hrsg), Fachwörterbuch zum bürgerlichen Recht (2005) Wien, Manz

Zankl (Hrsg), Bürgerliches Recht[6], Kurzlehrbuch (2012) Wien, facultas

–, E-Commerce Gesetz, Kommentar und Handbuch (2002) Wien, Verlag Österreich

–, Zivilrecht und E-Commerce, ÖJZ 2001, 542

–, Zur Umsetzung vertragsrechtlicher Bestimmungen der E-Commerce RL, NZ 2001, 288

AUSZUG ONLINE-QUELLEN

Nachfolgende Online-Quellen sowie alle im Hauptdokument zitierten Webseiten wurden zuletzt am 8.10.2012 besucht und kontrolliert.

Bundeskanzleramt, Rechtsinformationssystem

http://www.ris.bka.gv.at

Europäische Kommission

http://ec.europa.eu

Eurolawyer, RA Dr. Clemens Thiele, LL. M.

http://www.eurolawyer.at/

Heise online

http://www.heise.de

Internet-Law, Onlinerecht und Bürgerrechte

http://www.internet-law.de

RDB, die Rechtsdatenbank

http://www.rdb.at/home.html

Rockefeller-News

http://www.rockefeller-news.com

Süddeutsche Zeitung

http://www.sueddeutsche.de

Wikipedia, die freie Enzyklopädie

http://de.wikipedia.org/wiki/Wikipedia:Hauptseite

ENTSCHEIDUNGEN

Österreich

OGH 11.6.1952, 3 Ob 295/52

OGH 3.2.1966, 1 Ob 24/66

OGH 29.6.1971, 4 Ob 330/71

OGH 14.6.1977, 4 Ob 320/77

OGH 22.11.1977, 4 Ob 377/77

OGH 23.5.1984, 1 Ob 550/84

OGH 30.4.1987, 7 Ob 535/87

OGH 22.9.1988, 7 Ob 649/88

OGH 25.1.1995, 6 Ob 37/95

OGH 24.2.1998, 4 Ob 368/97 i

OGH 25.5.2000, 1 Ob 341/99 z

OGH 5.10.2000, 8 ObA 136/00 h

OGH 23.11.2000, 6 Ob 109/00 y

OGH 14.12.2000, 6 Ob 291/00 p

OGH 29.8.2002, 6 Ob 283/01 p

OGH 11.12.2003, 6 Ob 274/03 t

OGH 16.12.2003, 4 Ob 211/03 p

OGH 19.2.2004, 6 Ob 190/03 i

OGH 21.12.2006, 6 Ob 178/04 a

OGH 23.9.2008, 4 Ob 150/08 z

OGH 24.2.2009, 17 Ob 2/09 g

OGH 23.1.2014, 6 Ob 133/13 x

HG Wien 10 Cg 115/10 g

HG Wien 39 Cg 75/10 p

Deutschland

ArbG Bochum 9.2.2012, 3 Ca 1203/11 und LAG Hamm 5 Sa 451/12 (Verfahren ohne Entscheidung erledigt)

KG Berlin 29.4.2011, 5 W 88/11

LG Frankfurt/Main 20.4.2010, 3-08 O 46/10

LG Berlin 14.3.2011, 91 O 25/11

LG Aschaffenburg 19.8.2011, 2 HK O 54/11

LG Berlin 6.3.2012, 16 O 551/10, anhängiges Rechtsmittelverfahren: KG Berlin 5 U 42/12

LG Hamburg 20.4.2012, 310 O 461/10

OLG München 21.9.2011, 6 W 1551/11

OLG Bremen 14.1.2011, 2 U 115/10

OLG München 26.6.2007, 18 U 2067/07

OLG Köln 9.2.2010, 15 U 107/09

BGH 17.3.1999, IV ZR 218/97 NJW 1999, 1865

BVerfG 15.12.1983, 1 BvR 209, 269, 362, 420, 440, 484/83

BVerfG 15.12.1999, 1 BvR 653/96, *Caroline von Monaco II*

VGH Bayern 29.2.2012, 12 C 12.264

EGMR

24.6.2004, 59320/00, *Hannover gegen Deutschland*, MR 2004, 246

EuGH

7.12.2006, C-306/05

19.2.2012, C-360/10

X. **ABSTRACT**

Der Umgang der Gesellschaft mit Daten, Informationen und Kommunikationsmöglichkeiten im Internet war in den letzten Jahren großen Veränderungen unterworfen. Aus dem Internet ist eine Selbstverständlichkeit geworden und unsere Gesellschaft immer mehr eine sog Informationsgesellschaft. Als eine der einflussreichsten Errungenschaften der letzten Jahre im Bereich Kommunikation und Vernetzung können Social network-Plattformen genannt werden, welche zwischenzeitig aus dem alltäglichen Leben kaum mehr wegzudenken sind.

In diesem Zusammenhang werden aber auch einige rechtliche Fragestellungen im Zusammenhang mit dem Speichern, Verwenden und Weitergeben von Daten und Informationen aufgeworfen, die in dieser Arbeit angesprochen und analysiert werden sollen.

Zunächst wird ein genereller Überblick über die Entstehung ausgewählter Social network-Plattformen verschafft und in der Folge werden einige Funktionen beschrieben. Sodann folgt nach Rechtsgebieten unterteilt, eine Analyse der rechtlichen Rahmenbedingungen im Zusammenhang mit Social network-Plattformen.

Die vorliegende Arbeit stellt nicht den Anspruch, sämtliche Problemfelder iZm Social network-Plattformen lösen zu wollen, sondern sollen vielmehr nachvollziehbare Grundsätze erarbeitet und aufgezeigt werden.

XI. CURRICULUM VITAE

Persönliche Daten: Mag. Caterina Laura Hartmann

Berufserfahrung:

15.02.2013 – 30.06.2015	Rechtsanwaltsanwärterin bei Dorda Brugger Jordis Rechtsanwälte GmbH, Universitätsring 10, 1010 Wien
15.02.2012 – 15.09.2012	Rechtsanwaltsanwärterin bei Hausmaninger Kletter Rechtsanwälte GmbH, Franz-Josefs-Kai 3, 1010 Wien
15.03.2010 – 31.12.2011	Rechtsanwaltsanwärterin bei Eustacchio und Schaar Rechtsanwälte, Währingerstraße 26, 1090 Wien
Seit 09/2009	Wissenschaftliche Mitarbeiterin im Internationalen Zentrum für e-commerce und Internetrecht (e-center), unter der Leitung von ao. Univ.-Prof. Dr. Wolfgang Zankl, Graben 17/10, 1010 Wien Studienleiterin der im Jahr 2010 von ao. Univ.-Prof. Dr. Wolfgang Zankl initiierten Studie zum Thema „Social networks“
03/2007 – 10/2009	Juristische Mitarbeiterin in der italienisch/österreichischen Rechtsanwaltskanzlei Petsch Frosch Klein Arturo Rechtsanwälte OG, Dr. Karl-Lueger Platz 5, 1010 Wien
03/2007 – 11/2007	Gerichtspraxis beim Bezirksgericht Fünfhaus und beim Landesgericht für Zivilrechtssachen Wien
07 – 08/2006	Rechtspraktikum in der Rechtsanwaltskanzlei Freshfields Bruckhaus Deringer, Piazza di Monte Citorio, 00186 Roma, Italia

08/2002 – 02/2007	Juristische Mitarbeiterin bei Weiler und Kohlbacher Rechtsanwälte, Franziskanerplatz 3, 1010 Wien
05/2001 – 06/2003	Geringfügige Beschäftigung bei Richter Rechtskurse, Tulpengasse 2, 1080 Wien

Ausbildung:

Seit 03/2007	Doktoratsstudium der Rechtswissenschaften, Universität Wien, in den Gebieten Zivil-, Verfassungs- und Datenschutzrecht
03/2001 – 11/2006	Diplomstudium der Rechtswissenschaften an der Universität Wien
2000	Reifeprüfung Katholische Privatschule St. Ursula Wien