universität wien

MAGISTERARBEIT

Titel der Magisterarbeit

Meine Daten sind deine Daten

Facebook – eine Gratwanderung zwischen Selbstdarstellung und Privatsphäre

Verfasserin

Christine Weilhartner, Bakk. phil.

angestrebter akademischer Grad

Magistra der Philosophie (Mag. phil.)

Wien, 2010

Studienkennzahl lt. Studienblatt:	A 066 841
Studienrichtung lt. Studienblatt:	Magisterstudium Publizistik- u. Kommunikationswissenschaft
Betreuerin:	PD Mag. Dr. Gerit Götzenbrucker

Eidesstattliche Erklärung

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.
Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Wien, 21. Juni 2010

Christine Weilhartner

INHALT

1. Einleitung

1.1. Problemaufriss und aktueller Bezug

Nach dem Aufstehen wird als erstes der Laptop aus dem Standby-Schlaf geholt und gepostet, dass man heute noch gar keine Lust hat, das Bett zu verlassen. Ab unter die Dusche und dann schnell ins Büro. Wenn's doch nur schnell ginge … denn die Straßenbahn braucht ewig. Da bleibt genug Zeit, um noch kurz auf Flickr die neuesten Fotos anzusehen, die eine Freundin online gestellt hat. Endlich kommt die Bim. Aber wie sieht die denn aus? Sie ist vollgesprayt von oben bis unten. Der Bim-Fahrer wirkt ob der belustigten Blicke genervt und blickt unwirsch aus seinem Fenster. Das ist ein Foto wert. Schnell einen Schnappschuss gemacht und via Facebook-Handy hochgeladen: „Bunte Bim, brummiger Fahrer". Später am Tag checkt man noch unzählige Male den Facebook-Account oder den einer anderen Social Network Seite; man wird auf zwei Fotos verlinkt, die am Vorabend geschossen wurden, und ein Freund kommentiert den morgendlichen Status und fragt gleichzeitig, ob man sich am Abend treffen will. Ja, wir sind gut vernetzt. Wir sind am Puls der Zeit, wir wissen alles sofort und geben Informationen in unserem Netzwerk wiederum sofort weiter. Die Nutzung von Social Network Seiten ist in den letzten Jahren drastisch gestiegen (Gross/Acquisti 2005). Im Juni 2010 hatten 2.047.840 Österreicherinnen und Österreicher[1] einen Facebook-Account (digitalaffairs.at), das sind über 24 % der österreichischen Bevölkerung (Statistik Austria). Mit über 400 Millionen Mitgliedern ist Facebook der größte Social Network Dienst weltweit.

Aber wie viel Veröffentlichung tut uns gut? Wie sorgsam sind wir, wenn wir mit persönlichen Informationen um uns werfen? Unsere Kommentare sind ja eigentlich nur für unseren Freundeskreis gedacht. Aber haben wir auch dafür gesorgt, dass niemand sonst sie lesen kann?

Wo hat denn mein zukünftiger Arbeitgeber diese Informationen über mich her? Aus dem Internet? Aber die Daten habe ich doch schon lange von meinem Profil gelöscht. Woher kommt das plötzlich? Aha, digitale Spuren … das Internet vergisst nichts. So, so.

1.2. Forschungsgegenstand und Aufbau der Arbeit

Das Web2.0 ist wie eine Welle über die Internet-Gesellschaft geschwappt – eine Welle, die für viele Privatpersonen zu schnell kam, um darauf vorbereitet zu sein. Plötzlich haben Userinnen und User ungeahnte Möglichkeiten. Sie können ihre Meinung öffentlich kund tun, sich online mit dem Freundeskreis und der Familie austauschen, sich vernetzen – kurz: Inhalte generieren und Daten

[1] In der vorliegenden Arbeit wurde bewusst auf eine gendergerechte Formulierung geachtet. Wenn an mancher Stelle (z.B. bei Definitionen) aus Gründen der besseren Lesbarkeit eine geschlechtsspezifische Formulierung verwendet wurde, gilt die gewählte Form für beide Geschlechter.

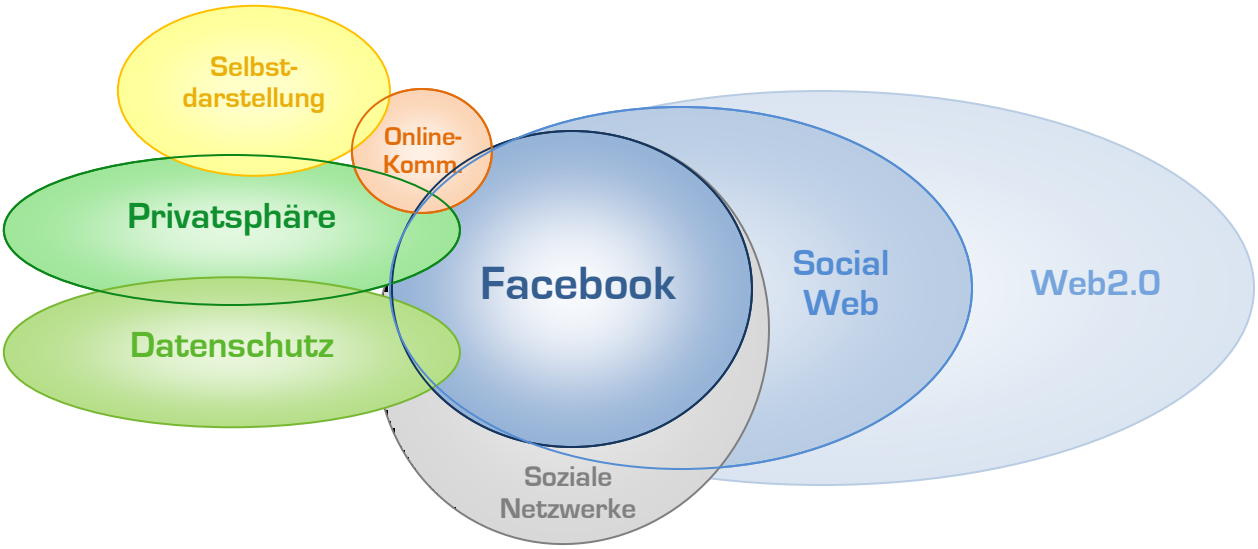
einfach und unkompliziert online stellen. Das Konzept der Selbstdarstellung erfährt dadurch eine völlig neue Dimension, genauso wie das der Privatsphäre.

Während die einen noch damit beschäftigt sind, sich zu überlegen, wie sie sich am besten online präsentieren, schlagen Datenschützer und Datenschützerinnen Alarm und bemühen sich händeringend um mehr Achtung der Privatsphäre. Denn die technischen Neuerungen ermöglichen nicht nur neue Wege der Kommunikation, sie schaffen gleichzeitig die Grundlage für eine unendlich große Ansammlung von Daten.

Für die Kommunikationswissenschaft eröffnet sich mit dem Web2.0 ein riesiges neues Forschungsfeld, das es zu beackern gilt. Manche bewährte Konzepte müssen adaptiert und um neue Aspekte erweitert werden. An anderer Stelle müssen gänzlich neue Ansätze generiert werden, wenn die Forschung mit der technischen Entwicklung mithalten will. In der vorliegenden Arbeit werden bestehende Konzepte auf die Social Network Seite Facebook angewandt. Es stellt sich die Frage, wie Individuen im Zeitalter des Web2.0 mit ihren Daten umgehen – achtsam oder achtlos? Was wissen Facebook-Userinnen und –User über Datenschutz? Und hat dieses Wissen einen Einfluss auf ihr Darstellungsverhalten im Netz? Diesen Fragen soll mit Hilfe einer umfassenden Literatur-Recherche und einer empirischen Studie auf den Grund gegangen werden.

So vernetzt das Web2.0 ist, so verflochten ist auch die vorliegende Arbeit. Die Themenbereiche greifen an vielen Stellen ineinander. Abbildung 1 soll veranschaulichen, auf welchen Pfeilern die Arbeit steht, wo sie theoretisch verortet ist.

Abbildung 1: **Verortung der Arbeit**



Im Zentrum der Arbeit steht der Untersuchungsgegenstand **Facebook**. Dieser bildet die **Schnittmenge zwischen Sozialen Netzwerken und dem Social Web**. Denn einerseits stellt Facebook ein Soziales Netzwerk dar, andererseits befindet es sich im virtuellen Raum – es ist ein **Soziales Online-Netzwerk**, das entstanden ist, wo Soziale Netzwerke auf das Internet treffen.

Das **Web2.0** mit seinen **Social Web Anwendungen** bildet den Nährboden, auf dem sich die Social Network Seite Facebook entwickeln konnte. Die drei blauen Blasen im rechten Teil der Grafik stellen den virtuellen Raum dar: Das Web2.0 ist das Basis-Konstrukt, Social Web ist ein Teilbereich des Web2.0 und Facebook wiederum ist eine der vielen Anwendungen des Social Web. Andere Bestandteile wie Blogs oder Wikis wurden der Einfachheit halber nicht in der Grafik berücksichtigt.

Die Arbeit legt ihren Fokus auf bestimmte Aspekte von Facebook, diese sind im linken Teil der Grafik dargestellt: Mit der rasanten Entwicklung des Web2.0 müssen das Konzept der **Privatsphäre** und ihre rechtliche Entsprechung, der **Datenschutz**, neu überdacht werden. Das Recht auf Privatheit ist ein Grundrecht und trotzdem gerät es immer wieder in Bedrängnis. Der Datenschutz seinerseits ist in verschiedenen Ländern unterschiedlich geregelt. Die größte Schwierigkeit besteht derzeit darin, bei den gesetzlichen Normen und Richtlinien mit den rasanten Entwicklungen der Technik Schritt zu halten. Das Konzept der **Selbstdarstellung** liefert Erklärungen, warum sich Menschen gerne selbst präsentieren. Genau das tun sie auf Facebook – allerdings nicht direkt wie in einem persönlichen Gespräch, sondern durch **computervermittelte Kommunikation**. Erst durch die Möglichkeit der Online-Kommunikation können Personen im Web2.0 interagieren. Darum werden die Besonderheiten der computervermittelten Kommunikation beleuchtet.

Die vorliegende Arbeit befindet sich im Schnittpunkt all dieser Konzepte: Wo Selbstoffenbarung durch computervermittelte Kommunikation auf die Social Web Anwendung Facebook trifft und dabei Privatsphäre und das Recht auf Datenschutz beeinflusst werden, da setzt die Studie an. Im Fokus des Interesses liegt die Social Network Site Facebook im Kontext von Privatsphäre und Selbstdarstellung. Die Studie positioniert sich, wo sich die unterschiedlichen Konzepte kreuzen und gegenseitig beeinflussen.

Die Arbeit versucht, die abgebildeten Bereiche möglichst scharf getrennt und übersichtlich abzuhandeln.

In **Kapitel 2** wird auf die Definition und die Besonderheiten des **Web2.0** eingegangen, auf die Nutzertypologien und die Begrifflichkeiten „Social Web“ und „Social Software“ sowie auf Anwendungen wie Blogs und Social Network Sites. Um Soziale Online-Netzwerke besser zu verstehen, werden in diesem Zuge auch Soziale Netzwerke behandelt, wie sie fernab des Internets existieren.

Kapitel 3 stellt die Konzepte der **Selbstdarstellung** im Wandel der Zeit vor. Die Grundannahmen von Goffman aus dem Jahr 1959 sind noch immer aktuell, doch mit dem technischen Fortschritt kommen viele neue Aspekte hinzu. Es wird geklärt, welche Unterschiede es macht, wenn Selbstdarstellung durch computervermittelte Kommunikation stattfindet und welche Faktoren der Privatsphäre bedacht werden müssen, wenn man sich online präsentiert.

Kapitel 4 hat sich ganz der **Privatsphäre** und dem **Datenschutz** verschrieben. Es werden die geschichtlichen Hintergründe und die gesetzlichen Bestimmungen sowie der Begriff „Daten“ geklärt. Besonders eingegangen wird auf die gesetzliche Situation in Österreich: das Datenschutzgesetz 2000.

Kapitel 5 widmet sich dem Untersuchungsgegenstand, der **Social Network Site Facebook**. Es werden alle bis dahin besprochenen Stränge zusammengeführt und die Aspekte des Web2.0, der Selbstdarstellung und der Privatsphäre auf Facebook angewandt. Neben der Entstehungsgeschichte und dem formalen Aufbau der Plattform wird besonders Bezug genommen auf die Datenschutzrichtlinien von Facebook. In diesem Abschnitt der Arbeit ist die Aktualität des Themas besonders zu spüren. Es wird versucht, ihr Rechnung zu tragen und alle aktuellen Entwicklungen einfließen zu lassen.

Nach diesen theoretischen Fundierungen beginnt mit **Kapitel 6** der **empirische Teil** der Arbeit. Forschungsfragen und Hypothesen werden erarbeitet, das Untersuchungsdesign vorgestellt und die Erhebungsinstrumente sowie die Operationalisierung erklärt.

In **Kapitel 7** folgen dann die Dokumentation der Ergebnisse und die Überprüfung der Hypothesen. Die Arbeit schließt mit einer Zusammenfassung und einem Ausblick.

THEORETISCHER RAHMEN

„Jeder wird zum Produzenten einer Welt – seiner Welt –
und beeinflusst gleichzeitig die Welt der anderen.
Jeder kann seine ewigen Spuren ziehen.“

Hans G. Zeger 2009

2. Web2.0

> „Was wir erleben ist eine Revolution, die so groß ist, dass sie auch viele Eingeweihte noch gar nicht abschätzen können. Vergleiche wie Gutenbergs Erfindung der Druckerpresse greifen wahrscheinlich zu kurz. Der Vergleich wäre richtig, wenn man sagen würde, Gutenberg hat einen Buchdruck erfunden, um Bücher zu publizieren, die wir lesen und die gleichzeitig in der Lage sind, uns zu lesen.“ (Schirrmacher 2010 in: ORF 2, Club2)

Frank Schirrmacher, Herausgeber der Frankfurter Allgemeinen Zeitung, sieht mit dem Web2.0 einen gesellschaftlichen Wendepunkt gekommen. Damit steht er nicht allein. Das Web2.0 wird als etwas Großes angesehen. Oftmals definiert und viel zitiert, ist es eines der Schlagworte des Jahrzehnts. Oder hält man es mit Schirrmacher, vielleicht sogar das Schlagwort des Jahrhunderts. Da es sich bei Facebook um eine Plattform handelt, die nur auf Grund von Web2.0-Technologien entstehen konnte, und die auch viele typische Merkmale des Web2.0 verkörpert, wird als Basis für die vorliegende Arbeit eine Annäherung an den Web2.0-Begriff versucht.

2.1. Entstehung und Definition

Wo immer man etwas über die Anfänge des Web2.0 liest, taucht der Name Tim O’Reilly auf. In der Literatur ist man sich einig, dass es der amerikanische Verleger war, der den Begriff einführte und prägte. Zum ersten Mal benutzte er den Begriff auf einer Konferenz im Oktober 2004. Kurz darauf widmete er dem Thema Web2.0 einen Online-Text, der den Begriff in Fachkreisen etablierte.

> „Web 2.0 is a set of economic, social and technology trends that collectively form the basis for the next generation of the Internet — a more mature, distinctive medium characterized by user participation, openness and network effects.” (Musser/O’Reilly 2006, S.4)

In der Welt der Software und Programme ist es üblich, neue Versionen mit Nummern zu versehen. In Anlehnung daran erfindet O’Reilly den Titel Web2.0 – denn er sieht das Internet an einem

Wendepunkt: Für O'Reilly ist das Internet nach dem Platzen der Dot.com-Blase 2001 in eine neue Ära eingetreten. Es hat sich durch neue Trends weiterentwickelt und erstrahlt nun als Web2.0 in neuem Glanz – offen, partizipativ und vernetzt. (2005, S.1) Schmidt ist der Meinung, es sei zu extrem, von einer Internet-Revolution zu sprechen. Vielmehr ist er der Ansicht, dass sich das Internet stetig weiterentwickle und man keineswegs von einem „abrupten Sprung auf eine neuere ‚Version' des Internets" sprechen könne. (2008, S.20f) Abgesehen von einzelnen definitorischen Kritikpunkten ist man sich in der Literatur aber relativ einig, was Web2.0 ist und welche Bereiche es umfasst.

Im Folgenden wird Web2.0 nach Tim O'Reilly definiert, da er den Begriff nachweislich prägte.

Das Web2.0 positioniert sich als **Plattform, auf der Userinnen und User die eigenen Daten kontrollieren**. O'Reilly (2005) nennt sieben Kernkompetenzen, die das Web2.0 kennzeichnen:

- **Services, not packaged software**
  Die Software-Industrie wird von Service-Angeboten abgelöst, die nicht verkauft, sondern online zur Verfügung gestellt werden. An die Stelle von geplanten Releases tritt eine kontinuierliche Verbesserung; Lizensierung und Verkauf müssen der reinen Bereitstellung weichen.
- **Control over unique, hard-to-recreate data sources that get richer as more people use them**
  Wichtige Datenquellen werden kontrolliert, vor allem wenn ihre Erstellung teuer ist oder sie empfänglich für immer größer werdende Rückflüsse durch Netzwerkeffekte sind.
- **Trusting users as co-developers**
  Userinnen und User werden als Mitentwickler gesehen, die ihren Teil zum Inhalt beisteuern. Das Credo lautet: „Users add value!" Allerdings kann davon ausgegangen werden, dass nur ein kleiner Prozentsatz der Nutzenden Zeit investiert, um altruistisch den Wert einer Anwendung zu vergrößern. Die Architektur des Internets ist darum so aufgebaut, dass ein kollektiver Nutzen als Nebenprodukt entsteht, wenn jemand eigene Interessen im Internet verfolgt.
- **Harnessing collective intelligence**
  Eine Stärke des Web2.0 ist die effektive Nutzung kollektiver Intelligenz. Ein Paradebeispiel dafür ist Wikipedia, die freie Online-Enzyklopädie, die von jedem und jeder erweitert und verändert werden kann. So entsteht eine Wissenssammlung enormen Ausmaßes durch virtuelle Kollaboration. Auch die Plattform YouTube lebt von der Partizipation der Userinnen und User. (Auch wenn bei so manchen Videos der Terminus „kollektive Intelligenz" kaum angebracht scheinen mag). Durch das ständige Hochladen neuer Clips kann die Video-Sammlung interessant bleiben. Netzwerkeffekte durch Beiträge von Userinnen und User sind der Schlüssel zur Marktbeherrschung in der Web2.0-Ära.

- **Leveraging the long tail through customer self-service**
  "The long tail" steht für viele kleine Internet-Seiten. Diese einzelnen Seiten bilden den Hauptbestandteil des Internets und sind darum für den Werbemarkt interessanter als so manche große Seite. Das Web2.0 macht sich die Selbstbedienung der Kunden zu Nutze, um jeden Winkel des Webs zu erreichen – nicht nur den Kopf, sondern auch die vielen Enden, eben den „long tail".
- **Software above the level of a single device**
  Software wird nicht mehr nur für den PC geschrieben, sondern setzt sich über Gerätegrenzen hinweg. Ein gutes Beispiel dafür liefert iTunes: Diese Anwendung läuft über mobile Endgeräte und nutzt den PC als lokalen Zwischenspeicher.
- **Lightweight programming models**
  Das Web2.0 wird dem Wunsch nach Simplizität gerecht und statuiert ein Exempel: Die Web-Services mit der größten Reichweite sind die, die am wenigsten komplex sind und sich durch Einfachheit auszeichnen (z.B. RSS).

Tim O'Reilly ist sich also sicher: Das Internet hat nach dem Platzen der Dot.com-Blase nicht ausgedient, sondern es hat sich nur gehäutet. Es stellt nun eine Plattform dar, die Anwendungen hervorbringt, die umso besser werden, je mehr Leute sie nutzen und die genau von diesen Leuten lernen und von Netzwerkeffekten profitiert kann. (O'Reilly/Battele 2009, S.1)

Obwohl O'Reilly seine sieben Web2.0-Kennzeichen nicht bewusst reiht, scheinen manche Punkte größer und relevanter zu sein als andere. Als Kernkompetenz des Web2.0 lässt sich zusammenfassen, dass es den passiv Nutzenden zum aktiv Teilnehmenden macht. Inhalte werden dynamisch von vielen verschiedenen Personen generiert und die kollektive Intelligenz wird zur stetigen Weiterentwicklung genutzt. Auf Besonderheiten dieser neuen Art der Nutzung wird in Kapitel 2.2 näher eingegangen.

Seit den ersten Versuchen, das Web2.0 zu erfassen sind fünf Jahre vergangen. In diesen fünf Jahren zeigte sich die Definition von O'Reilly durchaus praktikabel. Natürlich ist das Web2.0 aber in dieser Zeit gewachsen und hat sich somit weiterentwickelt. O'Reilly prognostiziert, dass die Möglichkeiten des Web2.0 exponentiell steigen und hält fest, das Web2.0 sei den Kinderschuhen entwachsen. Durch die kollektive Intelligenz hat es sich stetig weiterentwickelt und macht große Schritte in die Zukunft. (O'Reilly/Battele 2009, S.3)

Das neue Stichwort lautet "lernen". Das Internet ist „lernfähig", durch unsere Handlungen bringen wir ihm etwas bei. Das Foto-Programm wird dazu gebracht, bestimmte Gesichter zu erkennen, wichtige Infos werden online geteilt und Personen werden auf Plattformen verlinkt, um das Kontakthalten zu erleichtern. Mit jedem Mehrwert, den Userinnen und User für sich schaffen, generieren sie gleichzeitig auch einen Mehrwert für das Social Web. (O'Reilly/Battele 2009, S.8)

Darüber hinaus spannt das Web2.0 sein Netz immer weiter und ist inzwischen fest mit der realen Welt verwoben. O'Reilly nennt in seinen Überlegungen Kuniavskys „information shadows": Demnach haben alle Dinge der realen Welt einen Schatten im Cyberspace. Bücher beispielsweise werfen ihre Schatten auf Amazon, eBay, Google Book Search, Twitter etc. Genauso hat auch ein Mensch seine digitalen Schatten: in E-Mails, in Instant-Messages, in Blog-Einträgen, auf Fotos oder Videos etc. (Kuniavsky 2009 zit.n. O'Reilly/Battele 2009, S.7).

Mit dieser Fortführung seiner Überlegungen macht O'Reilly deutlich, dass das Web2.0 weiterhin am aufstrebenden Ast ist und noch viele Möglichkeiten in sich birgt.

Nach diesen sehr ausführlichen Vorstößen des Web2.0-Pioniers O'Reilly wird hier die Meinung anderer Experten auf den Punkt gebracht:

Gerhards et al. (2008, S.129f) beschreiben zwei Dimensionen des Web2.0: Die Möglichkeit zur Gestaltung oder Mitgestaltung von eigenen Webangeboten sowie die Verwendung des Internets als öffentliche Kommunikationsplattform. Ein hoher Gestaltungs- und Kommunikationsgrad ist es, was das Web2.0 von seinem Vorgänger, dem „alten" Internet unterscheidet. Während früher das Internet passiv genutzt wurde, also eher betrachtend, und vor allem für individuelle Kommunikation (z.B. E-Mail), verschiebt sich die Nutzung inzwischen hin zu einer aktiven Beteiligung, zur Selbstgestaltung und zur öffentlichen Kommunikation (z.B. Blog-Einträge). Userinnen und User haben die Möglichkeit, durch User-generated-content, also einem selbst geschaffenen Inhalt, die mediale Welt selbst mitzugestalten. So ist jeder in der Lage, im Web2.0 aktiv mitzuarbeiten. (Reinecke et al. 2008, S.210)

Auch der Datenschützer Zeger sieht als wesentliche Komponente einer Web2.0-Definition die Partizipation der Userinnen und User. Er betrachtet diese Tatsache allerdings zynisch:

> „Web2.0 ist die Produktion von Inhalten durch Nutzer für Nutzer auf Plattformen, die ihnen nicht gehören, mit technischen Mitteln, die sie nicht verstehen, und in einem organisatorischen Umfeld, das sie nicht durchschauen (user-driven)." (Zeger 2009, S.17)

Auf solche und ähnliche Kritik am Web2.0 und all seinen Begleiterscheinungen wird im Laufe der Arbeit noch an mehreren Stellen eingegangen. (Kapitel 2.2.1, 3.3 und 4.4.4)

2.2. Nutzung des Web2.0

Seit 1996 untersucht das Marktforschungsinstitut GfK Austria den Zugang und die Nutzung des Inernets in Österreich. Instrument dafür ist der GfK Online Monitor, mit dem kontinuierlich der österreichische Internetmarkt beobachtet wird. Durch 16.000 Telefon-Interviews im Jahr können repräsentative Aussagen über die österreichische Bevölkerung ab 14 Jahren getroffen werden. Die

Studie enthält Daten zur Entwicklung des Internetmarktes und zur Struktur der Internet-Nutzenden, nicht aber zur Nutzung von einzelnen Anwendungen des Internets. (gfk.at)

In Deutschland untersucht seit 1997 die repräsentative ARD/ZDF-Online-Studie die Entwicklung der Internetnutzung sowie den Umgang der Nutzerinnen und Nutzer mit den Angeboten. Seit 2006 werden im Zuge dieser Studie auch die Nutzungsdaten von Web2.0-Anwendungen erhoben. (ard-zdf-onlinestudie.de) Da der österreichische GfK Online Monitor keine Ergebnisse in diesem Punkt liefert, werden an dieser Stelle die deutschen Daten berücksichtigt.

Betrachtet man Tabelle 1 zur Nutzung der Web2.0-Angebote 2009, wird deutlich, dass die Nutzungswahrscheinlichkeit umso geringer ist, je älter die Befragten sind.

Tabelle 1**: Web2.0-Angebote**
Basis: Onlinenutzende ab 14 Jahren in Deutschland (2009: N=1212)

Web2.0-Angebote Zumind. selten genutzt Angaben in %	Gesamt	Frauen	Männer	14-19	20-29	30-39	40-49	50-59	60+
Wikipedia	65	64	67	94	77	70	62	50	39
Videoportale	52	45	58	93	79	55	45	27	12
Private Netzwerke	34	36	32	81	67	29	14	12	7
Fotosammlungen	25	25	26	42	41	20	19	19	14
Berufliche Netzwerke	9	8	11	6	16	13	8	7	1
Weblogs	8	6	10	12	16	10	5	4	1
Lesezeichen-sammlungen	4	4	4	9	6	4	2	2	2

Quelle: ARD/ZDF-Online-Studie 2009

Was durch die bloße Betrachtung der Nutzungshäufigkeit nicht abgebildet wird, ist die **Art der Nutzung**. Eine wichtige Besonderheit des Web2.0 ist, wie oben ausgeführt, dass Userinnen und User nicht nur Inhalte rezipieren, sondern auch selbst produzieren können. Darum muss eine Unterscheidung getroffen werden zwischen passiv Nutzenden, die Informationen, Wissens- und Kulturgüter konsumieren und aktiv Nutzenden, die während der Nutzung neben der Rezeption auch Inhalte hervorbringen, bewerten oder verbreiten. (Schmidt 2008, S.26) Da Schmidt den Begriff Social Web so verwendet, wie in weiten Kreisen Web2.0 definiert wird, kann seine Social Web Aufstellung auf Web2.0-Anwendungen umgelegt werden. Tabelle 2 zeigt deutlich, dass das Web2.0 häufiger passiv genutzt wird als aktiv.

Tabelle 2**: Aktive & passive Social Web Nutzung**

Aktive & passive Social Web-Nutzung in % aller AnwendungsnutzerInnen	**Info nur abgerufen**	**Info verfasst/eingestellt und abgerufen**
Videoportale	93	7
Weblogs	76	24
Wikipedia	94	6

Quelle: Gscheidle/Fisch 2007, S.401 in: Schmidt 2008, S.27

2.2.1. Produsage

Im Zusammenhang mit aktiver Web2.0-Nutzung führt Burns den Begriff der „Produsage“ ein – eine neue hybride Form von „simultaneous production and usage“, also ein zeitgleiches Produzieren und Verwenden von Inhalten. (Bruns 2007)

Burns stellt den Begriff der *Produktion,* wie er zur Zeit der industriellen Revolution geprägt wurde, in Frage. Bei der klassischen Produktion wird von einem Produzenten oder einer produzierenden Gruppe ein fertig abgeschlossenes Produkt geschaffen, das von einem Distributor verteilt und vom Konsumenten gekauft wird. Die Konsumentinnen und Konsumenten sind meist nicht mit der produzierenden Person in Kontakt. Kommt vom erworbenen Produkt eine neue Version auf den Markt, muss ein ganzes neues Produkt gekauft werden.

Beim Konzept der *Produsage* hingegen steht nicht das eigenständige Produkt im Vordergrund, sondern vielmehr ein sich ständig ändernder Inhalt.

> Produsage is „the collaborative and continous building and extending of existing content in pursuit of further improvement.“ (Bruns 2007, S.3)

Vier Merkmalen kennzeichnen die Produsage:

- eine große Gruppe von Teilnehmerinnen und Teilnehmern
- der fließende Übergang zwischen verschiedenen Rollen (z.B. Leader, Teilnehmer, Nutzer)
- unfertige Erzeugnisse, die sich stets in Entwicklung befinden
- eine Ordnung, die auf Leistung basiert, nicht auf Besitz

In der Praxis gibt es viele Beispiele, wo Produsage schon lange praktiziert wird. Etwa auf Social Networking Sites und Blogs, bei gemeinschaftlich geschaffenen Wissens-Ansammlungen wie Wikipedia und Google Earth oder bei Multi-User Online Games, bei denen die Spielerinnen und Spieler zu Kreativen werden, um nur einige Beispiele zu nennen. Bruns sieht darin einen Trend weg von der Praxis des Industrie-Zeitalters und hin zu neuen Paradigmen, den *user-led information-age paradigms*.

Natürlich stellt sich die Frage, wem diese neue Art der Produktion einen Nutzen bringt. Privatpersonen speisen Wissen in das Internet ein, kreieren Inhalte, stellen Informationen online. Dadurch entstehen riesige Datensammlungen, die frei zugänglich sind und anderen Userinnen und Usern zur Verfügung stehen. Aber die Datenmengen stehen nicht nur anderen Privatpersonen zur Verfügung. Herbold (2009, S.67ff) liefert eine klare Antwort auf die Frage, wem der von Userinnen und Usern erstellte Inhalt am meisten bringt: der Werbeindustrie. Die Autorin sieht hinter der aktiven Teilnahme von Internet-Userinnen und –Usern an der Generierung von Content eine „Instrumentalisierung der Massen". Aus den riesigen Datensammlungen wird von den großen Konzernen, die hinter den einzelnen Plattformen stehen, Profit geschlagen. Die größten Nutznießer des Produsage-Internets sind die Giganten, denen gut besuchte Web-Seiten gehören. Diese Internet-Riesen hegen und pflegen eine Plattform, wie beispielsweise Amazon, Google oder Facebook und freuen sich daran, dass so viele Menschen bereitwillig die Seite vergrößern, ohne dafür bezahlt zu werden. Jeder Post, jeder Kommentar, jede Produktbewertung vergrößert die Datenbank der Seite, steigert den Werbewert und erhöht somit den Preis der Seite. Auch Schirrmacher (2010 in: ORF 2, Club2) sieht den Profit der Großkonzerne kritisch. Im Online-Geschäft profitieren sehr wenige sehr viel. Er bezeichnet darum Online-Handlungen der Userinnen und User als „kostenlose Arbeit für Konzerne wie Google und andere". Und dabei geht es nicht nur um bewusst erstellte Inhalte wie das Posting in einem Forum oder einem verfassten Wikipedia-Eintrag. Wertvolle Daten fallen schon bei den kleinsten Bewegungen im Netz an. Für Google beispielsweise ist jede Suchanfrage gleichzeitig eine Antwort, weil sie irgendwie verwertet werden kann. Nach Schirrmachers Meinung hat es eine „kostenlose Mikro-Arbeit" in diesem Ausmaß zuvor noch nie gegeben. Er plädiert dafür, Dinge kritisch zu hinterfragen und die verschiedenen Interessen zu ergründen.

Den meisten, die sich schon einmal damit auseinandergesetzt haben, wie im Internet Profite erzielt werden, ist wohl klar, dass der Umsatzbringer schlechthin die Werbeschaltungen sind. Je mehr Klicks eine Seite bekommt, je mehr Gäste sich auf einer Seite tummeln, desto teurer kann ein Werbeplatz auf dieser Seite verkauft werden. Denkt man diesen Gedanken fertig, wirtschaften alle Personen, die im Netz surfen, Inhalte generieren und damit weitere Nutzerinnen und Nutzer anlocken, in fremde Taschen. Sie erhöhen den Werbewert einer Seite ohne davon selbst einen materiellen Nutzen zu haben.

Das Konzept der Produsage erscheint vor diesem Hintergrund als zweischneidiges Schwert. Einerseits wird der Nutzer bzw. die Nutzerin zum Produzenten bzw. zur Produzentin, kann sich selbst einbringen, interaktiv auf Inhalte reagieren und selbst welche erstellen. Userinnen und User profitieren davon, dass die Informationsdichte im Internet beständig wächst und Inhalte ohne sichtbares Ende abgerufen werden können. Andererseits gibt es neben dem ideellen Gewinn der öffentlich zugänglichen Informationen auch einen hohen materiellen Gewinn. Und diesen streichen alleine die Konzerne ein, die die Internet-Seiten betreiben. Vom wirtschaftlichen Gewinn ihrer Beiträge sehen die engagierten Produserinnen und Produser nichts.

2.2.2. Nutzungstypen nach Motiven

Gerhards et al. (2008, S.132ff) haben in einer Studie die Auswirkungen des Web2.0 auf das allgemeine Mediennutzungsverhalten untersucht und eine **Typologie der Nutzerinnen und Nutzer von Web2.0** entwickelt. Die acht definierten Typen unterscheiden sich nach Haupt-Nutzungsmotiven.

Produzenten

Nutzerinnen und Nutzer, die Web2.0-Anwendungen nutzen, um Inhalte zu veröffentlichen[2]. Sie sind an der Verbreitung ihrer „Werke" interessiert und erstellen auf Blogs, Foto- oder Videoseiten Inhalte, die auch offline über andere Medien veröffentlicht werden könnten. Hobby-Musiker, -Fotographen oder Videokünstler sind besonders oft diesem Nutzertyp zuzuordnen.

Selbstdarsteller

Den Selbstdarstellern geht es wie den Produzenten um das Erzeugen von Inhalten, allerdings steht kein Werk im Vordergrund, sondern die Person selbst. Selbstdarsteller haben im Web2.0 zum Beispiel die Möglichkeit, einen Blog zu schreiben oder sich auf Social Network Sites zu präsentieren.

Spezifisch Interessierte

Spezifisch Interessierte nutzen das Web2.0 für ein ganz bestimmtes Interesse oder ein spezifisches Hobby. Dabei haben sie die unterschiedlichsten Möglichkeiten: Sie können über ein Thema recherchieren, etwas nachlesen, etwas auf YouTube dazu ansehen, sie können sich auf Foren mit Gleichgesinnten austauschen, einen Blog über das Thema schreiben, Fotos veröffentlichen und noch vieles mehr.

Netzwerker

Die Gruppe der Netzwerker nutzt das Web2.0 zum Austausch mit anderen. Sie will Leute kennenlernen oder bestehende Kontakte pflegen und vertiefen. Auch für diesen Nutzungstyp gibt es viele Möglichkeiten: das Führen eines Blogs, Veröffentlichen von Texten, Fotos und Videos, die Teilnahme auf einer Social Network Site, etc.

Profilierte Nutzer

Diese Nutzerinnen und Nutzer schöpfen die Möglichkeiten der Mitgestaltung und Kommunikation im Netz vollständig aus und verwenden das Web2.0 dazu, wozu es laut Definition fähig ist: zur Selbstdarstellung, zur Kontaktaufnahme und –pflege und zur Verbreitung von Inhalten. Als typisches Beispiel können Blogger genannt werden, die intensiv in die Blogosphäre eingebunden sind.

[2] Unter einer Veröffentlichung wird in der vorliegenden Arbeit der Prozess verstanden, in dem man Daten online allen uneingeschränkt zugänglich macht. Im Unterschied dazu zählt ein Inhalt nicht als veröffentlicht, wenn die Personengruppe, die Zugriff hat, eingeschränkt ist. In diesem Fall werden Termini wie „online stellen" verwendet. Die rechtlichen Grundlagen für diese Definition werden in Kapitel 4.3.2 erläutert.

Kommunikatoren

Kommunikatoren schätzen den Austausch über Inhalte und machen Gebrauch von den öffentlichen Kommunikationsmöglichkeiten des Web2.0. Beispiele für Kommunikatoren sind Blogleser, die Beiträge kommentieren, oder Menschen, die Videos im Netz anschauen, weiterleiten und kommentieren.

Infosucher

Viele Userinnen und User nutzen das Web2.0 nicht aktiv, sondern nur passiv und verwenden das Internet zur Recherche und Infosuche. Sie verwenden das Web2.0 oft in einer Art und Weise, wie sie bereits das Web1.0 verwendet haben, können aber auch durchaus von Web2.0-Angeboten profitieren, beispielsweise von der freien Online-Enzyklopädie Wikipedia, die als umfangreiches Nachschlagewerk nur durch kollektives Schreiben entstehen konnte.

Unterhaltungssucher

Für diese Gruppe steht vor allem der Unterhaltungsaspekt im Vordergrund, sie nutzt keine Kommunikations- und Mitgestaltungsmöglichkeiten, sondern rezipiert beispielsweise Videos auf YouTube, ohne sie zu kommentieren.

Die Auswertung der Studie ergab, dass **Kommunikatoren** und **Unterhaltungssucher** die häufigsten Nutzertypen sind – jeweils 34 % aller Nutzerinnen und Nutzer lassen sich diesen Gruppen zuordnen. An dritter Stelle kommen die **Infosucher**, zu denen 31 % aller Web2.0-Userinnen und –User zählen.

Natürlich kann eine Nutzerin oder ein Nutzer auch mehreren Typen entsprechen, wenn sie oder er beispielsweise unterschiedliche Anwendungen zu verschiedenen Zwecken nutzt. So kann man etwa ein Infosucher sein, weil man Wikipedia nur als Nachschlagewerk benutzt, aber selbst keine Beiträge verfasst. Gleichzeitig zählt man aber auch zu den Unterhaltungssuchern, weil man auf YouTube gerne Videos rezipiert.

Die Plattform Facebook, um die es in der vorliegenden Arbeit geht, stellt einen Raum für verschiedene Nutzungstypen dar. Stark vertreten ist sicher die Gruppe der Selbstdarsteller sowie die der Netzwerker. Aber auch für Kommunikatoren und Unterhaltungssucher sind die Angebote auf Facebook interessant. Die Mitglieder der Plattform können aus unterschiedlichen Motiven handeln und dementsprechend verschiedene Anwendungen nutzen.

2.3. Social Web & Social Software

Oft ist die Rede davon, dass das Web2.0 ein soziales Internet ist – ein Social Web. Die Begriffe Social Web und Social Software werden in der Kommunikationsbranche fast schon inflationär

gebraucht. Im folgenden Kapitel werden die beiden Begriffe abgegrenzt und es wird festgehalten, welche Bereiche des Web2.0 sie umfassen.

2.3.1. Definitionen

Schmidt (2008, S.22) plädiert in einem Aufsatz dafür, dass der Begriff „Social Web“ synonym für „Web2.0“ verwendet wird. Und er geht sogar noch weiter: Er schlägt vor, den derzeitigen Status des Internets nur noch Social Web und nicht wie weit verbreitet Web2.0 zu nennen. Seine Gründe dafür sind, dass das Social Web nicht zwischen zeitlichen Phasen unterscheidet, dass der Begriff auf das World Wide Web als zunehmend universaler Dienst des Internets verweist und dass der grundlegende soziale Charakter von Internet-Bereichen betont wird.

In der vorliegenden Arbeit wird das Social Web allerdings als Teilbereich des Web2.0 betrachtet und nicht als Synonym. Danach umfasst es den Bereich des Web2.0, der soziale Strukturen und Interaktionen im Netz unterstützt (Ebersbach et al. 2008, S.29).

Ebersbach, Glaser und Heigl liefern eine detaillierte Definition, nach der das Social Web sowohl Internet-Anwendungen als auch Daten und Beziehungen umfasst. Die sehr kompakte Definition wird unten genau erläutert und der von Social Software gegenübergestellt. Auch Social Software wird vereinzelt mit Web2.0 gleichgesetzt. Meistens wird es jedoch als Teilmenge von Web2.0 angesehen. (Hippner 2006, S.6)

> **Social Web** besteht aus „webbasierten Anwendungen (im Sinne des WWW), die für Menschen den Informationsaustausch, den Beziehungsaufbau und deren Pflege, die Kommunikation und die kollaborative Zusammenarbeit in einem gesellschaftlichen oder gemeinschaftlichen Kontext unterstützen, sowie den Daten, die dabei entstehen und den Beziehungen zwischen Menschen, die diese Anwendungen nutzen.“(Ebersbach et al. 2008, S.31)
>
> **Social Software** umfasst „webbasierte Anwendungen, die für den Menschen den Informationsaustausch, den Beziehungsaufbau und die Kommunikation in einem sozialen Kontext unterstützen und sich an spezifischen Prinzipien orientieren.“ (Hippner 2006, S.7)

Es ist leicht ersichtlich, dass sich die Definitionen von Social Web und Social Software in manchen Punkten gleichen und sich in anderen wesentlich unterscheiden.

Mit **„webbasierten Anwendungen“** meinen Ebersbach et al. Anwendungen, die über einen Browser laufen und keine zusätzliche Software oder externe Komponenten benötigen. Instant Messaging wäre nach dieser Definition also keine Anwendung des Social Web, da es nicht alleine über das Internet läuft, sondern man eine eigene Software dafür herunterladen muss. In der Definition von „Social Software“ sind hingegen alle webbasierten Anwendungen enthalten, auch jene, die nicht auf dem WWW aufsetzen.

Für wen die Anwendungen gedacht sind, darin ist man sich einig: Social Web und Social Software haben beide in ihrer Definition verankert, für den **Menschen** zu sein.

Beide Definitionen enthalten den **„Beziehungsaufbau“**, der unterstützt werden soll. Das Social Web geht an dieser Stelle aber noch etwas weiter: Es unterstützt nicht nur den Aufbau von Beziehungen, sondern auch deren Pflege. Dabei handelt es sich nicht ausschließlich um neue Kontakte, sondern viel öfter um bereits bestehende Beziehungen, die vielleicht schon länger nicht mehr allzu gut gepflegt wurden und jetzt im Social Web aufgefrischt werden.

Ein weiterer Punkt, in dem sich Social Web und Social Software unterscheiden, ist der **„Informationsaustausch“**. Während nach Hippner Social Software „nur“ den Austausch von Informationen unterstützt, hat im Social Web auch die Erstellung der Information Bedeutung – durch kollaborative Verfahren wird gemeinsam etwas Neues geschaffen. Voraussetzung dafür ist eine elektronische Vernetzung, die solch eine Zusammenarbeit erst möglich macht.

Während laut Definition Social Software die Menschen **in sozialem Kontext** unterstützt, wird für das Social Web der Begriff „sozial“ aufgespalten in „gesellschaftlich und gemeinschaftlich“. Einer Gesellschaft schließen sich Personen eher aus rationalen Gründen an, einer Gemeinschaft aus emotionalen. Beide Gründe können im Social Web vorkommen.

Als großer Unterschied zwischen Social Web und Social Software ist die Breite der Definition zu nennen: Während Social Software nur **Programme und Anwendungen** umfasst, zählen zum Social Web zusätzlich auch die bereitgestellten Daten und das soziale Geflecht der Beteiligten. (Ebersbach et al. 2008, S.29ff)

Der letzte Punkt der Social Software Definition besagt, dass Anwendungen nur dann als Social Software gelten, wenn sie sich an **spezifischen Prinzipien** orientieren. Mit diesem Punkt packt Hippner weitere sechs Kriterien in die Definition von Social Software. Die Punkte mögen teilweise auf Anwendungen des Social Web umgelegt werden können, werden aber nach der Definition von Social Web nicht explizit eingefordert.

Die **Prinzipien von Social Software** sind nach Hippner (2006, S.7):

- **Das Individuum bzw. die Gruppe steht im Mittelpunkt**: Das Augenmerk liegt auf Gestaltung von Beziehungen
- **Selbstorganisation**: Demokratisierung des Web durch Entwicklung von nicht kommerziellen Diensten wie Wikis oder Weblogs
- **Soziale Rückkoppelung**: Social Ratings sind möglich durch Kommentare, Verlinkungen etc. und ermöglichen eine Bewertung
- **Verknüpfung von Informationen:** Der Fokus liegt nicht auf einzelnen Infos, sondern auf möglichst ausgiebiger Vernetzung von Informationen und Personen.
- **Integration in einer Gruppe**: Das Individuum integriert sich, One-to-one-Kommunikation ist nicht erwünscht.
- **Sichtbare Personen, Beziehungen, Inhalte und Bewertungen**: Der einzelne Internetnutzer stellt sich und sein Wissen der Gemeinschaft zur Verfügung.

Es lässt sich also zusammenfassen, dass Social Web und Social Software zwei Teilbereiche des Web2.0 sind, die einige Überschneidungsmengen haben, sich aber auch in manchen wesentlichen Punkten unterscheiden. In Tabelle 3 sind noch einmal die wichtigsten Unterscheidungsmerkmale zusammengefasst.

Tabelle 3: **Unterschiede zwischen Social Web und Social Software**

Social Web	Social Software
Umfasst Anwendungen, die im Browser laufen, Daten und Beziehungen	Umfasst alle webbasierten Anwendungen und Programme
Unterstützt Beziehungsaufbau und –pflege	Unterstützt Beziehungsaufbau
Unterstützt Informationserstellung und -austausch	Unterstützt Informationsaustausch
Weit gefasste Definition	Detaillierte charakteristische Prinzipien

Szugat et al. (2006, S.13) definieren Social Software als „diejenigen Webanwendungen, die dazu dienen, die Kommunikation innerhalb menschlicher Netzwerke zu unterstützen“ mit einem Schwerpunkt auf „Many-to-many-relationships, also Beziehungen, wie sie innerhalb von Gruppen bestehen“. Dabei steht der Mensch im Mittelpunkt, nicht der in ein Netzwerk eingebundene Rechner.

Es gibt zwei Voraussetzungen, die erfüllt werden müssen, um Social Software möglich zu machen:

- Bereitschaft der Nutzerinnen und Nutzer, selbst Inhalte für das Web zu schaffen, den sogenannten „User-generated-content“
- Bereitschaft der Nutzerinnen und Nutzer, ihre Anonymität im Netz zumindest teilweise aufzugeben (Szugat et al. 2006, S.13f)

Es gilt das Motto: „Fragen Sie zehn Experten, was Social Software ist, und Sie erhalten mindestens zehn unterschiedliche Antworten.“ In diesem Sinne gibt es noch viele weitere Definitionen zu Social Software und ebenso zu Social Web. Auch wenn diese Definitionen in dem einen oder anderen Punkt voneinander abweichen, gibt es einen großen Konsens: Im Mittelpunkt steht sowohl bei der Social Software als auch beim Social Web immer der Mensch, der im Internet bei sozialen Interaktionen unterstützt werden soll.

2.3.2. Funktionen

Schmidt (2008, S.23f) beschreibt drei **Funktionen des Social Webs**, die fast deckungsgleich sind mit den Funktionen, die aus der Definition nach Ebersbach hervorgehen.

Identitätsmanagement: Userinnen und User haben im Social Web die Möglichkeit, sich selbst zu präsentieren. Beispielsweise durch das Publizieren von Videos auf YouTube oder der Artikulation der eigenen Meinung auf Blogs.

Beziehungsmanagement: Das Social Web kann zur Pflege bestehender Kontakte oder zum Knüpfen von neuen Kontakten verwendet werden. Besonders geeignet dafür sind Social Network Sites wie Facebook oder auch die Möglichkeit, sich auf Blogs gegenseitig zu verlinken.

Informationsmanagement: Userinnen und User des Social Webs können vorhandene Informationen rezipieren.

Hippner sieht das ähnlich und definiert folgende drei **Ziele von Social Software** (2006, S.8):

- Publikation und Verteilung von Informationen
- Kommunikation zwischen Internetnutzern
- Aufbau und Verwaltung von Beziehungen

2.3.3. Anwendungen

Was sind nun in der Praxis die oben definierten Anwendungen, die sich Social-Web- oder Social Software-Anwendungen nennen dürfen? Hippner (2006, S.8ff) stellt fest, dass es noch keine allgemein akzeptierte Meinung gibt, welche Anwendungen der Social Software zuzuordnen sind. Dennoch gibt es einige Anwendungen, die er eindeutig als Social Software bezeichnet. Ebersbach et al. nennen vier große Hauptgruppen von Social Web Anwendungen: Wikis, Blogs, Social Sharing und Social-Network-Dienste. Diese vier dienen als Überbegriffe für viele Anwendungen und können alle auch als Social Software bezeichnet werden. Sie werden darum im Folgenden als Social Web- und Social Software Anwendungen kurz vorgestellt. (nach Ebersbach et al. 2008, S.33ff) Näher eingegangen wird dabei auf Social Network Dienste, da es diese Gruppe ist, zu der die Social Network Seite Facebook gehört.

Wikis

> „Ein Wiki ist eine webbasierte Software, die es allen Betrachterinnen und Betrachtern einer Seite erlaubt, den Inhalt zu ändern, in dem sie diese Seite online im Browser editieren." (Ebersbach et al. 2008, S.35f)

Wikis dienen der kollaborativen Erstellung von Texten. Ziel der Community ist es, Inhalte gemeinsam zu schreiben. Dafür wird die sogenannte *Crowd Intelligence* genutzt – das Phänomen, dass eine Gruppe von Menschen ein besseres Ergebnis erzielt als ein einzelner noch so genialer Mensch es könnte. (Zeger 2009, S.39) Bei Wikis steht der generierte Inhalt im Mittelpunkt, die einzelnen Autorinnen und Autoren sind kaum erkennbar. Jeder der Mitwirkenden hat

grundsätzlich die gleichen Rechte und Möglichkeiten, sich zu beteiligen und Texte zu schreiben, zu verändern oder zu löschen – außer die Bearbeitungsrechte werden in irgendeiner Weise eingeschränkt. Texte auf Wikis sind dadurch dynamisch und ändern sich mehr oder weniger oft – je nachdem, wie oft jemand etwas ergänzt oder umschreibt. Die Leserinnen und Leser eines Wiki-Textes sehen immer die aktuellste Version, den letzten Stand des Textes. Zu beachten ist dabei, dass Wikis keine Garantie für Richtigkeit oder Vollständigkeit abgeben können, es sei denn, eine kontrollierende Instanz prüft das vom Kollektiv Geschriebene. (Ebersbach et al. 2008, S.36)

Das wahrscheinlich berühmteste Beispiel eines Wikis ist *Wikipedia*, ein Open-Source-Projekt, das es seit seiner Gründung 2001 zur größten jemals dagewesenen Enzyklopädie schaffte. Wikipedia gibt es derzeit in 260 Sprachen (Stand 1.2.2010), die englische Ausgabe ist mit über 3,16 Millionen Artikeln die größte, die zweitgrößte ist die deutsche Ausgabe mit 1.018.928 Artikeln (Stand 1.2.2010). (Wikipedia)

Blogs

Weblogs (kurz: Blogs) sind Online-Tagebücher, die meistens von Einzelpersonen geführt werden und alles zum Thema haben können, was der Schreiberin oder dem Schreiber beliebt. Geschrieben wird meistens in der ersten Person, in der Ich-Perspektive. So entstehen Journale, die tagesaktuelles Geschehen zum Inhalt haben, die einen bestimmten thematischen Schwerpunkt aufweisen oder die einfach nur den Alltag einer Person behandeln – ganz nach dem Geschmack der Autorinnen und Autoren. Die einzelnen Beiträge sind chronologisch in umgekehrter Reihenfolge geordnet – der aktuellste Beitrag steht immer ganz oben. Leserinnen und Leser des Blogs haben meist die Möglichkeit, Kommentare zu posten. Durch die Vernetzung einzelner Blogs entsteht eine Gemeinschaft. Portale, auf denen Interessierte ihren eigenen Blog erstellen können, gibt es viele. Wer bloggen möchte, kann sich einfach bei einem Anbieter anmelden, sich mit wenigen Klicks einen Blog einrichten und nur Minuten später den ersten Eintrag in die Welt hinaustippen.

Social Sharing

Social Sharing bezeichnet das Bereitstellen und Teilen von digitalen Inhalten wie Videos oder Bilder. Auf Plattformen des Social Sharing werden Inhalte verfügbar gemacht und somit geteilt und sie werden geordnet und bewertet. Ein berühmtes Beispiel für Social Sharing ist *Youtube* – auf der Plattform können Videos hochgeladen und bewertet werden. Je mehr Klicks ein Video bekommt, desto höher steht es auf der seiteneigenen Rangliste.

Social Network Dienste

Social Network Dienste, auch genannt **Soziale Online-Netzwerke** oder **Social Network Sites**, dienen dem Aufbau und der Pflege von Beziehungsnetzwerken. Durch eine Registrierung kann man Mitglied werden, ein Profil anlegen und sich dann mit anderen Mitgliedern vernetzen. Dabei besteht meist ein starker Bezug zu realen Sozialbindungen, und die Freundeslisten enthalten hauptsächlich Personen, mit denen man auch in der realen Welt in Verbindung steht. (Ebersbach et al. 2008, S.33ff)

Da Facebook eine Social Network Site ist, wird diese Art der Anwendungen in einem eigenen Kapitel beschrieben. Es wird im Folgenden auf den Begriff des Sozialen Netzwerks eingegangen, auf Besonderheiten von Social Network Sites, auf den aktuellen Forschungsstand sowie auf Gefahren und Risiken.

2.4. Soziale Netzwerke

Der Netzwerkgedanke wird in den letzten Jahren in vielen Bereichen großgeschrieben – in der Wirtschaftspraxis, in der ökonomischen sowie sozialwissenschaftlichen Forschung oder auch in der Industriepolitik (Weyer 2000, S.1). Soziale Netzwerke können dabei offline sowie online gepflegt werden.

2.4.1. Soziale Netzwerke offline

Als einer der Netzwerk-Pioniere gilt Moreno (1934), der als Erster Netzwerke in sogenannten Soziogrammen skizzierte. Dabei werden Akteure als Knoten abgebildet und die zwischen ihnen bestehenden Beziehungen als Linien dargestellt. (Jansen 2006, S.91)

Haythornthwaite bleibt Jahrzehnte nach Erfindung des Soziogrammes bei einer ganz ähnlichen Definition:

> „Social networks are built on the foundation of *actors* who are connected or *tied* by the maintenance of one or more *relations*." (Haythornthwaite 2007, S.126)

Soziale Netzwerke haben also drei tragende Komponenten: **Akteure**, die durch **Verbindungen** zu anderen **Beziehungen** haben. Die Summe der Verbindungen zwischen den Akteuren bezeichnet man als Social Network.

Bei den **Akteuren** handelt es sich meistens um Personen, besonders wenn man von Sozialen Netzwerken als Communities spricht. In der Theorie jedoch müssen Akteure nicht zwingend

Individuen sein. Organisationen, Veranstaltungen oder Homepages können genauso als Knotenpunkte in einem Netzwerk stehen.

Die **Beziehungen**, die zwischen den Akteuren bestehen, basieren auf Tauschgeschäften. Ausgetauscht werden entweder immaterielle Güter wie Information, moralische Unterstützung, Ratschläge etc. oder materielle Güter wie beispielsweise Geld oder Waren. Dabei spielt die Richtung, in der ein Tausch stattfindet, eine große Rolle. Wer gibt wie viel? Wer erhält wie viel? Und beruht der Fluss von Ressourcen auf Gegenseitigkeit? Antworten auf diese Fragen liefern ein Bild von Einfluss und Ansehen, das Individuen in einem Netzwerk haben.

Wird so eine Beziehung zwischen Akteuren durch Austausch gepflegt, spricht man von einer **Verbindung** zwischen den Personen. Diese Verbindung ist stark, wenn die Beziehung auf sozialem und emotionalem Austausch, auf Vertrautheit oder auf Selbstoffenbarung beruht. Man spricht dann von **Strong Ties**. Diese Strong Ties funktionieren meist wechselseitig – gibt ein Akteur etwas Intimes über sich preis, steigt die Vertrautheit und auch der andere gibt in einer passenden Situation etwas von sich preis. Strong Ties pflegt man vor allem mit Freunden und Freundinnen. Man neigt dazu, sich eher mit Leuten zu unterhalten, die einem ähnlich sind und sich in den gleichen sozialen Kreisen bewegen. Im Gegensatz dazu sind **Weak Ties** schwache Verbindungen, die wir beispielsweise zu Arbeitskolleginnen oder –kollegen haben. In solchen Verbindungen finden kein reger Austausch und nur wenig Interaktion statt. Die Personen, zu denen wir lose Beziehungen führen, sind uns meist nicht allzu ähnlich und bewegen sich in anderen sozialen Kreisen. Allerdings können Weak Ties sehr nützlich sein, weil sie verschiedene Informationen liefern können, an die man sonst nicht käme. (Haythornthwaite 2007, S.126f)

Diese Definition eignet sich gut für die vorliegende Arbeit, sie lässt sich perfekt auf den Untersuchungsgegenstand Facebook umlegen. Die Akteure des Netzwerkes stellen Facebook-Mitglieder dar, sie pflegen Beziehungen durch mehr oder weniger regen Austausch (Kommentar auf Pinnwänden, Nachrichten, geposteten Fotos, etc.) und sind verbunden miteinander – und das sogar sehr offensichtlich, nämlich durch Verknüpfungen ihrer Profile. Die Verbindung ist somit nicht nur ideell, sondern tatsächlich durch einen Klick hergestellt. Facebook ist also ein Soziales Netzwerk, das sich von anderen Sozialen Netzwerken darin unterscheidet, dass es online aufgebaut wird. Die Spezifika von Sozialen Online-Netzwerken werden im nächsten Kapitel (2.4.1) beschrieben.

Weyer trifft eine Einteilung in zwei soziologische Forschungsstränge, die sich mit Sozialen Netzwerken befassen. Nach seinem Modell unterscheidet man zwischen der **Formalen Netzwerkanalyse** und der **Analyse von Interorganisations-Netzwerken**. Beide Stränge untersuchen Soziale Netzwerke, verfolgen aber unterschiedliche Strategien der Annäherung.

Formale Netzwerkanalyse

… versteht sich primär als universal einsetzbare Methode, um die Strukturen der Interaktion von Akteuren zu beschreiben. Soziale Netzwerke werden dabei als Beziehungsgeflechte verstanden, deren Komponenten Akteure sind und deren Strukturen mit quantitativen Methoden erfasst werden können. Im Mittelpunkt stehen die Akteure und deren strukturelle Einbettung. Ego-zentrierte Netzwerke machen beispielsweise den Grad der sozialen Verankerung einer Person in einem Netzwerk sichtbar. Es lassen sich aber auch größere Einheiten analysieren, wie etwa das Beziehungsgeflecht in einem Wohngebiet oder einem Unternehmen.

Analyse von Interorganisations-Netzwerken

Bei diesem Konzept wird unter Vernetzung die zielgerichtete Koordination von Akteuren verstanden, die miteinander kooperieren, um ihre Interessen durchzusetzen. Netzwerke zählen dabei als planvolle Konstrukte strategisch handelnder Akteure, die ihre Handlungen in Erwartung konkreter Vorteile koordinieren. Mit qualitativen Methoden soll die Funktionsweise des Netzwerks und dessen spezifische Leistung erklärt werden.

Die beiden Modelle stehen in keinem Konkurrenzverhältnis, sie betrachten lediglich das selbe soziologische Phänomen aus unterschiedlichen Perspektiven. (Weyer 2000, S.14ff)

Bei Facebook würde wohl die formale Netzwerkanalyse zum Tragen kommen, da es sich bei der Plattform um ein Beziehungsnetzwerk handelt und nicht jedes Mitglied zielgerichtet nur mit Leuten befreundet (also verbunden) ist, die ihm in irgendeiner Weise einen Nutzen bringen.

Es wird an dieser Stelle nicht detaillierter auf Netzwerkforschung eingegangen, weil die vorliegende Arbeit nicht netzwerkanalytisch vorgeht oder sich mit den Beziehungen zwischen Facebook-Mitgliedern beschäftigt, sondern den Fokus auf Datenschutzwissen der Mitglieder und das Verhalten in Bezug auf Privatsphäre legt.

2.4.2. Soziale Online-Netzwerke

Die oben beschriebenen Sozialen Netzwerke bekommen durch die Entwicklung des Web2.0 ein zweites Standbein: Verbindungen können im Zeitalter des Internets auch online gepflegt werden. Die Plattformen, die das ermöglichen, nennt man Social Network Sites, Soziale Online-Netzwerke oder Social Network Dienste. Sie wurden dazu geschaffen, Freundes- und Bekanntenkreise oder Geschäftspartner online zu verbinden und stellen die Infrastruktur für ein virtuelles Kontakthalten zur Verfügung. Im Web2.0 findet sich inzwischen eine Unmenge von Social Network Diensten, die die verschiedensten Zielgruppen bedienen: Manche sind als Businessnetzwerke angelegt und spezialisieren sich auf die Herstellung von Kontakten, die beruflich von Nutzen sein können. Andere richten sich an Personen mit gemeinsamen Interessen. Und wieder andere heißen alle

Mitglieder willkommen und sind privat-freundschaftliche Netzwerke. (Ebersbach et al. 2008, S.83) Facebook zählt zu Letzteren. Es begann als studentisches Netzwerk und entwickelte sich im Laufe der Zeit zum offenen Netzwerk für alle, was es zur größten Social Network Seite weltweit werden ließ.

Soziale Online-Netzwerke haben stets einen starken Bezug zu realen Beziehungen, weisen aber umgebungsbedingt einige Spezifika auf:

- Um Teil des Netzwerkes zu werden, ist eine Registrierung erforderlich.
- Als Knotenpunkte dienen Profil-Seiten mit Interessen und Aktivitäten.
- Daten liegen hauptsächlich in strukturierter Form vor.
- Beziehungen zu anderen werden dargestellt.
- Bekanntschaften über mehrere Ecken werden nachvollziehbar. (Ebersbach et al. 2008, S.79)

Boyd und Ellison (2007) definieren Social Network Sites über die Funktionen, die solche Seiten haben:

> Social network sites are „web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."

Das Fundament, auf dem jede Social Network Seite aufbaut, sind die **Profile** der einzelnen Teilnehmerinnen und Teilnehmer. Sie werden automatisch angelegt, sobald sich jemand auf der Plattform registriert. Für die meisten Netzwerke reicht es aus, eine gültige Mail-Adresse zu haben, um sich anzumelden. Es gibt aber auch Netzwerke, zu denen man eingeladen werden muss, um teilzunehmen. Dies ist zum Beispiel bei Expertennetzwerken oft der Fall. Die Nutzung von freundschaftlichen Netzwerken ist meist kostenlos, manche Business Netzwerke bieten hingegen kostenpflichtige Premium-Mitgliedschaften an, die besondere Privilegien mit sich bringen. Ist man bei einem Netzwerk erst einmal angemeldet, hat man die Möglichkeit, sich über ein Profil zu präsentieren. Die eingegebenen Daten werden nicht kontrolliert, man kann also frei wählen, wie man sich darstellt. (Ebersbach et al. 2008, S.33ff) Auf den meisten Social Network Sites wird man ermuntert, online ein möglichst genaues Abbild von sich selbst zu generieren (Boyd/Ellison 2007). Dazu gibt es oft die Möglichkeit, die eigenen Interessen nach Kategorien anzugeben. So gibt Facebook beispielsweise eine Unmenge von Feldern vor, in denen man Angaben über sich selbst machen kann: von Geschlecht, Geburtstag und derzeitigem Wohnort über den Beziehungsstatus, die politische Einstellung und die religiösen Ansichten bis hin zu Interessen, bevorzugten Aktivitäten, Lieblingsbüchern, -filmen, -zitaten und dergleichen mehr. Diese Informationen werden im Profil gespeichert und sind je nach Regelung entweder für alle Mitglieder oder nur für bestimmte Personen sichtbar. Auf Facebook kann jedes Mitglied selbst in den Privatsphäre-

Einstellungen festlegen, wer Zugang zu den eigenen Profil-Daten haben soll. Wie wichtig es ist, die Privatsphäre-Settings individuell zu regulieren, wird in Kapitel 4.3.2 und Kapitel 5.3 ausführlich dargestellt.

Nachdem das Profil erstellt wurde, kann eine **Freundesliste** angelegt werden – die Vernetzung beginnt. Denn die Hauptfunktion von Sozialen Online-Netzwerken besteht darin, Kontakte und Beziehungen aus dem realen Leben zu vertiefen (Döring 2008, S.30). Man sucht Leute, die man kennt und die auch Mitglied auf der Social Network Seite sind und fügt sie auf der eigenen Freundesliste hinzu. Meistens muss die andere Person zuerst bestätigen, dass sie damit einverstanden ist. Man verschickt dazu eine Freundschaftsanfrage und wartet, dass der oder die andere diese akzeptiert. Dann ist man offiziell nicht mehr nur im echten Leben, sondern auch in der virtuellen Welt befreundet. Die Freundeslisten können mitunter sehr lang sein. Online Social Networks sind im Durchschnitt größer als jene offline und haben mehr Weak Ties. Das rührt daher, dass es online leichter ist, jemanden in die Freundschaftsliste aufzunehmen, auch wenn man zu der Person in Wahrheit nur eine lose Bindung hat. (Gross/Acquisti 2005, S.3) Hinter den Freundschaftsverlinkungen stehen verschieden enge Beziehungen. Die Verbindung auf Plattformen wie Facebook haben vor allem einen praktischen Wert: Über die Freundesliste kann man rasch mit Bekannten in Kontakt treten, ihnen Nachrichten zukommen lassen oder sich über aktuelle Aktivitäten informieren. So wird verhindert, dass man jemanden aus den Augen verliert. Kontakthalten für Dummies sozusagen. Doch auch für wirklich enge Freundschaften bringen Social Network Seiten einen Nutzen: Der Austausch von Neuigkeiten wird gefördert und man fühlt sich noch besser verbunden, wenn man beispielsweise im Laufe des Tages auf Facebook den Status des anderen liest und kommentiert, als wenn man sich nur alle zwei oder drei Tage trifft. (Döring 2008, S.31)

Die dritte Funktion, die eine Social Network Seite ausmacht, ist die Möglichkeit, die **Freundeslisten von anderen einzusehen**. Jedes Mitglied hat auf seinem Profil eine Liste aller vernetzten Freunde. So kann man nachschauen, wer wen kennt.

Die erste Internet-Plattform, die die drei beschriebenen Funktionen (Profil, Freundeslisten und die Möglichkeit, Freundeslisten zu browsen) vereinte, war *SixDegrees*. Die Plattform wurde 1997 gegründet und kann nach den oben definierten Kriterien als erste Social Network Site bezeichnet werden. (Boyd/Ellison 2007)

Es folgten viele weitere Plattformen, die online und teilweise auch wieder offline gingen, und in den letzten Jahren kam es bei der Entwicklung sowie auch bei der Nutzung von Social Network Seiten zu einem wahren Hype. Social Network Dienste haben sich von einem Nischen- zu einem Massen-Phänomen entwickelt. (Gross/Acquisti 2005, S.1) Die Zahl der angebotenen Social

Network Seiten ist groß und die Arten sind vielfältig. Hunderte Social Network Sites bringen die unterschiedlichsten technischen Voraussetzungen mit und bedienen genauso unterschiedliche Bedürfnisse: Manche unterstützen bereits existierende Soziale Netzwerke, andere helfen dabei neue Leute kennenzulernen, mit denen man Interessen teilt. Die einen richten sich an ein breites Publikum, andere sprechen ganz bestimmte Zielgruppen an. Die Online-Netzwerke unterscheiden sich außerdem in den Informations- und Kommunikationsinstrumenten, die eingesetzt werden. So kann man beispielsweise auf manchen Portalen bloggen, Fotos und Videos teilen oder einen Live-Chat führen. (Boyd/Ellison 2007)

Gross und Acquisti (2005, S.1) erkennen aber einige Punkte, in denen sich alle Sozialen Online-Netzwerke gleich sind: Personen erstellen ein Profil, eine Repräsentation ihrer selbst, das von anderen eingesehen werden kann. Sie verfolgen das Ziel, mit anderen in Kontakt zu treten, für unterschiedliche Zwecke.

Je mehr Mitglieder eine Social Network Site hat, umso interessanter ist sie, denn desto größer ist der Nutzen für die Angemeldeten. Ist nur eine Freundin bei einer Social Network Seite Mitglied, ist die Motivation wahrscheinlich gering, sich selbst auch anzumelden. Sind aber bereits zehn Bekannte bei einem Netzwerk, ist man eher interessiert, ebenfalls beizutreten. Ist man dann erst einmal dabei, versucht man oft, weitere Freunde zu werben, um den eigenen Nutzen zu erhöhen. So funktioniert die Vergrößerung von Online-Netzwerken nach dem Schneeballprinzip.

Zu bedenken gilt dabei, dass eine Sache oft uninteressant wird, wenn alle sie haben. Aus einer Social Network Seite wird schnell eine chaotische Masse, wenn sie unstrukturiert und ununterscheidbar ist. Eine soziologische Regel lässt sich auch auf Social Network Sites anwenden: Ein *wir* gibt es nicht, wenn es keine *anderen* gibt. Manchmal macht erst ein Ausschluss das eigene Dabeisein attraktiv. So balancieren Soziale Online-Netzwerke dauernd am Grat zwischen möglichst hohen Teilnehmerzahlen und guter Unterscheidbarkeit zu *anderen*. (Zeger 2009, S.30)

Vorsicht ist geboten!

Gross und Acquisti (2005, S.2f) sehen in der Offenheit, mit der in Online-Netzwerken Informationen preisgegeben werden, allen Grund zur Besorgnis. Sie stellen fest, dass Mitglieder von Social Network Sites oft möglichst viele Informationen an möglichst viele Kontakte verbreiten. Als einen der Gründe dafür nennen die beiden Autoren, dass Mitglieder von Social Network Sites oft den Nutzen des Social Networking höher einschätzen als den Preis, den man dafür bezahlt – ein Preis, der in Form von Datenmissbrauch, Stalking oder Datenansammlungen von Dritten viele verschiedenen Formen annehmen kann.

Datensammlungen im großen Stil: Es liegt in der Natur von Sozialen Online Netzwerken, dass viele private Daten offengelegt werden. In Wahrheit stellt genau diese freizügige Offenlegung den Erfolgsfaktor von Plattformen wie Facebook dar. Der Haken daran ist, je bereitwilliger Netzwerk-

Mitglieder Inhalte über sich veröffentlichen, desto leichter können ihre Daten gesammelt werden. Und zwar ohne weitreichende Hacker-Kenntnisse. Name, Foto, Geburtsdaten, Wohnort, Lieblingsmarken, Lieblingsmusik und vieles mehr werden auf einem Silbertablett serviert. Werbetreibende, Datenbankbetreiber oder auch Trickbetrüger bedienen sich nur allzu gerne von diesem.

500 Freunde: Die Freundeslisten auf Social Network Sites sind oft so lang, dass man sich jeden Tag mit mindestens einem Freund treffen müsste, möchte man jeden seiner Freunde einmal im Jahr sehen. Der Grund dafür liegt darin, dass es sehr einfach ist, seine Beziehungen online zu verwalten. Zur Kontaktaufnahme reicht ein Klick und wenn eine Person erst einmal der eigenen Freundesliste hinzugefügt ist, ist sie sehr pflegeleicht. Man kann ohne viel Aufwand ihren Werdegang verfolgen und den Kontakt mit ein paar Nachrichten oder Kommentaren aufrecht erhalten.

Schwarze Schafe: Die oben beschriebene Daten-Ansammlung durch die Freizügigkeit der Userinnen und User öffnet der Spionage Tür und Tor. Gibt ein Netzwerk-Mitglied nicht viel von sich preis, liest aber ständig die Beiträge und Informationen anderer, spricht man von einem Lurker, einem passiven Nutznießer. Ist eine Person offensiver und verfolgt oder kontaktiert jemanden wider dessen Willen, nennt man sie einen Stalker.

Identitäten-Klau: Wie oben beschrieben kann jedes Mitglied auf einer Social Network Seite sein Profil frei gestalten und unterliegt keiner Kontrolle, was die personenbezogenen Informationen betrifft. Es ist also möglich, anstatt sich selbst darzustellen, in die Rolle einer anderen Person zu schlüpfen und ein Profil unter einer falschen Persönlichkeit aufzubauen.

Mobbing: Immer häufiger tritt auf Social Network Seiten leider das Phänomen des Cyber Mobbings auf. Dabei werden Mitglieder von anderen über Nachrichten oder Pinnwand-Einträge drangsaliert. (Ebersbach et al. 2008, S.93f)

Für Facebook als Social Network Seite gelten alle oben definierten Merkmale genauso wie die beschriebenen Risiken. Auf der Plattform hat jeder Akteur ein eigenes Profil, das gemäß der Netzwerkanalyse einen Knotenpunkt darstellt. Die Verbindungen zwischen einzelnen Profilen stellen Beziehungen dar. Über 400 Millionen Mitglieder nutzen Facebook, um mit Freunden und Bekannten in Kontakt zu bleiben. Dafür nehmen sie bewusst oder auch unbewusst die Risiken in Kauf, die ein Online-Netzwerk mit sich bringen kann.

Facebook stellt ein typisches Beispiel für eine Web2.0-Anwendung dar. Die Mitglieder der Plattform können interaktiv agieren und generieren selbst Inhalte. Sie nutzen die Plattform nicht nur, sondern gestalten sie mit eigenen Inhalten mit – sie werden zu Produsern.

Nach der Beschreibung des Status Quo des Web2.0 wird im nächsten Kapitel ein Ausblick auf eine mögliche Weiterentwicklung gegeben.

2.5. Semantic Web – Das Web3.0?

Die *Semantik* oder *Bedeutungslehre* ist das Teilgebiet der Sprachwissenschaft, das sich mit den Bedeutungen sprachlicher Zeichen befasst (Duden Fremdwörterbuch 2001, S.902). Spricht man von einem semantischen Internet bedeutet das, dass Inhalte nicht mehr nur eine Aneinanderreihung von Buchstaben darstellen, sondern dass das Internet Bedeutungen erkennt, die hinter Wörtern stecken – Bedeutungen, die bisher nur der Mensch erkannte.

Das Semantic Web zeichnet sich aus durch eine „Speicherung von Internet-Inhalten in einer für Maschinen interpretierbaren und dadurch vielfältig weiterverarbeitbaren Form." (Schneider 2008, S.112).

Der Begriff wurde von Tim Berners-Lee, dem Erfinder des World Wide Web, auf's wissenschaftliche Tablett gebracht. Er veröffentlichte zusammen mit Hendler und Lassila im Jahr 2001 einen Artikel im Scientific American Magazine, in dem er beschrieb, dass das Internet in Zukunft Sinnzusammenhänge herzustellen können würde.

> "The Semantic Web will bring structure to the meaningful content of Web pages, creating an environment where software agents roaming from page to page can readily carry out sophisticated tasks for users." (Berners-Lee 2001)

Berners-Lee hatte die Vision eines Internets, in dem Inhalte nicht mehr nur von Menschen interpretiert werden können, sondern in dem Informationen so codiert sind, dass sie auch für Computerprogramme fassbar werden. In der Praxis würde das bedeuten, dass nicht der Mensch im Internet gefundene Inhalte verknüpfen muss, sondern dass dies bereits im Vorfeld die Technik für ihn übernimmt. Der Computer spuckt nicht mehr nur Worte aus, er „weiß" gleichzeitig, was hinter den Worten steckt: Er weiß, dass Wien eine Stadt ist, dass diese Stadt in Österreich liegt und dass in der Stadt 1,7 Millionen Menschen wohnen. – Die Inhalte des World Wide Webs existieren nicht länger unabhängig nebeneinander, ähnlich wie auf einer Plattform, vielmehr werden sie im Semantic Web miteinander verknüpft wie in einer Datenbank.

> "The Semantic Web is not a separate Web but an extension of the current one, in which information is given well-defined meaning, better enabling computers and people to work in cooperation. The first steps in weaving the Semantic Web into the structure of the existing Web are already under way. In the near future, these developments will usher in significant new functionality as machines become much better able to process and "understand" the data that they merely display at present." (Berners-Lee 2001)

Berners-Lee sieht das Semantic Web also nicht als neues Internet, sondern vielmehr als Erweiterung des bereits bestehenden Netzes.

Die Entwicklung des Semantic Web war 2001, als Berners-Lee das erste Mal darüber schrieb, ein konkret realisierbares Konzept. Heute, fast ein Jahrzehnt später, ist es trotzdem noch lange nicht umgesetzt. Es gilt weiterhin als Vision für die Zukunft. Das Web2.0 hingegen, das von Tim O'Reilly erstmals 2004 – also drei Jahre nach der Idee zum Semantic Web – erwähnt wurde, wurde in

Fachkreisen und den Medien als Trend-Schlagwort aufgegriffen und fand Eingang in zahlreiche wissenschaftliche Untersuchungen und Thesen. (Schneider 2008, S.114f)

Ob das Semantic Web tatsächlich die Zukunft des Internets ist, wird sich zeigen. Vielleicht ist nach sechs Jahren Web2.0 die Zeit bald reif für ein neues Schlagwort und das Semantic Web wird von Fachkreisen neu entdeckt und gehyped. Sollte dies der Fall sein, wird mit Sicherheit das Internet selbst einen wesentlichen Teil zur Verbreitung des Booms beitragen.

„Wir sind so gewöhnt, uns vor anderen zu verstellen,
dass wir es zuletzt auch vor uns selber tun.“
François de La Rochefoucauld 1664

3. Selbstdarstellung

3.1. Grundlegende Theorien

Es liegt in der Natur des Menschen, bei anderen ein positives Bild von sich selbst erzeugen zu wollen. Man will verstanden, gemocht, akzeptiert, bewundert werden und ist darum bemüht, sich selbst und seine Eigenschaften ins rechte Licht zu rücken. Sobald man weiß, dass man beobachtet wird, arbeitet man aktiv daran, ein gutes Bild abzugeben. Dies kann ganz bewusst und gesteuert passieren oder auch unbewusst. So ändern viele Menschen ihre Handlungsweisen in der Gegenwart anderer, ohne es selbst zu bemerken. Chester und Bretherton (2007, S.223) nennen diesen Umstand **Impression Management**. Die Menschen wollen kontrollieren, welchen Eindruck andere von ihnen gewinnen. Die Versuche, die eigene Selbstdarstellung und damit das Bild, das andere von einem haben, zu kontrollieren, bestimmen unser Verhalten und unseren Alltag.

Goffman (2007, S.17) beschreibt in seinem Buch „Wir alle spielen Theater“ wie jeder Mensch versucht, den Eindruck, den andere von ihm haben, unter Kontrolle zu bringen. Wie der Titel des Buches bereits aussagekräftig sagt, postuliert Goffman, dass alle Menschen Selbstdarstellung betreiben – sowohl bewusst als auch unbewusst.

> „Der Einzelne wird sich also bei seiner Darstellung vor anderen darum bemühen, die offiziell anerkannten Werte der Gesellschaft zu verkörpern und zu belegen, und zwar in stärkerem Maße als in seinem sonstigen Verhalten.“ (Goffman 2007, S.35)

Doch was genau ist **Selbstdarstellung**?

Misoch (2004, S.29f) bezeichnet Selbstdarstellung als das Sichtbarmachen der eigenen Identität, das „Darstellen der eigenen Persönlichkeit“. Dies kann sowohl bewusst als auch unbewusst vor sich gehen und steht für Menschen einer modernen Gesellschaft im alltäglichen Leben auf der Tagesordnung.

Selbstdarstellung bezieht sich also auf die eigene Identität, die man in einer gewissen Art und Weise zur Schau stellt und damit anderen präsentiert. Im Laufe der Arbeit wird deutlich werden, dass dabei nicht immer 1:1 das eigene Selbst mit all seinen Facetten abgebildet wird. Oft wird Identität selektiv, verzerrt oder gar völlig fern der Realität dargestellt.

Für den Begriff der **„Identität“** gibt es zahlreiche Definitionen.

> Identitäten sind subjektiv besonders wichtige Selbst-Aspekte: kontextspezifisch gebündelte und strukturierte kognitive, emotionale und konative Selbstinhalte hoher subjektiver Relevanz. (Döring 2003, S.328)
>
> Identität „bezeichnet zum einen im allgemeinen Sinne die vollständige Übereinstimmung eines Objekts oder eines Subjekts in allen Einzelheiten mit sich selbst und zum anderen die auf relativer Konstanz von Verhaltensmustern und/oder Einstellungen beruhende einheitliche (personale) Betrachtung seiner selbst.“
>
> „Die Einzigartigkeit jedes Individuums wird durch die Summe der Eigenschaften und Merkmale erzeugt, welche das Individuum kennzeichnen. Wenn alle diese Einzelaspekte zu einem schlüssigen Ganzen zusammengefasst werden, sich innerhalb diesem stimmig und in innerer Kohärenz zueinander befinden, über einen zeitlichen Verlauf hin sich treu bleiben (Kontinuität), so verwendet man für dieses relativ einheitliche Konstrukt einer Person den Terminus der Identität.“ (Misoch 2004, S.18f)

Identität stellt also – vereinfacht gesagt – die Summe aller Eigenschaften einer Person dar. Und diese Eigenschaften, oder Teile davon, werden bei der Selbstdarstellung präsentiert.

Selbstdarstellung hat immer etwas mit **Selbstoffenbarung** zu tun. Will man sich selbst präsentieren, muss man unweigerlich etwas über sich preisgeben. Man muss Informationen, die einen selbst betreffen, teilen. In der Literatur – auch in der deutschsprachigen – findet sich häufig der Begriff „Self-disclosure“.

Self-disclosure, wörtlich: Selbstoffenbarung oder Selbstenthüllung, bezeichnet die „Preisgabe von Informationen über das Selbst“ (Wheeless 1976, S.47 zit.n. Reinecke et al. 2008, S.206f). Es beinhaltet, dass Menschen anderen etwas von sich mitteilen und sich somit gegenseitig bekannt machen (Joinson/Paine 2007, S.237). Es gibt drei Stufen der Self-disclosure: Auf der ersten Ebene werden grundsätzliche Daten verraten, wie das Alter oder der bisherige Werdegang. Darauf folgt die zweite Ebene, auf der Meinungen ausgetauscht und Werte diskutiert werden. Und auf der dritten, der höchsten Ebene werden ernste Themen wie fest verankerte Grundsätze, Ängste oder der persönliche Glaube thematisiert. (Altman/Taylor 1973 zit.n. ebd. S.238)

Goffman vertritt die Theorie einer **Idealisierung**, damit meint er die „Tendenz der Darsteller, beim Publikum einen auf verschiedene Art idealistischen Eindruck zu erwecken“ (2007, S.35). Dabei spricht er natürlich nicht nur von Schauspielern. Wir alle sind Darsteller in der Definition von Goffman. Darsteller, die sich ständig der Kritik oder dem Urteil anderer aussetzen und sich einem Publikum präsentieren. Wir präsentieren uns auf der Bühne des Lebens – um bei seiner Metapher zu bleiben. Und bei dieser Darbietung, der Vorstellung, für die sich jeden Tag auf’s Neue der Vorhang hebt, versuchen wir, einen idealistischen Eindruck zu erwecken. Dafür gibt es zwei unterschiedliche Ausdrucksmöglichkeiten:

- **Die Ebene der Äußerungen**, auf der man verhältnismäßig leicht nach dem eigenen Willen handeln kann. Will man einen bestimmten Eindruck bei einer anderen Person wecken, ist das erste, das man beachtet, die Kontrolle der eigenen Aussagen.
- **Die Ebene der Ausstrahlung**, die weitaus schwieriger zu kontrollieren ist. Natürlich kann man versuchen, die eigene Gestik und Mimik für sich einzusetzen, aber letztendlich hat man nur wenig Macht darüber, wie man auf ein Gegenüber wirkt.

Da die zweite Ebene als nicht oder kaum manipulierbar angesehen wird, liefert sie wichtige Informationen über die Aufrichtigkeit einer Person. Anhand der Beobachtung von Gestik, Mimik und Verhalten einer Person, kann man laut Goffman einschätzen, ob die Äußerungen dieser Person stimmen, oder ob sie versucht, sich anders darzustellen, als sie tatsächlich ist. (Goffman 2007, S.10f)

> „Die Ausdrucksmöglichkeit des Einzelnen (und damit seine Fähigkeit, Eindrücke hervorzurufen) scheint zwei grundlegend verschiedene Arten von Zeichengebung in sich zu schließen: der Ausdruck, den er sich selbst gibt, und der Ausdruck, den er ausstrahlt. Die erste Art umfasst Wortsymbole und ihre Substitute, die der Einzelne eingestandenermaßen und ausschließlich dazu verwendet, diejenigen Informationen zu vermitteln, die er und die anderen mit diesen Symbolen verknüpfen. Hier haben wir es mit Kommunikation im traditionellen und engeren Sinne zu tun. Die zweite Art umfasst einen weiten Bereich von Handlungen, die von den anderen als aufschlussreich für den Handelnden aufgefasst werden, soweit sie voraussetzen können, dass diese Handlungen aus anderen Gründen als denen der Information unternommen wurden.“ (Goffman 2007, S.6)

Goffman erkennt darin eine „**fundamentale Asymmetrie des Kommunikationsprozesses**, da der Einzelne sich anscheinend nur eines Kommunikationsstroms bewusst ist, während die Beobachter neben diesem noch einen zweiten Kommunikationsstrom wahrnehmen.“ (Goffman 2007, S.10f)

Es gibt **drei Faktoren für die Motivation**, einen bestimmten Eindruck beim Gegenüber zu erwecken (nach Leary 1995 zit.n. Chester/Bretherton 2007, S.225):

- Wie sehr nützt der erwünschte Eindruck einem gesteckten Ziel?
- Wie wertvoll ist dieses Ziel?
- Wie sehr unterscheidet sich der gewünschte Eindruck von dem Bild, das die anderen derzeit von einem haben?

Goffmans „Wir alle spielen Theater“ (original: The Presentation of Self in Everyday Life) wurde in der ersten Auflage 1959 veröffentlicht, doch es hat nichts an Aktualität eingebüßt. Bis heute schlagen Expertinnen und Experten zum Thema in dieselbe Kerbe und widersprechen dem Pionier nicht.

Döring (2003, S.334) erkennt beispielsweise an Menschen ein „Selbstdarstellungsverhalten". Darunter versteht sie,

> „dass wir unser soziales Verhalten in der Regel so gestalten, dass wir bei denjenigen Personen, die gerade anwesend sind oder denen unser aktuelles Verhalten bekannt werden könnte, einen günstigen Eindruck hinterlassen." (Döring 2003, S.334)

Ein „günstiger Eindruck" muss dabei nicht zwingend ein positiver Eindruck sein, sondern vielmehr der Eindruck, den eine Person in der jeweiligen Situation bewirken möchte – also ein zielkonformer Eindruck.

Jedes öffentliche Verhalten beinhaltet selbstexpressive Aspekte und selbstdarstellerische Komponenten. Letztere sorgen dafür, dass wir mögliche Reaktionen beim Publikum vorhersehen und eventuell das eigene Verhalten beeinflussen. Ausnahmen bilden existenzielle oder soziale Extremsituationen, in denen der Mensch nur über eingeschränkte Selbstkontrolle verfügt. (Döring 2003, S.334)

Es gibt **sieben Faktoren, die das Selbstdarstellungsverhalten beeinflussen** (nach ebd., S.335ff):

1. **Öffentlichkeit:** Selbstdarstellung ist nur notwendig, wenn das Verhalten öffentlich beobachtbar ist oder bekannt werden kann.
2. **Adressat:** Erfolgreiche Selbstdarstellung muss inhaltlich und taktisch auf das Publikum abgestimmt werden.
3. **Art des Kontakts:** Je intensiver und länger ein Kontakt ausfällt, desto nötiger aber auch besser möglich ist die Abstimmung der Selbstdarstellung auf die Erwartung des Publikums.
4. **Intention:** Die Selbstdarstellungstaktik ist vom intendierten Ziel abhängig. Will man einen positiven Eindruck erwecken, verfolgt man ein assertives Ziel. Will man nur einen negativen Eindruck verhindern, spricht man von einem defensiven Ziel.
5. **Inhaltsbereich:** Assertive oder defensive Selbstdarstellungsziele können sich auf unterschiedliche Inhaltsbereiche beziehen.
6. **Selbstaufmerksamkeit:** Ob und wie in einer bestimmten Situation Selbstdarstellung betrieben wird, hängt davon ab, wie stark man sich bewusst macht, von anderen Menschen beobachtet und beurteilt zu werden.
7. **Selbstwirksamkeit der Selbstdarstellung:** Man muss davon überzeugt sein, beim Gegenüber den gewünschten Eindruck hinterlassen zu können.

Mit der Entwicklung der neuen Medien bekommt das Thema frischen Wind in die Segel. Was ändert sich in der Selbstdarstellung, wenn einem der Interaktionspartner oder die Interaktionspartnerin auf einmal nicht mehr unmittelbar gegenüber sitzt, sondern ein Computer dazwischen geschaltet ist? Was passiert, wenn die Beurteilung einer anderen Person nicht mehr

zeitgleich zur Selbstdarstellung stattfindet, sondern zeitversetzt? Wenn sich beispielsweise eine Person online präsentiert und sich andere auf Grund dieser Inszenierung zu einem späteren Zeitpunkt ein Bild von dieser Person machen?

Gleichzeitig betrifft Selbstdarstellung auch den Bereich der Privatsphäre. Was gebe ich über mich preis, was behalte ich lieber für mich? Wo hört Selbst-Inszenierung auf, wo beginnt der Verzicht auf Privatheit?

Die folgenden Kapitel widmen sich der Gratwanderung zwischen Selbstoffenbarung und Privatsphäre und befassen sich mit den Besonderheiten der Selbstdarstellung im Internet.

3.2. Selbstdarstellung im Internet

Das Internet ermöglicht eine völlig neue Art der Selbstdarstellung. Menschen können auf einmal in die Öffentlichkeit treten, ein Publikum erzeugen und sich an eine breite Masse wenden, wie es in der Offline-Welt nur mit großen Ressourcen möglich wäre. (Boyd 2010) Im Internet können Userinnen und User ihrem Mitteilungsbedürfnis freien Lauf lassen. Urlaubsfotos, Kinderfilme, Tagebucheinträge, Kommentare, Gedichte, selbst produzierte Musik … all das und noch viel mehr kann auf einmal an die Öffentlichkeit gebracht werden, ohne dafür große Kosten oder Mühen auf sich nehmen zu müssen. (Zeger 2009, S.16) Beinahe jeder kann sich heutzutage im Internet präsentieren, kann sich im virtuellen Raum selbst darstellen. Das Impression Management betritt damit völlig neuen Boden.

Döring zieht eine klare Grenze zwischen Online-Selbstdarstellung und virtueller Identität:

> „Mit **Online-Selbstdarstellung** (synonym: virtuelle Selbstdarstellung) ist die dienst- oder anwendungsspezifische Repräsentation einer Person im Netz gemeint. Die Online-Selbstdarstellung impliziert im Unterschied zur Online-Identität weder Dauerhaftigkeit noch subjektive Relevanz.
>
> Mit **virtueller Identität** (synonym: Online-Identität) ist eine dienst- oder anwendungsspezifische, mehrfach in konsistenter und für andere Menschen wieder erkennbarer Weise verwendete, subjektiv relevante Repräsentation einer Person im Netz gemeint.“ (Döring 2003, S.341)“

Das bedeutet, dass nur ein Bruchteil aller Online-Selbstdarstellungen auch Online-Identitäten sind (ebd. S.341). Bei Facebook ist das aber fast immer der Fall. Mitglieder melden sich im Netzwerk nicht nur einmalig an und verschwinden wieder von der Bildfläche, sondern erstellen im Normalfall ein Profil, das dauerhaft betreut und genutzt wird. Sie betreiben Online-Selbstdarstellung so kontinuierlich, dass man von einer Online-Identität sprechen kann.

Die Repräsentation im Internet liegt aber nicht immer allein in der Hand der betroffenen Person. Eine Online-Identität ist eine Mischung aus **nutzerdefinierten**, **systemgenerierten** und **mitnutzerproduzierten** Attributen. (Döring 2003, S.343) Auf Facebook hat jedes Mitglied die Möglichkeit, selbst Inhalte auf sein Profil zu stellen (= nutzerdefinierte Selbstdarstellung), gleichzeitig können aber auch andere Mitglieder Einfluss auf die Darstellung nehmen, indem sie beispielsweise die Person auf Fotos verlinken oder ihr auf die Pinnwand schreiben (= mitnutzerproduziert). Als systemgeneriert gelten Inhalte, wenn sie von Facebook erzeugt wurden und das Mitglied sie nicht ausblenden kann. So zum Beispiel das Herauspicken eher inaktiver Mitglieder mit der Aufforderung, ihnen mal wieder eine Nachricht zu schicken.

3.2.1. Selbstdarstellung durch computervermittelte Kommunikation

> „Unter computervermittelter Kommunikation werden alle kommunikativen Handlungen, d. h. sozialen Austauschprozesse verstanden, die durch einen Computer als vermittelndes technisches Medium stattfinden (…).“ (Misoch 2006, S.37)

Computervermittelte Kommunikation basiert auf drei technologischen Komponenten: Für einen Austausch-Prozess werden immer ein Computer als Eingabegerät auf Senderseite, ein Computer als Endgerät auf Empfängerseite sowie eine Vernetzung der Computer untereinander benötigt (Misoch 2006, S.37). Die Vernetzung stellt heutzutage meistens das Internet dar.

Im Folgenden wird dargestellt, welche Auswirkungen es hat, wenn im Zuge des Impression Managements Kommunikation computervermittelt stattfindet und nicht direkt, also Face-to-Face. Zur computervermittelten Kommunikation gibt es weitreichende Literatur[3], es wird in der vorliegenden Arbeit nur auf die Aspekte eingegangen, die die Selbstdarstellung betreffen.

Wie im letzten Kapitel erläutert, birgt jede persönliche Begegnung großes Informationspotential. Man kann sein Gegenüber beobachten, kategorisieren, seine körperliche Erscheinung beurteilen. Begegnen sich zwei Menschen hingegen online, gehen oft viele Informationen verloren. Dies kann einerseits daran liegen, dass jemand bewusst den Deckmantel des Internets nutzt, um sich anders darzustellen, als er in Wirklichkeit ist. Andererseits kann es aber auch passieren, dass ein falscher Eindruck entsteht, weil wichtige Bestandteile zur Meinungsbildung fehlen, die wir aus der Face-to-Face-Kommunikation gewöhnt sind. (McKenna 2007, S.205) In einem Chat beispielsweise erfährt man nur, was der andere von sich preisgibt, man kann lediglich empfangen, was das virtuelle Gegenüber sendet. Die oben beschriebene Ebene der Ausstrahlung kann nicht beurteilt werden. Man bekommt nur die Informationen erster Ebene, diejenigen, die bewusst gegeben werden. Will einer der Gesprächspartner etwas verheimlichen, bringt er es einfach nicht in den Chat ein. In

[3] Einen übersichtlichen Einblick geben beispielsweise Misoch (2006): Online-Kommunikation oder Döring (2003): Sozialpsychologie des Internet

einem realen Gespräch würde dies vielleicht nicht unbemerkt bleiben. Auf der nonverbalen Ebene würde der Drückeberger vielleicht Unbehagen, Scham oder Betretenheit kommunizieren, woraus das Gegenüber den Schluss ziehen könnte, dass etwas im Busch ist. In einem Online-Chat stehen die Chancen gut, dass die Verheimlichung gelingt. Es müssen nur die richtigen Sätze geschrieben werden. Keine Körpersprache kann einen verraten, der Wahrheitsgehalt von Aussagen kann nur schwer kontrolliert werden.

Trotz der **fehlenden nonverbalen Kommunikation** bei computervermitteltem Austausch muss eine Online-Konversation nicht zwingend emotionslos sein. Döring (2003, S.161f) schreibt, es werde „nicht etwa die Beziehungsebene ausgeblendet, Emotionalität reduziert oder der soziale Hintergrund herausgefiltert“, sondern es werden neue Wege gefunden, diese Zusatzinformationen einer Konversation auszudrücken, beispielsweise durch Smileys, Soundwörter oder Großbuchstaben. Bahl (2002, S.70) sieht in diesen Möglichkeiten allerdings nur grobe Hilfsmittel. Sie findet in der computergestützten Kommunikation keine adäquaten Äquivalente zu Tonfall und Mimik, die in Face-to-Face-Gesprächen als nichtsprachliche Signale zum Ausdruck kommen.

Dass man in der computervermittelten Kommunikation nicht direkt vom Gegenüber beobachtet werden kann, bedeutet gleichzeitig, dass jede Person eine **erhöhte Kontrolle** über die eigene Selbstdarstellung hat. Sie kann sich überlegen, wie sie sich präsentieren will und kann dementsprechend bewusste Handlungen setzen. Sender und Empfänger kommunizieren nie direkt miteinander, wenn sie sich im Internet begegnen. Zwischen jede soziale Interaktion sind Computer geschaltet, die Zeichen digitalisieren, übermitteln, wieder dekodieren und als Text, Bild oder Ton wiedergeben. Im Rahmen der computervermittelten Kommunikation kann kein Zeichen unvermittelt gesendet oder empfangen werden. Das bedeutet gleichzeitig, dass keine unbewusst gegebenen Zeichen übermittelt werden. Kein Stottern, kein Erröten, nichts Unbeabsichtigtes erreicht den Empfänger. Nur was der Sender bewusst auf die Reise schickt, macht sich auf den Weg. (Misoch 2004, S.117f) Das führt dazu, dass Darstellungen im Internet körperlos, konstruiert und vermittelt sind und zum Teil textuell verlaufen:

<u>Körperlosigkeit</u>

Betritt eine Person einen realen Raum, ist sie in diesem physisch präsent und kann von anderen wahrgenommen werden. Nicht so im Internet: Dort können Personen nicht materiell, sichtbar und körperlich anwesend sein. Will man das, muss man sich bemerkbar machen, man muss sich „konstruieren“. Etwa durch einen Namen, den man sich gibt, Beschreibungen seiner selbst oder Fotos, die man hochlädt. Man muss sich einen Körper schaffen, ansonsten ist ein Auftritt im Internet körperlos.

Textualität

Die Verkörperung im Internet findet hauptsächlich durch Texte statt. Es handelt sich also meist um eine textuelle Selbstdarstellung, wenn man im virtuellen Raum auftritt. Personen beschreiben sich selbst, schreiben von und über sich und vermitteln so dem Interaktionspartner, wer sie sind – oder, wie sie gerne gesehen werden möchten. Denn der eigene Identitätstext wird von jeder Person selbst zur Präsentation verfasst und kann ganz nach Vorstellung des Verfassers oder der Verfasserin entworfen werden. Selten kann man so genau kontrollieren, wie man sich selbst darstellt, wie im Internet: Das eigene Selbst kann quasi neu erfunden werden.

Konstruktion des Selbst

Eine im Internet präsentierte Identität ist immer ein konstruiertes Selbstbild, das mit medialen Mitteln dargestellt wird. Bei der computervermittelten Kommunikation ist kontrollierbar, wie man sich darstellt, die Identitätspräsentation wird dadurch zum bewussten Akt.

Simulationspotential

Mediale Vermittlung und Kontrollgewinn öffnen Internet-Nutzerinnen und –Nutzern das Tor zur willkürlichen Selbstdarstellung. Das eigene Selbst kann selektiv oder gar völlig abweichend von der Realität präsentiert werden. Damit steigt aber auch die Unsicherheit über die Identität anderer. Stellen sich die anderen wahrheitsgetreu dar? Die Konsistenz von Selbstpräsentationen sowie ihre Kontinuität können zur Bestätigung herangezogen werden. Doch erst bei einem Vergleich zwischen Online- und Offline-Identität kann definitiv festgestellt werden, ob die Darstellung stimmt.

(Misoch 2004, S.130ff)

In den Ausführungen von Misoch wird immer wieder die Kontrolle betont, die man über seine eigene Selbst-Präsentation im Internet hat. Dabei stellt sich die Frage, in wie weit sich Personen über die Selbstdarstellungs-Effekte bewusst sind, die online entstehen. Ob sie eine gewisse Selbstdarstellung beabsichtigen und bewusst Handlungen setzen, um diese zu erreichen, oder ob sie die Unterschiede zwischen Face-to-Face- und Online-Kommunikation womöglich gar nicht kennen. Man unterscheidet darum zwischen bewussten und automatischen Prozessen. **Bewusste Prozesse** sind von Personen beabsichtigt. Solche Prozesse erfordern Aufmerksamkeit und sind kontrollierbar. **Automatische Prozesse** hingegen sind nicht geplant und auch nicht kontrollierbar. (McKenna 2007, S.206f)

Im Internet findet häufig **asynchrone Kommunikation** statt. Im Gegensatz zu synchroner Kommunikation, bei der sich Gesprächspartner zeitgleich austauschen (etwa, wenn sie sich zu einem Gespräch treffen und gegenübersitzen, aber auch wenn sie skypen), wird bei asynchroner Kommunikation zeitversetzt kommuniziert. (Misoch 2006, S.54) Das ist zum Beispiel der Fall beim Versenden von E-Mails, beim Hinterlassen einer Nachricht auf der Facebook-Pinnwand oder auch, wenn man Inhalte in das eigene Facebook-Profil einfügt und diese zu jedem x-beliebigen Zeitpunkt

von anderen rezipiert werden können. Durch die Asynchronizität hat man die Möglichkeit, sich genauer als in der direkten Begegnung zu überlegen, was und wie man kommuniziert. Man kann sich Zeit zum Formulieren nehmen und Inhalte editieren, bevor man sie weitergibt. (McKenna 2007, S.212) Dadurch kann die Flüchtigkeit verlorengehen, die eine mündliche Kommunikation oft mit sich bringt. Der Sender wird sich seiner Worte bewusster, wenn er sie niederschreiben muss, so beeinflusst die Verschriftlichung die Spontaneität der Kommunikation. (Bahl 2002, S.69)

In ihren Ausführungen zu Identitäten im Internet widmete sich Misoch besonders den privaten Homepages. „Die Bereitstellung eines *Raumes für ausschließliche Selbstpräsentation* ist historisch völlig neu." beschreibt sie die Möglichkeiten der Selbstdarstellung im Netz. (2004, S.134) Auch Facebook kann als solcher „Raum der Selbstpräsentation" gesehen werden. Zwar dient die Plattform nicht ausschließlich der Identitäts-Präsentation, doch hat jedes Mitglied auf der eigenen Profil-Seite die verschiedensten Möglichkeiten, sich darzustellen und ein Bild von sich zu zeichnen. Teil dieser Selbstdarstellung ist das Herstellen von Verbindungen zu anderen. Denn ein Facebook-Profil ist nicht so alleinstehend wie eine Homepage, es ist eingebettet in ein Netzwerk. Es handelt sich bei Facebook in diesem Sinne vielleicht nicht um einen Raum für ausschließliche Selbstpräsentation, aber dafür um einen *Raum vieler verschiedener, vernetzter Selbstpräsentationen*.

Die computervermittelter Kommunikation ist also eine indirekte und oft asynchrone Kommunikation, bei der die nonverbale Ebene fehlt. Zwischen Sender und Empfänger kann nichts ausgetauscht werden ohne Vermittlung. Jede Darstellung ist körperlos und muss bewusst erstellt, codiert und verschickt werden. Dadurch kann es verglichen mit Face-to-Face-Kommunikation zu Unterschieden im Austausch kommen. Seitens des Senders kann leichter beeinflusst werden, wie man sich selbst darstellt, da das Gegenüber nur empfangen kann, was bewusst gesendet wird und keine zusätzlichen Informationen anfallen. Die Selbstdarstellung kann unter Umständen aber auch unbewusst beeinflusst werden, wenn sich der Sender nicht über die Effekte der computervermittelten Kommunikation im Klaren ist. Auf Empfänger-Seite kann es leichter zu Verständnis-Problemen kommen als bei angesichtiger Kommunikation, da nonverbale Zusatzinformationen fehlen. Man hat außerdem kaum Möglichkeiten, die Richtigkeit der Präsentation von anderen zu überprüfen, außer man kann den Vergleich zur Offline-Identität ziehen.

3.2.2. Web2.0 – Anonymität war gestern

Dass das Internet die Selbstpräsentation unterstützt und oft erhöht, wurde lange Zeit auf den Faktor der Anonymität zurückgeführt. Viele Kommunikationskanäle des Internets kann man nutzen, ohne identifiziert zu werden. So kann man beispielsweise unter einem selbstgewählten

Nick-Name chatten oder Beiträge in Foren posten, ohne seinen vollständigen Namen anzugeben. Unbekannt und unerkannt kann man seine Meinung sagen, kommunizieren, sich selbst präsentieren, frei von den Zwängen der eigenen Identität. Man kann sich quasi selbst neu erfinden, selbst neu definieren. Wer auch immer im Internet liest, was man von sich gibt, wird nie erfahren, welche reale Person hinter den Online-Inhalten steckt. McKenna (2007) vergleicht diesen Umstand mit dem „Strangers on a train"-Phänomen: 1975 konstatierte Rubin, dass Menschen geneigt sind, sich völlig Fremden anzuvertrauen und intime Informationen von sich preiszugeben, wenn sie annehmen, diese fremde Person nie mehr wieder zu sehen. (S.210) Ähnlich lief die Kommunikation in weiten Teilen des Internets: Man konnte persönliche Informationen austauschen, ohne das Gegenüber zu kennen, man konnte sich etwas von der Seele schreiben, ohne dass das Geschriebene auf die eigene Person zurückzuführen gewesen wäre.

Diese Tatsache hat sich in den letzten Jahren stark geändert. Das Internet ist nicht länger ein großer, weiter Raum der Anonymität. Viele Anwendungen beruhen darauf, dass man sie mit dem vollen Namen und somit mit der eigenen Identität nutzt. Das Web2.0 bietet mehr Raum zur Selbstdarstellung denn je – allerdings keinen anonymen Raum. **Online- und Offline-Selbstdarstellung** sind im Social Web oft **untrennbar miteinander verbunden**. Wer im Internet Dinge über sich preisgibt, wird nicht drum herum kommen, zu diesen Dingen auch in der realen Welt zu stehen. Sobald Inhalte im Netz unter dem eigenen Namen veröffentlicht werden und der eigenen Person eindeutig zuzuordnen sind, können diese Inhalte nicht mehr von der realen Person getrennt werden. Es gibt in diesem Sinne kein Online-Selbst und ein Offline-Selbst. Die Person wird von anderen als Ganzes wahrgenommen und alle Faktoren beeinflussen das Bild, das man sich von der Person macht. (Boyd 2010) Sieht man beispielsweise von seinem Chef eine Dating-Anzeige online, wird das Bild verändert, das der Vorgesetzte bisher abgab. Genauso, wenn man Party-Fotos eines Kollegen online entdeckt oder seine Zugehörigkeit zu einer Sekte herausfindet. Online- und Offline-Selbstdarstellung verschwimmen beim Betrachter bzw. bei der Betrachterin zu einem kompletten Ganzen. Dies gilt es stets zu beachten, wenn man versucht ist, sich online anders darzustellen als im echten Leben. Denn so groß das Internet auch sein mag, es stellt kein eigenständiges Universum dar, es ist und bleibt ein Teil unseres echten Lebens.

Dass die Online-Selbstdarstellung selten um 180° von der Offline-Präsentation abweicht, zeigt eine Studie von Chester und Bretherton (2007, S.229f). Sie fanden heraus, dass die Bilder, die jemand online von sich zeichnet, dem realen Selbstbild sehr ähnlich sind – nur dass die Schokoladenseite etwas in den Vordergrund gestellt wird. Man stellt sich also durchaus so dar, wie man auch wirklich ist, gibt dem Ganzen aber eine möglichst positive Note.

Genau so funktioniert es in den meisten Fällen auf Facebook. Die Mitglieder legen Profile an und präsentieren sich darauf selbst. Sie können in verschiedenen Kategorien Angaben zu ihrer Person machen, können Fotoalben erstellen, sich mit anderen Mitgliedern verlinken, als Statusmeldung schreiben, was sie gerade beschäftigt und vieles mehr (siehe Kapitel 5.2). Das Social Web bietet zahlreiche Möglichkeiten, sich den Mitmenschen zu präsentieren. Im nächsten Kapitel wird dargelegt, warum viele Leute großen Gefallen an der virtuellen Selbstdarstellung finden.

3.2.3. Gründe für Online-Selbstdarstellung

Zahlreiche Studien deuten darauf hin, dass das Social Web die Bereitschaft zur Selbstoffenbarung noch erhöht. Bei Handlungen im Internet wird oft eine gewisse Anonymität verspürt, die die Offenherzigkeit bei der Selbstdarstellung fördern kann. Wie oben beschrieben, ist die Anonymität aber längst nicht mehr allgegenwärtig im Netz. Fühlen sich Userinnen und User dennoch anonym und nicht so greifbar wie in einer direkten Gesprächssituation, dann beruht das auf subjektivem Wahrnehmen. Ein viel wichtigerer Faktor für die Bereitschaft zur Selbstoffenbarung sind die Gratifikationen, die Self-disclosure den Web2.0-Nutzerinnen und -Nutzern bringt. Beispielsweise die Möglichkeit, andere über das eigene Leben am Laufenden halten oder der eigenen Meinung Ausdruck zu verleihen. Dafür zahlen die Web2.0-Userinnen und –User gern den Preis der Herausgabe von privaten Informationen. Reinecke und Trepte (2008, S.207) ziehen den Schluss, dass Nutzerinnen und Nutzer Self-disclosure in Kauf nehmen, weil es eng mit Gratifikationen verbunden ist, die von Web2.0-Angeboten erwartet werden.

Natürlich bringt jede Selbstoffenbarung auch Risiken mit sich, wie beispielsweise eine mögliche soziale Zurückweisung oder einen Konflikt mit Freundinnen und Freunden. Reinecke und Trepte (2008, S.207) kommen in ihrer Studie zum Umgang mit User-generated-content zu dem Ergebnis, dass Web2.0-Angebote vor allem für Nutzerinnen und Nutzer attraktiv sind, die von vornherein eine hohe Bereitschaft zur Selbstoffenbarung haben. So haben nur Personen mit einem generellen Interesse an Self-disclosure Aussicht, von den spezifischen Gratifikationen des Web2.0 zu profitieren und sind gleichzeitig eher gewillt, die zu befürchtenden Risiken zu tragen. Es konnte ein signifikanter Zusammenhang festgestellt werden zwischen der Affinität zum Web2.0 und der Bereitschaft, intime Informationen preiszugeben.

Für die vorliegende Arbeit ist dieses Ergebnis relevant, weil es etwas über die Mitglieder von Facebook aussagt. In Anlehnung an die Studie lässt sich sagen, dass Besitzerinnen und Besitzer von Facebook-Profilen eine starke Bereitschaft zu Self-disclosure besitzen.

Während bisher immer nur von Selbstdarstellung und Selbstoffenbarung im Allgemeinen gesprochen wurde und dabei alle persönlichen Daten, die man preisgeben kann, in einen Topf geworfen wurden, trifft Boyd (2010) eine wichtige Unterscheidung. Sie differenziert zwischen **Personally Identifiable Information** (PII) und **Personally Embarrassing Information** (PEI).

Menschen veröffentlichen online relativ freizügig persönliche Daten über sich und empfinden das als Usus, um auf Social Network Sites gefunden zu werden und zu interagieren. Gleichzeitig versuchen sie aber, Informationen, die ihnen peinlich erscheinen, geheim zu halten. Mit jeder Information, die man über sich preisgibt, macht man sich verletzbar. Diese Verletzlichkeit nimmt man oft in Kauf, um soziale Kontakte zu knüpfen, Freundschaften zu schließen oder bestehende Beziehungen zu vertiefen. Man bringt jemandem Vertrauen entgegen und vertraut ihm oder ihr Informationen an, in der Hoffnung, die Person würde sorgsam mit diesen umgehen. Dieses

Verhalten hat der Mensch evolutionär gelernt. Und dieses Verhalten wendet er auch in seinem technischen Umfeld an. Er vertraut Maschinen, dem Computer, dem Internet Informationen an, weil er sich einen Nutzen davon erhofft. Und er hofft, dass das Internet mit den Daten so sorgsam umgeht wie Freunde, denen man etwas anvertraut. Leider ist das nicht immer der Fall. Man kann nicht davon ausgehen, dass im Internet die eigenen Informationen nur von denen gelesen werden, von denen man möchte, dass sie sie rezipieren. Anders als im realen Leben, wo man einen Freund darauf ansprechen kann, wenn er intime oder peinliche Informationen weitergibt, ist das Internet nicht greifbar. Man hat Daten online gestellt und mit der Veröffentlichung auf das Recht auf Datenschutz verzichtet. Man hat die Privatsphäre freiwillig aufgegeben. Der Preis dafür ist oft eine schmerzliche Bloßstellung, eine Blamage oder einfach das Gefühl, die eigene Privatsphäre sei verletzt worden.

3.3. Online-Selbstdarstellung vs. Privatsphäre

Das Web2.0 bietet Userinnen und Usern die Möglichkeit, Inhalte zu erstellen, Geheimnisse in die ganze Welt hinauszuposaunen und Daten mit anderen zu teilen. Nicht wenige Menschen machen von diesen Möglichkeiten Gebrauch. Natürlich bedeutet veröffentlichen nicht gleichzeitig gesehen zu werden. Nur weil Inhalte online stehen, heißt das noch lange nicht, dass sie jemand rezipiert. Aber Fakt ist, dass es Menschen mit Internet-Zugang in Zeiten des Web2.0 sehr leicht haben, sich online zu präsentieren. Sie haben die verschiedensten Möglichkeiten, Dinge über sich im virtuellen Raum preiszugeben. Dinge, von denen sie sich vielleicht gar nicht bewusst gemacht haben, ob sie überhaupt die ganze Welt wissen sollte. Dinge, die im Internet gespeichert werden und zu jedem beliebigen Zeitpunkt wieder aus den Weiten des Netzes hervorgeholt werden können – etwa wenn ein potentieller Arbeitgeber vor einem Vorstellungsgespräch Erkundigungen über die Vorgeschichte der Bewerberinnnen und Bewerber anstellt. Das Internet vergisst nichts. Diese Tatsache kann leicht zum Karriere-Hemmer werden. Als eines von vielen Beispielen sei hier das Schicksal der jungen Amerikanerin Stacy Snyder genannt: Der Frau wurde von der Uni-Leitung der Abschluss als Lehrerin in Biologie und Englisch verweigert, nachdem sie ein Foto von sich selbst mit dem Titel „Drunken Pirate“ auf die Online-Plattform MySpace gestellt hatte. Das Foto schien relativ harmlos: Es zeigte die Studentin mit einem Piraten-Hut und einem Plastikbecher, dessen Inhalt nicht ersichtlich war, auf einer Halloween-Party. Doch die Leitung der Universität, auf der die 25-Jährige studierte, befand das Foto für unprofessionell und einer Erzieherin nicht würdig. Stacy Snyder bekam keine Lehrerinnen-Lizenz. Ein einziges Party-Foto auf einer Online-Plattform zerstörte ihre Karrierepläne. (Barth 2007, S.110)

Das Internet macht Privates öffentlich. Dass die virtuelle Selbstdarstellung Risiken mit sich bringt, deren Ausmaße um einiges größer sind als die der Selbstdarstellung in der realen Welt, liegt auf der Hand. Im Zeitalter des Web2.0 stellen persönliche Informationen nicht nur die Inhalte von

Kommunikation dar, sie sind vielmehr Daten, die von anderen gesammelt und verwendet werden können. Mit ständig erweiterten technischen Möglichkeiten werden Informationen über Personen archiviert und Userinnen und User werden immer mehr zum viel zitierten gläsernen Menschen. Dies geschieht meistens völlig legal, denn die Userinnen und User stellen die Inhalte ja selbst und freiwillig online. Ob sich jedoch alle der Datenmaschinerie bewusst sind, die im Hintergrund läuft, ist fraglich. (Joinson/Paine 2007, S.241ff)

Boyd (2010) machte in ihrer Rede am SXSW[4] darauf aufmerksam, dass Menschen immer versuchen, ihr **Umfeld einzuschätzen**. Wenn man sich in einem Cafe befindet, gibt es gewisse Personen, die man dort erwartet und andere Personen, von denen man sich sehr wundern würde, sie dort zu treffen. Fährt man nach der Arbeit mit der U-Bahn nach Hause, hütet man sich unter Umständen, am Handy lauthals über den Chef zu schimpfen, in dem Bewusstsein, es könnte jemand im Abteil sitzen, der den Chef kennt. Unsere Umwelt ist nicht vertrauenswürdig. Die sprichwörtlichen Wände, die manchmal Ohren haben, überraschen uns im Alltag immer wieder. Plötzlich steht jemand in einem Lokal vor einem, mit dem man überhaupt nicht gerechnet hat und hätte leicht etwas hören können, das eigentlich nicht für seine Ohren bestimmt war. Um solche Situationen zu vermeiden, schätzen wir unser Umfeld ab – bewusst so wie auch unbewusst. Es wird kalkuliert, was einen in einer bestimmten Situation erwartet, wer anwesend ist, wer mithören könnte. Nach dieser Einschätzung richtet sich, wie man sich verhält. Verlässt man in der Offline-Welt seine eigenen vier Wände, die Zone der eigenen Privatsphäre, und geht außer Haus, so spricht man von **schwacher Öffentlichkeit**. Diese Öffentlichkeit ist überschaubar, einfach organisiert und besteht gewöhnlich aus einer geringen Anzahl von Menschen – den Wartenden an einer Supermarkt-Kasse, den Passagieren in einem Flugzeug, den Leuten in einer Bar, etc. An diese Art der Öffentlichkeit ist der Mensch gewöhnt. Und aus alter Gewohnheit verhält er sich oft in der Öffentlichkeit des Internets genauso, wie in seiner persönlichen schwachen Öffentlichkeit. Das Problem ist, dass das Internet bei weitem nicht so überschaubar ist wie unsere Offline-Umwelt. Online kann man oft nur schwer einschätzen, wen eine Aussage erreichen kann, die man tätigt. Oft verhalten sich Personen online trotzdem so, wie sie es offline gelernt haben. Statt am Stammtisch wird dann eben auf Facebook die Meinung kundgetan; statt beim Heurigen eine Anekdote der letzten Woche zu erzählen, wird sie noch in derselben Minute, in der man sie erlebt hat, via Twitter verbreitet. Die handelnden Personen vergessen dabei schnell, dass das Internet nicht mit einem Vereinslokal oder einer Party unter Freunden gleichzusetzen ist. (Zeger 2009, S.58f) Der Haken an der Sache ist, dass Online-Umgebungen bei weitem nicht so überschaubar sind wie reale Plätze. Die Wände in den Straßen können Ohren haben, die Wände im Internet hingegen haben immer Ohren. Zu diesem Schluss kommt Boyd (2010) und warnt vor dem Internet, das veröffentlichte Inhalte dauerhaft speichert, sortiert und für Suchmaschinen zugänglich macht. In einem realen Raum mögen Stimmen verhallen und Gesagtes vergessen werden, wenn nicht gerade

[4] Das South by Southwest (SXSW) ist ein Festival in Austin / Texas (USA), das seit 1987 jährlich zu den Themen *Music*, *Film* und *Interactive* stattfindet (sxsw.com).

zufällig die falschen Ohren mithörten. Im virtuellen Raum jedoch wird nichts vergessen. Und selbst wenn es bei der Veröffentlichung nicht interessant war, kann es jederzeit wieder ausgegraben und vielleicht zu einem späteren Zeitpunkt interessant werden. In der Web2.0-Kommunikation bleibt alles aufbewahrt, egal in welcher Laune oder welchem Zusammenhang es geäußert wurde.

3.3.1. Need for privacy

Viele Menschen sorgen sich um die eigene Privatsphäre und den möglichen Missbrauch personenbezogener Daten, wenn sie sich im Internet bewegen. Dieses Schutzbedürfnis wird in der Literatur **Need for privacy** genannt, das „allgemeine psychologische Bedürfnis nach Privatsphäre“ (Marshall 1974 zit.n. Reinecke et al. 2008, S.208).

Dem Need for privacy steht der oben beschriebene wachsende Trend der digitalen Selbstdarstellung gegenüber (Reinecke et al. 2008, S.205f). Studien zeigen, dass es eine große Diskrepanz gibt zwischen der Einstellung, die Personen zu Privatsphäre haben und dem Verhalten, das sie an den Tag legen. Viele erachten Privatsphäre zwar als enorm wichtig, handeln online aber gleichzeitig so offenherzig, dass jeglicher Schutz der Privatsphäre über Bord geworfen wird.

Reinecke und Trepte (2008) untersuchten, ob es beim Bedürfnis nach Privatsphäre einen Unterschied zwischen drei verschiedenen Internetgruppen gibt: den **Produzenten**, die eine hohe Web2.0-Affinität haben, eine hohe Produktion von User-generated-content an den Tag legen und das Web2.0 aktiv mitgestalten, den **Rezipienten**, die Web2.0-Inhalte zwar intensiv rezipieren, jedoch selbst keine Inhalte produzieren und den **Abstinenzlern**, für die Web2.0-Services so gut wie keine Rolle spielen.

Die Ergebnisse zeigten, dass es zwischen den drei Nutzergruppen keine Unterschiede bezüglich des Bedürfnisses nach Privatsphäre gibt. Produzenten zeigten in der Studie zwar ein geringeres Need for privacy als Rezipienten oder Abstinenzler, jedoch beschränkte sich dieser Unterschied auf die Bereitschaft zur Selbstoffenbarung. Ein grundsätzlich geringeres Bedürfnis nach Privatsphäre, das über die Bereitschaft zur Preisgabe persönlicher Informationen hinausgeht, kann man Web2.0-Affinen keineswegs nachsagen.

Die Autoren kommen zu dem Schluss, dass der Stellenwert von Privatsphäre im Web2.0 auf zwei Ebenen zu betrachten ist: Produzenten sind bereit, private Informationen in Form von User-generated-content preiszugeben und haben dabei ein geringeres Bedürfnis nach Privatsphäre als weniger Web2.0-affine Nutzergruppen. In anderen Bereichen des Alltags weisen sie allerdings einen genauso hohen Wert an Need for privacy auf wie alle anderen. Es darf also nicht fälschlicherweise der Schluss gezogen werden, dass Web2.0-affine Nutzerinnen und Nutzer unreflektierte Exhibitionisten sind. Sie geben zwar freizügiger Persönliches über sich preis, haben aber keineswegs ein niedrigeres Bewusstsein für die Wichtigkeit von Privatsphäre.

Produzenten befinden sich daher auf einer ständigen Gratwanderung zwischen dem Bedürfnis nach Mitteilung und dem Bedürfnis nach Privatsphäre.

Rezipienten haben dieses Problem nicht. Sie profitieren bei ihrer Web2.0-Nutzung von der Selbstoffenbarung anderer, ohne den Schutz der eigenen Privatsphäre aufgeben zu müssen. Die Autoren gehen sogar soweit zu sagen, der Schutz der Privatsphäre stünde den Rezipienten im Wege, weil sie das Web2.0 unter Umständen gerade deshalb aufsuchen, um auf private Details aus dem Leben anderer zugreifen zu können.

Das Konzept der Selbstdarstellung ist alt und erprobt. Zusammenfassend lässt sich sagen, dass jeder Mensch versucht, sich selbst in das Licht zu rücken, in dem er gerne gesehen werden möchte. Dazu hat man in Zeiten des Web2.0 mehr als genug Gelegenheit. Viele Menschen nutzen das Internet, um Inhalte zu veröffentlichen, sich Gehör zu verschaffen, sich vor einem größeren Publikum zu präsentieren, als dies offline möglich wäre. Dem Drang zur Self-disclosure, der Selbstoffenbarung, steht dabei stets das Need for privacy, das Bedürfnis nach Privatsphäre gegenüber. In Zeiten des Internets, der Blogs und der Social Network Sites gleicht die Selbstdarstellung einer Gratwanderung. Denn was erst einmal im Netz veröffentlicht ist, das kennt kein Zurück mehr. Das Internet vergisst nichts und stellt somit für die Privatsphäre eine große Herausforderung dar. Alle Personen, die im Internet surfen, müssen sich überlegen, wie sie mit den neuen Möglichkeiten der Selbstdarstellung umgehen.

3.4. Selbstdarstellung auf Facebook

In den vorangegangenen Abschnitten wurde an manchen Stellen bereits ein Bezug zum Untersuchungsgegenstand hergestellt. Die Theorie wird nun nochmals zusammengefasst auf die Plattform Facebook umgelegt.

Die vorliegende Arbeit basiert auf der Annahme, dass die Mitglieder auf Facebook ihr Selbst präsentieren und keine völlig neue Identität erschaffen. Sie nutzen die Plattform großteils, um bereits bestehende Kontakte zu pflegen (Döring 2008, S.30) und geben sich darum als sich selbst aus, nicht als eine frei entworfene Persönlichkeit.

Es kann außerdem davon ausgegangen werden, dass sich ein durchschnittliches Facebook-Mitglied in keiner existentiellen oder sozialen Extremsituation befindet, wenn es Inhalte online stellt, darum wird das Verhalten von einer selbstdarstellerischen Komponente beeinflusst.

Bei der Selbstdarstellung auf Facebook handelt es sich um eine Online-Selbstdarstellung, bei der eine Online-Identität geschaffen wird. Da dafür in jedem Fall das Internet via Computer oder Handy benötigt wird, handelt es sich um computervermittelte Kommunikation mit allen oben beschriebenen Besonderheiten: Die Präsentation ist indirekt, weil nie unvermittelt, und verläuft oft asynchron. Mitglieder haben eine erhöhte Kontrolle über die Selbst-Präsentation, weil nur Inhalte übertragen werden, die bewusst gesendet wurden. Man kann somit versuchen, sich selbst

möglichst positiv darzustellen – das entspricht der Selbstdarstellungstheorie, der zufolge jeder Mensch bemüht ist, sein Verhalten zu kontrollieren und einen günstigen Eindruck zu erwecken. Eine Idealisierung (nach Goffman) gelingt auf Facebook besonders leicht, da die schwer zu kontrollierende Ebene der Ausstrahlung außen vor gelassen wird und nur Inhalte kommuniziert werden, die der Sender bewusst schickt. Zudem kann sich jedes Mitglied alle Zeit der Welt nehmen, um Kommentare zu formulieren, die besten Fotos für die Veröffentlichung auszuwählen oder an einem Inhalt für Profil-Informationen zu feilen. Die Spontaneität der Kommunikation weicht zu Gunsten der Kontrolle.

Es wird deutlich, dass auf Facebook viel Platz für Selbstdarstellung ist. In Anlehnung an Misoch könnte man die Plattform vielleicht als „Raum vieler verschiedener, vernetzter Selbstpräsentationen“ bezeichnen. Zu beachten ist aber, dass auf Facebook oft Leute miteinander kommunizieren, die sich auch außerhalb des Internets kennen. Die Online- und Offline-Selbstdarstellung ist in diesem Fall untrennbar miteinander verbunden. Facebook-Mitglieder können also zwar versuchen, die eigene Schokoladenseite ein bisschen zu betonen und sich im bestmöglichen Licht zu präsentieren, dreiste Lügen würden aber wahrscheinlich nicht unerkannt bleiben.

Mit der Selbstdarstellung auf Facebook verzichten die Mitglieder auf ein Stück Privatsphäre. Sie akzeptieren das, weil ihnen die Gratifikation, die sie durch die Teilnahme am Netzwerk erhalten, größer erscheint als der Verzicht auf Privatheit. Viele Mitglieder sind sich aber vielleicht auch gar nicht bewusst, dass sie durch die Preisgabe ihrer Daten auf Facebook auf Privatsphäre verzichten. Sie haben die Risiken des Internets noch nicht ausreichend erkannt und verhalten sich auf Facebook so wie bei einem privaten Kaffee-Kränzchen unter Freundinnen. Das Internet wird mit der schwachen Öffentlichkeit der realen Welt verwechselt, an die wir gewöhnt sind.

„Selbstdarstellung auf Facebook – Segen oder Fluch?“ bleibt darum die Frage. Im Endeffekt muss jedes Mitglied selbst entscheiden, wie es sich darstellt und was es über sich preisgibt. Die Möglichkeiten sind schier unbegrenzt. Die Risiken aber leider auch.

“Was? Der Staat soll Ihnen vertrauen? Wo kämen wir da hin!
Schon das Grundgesetz sagt, dass alle Gewalt vom Volke
ausgeht. Und Gewalt gilt es einzudämmen.
Da sind Sie ja wohl einer Meinung mit dem Innenministerium.”

Trojanow & Zeh 2009

4. Privatsphäre und Datenschutz

Die Privatsphäre und der Datenschutz sind viel zitierte Stichworte, wenn es um Facebook oder das Web2.0 geht. Die rasanten technischen Entwicklungen und die wachsenden Möglichkeiten, Inhalte über das Internet zu veröffentlichen, lenken das Augenmerk immer wieder auf die Gefährdung der Privatsphäre. Die vorliegende Arbeit hat es sich zur Aufgabe gemacht, den Zusammenhang zwischen Facebook-Nutzung und Privatsphäre in einigen Aspekten näher zu beleuchten. Darum wird an dieser Stelle auf die Geschichte und die Entwicklung der Privatsphäre eingegangen sowie auf den Begriff „Daten“ und die rechtliche Situation des Datenschutzes.

Privatheit, Privatsphäre, Privacy – in der Literatur bedient man sich der unterschiedlichsten Begriffe, wenn es um den Schutz der eigenen Daten vor der Öffentlichkeit geht. Kuhlen (2004, S.177ff) versucht die Begriffe zu trennen und zu analysieren, welche gemeinsamen Mengen sie haben und wo Unterschiede in der Definition liegen. Am Ende kommt er zu dem Schluss, dass weder die Bezeichnung „Privatheit“ noch „Privacy“ alle Bereiche abdeckt und er kommt zu keiner Antwort, welcher Begriff zu bevorzugen ist. In der vorliegenden Arbeit wird es so gehandhabt, wie im Buch des Experten: Die Begriffe werden abwechselnd und synonym verwendet.

4.1. Privatsphäre

Privatsphäre stellt das Gegenstück zur Öffentlichkeit dar. Diese Unterscheidung ist nichts Neues, man kann sie geschichtlich weit zurück verfolgen: In der Antike entwickelte sich in den griechischen Stadtstaaten eine private und eine öffentliche Ordnung. Die private Ordnung des Hauses bildete den Gegenpart zur öffentlich-politischen Ordnung des Marktplatzes. Im Römischen Reich wurde diese Teilung in zwei Sphären beibehalten. Vom Verb „privare“ (berauben) abgeleitet bezeichnete man den Bürger als „privatus“, soweit er nicht politisch tätig und somit der öffentlichen Beobachtung entzogen – also „beraubt“ – war. Das Wort „privat“, wie wir es heute verwenden, hat seinen Ursprung im 16. Jahrhundert und bezeichnet seit damals die Unabhängigkeit von Sachverhalten und Personen.

Die wohl wichtigste Funktion der Privatheit ist, dass die Privatsphäre gegen Einblicke Dritter geschützt wird. Nur so ist individuelles Handeln möglich. (Schaar 2007, S.15ff) Privatsphäre ist eine Grundvoraussetzung für Demokratie. Erst durch Privatsphäre wird es den Menschen möglich, selbstständig zu denken und individuell zu handeln. Es gehört zur demokratischen Idee, frei denkende und handelnde Bürgerinnen und Bürger zu stärken und die Eingriffsbefugnisse des Staates zu beschränken. Die Geschichte liefert zahlreiche Beispiele, wohin es führt, wenn der Staat die Wichtigkeit der Privatheit vergisst und sein Volk kontrolliert, überwacht, verfolgt. (Trojanow/Zeh 2009, S.11 & S.78)

So wichtig die Privatsphäre auch für eine demokratische Gesellschaft ist, so akut lauern ihr doch Gefahren auf: Der technologische Fortschritt, wirtschaftliche Interessen, staatliche Kontrollen und auch die zunehmende Bereitschaft vieler Menschen, auf die eigene Privatsphäre zu verzichten, stellen Gefahren für die Gewährleistung der Privatsphäre dar. (Schaar 2007, S.11)

Während früher die Privatsphäre gestört werden konnte durch Bespitzelung, Belauschen und vielleicht darauf folgende Mund-Propaganda und die viel zitierte Gerüchteküche in einem Dorf oder einer Stadt, stiegen im Zuge der **industriellen Revolution** und der fortschreitenden Entwicklung der Gesellschaft beständig die Risiken, die Privatsphäre zu gefährden. An die Stelle von persönlichen Beziehungen traten oftmals flüchtige Kontakte. Geschäfte wurden nicht mehr nur mit Personen gemacht, die man persönlich kannte – so war man plötzlich auf Informationen angewiesen, die eine Grundlage für Vertrauen bildeten. Denn wie soll man ohne jegliche Information wissen, ob man einer fremden Person trauen kann? Man kann also sagen, dass die Erhebung von Daten es gestattete, trotz zunehmender Anonymität zu handeln und zu planen. Die Erhebung, Dokumentation und Nutzung von Informationen war eine logische Notwendigkeit im Zuge des industriellen Fortschrittes. Schaar geht sogar so weit zu sagen, es war eine Voraussetzung für die Herausbildung moderner Gesellschaften. (2007, S.33) Hätte man im späten 18. Jahrhundert keinen neuen Weg gefunden, um mit Daten umzugehen und somit dem Vertrauensverlust entgegenzuwirken, wer weiß, wo wir heute wären. Und doch mutet die Überlegung seltsam an, dass es gerade der Wandel zu mehr Anonymität war, der den Schutz der Privatsphäre bröckeln ließ.

Datensammlungen zur Bekämpfung des Vertrauensverlustes sind ein Faktor in der Geschichte der Bedrohung der Privatsphäre. Ein anderer Faktor ist die Entwicklung der Medien. Durch sie wurden erstmals Informationen nicht persönlich one-to-one weiter gegeben, sondern Inhalte quasi unkontrollierbar one-to-many verbreitet. Damit vergrößerte sich die Reichweite der Öffentlichkeit. Vor allem den Personen, die in der Öffentlichkeit bereits bekannt sind (beispielsweise aus Politik, Showbusiness oder Sport) wird kaum eine Privatsphäre gewährt – die Medien veröffentlichen große Teile ihres Privatlebens. Dazu muss erwähnt werden, dass Privatangelegenheiten heute im Allgemeinen freizügiger öffentlich gemacht werden als früher. Und da kommt das Internet ins Spiel. Denn wo können Bürgerinnen und Bürger leichter etwas veröffentlichen als im World Wide Web? Viele Internetangebote bauen auf einen einzigen Erfolgsfaktor: auf die Freizügigkeit der

Userinnen und User, die über ihr Privatleben berichten. Auch Facebook wäre ohne diese Freizügigkeit verloren. (Schaar 2007, S.17ff)

Nach diesen Überlegungen kommt Schaar zu folgender Definition:

> „Die Privatsphäre ist Raum des individuellen Rückzugs und zugleich unverzichtbare Voraussetzung einer freien Meinungsbildung." (Schaar 2007, S.15)

Kuhlen liefert eine etwas detailliertere Definition, die auch Bezug auf den technischen Fortschritt nimmt:

> Privatsphäre ist ein „Raum, (…) den jeder Mensch für sich definiert und über den er entsprechend verfügen kann und gegen dessen Verletzung er sich wehren kann – sei es, dass in diesen Raum eingedrungen wird oder dass aus diesem Raum ohne Einwilligung etwas entfernt bzw. nach außen getragen wird. In erster Linie ist damit ein physischer, unbegrenzter Raum gemeint, in dem sich das private Leben abspielt, zu dem andere keinen Zugriff haben. (…) Dass sich dieser physische Raum heute in einen elektronischen virtuellen erweitert, über den ebenfalls verfügt werden soll, macht Schutz und Kontrolle über diesen Raum nicht leichter." (Kuhlen 2004, S.178)

Das *Electronic Privacy Information Center* unterscheidet vier Arten von Privatheit (Kuhlen 2004, S.178):

Information Privacy umfasst die Sammlung und Handhabung persönlicher Daten wie beispielsweise medizinische Auskünfte oder Konto-Stände. Die Privatsphäre solcher Informationen wird auch Datenschutz genannt.

Bodily Privacy dient dem Schutz des Körpers vor Eingriffen wie Gen-Tests oder Drogentests.

Privacy of Communications umfasst den Schutz der Privatheit von Post, Telefonaten, E-Mails und anderen Kommunikationsformen.

Territorial Privacy steht für die Richtlinien, die vor Eindringen beispielsweise in das eigene Heim oder den Arbeitsplatz schützen.

Wenn in der vorliegenden Arbeit von Privatsphäre geschrieben wird, bezieht es sich auf die erste Art von Privacy: der informationellen Privatsphäre.

4.1.1. Privatheit als Menschenrecht

Kuhlen tritt in seinem Buch zur Informationsethik den Beweis an, dass das „Recht auf Privatheit" ein Menschenrecht und somit „wie auch andere Menschenrechte ein persönliches, gegenüber dem Staat (und heute zunehmend auch der Wirtschaft) einklagbares Recht ist".[5] (2004, S.177)

1948 wurde in Artikel 12 der **Allgemeinen Erklärung der Menschenrechte** der Vereinten Nationen festgeschrieben:

> „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen." (Kuhlen 2004, S.180)

Da Menschenrechte nicht einklagbar sind, sondern nur durch eine Kodifizierung in der nationalen Gesetzgebung bindend werden, ist für Europa die **Charta der Grundrechte** der Europäischen Union von großer Bedeutung. Die Charta regelt unter Kapitel II (Freiheiten) in Artikel 7 das „Recht auf Privatleben" und in Artikel 8 den „Schutz personenbezogener Daten".

> **Artikel 7: Achtung des Privat- und Familienlebens**
>
> Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

> **Artikel 8: Schutz personenbezogener Daten**
>
> (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
>
> (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
>
> (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.
>
> (Amtsblatt der Europäischen Gemeinschaften 2000, S.10)

Diese Menschenrechte gelten wie alle Menschenrechte universal aber nicht absolut. Das bedeutet, dass sie unter bestimmten Bedingungen eingeschränkt werden – meist auf Grund einer Überschneidung mit einem anderen Menschenrecht (etwa dem „Recht auf freie Meinungsäußerung"). Problematisch wird diese Regelung der Nicht-Absolutheit, wenn die

[5] Kuhlen definiert Menschenrechte als „individuelle und universal gültige Rechte, die Staaten allen ihren Bürgern garantieren sollen" und sieht sie als „ethischen Konsens der Weltgemeinschaft" an. Die Einlösung der Menschenrechte beruht auf dem Prinzip des Sollens, sie ist ein ethischer Imperativ. In vielen Ländern der Welt wurden die Menschenrechte aber im Grundrecht verankert (= nationalstaatliche Kodifizierung) und haben eine rechtliche Entsprechung im Gesetz – dadurch werden sie zu direkt einklagbaren Rechten. Menschenrechte gelten im elektronischen Raum genauso wie in der realen Welt. (Kuhlen 2004, S.97ff)

Einschränkungen wichtiger erscheinen als das Menschenrecht. So besitzen beispielsweise – insbesondere nach den Anschlägen auf das World Trade Center am 11. September 2001 – Sicherheitsinteressen oft einen höheren Stellenwert als der Schutz der Privatsphäre. Darauf wird in Kapitel 4.3. näher eingegangen.

Das Recht auf Privatheit beinhaltet nicht nur das Recht, in Ruhe gelassen zu werden, sondern es bedeutet auch das Recht auf eigene Kontrolle über die in der Kommunikation sowie der elektronischen Interaktion abgegebenen Daten (Kuhlen 2004, S.184ff). Jeder Mensch sollte also selbst unter Kontrolle haben, welche Daten er von sich preisgibt. Dieses Prinzip mag in der Theorie sehr schön klingen, in der Praxis wird es aber leider nicht immer umgesetzt. Jeder Mensch hätte theoretisch das Recht dazu, seine eigenen Datenflüsse zu kontrollieren; praktisch gesehen haben aber lange nicht alle Personen ihre Daten unter Kontrolle.

Dabei sind zwei Punkte ganz wesentlich: das Wissen, wie man die eigene Privatsphäre schützt und der Wille, das auch zu tun.

Kuhlen sieht die Sicherung von Privatheit als Basiskompetenz von Personen, die online agieren. Gleichzeitig erkennt er eine große Gefahr darin, dass viele Menschen nicht über das Know-How verfügen, sich und ihre Daten im elektronischen Umfeld ausreichend zu schützen. (2004, S.189)

Bezüglich des Willens, die eigene Privatsphäre zu schützen, geht Kuhlen sogar so weit, Privatheit als „durchaus aushandelbares und partiell aufgebbares Gut“ zu bezeichnen. Auf vorhandene Schutzmöglichkeiten greifen Userinnen und Usern nur selten zurück, darum schließt Kuhlen auf ein Desinteresse an Privatheit. Er erkennt, dass Personen bereit sind, auf das Recht auf Privatheit zu verzichten, wenn nur der Anreiz groß genug ist. Der Trend führt also dahin, wo er herkommt: Privatheit wird wieder auf den Bereich zurückgeführt, der sich wirklich auf das Private bezieht (z.B. auf den Wohnraum) und nicht mehr auf das private Auftreten und das Wahrgenommenwerden in der Öffentlichkeit. (2004, S.190ff)

Kuhlen kommt zu dem ernüchternden Resumée, dass auf Grund erhoffter ökonomischer Vorteile, vermeintlicher Sicherheit oder auch aus Gleichgültigkeit oder Unwissenheit der Status von Privatheit oft relativiert wird.

> „Ohne informationelle Autonomie und Bildung wird sich Privatheit angesichts ökonomischer und sicherheitspolitischer Begehrlichkeit von selbst aufgeben.“ (Kuhlen 2004, S.175)

4.2. Daten

4.2.1. Daten – Information – Wissen

Der Zusammenhang zwischen Daten, Information und Wissen ist ein stetiger Kreislauf:

> „Daten sind (…) gemessene Einheiten, die durch Beobachtung von natürlichen bzw. konstruierten oder simulierten Gegenständen oder Ereignissen gewonnen und nach syntaktisch wohlgeformten Regeln in einem vereinbarten Zeichensystem dargestellt werden." (Kuhlen 2004, S.159)

Daten bedeuten nach Kuhlen für sich genommen nichts. Erst wenn sie einen Bezugsrahmen bekommen, sind sie aussagekräftig. Kuhlen bezeichnet Daten als „virtuelle Informationen", die das Potenzial haben, zu Information zu werden. „Zu Informationen werden Daten, wenn sie in einem bestimmten Kontext und/oder zu einem bestimmenden Zweck wahrgenommen oder gezielt aus Daten-/Informationssystemen abgerufen werden." Wurden die Daten durch das Herstellen eines Kontextes zu Informationen, können sie die nächste Stufe der Transformation beschreiten: Sie können zu **Wissen** werden. Dies geschieht, wenn Informationen durch Lernen in interne und dauerhafte Wissensstrukturen eingebunden und somit in einen größeren kognitiven Zusammenhang gestellt werden. Wissen kann somit als gelernte Information bezeichnet werden. Im Umkehrschluss kann man **Information** als besondere Form des Wissens definieren: Information ist die Art und Weise, wie sich Wissen transportabel macht. Oder wie es Kuhlen kurz und prägnant auf den Punkt bringt: „Information ist Wissen in Aktion". Der Weg von den Daten über Information zum Wissen ist keine Einbahn: Durch die Darstellung in einem formalen Zeichensystem verwandelt sich Wissen wieder in Daten, die in der realen Welt wahr- und aufgenommen werden können. Wissen wird als Information transportiert; diese Information hat als kleinste Einheit Daten – so werden aus Wissen wieder Daten über den Weg der Information. (Kuhlen 2004, S.159f)

4.2.2. Daten im Zeitalter des Internets

Wie oben beschrieben, wurde die computergestützte Datenerfassung erst im Zuge der industriellen Revolution zum Thema. Die moderne Massendatenverarbeitung hatte ihre Sternstunde in den USA der 1890er: Es wurden erstmals Lochkarten zur Volkszählung eingesetzt. Auf die Lochkarten-Technologie folgte die unaufhaltsame Weiterentwicklung des modernen Computers, mit dessen Hilfe Datenmengen bewältigt werden konnten, die vorher einen manuellen Aufwand sondergleichen bedeutet hätten. Auf einmal konnten ungeheure Datenmengen erfasst, gespeichert und bewegt werden – wirtschaftliche oder gesellschaftliche „Sättigungsgrenzen" waren keine in Sicht. Mit den Möglichkeiten, ohne großen Aufwand Daten zu verarbeiten, kam gleichzeitig der Reiz, dies auch zu tun, wenn es zu Lasten des Datenschutzes ging. Das erkannten kritische Zeitgenossen und forderten Anfang des 20. Jahrhunderts zum ersten Mal, die Menschen

vor den negativen Folgen zu schützen und Vorkehrungen zum Schutz der Privatsphäre zu treffen. (Schaar 2007, S.32ff)

Inzwischen ist die Beschaffung personenbezogener Daten so einfach wie nie. Jeder Nutzer und jede Nutzerin hinterlässt im Internet Spuren, die von interessierten Stellen gesammelt und ausgewertet werden können. (Schaar 2007, S.38f) Das Internet bringt damit keine neuen Arten der Verletzung hervor, aber es lässt Verletzungen einfacher, schneller und innerhalb größerer Kreise geschehen. Losgelöst von klassischen, physischen Print- und Funkmedien erfolgt die Verbreitung von Daten weltweit in Sekundenschnelle und unterscheidet sich zudem durch die permanente Speicherung und Verfügbarkeit. (Ghazal 2010, S.45) Das Wort „Daten" klingt vor diesem Hintergrund beinahe banal. Hinter dem einfachen Wort stellt man sich einzelne Informationen vor: den eigenen Namen, die Adresse oder die Sozialversicherungsnummer – alles einzelne Daten, die in der Offline-Welt einem Menschen anhaften. Daten im Internet stellen aber ungleich mehr dar, als sie dies je zuvor offline konnten. Daten im Internet sind fast immer vernetzte Daten. Es werden Zusammenhänge zwischen Daten aus den verschiedensten Bereichen hergestellt und ganze Daten-Konstrukte gebildet. Beispielsweise werden die Daten über Online-Kaufverhalten verknüpft mit Informationen des Facebook- oder MySpace-Profiles sowie mit den Suchanfragen auf Google der letzten Jahre. (Zeger 2009, S.101) Diese Daten-Konstrukte werden dann einem Menschen zugeordnet. Oder gar als Synonym für den Menschen angesehen. Der angesammelte Datenhaufen wird als Bewertungsgrundlage verwendet. Google, Marketing-Büros, zukünftige Arbeitgeber oder wer immer sonst Interesse daran hat, kann eine Person auf Grund von Daten bewerten, ohne sie jemals persönlich kennen gelernt zu haben. Ob diese Bewertung zutreffend ist, ist natürlich nicht gewiss. (Schirrmacher 2010 in: ORF 2, Club2)

Im Internet gibt es drei verschiedene Arten von Daten (Kuhlen 2004, S.186f):

Distributionsdaten sind Daten, die online verbreitet werden etwa via E-Mails oder auf Plattformen wie Facebook. (Wenn im weiteren Verlauf der Arbeit von Daten gesprochen wird – insbesondere im Teil der empirischen Untersuchung – sind immer Distributionsdaten gemeint, also die Daten, die Userinnen und User online stellen.)

Interaktionsdaten sind alle Daten, die entstehen, wenn Webdienste (wie beispielsweise Suchmaschinen oder elektronische Auktionen) benutzt werden. Die Daten können vom Dienst-Anbieter gespeichert werden und werden häufig genutzt, um den Userinnen und Usern ein personalisiertes Service zu bieten, beispielsweise das Vorschlagen von Produkten auf Amazon.

Transaktionsdaten sind personenbezogene Daten, die bei der Durchführung von geschäftsrelevanten Handlungen anfallen. Jede Bestellung, jede Bezahlung auf elektronischen Marktplätzen hinterlässt Spuren.

Diese drei Arten von Daten geben Userinnen und User über sich im Netz preis. Hinzu kommen **Verbindungsdaten** (auch: Verkehrsdaten). Durch die IP-Adresse ist jeder Rechner identifizierbar, von dem aus das Internet benützt wird. Die Anbieter brauchen lediglich die Daten speichern, die aufgezeichnet werden, schon kann in Form von Logprotokollen jegliche Online-Aktivität ausgewertet werden. (Schaar 2007, S.42f) Dass Internet-Provider die technische Möglichkeit der Speicherung auch nutzen, dafür sorgen die Gesetze: Laut EU-Richtline von 2006 müssen die Verkehrsdaten aller Aktivitäten von Telefonie- und Internetprovider mindestens sechs und höchstens 24 Monate gespeichert werden. (ebd. S.116f) Diese Richtlinie zur Vorratsdatenspeicherung erregte jüngst die Gemüter. Sie ist in Österreich derzeit noch nicht umgesetzt, wird sich aber früher oder später nicht mehr abwenden lassen. (vgl. Kapitel 4.4.3)

Es gilt zu bedenken, dass durch die stetige Erhebung, Speicherung, Übermittlung sowie Auswertung von persönlichen Daten der Laie leicht die Kontrolle darüber verlieren kann, wer was über ihn weiß (Schaar 2007, S.50). Eine aktuelle Oekonsult-Umfrage bestätigt das. Ihr zufolge wissen 81,6 % aller Österreicherinnen und Österreicher nicht genau, wer aller über ihre personenbezogenen Daten verfügt. 76,7 % denken erschreckender Weise nicht, dass sie alles in ihrer Macht Stehende tun, um die eigenen Personendaten wirksam zu schützen. (Oekonsult 2010)

Kuhlen (2004, S.175) attestiert in diesem Zusammenhang, dass die Privatsphäre nur dann zu bewahren ist, wenn die Bürgerinnen und Bürger so informationell aufgeklärt und kompetent sind, dass sie die Schutzmöglichkeiten nutzen, die es vor Missbrauch ihrer persönlichen Daten gibt.

4.3. Datenschutz

Nachdem die Begriffe „Privatsphäre“ und „Daten“ geklärt wurden, gilt es nun, sich den Datenschutz anzusehen, der untrennbar mit dem Schutz der Privatsphäre verbunden ist.

Das Grundrecht auf Datenschutz bezeichnet den Schutz der Betroffenen vor Ermittlung ihrer Daten sowie Weitergabe der ermittelten Daten (Ghazal 2010, S.47f).

Experten sehen schwierige Zeiten auf sich zukommen, was die Wahrung dieses Grundrechtes betrifft:

> „Die Frage drängt sich auf, ob es angesichts der durch das Internet geprägten neuen digitalen Realität noch einen wirksamen Datenschutz geben kann.“ (Schaar 2007, S.48)
>
> „Derzeit ist unklar, inwieweit neue Grenzen durch die Software-Architektur gezogen werden und inwieweit neue soziale Normen inklusive angepasster Gesetze nötig sind, um einen Freiraum für Meinungsäußerung und Selbstdarstellung zu erhalten, aber den Schutz der Privatsphäre weiterhin zu gewährleisten.“ (Schmidt 2008, S.34)

Die Gesetzgebung wird auf eine harte Probe gestellt, wenn es darum geht, den Datenschutz angemessen rechtlich zu verankern. Denn die Herausforderungen in Form von wirtschaftlichen Interessen, rasender technologischer Entwicklung, digitaler Datenverarbeitung und nicht zu vergessen staatlicher Überwachung unter dem Deckmantel der Sicherheit sind schier unermesslich. (Schaar 2007, S.19ff) Das Recht auf informationelle Privatheit ist besonders in elektronischen Räumen relevant, da diese viel transparenter sind als physische Räume. Es stellt sich die Frage, wie man mit dem Konzept der Privatheit umgeht, das entstanden ist, lange bevor das Internet die Haushalte eroberte. (Kuhlen 2004, S.184)

Wie oben beschrieben, ist Privatheit ein Menschenrecht mit universalem Anspruch. Dieser Anspruch wird verteidigt durch das Prinzip der informationellen Selbstbestimmung und juristisch umgesetzt als Anspruch auf Datenschutz. (Kuhlen 2004, S.193) Datenschutz stellt im jeweiligen Staat die rechtliche Rahmenbedingung zum Menschenrecht auf Privatheit dar.

Im Aufsatz „The Right to Privacy“ leiteten die amerikanischen Anwälte Samuel Warren und Louis D. Brandeis 1890 aus den Rechtsgrundsätzen des Schutzes der Person und des Eigentums ein „Right to be left alone“ ab. Jede Person soll selbst über die Preisgabe der sie betreffenden Informationen entscheiden können. Der Aufsatz stellt einen Grundstein dar für viele Debatten und gesetzliche Regelungen auf der ganzen Welt zum Thema Privatsphäre und Datenschutz. Zusammenfassend lässt sich sagen, dass es große Unterschiede gibt, wie in verschiedenen Ländern und auf verschiedenen Kontinenten mit dem Thema umgegangen wird. Während beispielsweise der 1974 vom US-Kongress verabschiedete „Privacy Act“ die Wirtschaft außen vor lässt, um nicht in den Wettbewerb einzugreifen, werden die von der US-Gesetzgebung vernachlässigten Bereiche in Europa durchaus berücksichtigt. (Schaar 2007, S.112f)

4.3.1. Datenschutz in Europa

In den letzten 25 Jahren entwickelte sich das Datenschutzrecht in Europa beständig in die gleiche Richtung. Mayer-Schönberger und Brandl gliedern die Entwicklung in vier Generationen (2006, S.12f).

1. Generation

In den 70er-Jahren wollten viele Staaten und Unternehmen neue technische Möglichkeiten nutzen, um Datenbestände in alles umfassenden, zentralen, nationalen Datenbanken zu speichern. Dieses Vorhaben wurde als technisches „Großrisiko“ gesehen, vergleichbar mit Kernenergie. Als Reaktion darauf wurde durch Datenschutznormen dieser Zeit die zentralisierende Technik der Datenverarbeitung einer staatlichen Kontrolle unterworfen.

2. Generation

Die Pläne zentraler Datenbanken wurden nicht Realität. Anstatt weniger zentraler Hochleistungs-Rechner gab es bald viele und immer billigere Personal Computer. Der Datenschutz musste darum nicht mehr auf Groß-Datenbanken angewendet werden, sondern auf unzählige EDV-Anlagen in Verwaltung und Wirtschaft. Es wurden Betroffenenrechte eingefordert.

3. Generation

Der Datenschutz wurde nicht mehr als bloßes Abwehrrecht, sondern als Gestaltungsrecht gesehen. Privatpersonen sollten die Verwendung personenbezogener Daten mitbestimmen und –gestalten können. Das Grundrecht auf informationelle Selbstbestimmung wurde formuliert.

4. Generation

Bürgerinnen und Bürger forderten die Datenschutzrechte nicht ausreichend ein und verzichteten regelmäßig darauf, beispielsweise bei Vertragsverhandlungen. Außerdem entstanden neue Sektoren (z.B. Direktmarketing) in denen es zu datenschutzrechtlichen Problemen kam. Als Konsequenz wurden in den Datenschutznormen Betroffenenrechte besonders bewehrt, die Haftung wurde durch Beweislastumkehr und Verschuldensregelungen erweitert und durch sektorale Vorschriften zusätzlich ergänzt.

Die Datenschutzrichtlinie, die 1995 von der Europäischen Union verabschiedet wurde, ist eine Datenschutznorm dieser vierten Generation. Sie soll den Datenschutz auf hohem Niveau innerhalb der EU harmonisieren.

Wie viele rechtliche Bestimmungen ist auch die europäische Datenschutzrichtlinie sehr komplex und umfangreich. Eine Vertiefung in den Gesetzestext würde an dieser Stelle den Rahmen sprengen. Einen guten Überblick über Grundsätze und Definitionen liefern Mayer-Schönberger und Brandl (2006, S.14ff).

4.3.2. Das österreichische Datenschutzgesetz

In Österreich ist der Datenschutz seit Jahrzehnten gesetzlich verankert. Das Bundesgesetz vom 18. 10. 1978 über den Schutz personenbezogener Daten stellte das Fundament des österreichischen Datenschutzes dar. (Mayer-Schönberger/Brandl 2006, S.11) Seit den 70er-Jahren hat sich einiges verändert. Besonders die immer weiter verbreitete elektronische Datenverarbeitung, der Vormarsch des Computers und die steigende Internetnutzung der Bevölkerung stellen das Datenschutzgesetz vor immer neue und wachsende Herausforderungen. In dieser „Aufbruchszeit“ elektronischer Datenverarbeitung wurde von der Europäischen Union in der EG-Datenschutzrichtlinie (95/46/EG) zu einer Vereinheitlichung des europäischen Datenrechts aufgerufen. (Drobesch 2000, S.7) 1995 wurden Richtlinien zum Datenschutz verabschiedet, die von allen Mitgliedsstaaten bis zum 24. 10. 1998 umzusetzen waren. Österreich setzte die Richtlinie mit 1. 1. 2000 um und verabschiedete das Datenschutzgesetz 2000 (DSG 2000). Es ist im Kern ein völlig

neues Datenschutzrecht, das mit dem vorangegangenen Datenschutzgesetz nicht viel gemein hat. (Mayer-Schönberger/Brandl 2006, S.11f)

Die Datenschutzbestimmungen gelten grundsätzlich für jede Art von Datenverarbeitung: online, offline und auch manuell geführte Karteien. Sie gewähren ein Recht auf Geheimhaltung personenbezogener Daten zum Schutz der Privatsphäre natürlicher oder juristischer Personen. Voraussetzung der Anwendbarkeit des Datenschutzrechtes ist, dass Daten personenbezogen sind, also Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Als besonders schutzwürdig gelten sensible Daten. Anonymisierte Daten, die man nicht auf eine konkrete Person zurück führen kann, unterliegen nicht dem DSG. (Janisch/Mader 2006, S.32)

Das Grundrecht auf Datenschutz im Wortlaut (§ 1 DSG):

> „Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind." (RIS BKA)

Genaue Begriffsdefinitionen dazu finden sich in § 4. Unter Absatz 1 und 2 werden „Daten" und „sensible Daten" beschrieben:

Daten („personenbezogene Daten") sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Als **sensible Daten** („besonders schutzwürdige Daten") gelten Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben. (Drobesch 2000, S.22)

Die Verwendung von personenbezogenen Daten ist also laut § 1 des Datenschutzgesetzes nur dann zulässig, wenn sie die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzt. § 9 legt fest, unter welchen Voraussetzungen diese schutzwürdigen Betroffenen-Interessen bei Verwendung „sensibler" Daten nicht verletzt werden. Es werden 13 Ausnahmetatbestände aufgelistet, die das Verwendungsverbot aufheben. (Mayer-Schönberger/Brandl 2006, S.33f) So heißt es beispielsweise im Gesetzestext:

> „Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn der Betroffene die Daten offenkundig selbst öffentlich gemacht hat (…)" (Drobesch 2000, S.28)

Drobesch und Grosinger erläutern: „Die Veröffentlichung muss durch den Betroffenen selbst erfolgt sein, z.B. in öffentlichen Registern, Teilnahmeverzeichnissen, durch Presseaussendungen oder Veröffentlichungen im Internet." (2000, S.144)

Bereits in § 1 wird als Bedingung für Datenschutz gestellt, dass ein schutzwürdiges Interesse an den Daten besteht. In § 9 wird konkretisiert, dass das Geheimhaltungsinteresse nicht verletzt wird, wenn Daten von der oder dem Betroffenen selbst veröffentlicht wurden. Das Geheimhaltungsinteresse ist also nicht mehr gegeben, sobald man Daten selbst veröffentlicht. Umgelegt auf Facebook bedeutet das: Wer auf der Plattform personenbezogene Daten allen zur Verfügung stellt, verzichtet freiwillig auf Datenschutz.

Einem OGH-Urteil nach ist das schutzwürdige Interesse allerdings aufrecht, wenn ein Betroffener seine personenbezogenen Daten nur einem begrenzten Personenkreis anvertraut hat:

> „Das schutzwürdige Interesse an dem Grundrecht auf Geheimhaltung personenbezogener Daten (§ 1 Abs1 DSG 1978, nunmehr § 1 Abs 1 DSG 2000) wird auch dann nicht ausgeschlossen, wenn der Betroffene selbst geschützte Daten einem (begrenzten) Personenkreis offenbart." (OGH 3.9.2002, 11 Os 109/01)

Was bedeutet das nun für **Facebook**?

Einerseits verzichtet man in Österreich auf Datenschutz, wenn man Daten freiwillig veröffentlicht, also beispielsweise im Internet preisgibt. Andererseits greift das Datenschutzgesetz sehr wohl, wenn man seine Daten nur einem begrenzten Personenkreis offenbart. Wo die Grenze zu ziehen ist zwischen einer kompletten Veröffentlichung und der Offenbarung an einen begrenzten Personenkreis, ist schwer zu definieren.

Wann eine Veröffentlichung auf Facebook vorliegt, wurde mit Frau Mag. Zimmer, Datenschutz-Expertin der AK Österreich, geklärt. Sie sieht es durchaus als begrenzten Personenkreis an, wenn Facebook-Userinnen und –User ihre Inhalte beschränkten Personengruppen zugänglich machen. Wenn die Voreinstellungen so gewählt werden, dass Inhalte nur partiell von anderen gesehen werden können, unterliegen diese Inhalte laut der Expertin dem österreichischen Datenschutzrecht.

Das bedeutet, dass auf Facebook den Privatsphäre-Einstellungen eine enorme Wichtigkeit zukommt. Wer seine Daten auf Facebook veröffentlicht – im Sinne von „allen" zugänglich macht – verzichtet auf Datenschutz. Es gibt kein schutzwürdiges Interesse mehr für diese Daten. Zeigt man seine Inhalte aber nur Freunden bzw. bestimmten Personengruppen, gilt dies nicht als Veröffentlichung, wie sie im Gesetzestext steht. Es besteht ein überwiegendes berechtigtes Geheimhaltungsinteresse und die Personen, die die Daten sehen können, dürfen diese nicht einfach weiterverwenden, weil sie datenschutzrechtlich geschützt sind.

Wie wichtig es ist, seine Privatsphäre-Einstellungen auf Facebook zu regulieren, kann an dieser Stelle gar nicht vehement genug betont werden. Denn wer es nicht tut, verzichtet freiwillig auf das Recht auf Datenschutz und stellt somit seine Daten aller Welt zur Verfügung.

4.4. Bedrohungen für Privatsphäre und Datenschutz

In den vorangegangenen Abschnitten wurde immer wieder deutlich, dass das Recht auf Privatsphäre an vielen Stellen beschnitten wird und Datenschutz-Expertinnen und –Experten harte Kämpfe ausfechten, um die informationelle Selbstbestimmung weiterhin zu garantieren. Um eine bessere Übersicht über das komplexe Thema zu gewähren, wird an dieser Stelle noch einmal zusammengefasst, welche Faktoren unser aller Privatsphäre bedrohen.

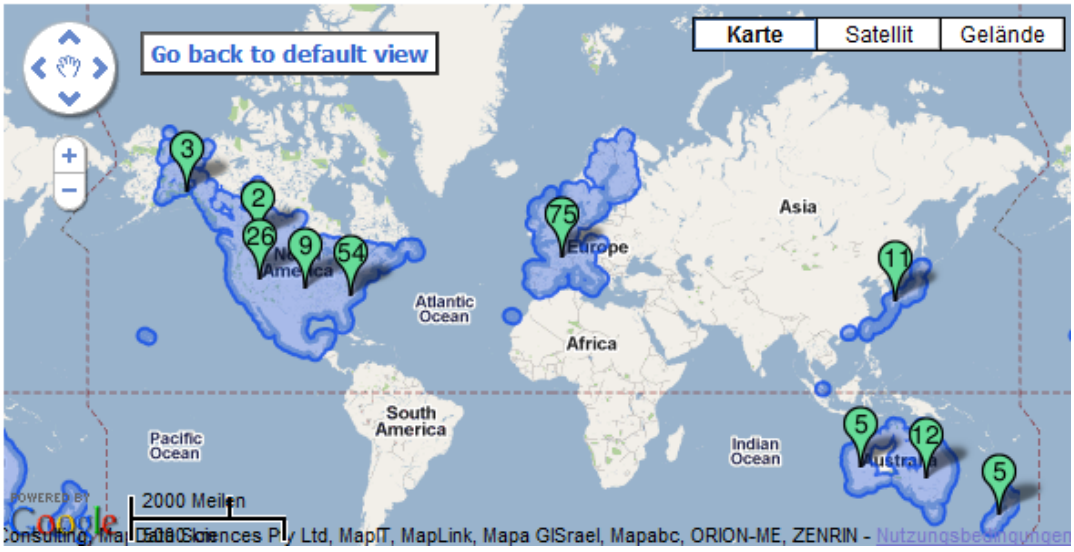
4.4.1. Technischer Fortschritt

Wie bereits an mehreren Stellen erwähnt, bedarf es auf Grund neuer technischer Möglichkeiten auch neuer Regelungen in Bezug auf den Datenschutz. Das Internet stellt eine Riesen-Plattform zur Daten-Verbreitung dar und rückt die Privatsphäre in ein völlig neues Licht. Informationen werden in einem Ausmaß verbreitet, das noch vor wenigen Jahrzehnten unvorstellbar war. Ein plakatives Beispiel dafür ist das Fernmeldegeheimnis. Unter dem Namen „Briefgeheimnis“ kann sich im Allgemeinen jeder etwas vorstellen: Jeder kann sich sicher sein, dass seine Briefe ungelesen an ihr Ziel kommen und dass Gedanken darin unbeobachtet transportiert werden. Mit der Entwicklung des Internets bekam der Postweg einen Kollegen: den E-Mail-Versand. E-Mails werden heutzutage beinahe inflationär verschickt. Sie dienen der schnellen Weitergabe von Informationen oder enthalten Roman-ähnliche Erzählungen. Sie werden privat wie auch beruflich benutzt. Kurz: Ein Mail erfüllt heute alle Aufgaben eines Briefes, nur schneller. Auch die Symbolik im Mail-Verkehr lässt an die gute alte Post erinnern: Im E-Mail-Account findet sich ein „Postfach“ und als Sinnbild für ein Mail wird häufig ein Briefumschlag genutzt. Was die elektronische Post allerdings von der haptischen unterscheidet, ist der Datenschutz. Jedes Mail gleicht einem unverschlossenen Brief. Sie kann weltweit von jeder Person, die einen Internet-Zugang besitzt, gelesen werden. Das Briefgeheimnis gilt für die elektronische Post nicht. Sie unterliegt trotz ihres Namens nicht dem Postgeheimnis. (Trojanow/Zeh 2009, S.24f) Der technische Fortschritt bringt neue Möglichkeiten mit sich, an welche die Gesetze noch nicht angepasst wurden. Dass das ein Versehen ist, ist kaum zu glauben. Viel naheliegender scheint, dass manche Stellen ein Interesse daran haben, das E-Mail-Wesen so lange wie möglich unreguliert zu lassen. Daten sammeln wo es geht, bis Datenschutzverbände ein Sprachrohr bilden, auf Missstände aufmerksam machen und den Druck auf die Politik erhöhen. Dass von Seiten der europäischen Regierungen kein Interesse an mehr Datenschutz besteht, zeigen die jüngsten Entwicklungen zur Vorratsdatenspeicherung. 2006 wurde eine EU-Richtlinie beschlossen, die die Mitgliedsstaaten zur Einführung von Mindestspeicherungsfristen für Verkehrsdaten der Telekommunikation und des Internets verpflichtet. Die Speicherungsfristen müssen mindestens ein halbes Jahr, höchstens zwei Jahre sein. (Schaar 2007, S.118) Dabei sollen zwar nicht die Inhalte von Telefon- und Mail-Verkehr gespeichert werden, sondern nur die Verbindungsdaten. Aber alleine der Gedanke an eine Liste, die detailliert aufzeichnet, wer wann mit wem kommuniziert hat, sollte übel aufstoßen. Diese

Richtlinie ist ein Beispiel dafür, wie großzügig Daten derzeit gespeichert und zur weiteren Verfügung aufbehalten werden. Die Technik macht's möglich und die Entscheidungsträger verwirklichen die Möglichkeiten.

Das Geschäft mit den Daten wird oft gewissenlos und dreist betrieben. Dass es dabei aber doch eine gewisse Schmerzgrenze gibt und Datenschutzgremien durchaus etwas bewirken können, zeigte jüngst der Fall **Google Street View** in Österreich. Seit Mai 2007 sammelt Google mit Hilfe von speziellen Kameras Bilder von öffentlichen Straßen. Die Bilder werden zu 360°-Panoramabildern zusammengefügt, die es Internet-Userinnen und –Usern ermöglichen, auf Google Maps nicht mehr nur Landkarten abzurufen, sondern direkt in die Umgebung einzusteigen und quasi virtuell auf der gewünschten Straße spazieren zu gehen. Die Fahrzeuge mit Spezial-Ausrüstung und Kameras, die auf dem Dach montiert wurden, hatten ihre ersten Einsätze in den USA. Inzwischen hat Google die Fühler aber weiter und weiter ausgestreckt und an verschiedenen Orten auf der ganzen Welt mehrere Millionen Bilder aufgenommen. (Google Street View) Wie Abbildung 2 zeigt, wurden in Europa bereits 75 Städte ins Google-Daten-Archiv aufgenommen.

Abbildung 2: **Übersicht Google Street View Standorte**



Quelle: http://www.google.de/help/maps/streetview/where-is-street-view.html

Auch in Österreich schickte Google seine eifrigen kleinen Street View Autos an verschiedene Standorte, um Momentaufnahmen der Straßenzüge zu erstellen. Allerdings wurden dabei nicht nur systematisch Straßenansichten abfotografiert, sondern gleichzeitig sämtliche drahtlosen Netzwerkverbindungen (W-LANs) registriert. Als dies Mitte Mai bekannt wurde, gab Google eine Stellungnahme ab, der zufolge „irrtümlicherweise" auch inhaltliche Daten aus unverschlüsselten Drahtlosnetzen aufgezeichnet wurden. Ein Irrtum, den Google seit 2007 in 34 Ländern betrieben hat. Es wurden seit drei Jahren in 34 Ländern W-LAN-Daten gesammelt, ohne dass dies jemandem aufgefallen sei? Die Skepsis von Datenschutzgremien sowie Medien ist verständlicherweise groß. In Österreich jedenfalls zog die Datenschutzkommission nach Bekanntwerden der Panne die

Notbremse. Die gesamte Datenanwendung Goolge Street View wurde untersagt, bis die besagte Speicherung von Daten aus Drahtlosnetzwerken, die nicht angemeldet war, geklärt ist. (ARGE DATEN / Österreichische Datenschutzkommission / Tzschentke 2010, S.20) Dieser Vorfall ist ein gutes Beispiel dafür, dass von vielen Global Playern oft prinzipiell erst einmal realisiert wird, was technisch machbar ist. Im Fall von Google Street View ging es drei ganze Jahre lang gut. Erst dann wurde bekannt, dass mehr aufgezeichnet wurde als angemeldet war. Dass nach Bekanntwerden dieses Fauxpas die österreichische Datenschutzkommission sofort reagierte und Googles Kamera-Autos in die Garage verbannte, zeigt, dass man sich nicht alles gefallen lassen muss und dass die Datenschützerinnen und Datenschützer nicht auf verlorenem Posten kämpfen. Das lässt hoffen.

4.4.2. Wirtschaftliche Interessen

Daten sind Geld. Produkte werden immer personalisierter an den Mann und die Frau gebracht, Werbung ist zielgruppenorientiert und Unternehmen erstellen Kunden-Profile, um deren Vorlieben zu erfassen. Darum ist die Wirtschaft an Daten interessiert. In den USA werden Nutzerdaten einer Person um sechs bis acht Dollar gehandelt. Das erscheint günstig. In Anbetracht der Größe von Netzwerken wie Facebook ist der Markt aber gewaltig. Der Handel mit Datensätzen floriert, denn Daten sind für Marketing-Zwecke Gold wert. (Semrad/Siebert/Pesendorfer 2010, S.37) Das ist auch der Grund, warum Plattformen wie StudiVZ oder Facebook zu horrenden Preisen verkauft werden. 2007 ließ es sich Microsoft 240 Millionen US-Dollar (168,6 Millionen Euro) kosten, um einen Anteil von 1,6 % an Facebook zu erhalten (Berger 2007). Plattformen wie Facebook stellen gigantische Daten-Sammlungen dar. Sie bieten einen Pool an potentiellen Kundinnen und Kunden, eine Liste mit unschätzbarem Informationsgehalt. Was jeder und jede von uns im täglichen Leben oft leichtsinnig von sich preisgibt, ist für die Werbewirtschaft bares Geld. Darum ist kein Geschäftsmann und keine Geschäftsfrau daran interessiert, den Trend zur Selbstveröffentlichung zu ändern. Und darum wird der Handel mit Daten immer größer.

Beachtet man, wie leichtfertig viele Menschen persönliche Daten online stellen, scheint es, als würde der Wert der eigenen Daten nicht erkannt. Was Daten tatsächlich wert sind, erfährt ein freizügiger Nutzer bzw. eine freizügige Nutzerin spätestens, wenn er oder sie die eigenen Daten wieder aus dem Internet entfernen möchte. Bis zu 10 € monatlich kann es kosten, das Netz dauerhaft nach dem eigenen Namen zu durchforsten – zuzüglich bis zu 30 € pro Löschung eines gefundenen Eintrages (ReputationsDefender / Saubere Weste). Da kann schnell ein Betrag von mehreren hundert Euro fällig werden, wenn beispielsweise ein Facebook-Mitglied, das auch andere Plattformen nutzte, auf Amazon einkaufte und eifrig in Foren und Blogs postete, seine Daten wieder aus dem Internet abziehen möchte.

Persönliche Daten sind also wertvoll. Trotzdem verhalten sich viele Userinnen und User nach dem Prinzip: „Meine Daten sind deine Daten." Sie teilen bereitwillig persönliche Informationen mit jedermann. Sie generieren Inhalte, ohne etwas dafür zu verlangen. Damit spielen sie den Internet-Riesen in die Taschen. Denn was von Millionen Internet-Nutzenden kostenlos an Inhalt generiert

wird, stellt für Unternehmen wie Google oder Facebook einen Riesen-Gewinn dar. Sie sammeln Daten und Informationen und ernten damit den finanziellen Profit, den viele andere säen.

4.4.3. Staatliche Eingriffe im Namen der Sicherheit

Wie bereits erwähnt, wurden nach den Terroranschlägen am 11. September 2001 viele Sicherheitsmaßnahmen verschärft – auf Kosten der Freiheitsrechte. „Ein Grundrechtsstandard, den wir als eine unserer größten Stärken betrachtet hatten, erschien plötzlich als Sicherheitslücke." bringen es Trojanow und Zeh auf den Punkt (2009, S.12). Staaten räumen der Sicherheit höhere Priorität ein als den bürgerlichen Freiheitsrechten und der Privatheit und die Bevölkerung nimmt die Einschränkungen der Privatsphäre zu Gunsten von vermeintlich mehr Sicherheit in Kauf. (Kuhlen 2004, S.175 / Schaar 2007, S.95f)

Der Staat fordert im Namen der Sicherheit mehr Kontrolle ein. Nicht nur in den Vereinigten Staaten werden die Sicherheitsbestimmungen strenger, auch in Europa bekommen Polizei und Geheimdienste mehr und mehr Befugnisse im plakativen „Krieg gegen den Terror". Es gibt Pläne zur Errichtung von zentralen EU-Datenbanken und Flugpassagierregistern (Trojanow/Zeh 2009, S.28), Nacktscanner sollen schon bald an allen internationalen Flughafen für größere Sicherheit sorgen (ebd. S.45), an die allgegenwärtige Videoüberwachung haben sich 61,5 % der Österreicherinnen und Österreicher bereits gewöhnt (Oekonsult 2010, S.11), Telefonüberwachungen sind zur Routine bei der Polizei-Arbeit geworden und seit dem Jahr 1997 sind Rasterfahndungen[6] in Österreich per Bundesgesetz erlaubt (BM.I Öffentliche Sicherheit 11-12/2001). Um ein Gesetz zur Erlaubnis von Online-Durchsuchungen[7] ist die Justiz redlich bemüht, und die Vorratsdatenspeicherung[8] steht auf Grund einer EU-Richtline unaufhaltsam auch in Österreich vor der Tür (Der Standard online, 6.11.2009). Zeger bezeichnet die Vorratsdatenspeicherung als den „Beginn präventivstaatlicher Maßnahmen" und sieht in Generalverdacht und Präventivüberwachung eine Gefahr für die Entwicklung der Gesellschaft. Alle

[6] **Rasterfahndung:** Daten werden automatisiert an Hand bestimmter Prüfmerkmale, die auf den (potenziellen) Täter vermutlich zutreffen, abgeglichen. Dabei werden polizeiliche Daten mit verschiedenen Datenbeständen bei nicht-polizeilichen Stellen verknüpft. Ziel ist es, die Personen mit tätertypisch bedeutsamen Merkmalen herauszufiltern. (Schaar 2007, S.128) In Österreich trat das Bundesgesetz zur Rasterfahndung am 1. Oktober 1997 in Kraft und wurde 2001 unbefristet verlängert. Die Fahndungsmethode wurde jedoch bis jetzt noch kein einziges Mal eingesetzt. (BM.I Öffentliche Sicherheit 11-12/2001)

[7] **Online-Durchsuchung:** Die Polizei oder ein Nachrichtendienst dringt unter Verwendung des Internetanschlusses in Rechner ein und installiert auf dem Computer der verdächtigen Person einen Trojaner, um sich Zugriff auf die dort gespeicherten Daten zu verschaffen. (Schaar 2007, S.120 / BM.I Öffentliche Sicherheit 1-2/2008, S.51)

[8] **Vorratsdatenspeicherung:** „Als Vorratsdatenspeicherung wird die präventive Erfassung des Telefonier- und Internetverhaltens der gesamten Bevölkerung aus sicherheitspolizeilichen Gründen verstanden." (Zeger 2010). Verkehrsdaten müssen laut EU-Richtline von 2006 verdachtsunabhängig von Telefonie- und Internetprovider mindestens sechs und höchstens 24 Monate gespeichert werden. Auch die E-Mail-Verbindungen und Standortinformationen von Mobiltelefonen werden gespeichert - nicht allerdings die Inhalte der Gespräche selbst. (Schaar 2007, S.116f / Hack 2009 auf ORF Futurezone)

Personen, die moderne Kommunikationsmittel nutzen, kommen automatisch in den Generalverdacht, diese missbräuchlich und für kriminelle Zwecke zu verwenden.

> „Die neuen Vorratsdatensammlungen stellen jedoch Bürger präventiv unter Generalverdacht. Erstmals seit Ende des DDR-Regimes wird in Europa die vorbeugende Datensammlung aller Bürger zu ausschließlich sicherheitspolitischen Zwecken installiert. Damit verlassen europäische Staaten die Grundsätze der Rechtsstaatlichkeit. Wesentlicher Teil dieser Rechtstaatlichkeit ist die Unschuldsvermutung und die Garantie solange unbeobachtet von polizeilicher Überwachung leben zu können, solange kein unmittelbarer Verdacht eines persönlichen kriminellen Fehlverhaltens besteht. Die Vorratsdatenspeicherung kehrt die Unschuldsvermutung um. Jeder Bürger muss in Zukunft rechnen, dass sein Internet- oder Telefonierverhalten ein verdächtiges Muster hat und er wird dann beweisen müssen, dass er zu Unrecht beschuldigt wird.“ (Zeger 2010)

Sieht man sich diese Entwicklungen an, kann man von einem Aufrüsten der Superlative sprechen. Politik und Justiz versuchen Daten zu sammeln, wo es nur möglich ist. Der Datenschutz wird durch immer mehr Ausnahmen ausgehöhlt, während die Exekutive immer mehr Rechte zugesprochen bekommt, Daten präventiv oder auf Grund von kleinen Verdachtsmomenten zu verwenden. Daten werden auf Vorrat gesammelt und damit viele Menschen erfasst, die in keinster Weise verdächtig sind. Dieses neue Verständnis von Sicherheit schränkt die Freiheitsrechte immer weiter ein.

Die Österreichische Gesellschaft für Datenschutz (ARGE DATEN) stellt Österreich in diesem Zusammenhang kein gutes Attest aus:

> „Österreich ist ein voll ausgebildeter Überwachungsstaat, unzählige Register und Evidenzen, die täglichen Forderungen von Politik und Bürokratie belegen dies. Der Weg zu einem Präventivstaat in dem jeder verdächtig ist, alles auf Vorrat aufzuzeichnen ist, wurde vehement befürwortet. Das Ende dieser Entwicklung, eine Scoringgesellschaft, in der jedes Verhalten bewertet wird, sodass am Ende nur mehr zwei Menschenklassen existieren, die VALIDs, mit gutem Scoring und die IN-VALIDs mit auffälligem Verhalten und schlechtem Scoring, ist absehbar. Die VALIDs erhalten raschen Zugang zum gesellschaftlichen Leben, bei ihnen wird in Zukunft Kontrolle reduziert werden, die INVALIDs, die Verdächtigen, werden vom wirtschaftlichen und gesellschaftlichen Leben zunehmend ausgeschlossen, müssen sich anhalten, kontrollieren lassen, erhalten weder Bankkonto, Kredit oder Sozialhilfe.“ (ARGE DATEN 2009)

Die Sicherheitsvorkehrungen greifen immer weiter in die Persönlichkeitsrechte der Bevölkerung ein. Dies wird legitimiert mit dem Argument der drohenden Gefahr. Sicherheit könne angeblich nur gewährleistet werden, wenn der Staat immer mehr Rechte und die einzelnen Bürgerinnen und Bürger davon immer weniger bekämen. Trojanow und Zeh treten zur Gegenargumentation an. Sie machen darauf aufmerksam, dass in Deutschland die Kriminalität im Bereich schwerer Delikte wie Mord, Totschlag und Vergewaltigung in den letzten Jahren kontinuierlich gesunken ist, während die Menschen von den Medien darauf gepolt werden, das Gegenteil zu denken. (2009, S.47) Auch in Österreich weisen die Statistiken eine stetig sinkende Kriminalität auf (siehe Kriminalstatistik 2009 des BM für Inneres). Und trotzdem glauben die Menschen, die Welt würde immer unsicherer

und ein Verzicht auf Privatsphäre sei nötig, um die drohenden Gefahren des Terrorismus, der Kriminalität und der Welt abzuwenden. Als zweites schlagendes Argument bringen Trojanow und Zeh vor, dass all die Vorkehrungen der europäischen Staaten bei Weitem nicht das halten, was sie versprechen. Sie erfüllen im Allgemeinen nicht den Zweck, für den sie eingeführt wurden. Videoüberwachung im öffentlichen Raum erhöht unabhängigen Studien zu Folge die Sicherheit kein bisschen. Die Kriminalität verlagert sich höchstens um ein paar Meter oder Häuserblocks. (Trojanow/Zeh 2009, S.60) Die Rasterfahndung wurde in Österreich am 1. Oktober 1997 eingeführt und sollte bei der Suche nach einem gefürchteten Briefbomber helfen. Zum Einsatz kam die Methode jedoch nicht, da der Täter Franz Fuchs gestellt werden konnte, noch bevor die Rasterfahndung aktiv war. Die Behörden betonen einen Zusammenhang zwischen der medialen Ankündigung der Rasterfahndung und dem Fang von Fuchs (Presseaussendung des BM für Inneres am 13.5.1998). Tatsache ist und bleibt jedoch, dass die Rasterfahndung in Österreich seit ihrer Einführung kein einziges Mal eingesetzt wurde. In Deutschland ist die Rasterfahndung seit April 2006 verboten. Die Online-Durchsuchung, die in Österreich noch auf eine gesetzliche Grundlage wartet, bekommt in Deutschland bereits ein vernichtendes Urteil ausgestellt. In dramatischen Fällen bringe sie nichts, flächendeckend sei sie verfassungswidrig. Mit diesem Argument wird die Nützlichkeit dieser Ermittlungs-Methode angezweifelt. (Trojanow/Zeh 2009, S.60) Auch biometrische Reisepässe können nur schwerlich im Kampf gegen den Terrorismus helfen, es ist nämlich kein einziger Fall bekannt, in dem Terroristen gefälschte Pässe bei sich hatten. (ebd. S.56) „Sicherheit lässt sich nicht herstellen, weil kein Risiko völlig ausgeschaltet werden kann.“ konstatieren Trojanow und Zeh (2009, S.48) und sehen in den ganzen Überwachungsszenarien nur einen Gewinner: den Staat und seine Kontroll-Lust.

4.4.4. Freizügigkeit

Die ersten drei beschriebenen Bedrohungen der Privatsphäre werfen ein schlechtes Licht auf Politik und Wirtschaft. Alle haben es auf unsere Daten abgesehen, niemand kümmert sich um unser schutzwürdiges Interesse. Es reicht jedoch nicht, mit dem Finger auf andere zu zeigen. In vielen Fällen sind die Personen selbst mit schuld, deren Daten gespeichert und weiterverarbeitet werden. Denn oft müssen Daten gar nicht heimlich von Computern gezogen oder mit ausgeklügelter Video-Technik ausspioniert werden. Vielmals geben Menschen ihre Daten ganz von alleine preis. Sie erteilen Auskunft über ihr Geburtsdatum, ihren Beziehungsstatus, ihren Beruf, sie füllen bereitwillig Fragebögen aus, um eine Kundenkarte im Supermarkt zu bekommen, sie kreuzen an, dass sie einverstanden sind, dass das Kaufverhalten bei jedem Einkauf gespeichert wird und sie geben Mail-Adresse und Telefonnummer an, um auch wirklich verständigt werden zu können, sollten sie beim Gewinnspiel gewonnen haben. Es gibt tausende Möglichkeiten, seine Daten weiterzugeben. Und viele von uns nutzen hunderte dieser Möglichkeiten, ohne sich den Kopf darüber zu zerbrechen.

So unzählig die Möglichkeiten der Datenverbreitung ohnehin schon sind, so schlagartig vermehrten sie sich noch, als das Internet die Privat-Haushalte eroberte. Mit einem Internet-Zugang sind die Möglichkeiten, Privates über sich preiszugeben und Daten aller Welt zugänglich zu machen schier unerschöpflich. Auf Twitter veröffentlicht man minutiös den eigenen Tagesablauf. Auf Facebook und MySpace tippt man Profil-Informationen ein, lädt die Fotos des letzten Urlaubs hoch und kommentiert fleißig die Aktivitäten anderer. In Foren postet man eifrig seine Meinung. Und für die Vorzüge des Online-Shoppings nimmt man gerne in Kauf, dass alle Einkäufe gespeichert und zu Analysen für zukünftige Produkt-Empfehlungen verwendet werden.

Es wäre also zu unkritisch, sich zurückzulehnen und zu fordern, die Privatsphäre müsse von anderen besser geschützt werden. Viele von uns müssen zuallererst bei sich selbst ansetzen. Der erste Schritt für mehr Privatsphäre und Datenschutz ist es, selbst auf die eigenen Daten besser Acht zu geben. Dazu gehört das Wissen, wie man die eigenen Daten im Zeitalter des Internets richtig schützt. Und der Wille, achtsam mit den eigenen Daten umzugehen, auch wenn man dafür vielleicht auf ein Gewinnspiel oder einen Treue-Kunden-Bonus verzichten muss.

Die hier beschriebene Freizügigkeit mit den eigenen Daten ist der Knackpunkt der vorliegenden Arbeit. Sie ist es, die Facebook groß gemacht hat. Die Auskunftsbereitschaft von Millionen Userinnen und User hat Facebook zu der Plattform gemacht, die sie heute ist. Facebook feiert so große Erfolge, weil Millionen Menschen weltweit freiwillig auf Privatsphäre verzichten. Spudich gibt den freizügigen Userinnen und Usern aus aller Welt einen Tipp mit auf den Weg ins Internet: „Sie haben das Recht zu schweigen. Alles, was sie posten, kann auch gegen Sie verwendet werden.“ (2010a, S.16)

In diesem Kapitel wurden die Gefahren für die Privatsphäre möglichst übersichtlich zusammengefasst. Für ausführliche Hintergrundinformationen und Beispiele empfiehlt sich eine Vertiefung in der Literatur. Es gibt aktuelle Werke, die zeigen, dass der Hut brennt. Durch und durch interessant und sehr lesenswert sind die Bücher von Trojanow & Zeh, Schaar, Zeger sowie Herbold, die alle herangezogen wurden, um für die vorliegende Arbeit einen Überblick über die aktuelle Datenschutz-Situation zu bekommen.

Die Homepages der ARGE DATEN sowie der österreichischen Datenschutzkommission bieten stets einen aktuellen Überblick über Geschehnisse, Neuerungen, Gerichtsbeschlüsse und auch Veranstaltungen zum Thema Datenschutz.

"I just think people are the most interesting thing. – Other people!"
Mark Zuckerberg 2002

5. Facebook

In den Kapiteln 2, 3 und 4 wurden die Konzepte des **Web2.0**, der **Selbstdarstellung** und der **Privatsphäre** vorgestellt. Diese drei Konzepte bilden das theoretische Fundament, auf dem die vorliegende Untersuchung aufbaut. Dass die drei Bereiche immer wieder Berührungspunkte haben, wurde an vielen Stellen bereits deutlich. Nun sollen die drei Ebenen zusammengeführt und auf den Untersuchungsgegenstand, die Social Network Site Facebook, umgelegt werden.

Mit über 400 Millionen Mitgliedern (Stand: Juni 2010) ist Facebook die Social Network Site mit den **meisten Mitgliedern** und belegt im Alexa-Ranking **Platz 2** in der Liste der weltweit **meistbesuchten Internet-Seiten**. Mehr Klicks pro Tag bekommt nur Google. Platz 3 bis 6 belegen YouTube, Yahoo!, Windows Live und Wikipedia. (Alexa Top Sites, Stand: 31. Mai 2010) Facebook spielt also ganz oben mit, an der Spitze des Web2.0 und kann sich zu den erfolgreichsten Web2.0-Unternehmen unserer Zeit zählen.

Facebook ist ein Soziales Online-Netzwerk (siehe Kapitel 2.4.2). Die registrierten Mitglieder stellen die Knotenpunkte des Netzes dar und sind mit beliebig vielen anderen Mitgliedern verbunden. Diese Verbindungen sind durch Freundeslisten besonders übersichtlich und leichter zu erkennen als in der Offline-Welt, in der Beziehungen zwischen Menschen für gewöhnlich nicht von vornherein graphisch dargestellt werden.

Ein Mitglied kann mit beliebig vielen anderen Mitgliedern verbunden sein. So baut sich jede Userin und jeder User ein ganz persönliches Netzwerk auf, in dessen Zentrum sie oder er selbst steht. Von diesem zentralen Punkt, dem eigenen Profil, können Verbindungen zu den verschiedensten Personen gehen. Facebook wird benutzt, um bestehende Beziehungen zu pflegen oder zu intensivieren und weniger, um neue Kontakte zu knüpfen (Boyd/Ellison 2007). In Österreich gaben bei einer Studie unter Studierenden 59 % aller Befragten an, der größte Vorteil von Social Network Seiten sei, dass man mit Freunden und der Familie Kontakt halten könne, 20 % sehen den größten Nutzen darin, alte Kontakte finden und erneuern zu können (Fuchs 2009). Die Mitglieder der Plattform spannen ihr Verbindungsnetz zu Personen aus den unterschiedlichsten Lebensbereichen: zu Arbeitskolleginnen und –kollegen, Freundinnen und Freunden, Familienmitgliedern, Leuten aus der Nachbarschaft, Mit-Studierenden oder auch Personen, zu denen man eine geschäftliche Beziehung hat. Im Schnitt pflegen Facebook-Mitglieder 90 bis 250 „Freundschaften" auf der Plattform. Mit so vielen Menschen gleichzeitig Kontakt zu halten, ist nur durch die Technologie des Online-Netzwerkes möglich. (Steinschaden 2010, S.17)

Dadurch, dass sich jedes Mitglied ein eigenes egozentriertes Netzwerk aufbaut, bilden sich innerhalb des großen Netzwerkes Facebook, das als unbegrenztes, totales Netzwerk bezeichnet

werden kann (Schenk 1995, S.14), Gruppen, die untereinander engere Verbindungen haben als zum Rest des Netzwerkes. Man kann sich Facebook als einen riesigen Topf voller unterschiedlicher Freundeskreise vorstellen – jeder Freundeskreis ist in sich dicht verwebt und überschneidet sich durch einzelne Personen an verschiedenen Stellen mit anderen Kreisen.

Selbstdefinition

Facebook bezeichnet sich selbst als Sozialen Dienst, der es Leuten ermöglicht, effizienter mit dem Freundeskreis, der Familie und Kolleginnen und Kollegen zu kommunizieren:

> "Founded in February 2004, Facebook is a social utility that helps people communicate more efficiently with their friends, family and coworkers. The company develops technologies that facilitate the sharing of information through the social graph, the digital mapping of people's real-world social connections. Anyone can sign up for Facebook and interact with the people they know in a trusted environment." (Facebook Pressebereich)

5.1. Entstehung & Entwicklung

2004 begann Mark Zuckerberg, ein amerikanischer Harvard-Student, ein Netzwerk zu entwickeln, das eigentlich nur für seine Universität gedacht war – es sollte eine Art Online-Jahrbuch werden, mit Fotos und Namen aller Studierenden. Zuckerberg erkannte, dass es interessant wäre, noch mehr Infos als nur Namen und Bilder zu veröffentlichen. Er wusste jedoch, dass man an weitere Daten nur käme, wenn die Leute diese selbst online stellten.

> "I just thought that being able to have access to different people's profiles would be interesting. (...) Obviously, there's no way you can get access to that stuff unless people are throwing up profiles, so I wanted to make an application that would allow people to do that, to share as much information as they wanted while having control over what they put up." (Zuckerberg in: Cassidy 2006, S.1)

Gemeinsam mit seinen Mit-Studenten Chris Hughes, Dustin Moskovitz und Eduardo Saverin kreierte Zuckerberg „Thefacebook", ein Netzwerk, in dem sich jeder und jede mit einer Harvard-Mail-Adresse registrieren konnte. Sie mailten eine Einladung zum neuen Netzwerk an alle Bewohner ihres Wohnhauses und die erste Handvoll Harvard-Studierender registrierte sich. Die Mitglieder der ersten Stunde schickten den Link an ihre Freunde weiter und diese erzählten es ihren Freunden und diese wiederum ihren Freunden. (Cassidy 2006) So wuchs das Netzwerk nach dem bekannten Schneeballsystem. – Und das tut es im Prinzip bis heute.

Im August 2005 bekam das Projekt den Namen „Facebook" und die Domäne www.facebook.com wurde erworben. Facebook wuchs stetig, nahm andere Universitäten und auch Schulen ins Netzwerk auf und wurde um immer neue Funktionen erweitert, wie beispielsweise der Möglichkeit, Fotoalben zu erstellen.

Im Dezember 2006 hatte das Netzwerk 12 Millionen aktive Nutzerinnen und Nutzer.

Im Mai 2007 wurde ein Meilenstein gesetzt: „Facebook Plattform" startete und verschaffte externen Sites und Anbietern über Applikationen Zugang zu den damals rund 25 Millionen Mitgliedern (Weigert 2008). Tausende Anwendungen bzw. die dahinter steckenden Akteure haben seither Zugriff auf die Daten der Mitglieder, sobald diese ihre Anwendungen wie beispielsweise ein Spiel, ein Horoskop oder ein Quiz nutzen.

Im Oktober 2007 verkaufte Mark Zuckerberg 1,6 % seiner Firma Facebook für 240 Millionen Dollar an den Software-Riesen Microsoft.

Im August 2008 erreichte Facebook die Mitgliedermarke von 100 Millionen. (Facebook Pressebereich)

Da Facebook immer größer und unübersichtlicher wurde, startete die Plattform 2009 eine abgespeckte Version: Parallel zum „normalen" Facebook wurde Facebook-Lite angeboten, das schlanker und unkomplizierter war und unter lite.facebook.com erreicht werden konnte. Die Lite-Version hatte 70.000 Fans, wurde aber im April 2010 sang- und klanglos wieder eingestellt.

Ein Grund dafür könnte sein, dass Facebook versuchte, allgemein übersichtlicher aufzutreten und somit die Lite-Version nicht mehr für notwendig erachtete. Im Februar 2010 wurde das Design von Facebook überarbeitet, es tritt seither schlanker auf als zuvor. (Die Presse online 21.4.2010)

Am 14. Jänner 2010 hatte Facebook nach eigenen Angaben über 350 Millionen aktive Userinnen und User. **Am 21. April 2010** waren es bereits über 400 Millionen[9]. Das entspricht einem Wachstum von über 14 % im Frühling 2010. (Facebook Pressebereich)

Die Hälfte der 400 Millionen Mitglieder loggt sich täglich auf Facebook ein und eine Umfrage in den USA ergab, dass 42 % der Facebook-Userinnen und –User jeden Morgen gleich als erste Aktivität die Plattform checken. Wiederum 15 % davon gaben an, dass es Facebook oder Twitter wären, von denen sie ihre News in der Früh bekämen. (Yarow/Angelova 2010)

Um das Netzwerk am Laufen zu halten, werden mehr als 1.000 Mitarbeiterinnen und Mitarbeiter beschäftigt. Mark Zuckerberg ist nach wie vor der CEO der Firma und trägt die Verantwortung für das Unternehmen. (Facebook Pressebereich) Tabelle 4 listet Statistiken zur derzeitigen Nutzung

[9] Zeger gibt zu bedenken, dass sich nicht nur reale Menschen auf Social Network Sites tummeln. Es gibt Profile für Unternehmen, Comic-Figuren oder Verstorbene, und es gibt für viele berühmte Personen mehr als nur ein Profil, wobei fraglich ist, ob überhaupt eines davon vom echten Star betrieben wird. Außerdem unterstellt Zeger den Social Network Seiten Identitätsvermehrung, um Content zu generieren. Darüber, wie hoch der Identitätsvermehrungsfaktor ist, gibt es allerdings keine zuverlässigen Angaben. Zeger hält ein Verhältnis von 1:10 bis 1:20 realistisch. Laut Zeger sagen die offiziellen Mitgliederzahlen einer Plattform also nur wenig aus und er generiert einen Faktor für die tatsächliche Community-Größe. Er argumentiert, wer sich einer Gruppe zugehörig fühle, solle zumindest alle zwei bis drei Wochen vorbeischauen und stellt auf Basis dieser Annahme folgende Berechnung an: Er nimmt die Zahl der Userinnen und User, die täglich online sind (dies sollten seiner Schätzung nach zwischen 5 und 10 % sein) und multipliziert sie mit 20. Das Ergebnis ist laut Zeger ein realistischer Indikator für die tatsächliche Mitglieder-Zahl einer Social Network Seite. (2009, S.74f) Bei Facebook lässt sich diese Gleichung nicht anwenden, da laut Angaben der Plattform-Betreiber nicht 5-10 % aller Mitglieder täglich online sind, sondern satte 50 %. Dies spricht entweder für eine tatsächlich sehr hohe Zahl an Mitgliedern oder aber für etwas manipulierte Zugriffszahlen.

von Facebook auf (Stand: April 2010). Die Zahlen sprechen Bände: Von den über 400 Millionen Mitgliedern aktualisieren 35 Millionen ihren Status täglich. Ein durchschnittliches Facebook-Mitglied hat 130 Freunde und ist Fan von 13 Seiten. Ein Viertel aller Mitglieder besucht Facebook via Handy und dieser Teil der User ist im Durchschnitt doppelt so aktiv auf der Plattform wie Mitglieder, die kein Facebook-Handy benutzen.

Tabelle 4: **Facebook-Statistik**

Company Figures

- More than 400 million active users
- 50% of our active users log on to Facebook in any given day
- More than 35 million users update their status each day
- More than 3 billion photos uploaded to the site each month
- More than 5 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc.) shared each week
- More than 3.5 million events created each month
- More than 1.5 million local businesses have active Pages on Facebook
- More than 20 million people become fans of Pages each day
- Pages have created more than 5.3 billion fans

Average User Figures

- Average user has 130 friends on the site
- Average user sends 8 friend requests per month
- Average user spends more than 55 minutes per day on Facebook
- Average user clicks the Like button on 9 pieces of content each month
- Average user writes 25 comments on Facebook content each month
- Average user becomes a fan of 4 Pages each month
- Average user is a member of 13 groups

International Growth

- More than 70 translations available on the site
- About 70% of Facebook users are outside the United States

Platform

- More than one million developers and entrepreneurs from more than 180 countries
- Every month, more than 70% of Facebook users engage with Platform applications
- More than 500,000 active applications currently on Facebook Platform
- More than 250 applications have more than one million monthly active users

Mobile

- There are more than 100 million active users currently accessing Facebook through their mobile devices.
- People that use Facebook on their mobile devices are twice more active on Facebook than non-mobile users.
- There are more than 200 mobile operators in 60 countries working to deploy and promote Facebook mobile products.

Quelle: Facebook Pressebereich, 21.4.2010

Dass sich Facebook großer Beliebtheit erfreut und die Nutzung von Social Network Seiten ungebrochen rapide steigt, wurde bereits mehrmals erwähnt. Bezeichnend ist aber auch, welchen

Stellenwert Social Online-Networks teilweise im Leben von Mitgliedern einnehmen. Welch skurrile Ausmaße der Besitz eines Facebook Profils annehmen kann, zeigte ein junges Pärchen in Joppa, Maryland in den USA. Das glückliche Paar hatte am Hochzeitstag im November 2009 die I-Phones dabei und zückte diese am Altar direkt nach dem Ja-Wort, um auf Facebook ihren Beziehungsstatus zu aktualisieren. Der etwas erstaunte Pfarrer kommentierte belustigt: „Oh, Dana is updating his relationship status on Facebook. (…) So as I was saying I now pronounce you husband and wife. It's official on Facebook, it's official on my book... Dana, you may kiss your bride." Unter dem Titel "At My Wedding Twitterring and Facebooking at the Altar" ist die Szene online auf YouTube zu bewundern – unter dem Gelächter der Hochzeitsgesellschaft. Diese Anekdote mag als Scherz geplant gewesen sein. Sie zeigt aber deutlich, in welch private Sphären Facebook bereits eindringt. Offensichtlich war für das junge Paar die Trauung erst offiziell, nachdem sie als solche auf Facebook durch die Änderung des Beziehungsstatus verzeichnet wurde. (YouTube)

5.2. Aufbau

Wie bereits beschrieben ist Facebook ein Netzwerk. Dementsprechend schwer lässt es sich auf Papier chronologisch beschreiben. Viel leichter erklärt ist es, wenn man vor einem Computer sitzt und sich durchklickt. Der Vollständigkeit halber wird trotzdem der Versuch unternommen, einen Überblick über den Aufbau zu geben.

Facebook setzt sich aus vielen verschiedenen Seiten zusammen. Die wohl wichtigsten sind dabei die **Profil-Seiten** der einzelnen Mitglieder. Jedes Facebook-Mitglied bekommt durch die Anmeldung eine solche Profil-Seite, die es mit Inhalten füttern kann. Das Layout kann man nicht verändern, wie es bei manchen anderen Social Network Sites üblich ist.

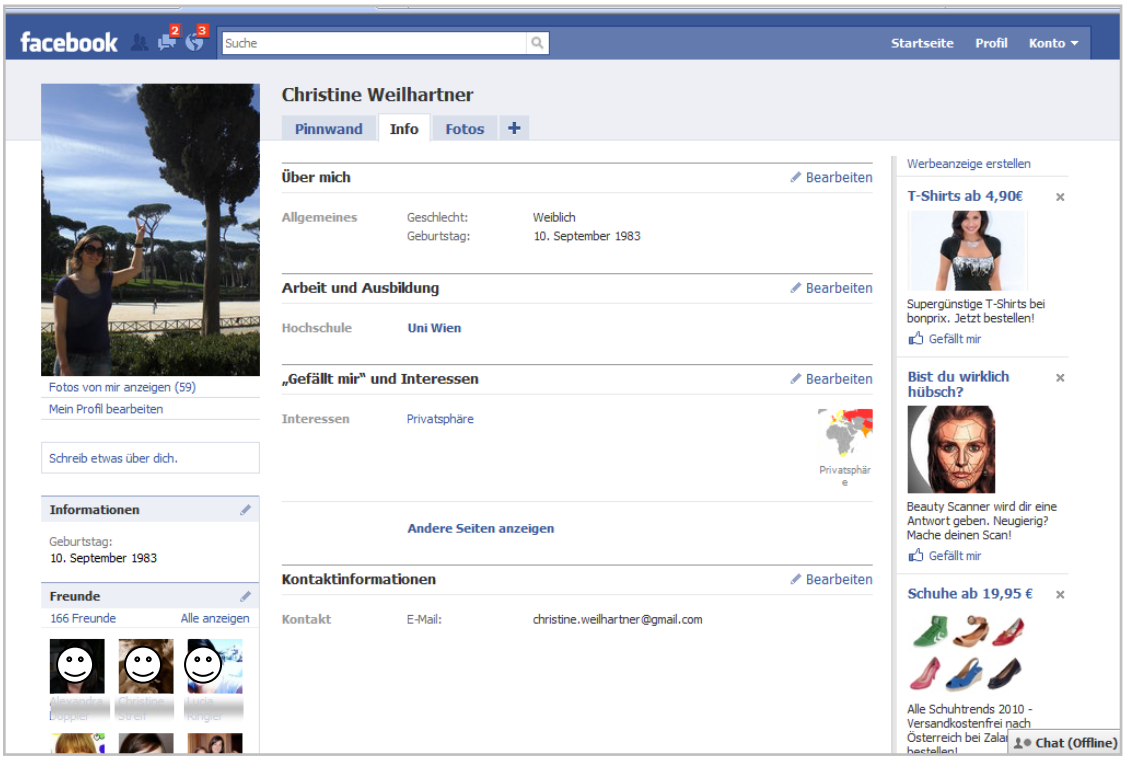
Abbildung 3 zeigt ein Beispiel einer Profil-Seite in der Info-Ansicht (ausgewählter Karteireiter oben: Info). Auf der linken Seite befindet sich das Profil-Foto, das man individuell hochladen kann. Darunter gibt es einen Link zu weiteren Fotos, eine Kurzfassung der allgemeinen Informationen über die Person (z.B. Geburtsdatum) und einen Link zur Liste aller Freunde, mit denen die Person verbunden ist. Im größeren rechten Teil finden sich Infos über das Facebook-Mitglied. In drei Kategorien können Inhalte erstellt werden: Unter **Allgemeine Informationen** können derzeitiger Wohnort, Heimatstadt, Geschlecht, Geburtsdatum, politische Einstellung, religiöse Ansichten, die eigene Biografie und Lieblingszitate angegeben werden sowie Auskünfte darüber, ob man an *Frauen* oder *Männern* interessiert ist und ob man auf der Suche ist nach *Freundschaft*, *Verabredungen*, *Feste Beziehung* oder *Kontakte knüpfen*. Unter **Information über Ausbildung und Arbeit** können Angaben zu Schule, Hochschule und Arbeitgeber gemacht werden inklusive genauer Details etwa über den Abschlussjahrgang, das Hauptfach oder die Länge des Dienstverhältnisses und die Position, die man innehat. Und unter **„Gefällt mir" und Interessen** schließlich kann man

seine Aktivitäten und Interessen eintragen sowie seine Vorlieben bei Büchern, Musik, Filmen und Fernsehen.

Unabhängig davon, was ein Mitglied in den verschiedenen Bereichen angibt, sind Datenschutzorganisationen schon alleine über die Art der Kategorien entsetzt. Sensible Daten wie religiöse Ansichten, die politische Einstellung oder die sexuelle Orientierung werden in einem Atemzug mit dem Geschlecht oder dem Musikgeschmack abgefragt. Die Beweggründe, warum jemand online seine politische Gesinnung und andere höchst sensible Informationen veröffentlichen möchte, sind fraglich. Tatsache ist jedoch, dass es Facebook mit dem Angebot an Kategorien zur Normalität macht, solch intime Informationen über sich zu offenbaren.

Die Inhalte können vom Profil-Inhaber bzw. der –Inhaberin jederzeit durch einen Klick auf den „Bearbeiten"-Button in der jeweiligen Kategorie geändert werden. Wer welche Inhalte sehen darf, kann individuell in den Privatsphäre-Einstellungen von Facebook festgelegt werden.

Abbildung 3: **Facebook Profil-Seite in der Info-Ansicht**



Quelle: http://www.facebook.com/home.php?#!/profile.php?id=1620027322&v=info

Neben der Info-Seite besitzt jedes Profil auch eine **Pinnwand**, auf der andere Facebook-Mitglieder Nachrichten hinterlassen können (siehe Abbildung 4). Die Pinnwand stellt außerdem eine Art Protokoll über die Aktivitäten des Profil-Besitzers bzw. der Profil-Besitzerin dar. Es wird unter anderem festgehalten, wenn das Mitglied eine Freundschaftsanfrage bestätigt, wenn es etwas kommentiert, ein Foto hochlädt oder auf einem Foto verlinkt worden ist. Die Pinnwand zeigt immer die letzten Aktionen an, in die der Profil-Besitzer bzw. die Profil-Besitzerin involviert war.

Abbildung 4: **Pinnwand auf einem Facebook-Profil**

Quelle: http://www.facebook.com/home.php?#!/profile.php?id=1620027322&v=wall

Wie Abbildung 3 und Abbildung 4 zeigen, ändert sich der Rahmen kaum, wenn man die Info-Seite oder Pinnwand aufruft. Am oberen Seitenrand steht immer ein Suchfeld zur Verfügung, in dem man nach anderen Mitgliedern oder auch Gruppen und Anwendungen suchen kann. Links daneben führen Shortcuts zu eventuell erhaltenen Freundschaftsanfragen oder Nachrichten sowie zu Benachrichtigungen, die man von Facebook erhalten hat. Gibt es Neuigkeiten in einer der Kategorien, werden die Buttons mit roten Fähnchen markiert. Rechts in der Menüzeile kann jederzeit zwischen dem eigenen Profil und der Startseite gewechselt werden. Unter dem Menüpunkt „Konto“ kommt man zu verschiedenen Einstellungen wie z.B. zu den Privatsphäre-Settings. Außerdem kann man sich hier von der Plattform ausloggen, wenn man seinen Besuch abgeschlossen hat. Im rechten Teil der Seite befindet sich immer eine Spalte mit Werbung, die man mit „Gefällt mir“ kommentieren kann. Und rechts unten im Eck hat man die Möglichkeit, mit Freunden zu chatten, die ebenfalls gerade online sind. Man kann sich entscheiden, ob man den anderen zeigt, dass man online ist, oder ob man den eigenen Status auf „offline“ setzt.

Loggt man sich als aktives Mitglied auf Facebook ein, kommt man zuerst nicht auf die eigene Profil-Seite, sondern auf die **Startseite**. Diese stellt einen News Feed aller Aktivitäten von Freunden dar – also quasi eine kollektive Pinnwand von allen, zu denen man eine Verbindung auf Facebook hat. Es wird auszugsweise angezeigt, was Personen, mit denen man auf Facebook befreundet ist, in letzter Zeit auf der Plattform getrieben haben. Wer seinen Status geändert, ein Fotos hochgeladen, oder einen Link gepostet hat, etc. Es kann zwischen zwei Ansichten unterschieden werden: Unter **Hauptmeldungen** werden nur „größere“ Aktivitäten angezeigt wie Status-Meldungen oder neue

Fotoalben, während unter **Neueste Meldungen** auch aufgelistet wird, wenn beispielsweise jemand etwas mit dem „Gefällt mir“-Button versehen oder jemand eine Veranstaltungseinladung angenommen hat.

Abbildung 5: **Startseite auf Facebook**

Quelle: http://www.facebook.com/home.php?#!/?ref=home

Befindet man sich auf der Startseite, werden links und rechts vom Aktivitäten-Stream Shortcuts angeboten. So kann man links zum Beispiel mit nur einem Klick zu den eigenen Nachrichten oder Fotos hüpfen, während rechts aufgelistet ist, welche der befreundeten Facebook-Mitglieder in nächster Zeit Geburtstag haben und welche Veranstaltungen anstehen.

Zusammenfassend lässt sich sagen, dass Facebook eine riesige Ansammlung von Verlinkungen ist. Man hat Verbindungen zu Freunden, ist auf Fotos verlinkt, kann mit einem Klick das Profil von anderen checken, findet dort vielleicht eine Gruppe, die einen interessiert, ist mit einem Klick auf der Gruppenseite und kann sich von dort weiterklicken im unendlich scheinenden Universum von Facebook. Hat man das Interesse am Pfad verloren, kommt man durch einen Klick rechts oben im Fenster auf die Startseite zurück und kann sich erneut auf die Suche nach Interessantem machen. Denn die nächste Attraktion ist oft nur einen Klick entfernt.

5.3. Facebook und Datenschutz

Die deutsche Verbraucherschutzorganisation „Stiftung Warentest“ veröffentlichte im April 2010 einen Testbericht zu Datenschutz bei Online-Netzwerken. Acht deutschsprachige Soziale Online-Netzwerke wurden auf ihre Organisation und Transparenz, auf den Umgang mit Nutzerdaten, die Datensicherheit, die Nutzerrechte, den Jugendschutz sowie Mängel in den AGBs untersucht. Dabei wurden bei Facebook „erhebliche Mängel“ festgestellt. Das vernichtende Test-Urteil lautete:

> „Schwachstellen in allen getesteten Bereichen. Besonders problematisch beim Umgang mit Nutzerdaten, den Nutzerrechten und in den AGB.“ (test 4/2010, S.43)

Facebook erzielte in allen Bereichen Minuspunkte. So wurden unter anderem die Datenschutzerklärung, die Zulässigkeit der Datenverarbeitung, die Weitergabe von Daten an Dritte oder das Jugendschutzmanagement negativ beurteilt.

Nach diesen erschreckenden Testergebnissen stellt sich die Frage, inwiefern Facebook gewissenlos mit Daten umgeht.

5.3.1. Rechtszuständigkeit

Durch das Internet kommt es rechtlich gesehen zu einer wesentlichen Zunahme von grenzüberschreitenden Sachverhalten. Internetverträge werden häufig über Staatsgrenzen hinweg abgeschlossen. Es stellt sich die Frage der anzuwendenden Rechtsordnung. (Janisch/Mader 2006, S.112)

Wenn man über Datenschutz im Zusammenhang mit Facebook spricht, muss eine grundsätzliche Unterscheidung getroffen werden:

Im Verhältnis zu Facebook gilt amerikanisches Recht. Hat man also das Gefühl, Facebook hätte gegen das Datenschutzgesetz verstoßen und die eigenen Daten missbräuchlich verwendet, muss man bedenken, dass nicht das österreichische Datenschutzgesetz zur Anwendung kommt, sondern das amerikanische. Dieses ist laut Expertenmeinung nicht mit österreichischem Recht zu vergleichen. In den Vereinigten Staaten ist man beim Konsumenten- und Datenschutz nicht annähernd so streng wie in Österreich. (Aichinger 2009)

Bei Sachverhalten zwischen Userinnen und Usern muss allerdings nicht zwangsweise das amerikanische Recht gelten. Kommt es zu datenschutzrechtlichen Streitigkeiten, die nicht Facebook, sondern entweder andere Userinnen oder User oder externe Dritte betreffen, muss der räumliche Anwendungsbereich geklärt werden. Wenn eine Handlung (Sendung, Vermittlung, Empfang) eindeutig Österreichbezug aufweist, kommt nationales Recht zur Anwendung. Für einen Rechtsträger mit Sitz in einem EU-Mitgliedstaat ist der Ort der Niederlassung maßgeblich für die Frage des anwendbaren nationalen Rechts. Hat der Rechtsträger seinen Sitz außerhalb der EU, ist

der Ort der Datenverarbeitung ausschlaggebend. Liegt dieser in Österreich, ist das DSG anwendbar. (Ghazal 2010, S.47) Handelt es sich bei der oder dem Betroffenen also um ein österreichisches Facebook-Mitglied und auch bei der beklagten Partei um eine Person oder ein Unternehmen mit einer Niederlassung in Österreich, kommt das österreichische Datenschutzgesetz zur Anwendung. Genauso, wenn die Daten eines österreichischen Facebook-Mitglieds in Österreich verarbeitet werden, auch wenn dies durch eine ausländische Institution geschieht.

5.3.2. Zeigt her eure Daten!

Prinzipiell ermöglicht jedes Facebook-Mitglied mit jeder einzelnen Veröffentlichung drei Parteien den Zugriff auf die eigenen Daten: der **Plattform Facebook**, die die Daten weiterverarbeiten kann und darf, dem eigenen **Netzwerk**, in dem sich Freundinnen und Freunde tummeln, in dem aber auch Fremde auf die eigenen Daten zugreifen können und **dritten Parteien**, die ganz ohne Zusammenarbeit mit der Plattform Zugriff auf die Daten erlangen können. (Gross/Acquisti 2005, S.3)

1. Facebook

Facebook sichert sich durch die AGBs allerlei Rechte an den Daten der Mitglieder. Jede Person, die sich auf Facebook anmeldet, geht mit Facebook einen Vertrag ein. Dieser Vertrag beinhaltet die **Datenschutzbestimmungen** von Facebook sowie **Rechte und Pflichten**. Wer ein Profil auf der Plattform erstellen will, muss – wie bei so vielen Online-Geschäften – durch einen Klick bestätigen, dass er die seitenlangen Geschäftsbedingungen akzeptiert. Damit werden Rechte an Facebook abgetreten, bei denen sich jeder Datenschützer die Haare rauft. Welche heiklen Stellen die Datenschutzrichtlinien von Facebook enthalten, wird in Kapitel 5.3.3 aufgelistet.

2. Netzwerk

Natürlich sind personenbezogene Daten auf Facebook dem eigenen Netzwerk zugänglich. Dabei spielt es eine große Rolle, wie man dieses Netzwerk definiert. Wie in Kapitel 4.3.2 ausgeführt, macht es einen großen Unterschied, ob man ein Facebook-Profil nur einem begrenzten Personenkreis zugänglich macht, oder ob man „alle“ die eigenen Daten sehen lässt. Facebook hat standardmäßig die Einstellungen sehr großzügig festgelegt. Es werden sehr viele Daten allen anderen zugänglich gemacht. Möchte man an den vordefinierten Settings etwas ändern, kann man in den Privatsphäre-Einstellungen regulieren, wer welche Inhalte sehen darf. Jedes Facebook-Mitglied ist gut beraten, von dieser Möglichkeit Gebrauch zu machen. Denn sobald Inhalte von „allen“ gesehen werden können, ist man nicht mehr gefeit davor, dass beispielsweise ein zukünftiger Arbeitgeber die Fotos der letzten feuchtfröhlichen Party durchklickt oder eine Firma die eigenen Hobbies für Werbezwecke ausschlachtet.

3. Dritte

Außenstehende Dritte haben die Möglichkeit, die Daten einzusehen und weiterzuverwenden, die „allen“ zugänglich gemacht wurden. Denn was „allen“ gezeigt wird, gilt als freiwillig veröffentlicht und unterliegt somit nicht dem Datenschutzgesetz. Was viele Userinnen und User zu unterschätzen scheinen, sind Anwendungen, die nicht von Facebook, sondern von externen Anbietern stammen. Spiele, Horoskope, etc. … die Liste der Unterhaltungsmöglichkeiten auf Facebook ist lang. Um sie zu nutzen, muss man zuerst einwilligen, dass die Anwendung auf die Profil-Informationen zugreifen darf. Ein kurzer Klick auf „Zulassen“ und schon sind einer Applikation Tür und Tor zu den eigenen Daten geöffnet. Und was noch schlimmer ist: Die Anwendung erfragt sich auch die Erlaubnis, auf Daten von Freunden zuzugreifen. Es bringt einem also wenig, selbst solche Anwendungen zu meiden wie die Pest, wenn Freunde ständig die Bewilligung zum Datenzugriff geben. Einmal mehr sei betont, wie wichtig es darum ist, seine Daten nicht „allen“ zugänglich zu machen, sondern sie mit restriktiven Privatsphäre-Einstellungen zu schützen.

Gross und Acquisti haben im Juni 2005 eine Studie unter 4.000 Facebook-Mitgliedern durchgeführt, die alle dem Netzwerk der Carnegie Mellon University angehören und kamen zu bezeichnenden Ergebnissen (2005, S.4ff): Ganz allgemein gesprochen veröffentlichen die Untersuchten eine riesige Summe an Informationen. 90,8 % der analysierten Profile enthalten ein Foto, 87,8 % geben das Geburtsdatum bekannt, 50,8 % geben den aktuellen Wohnsitz an und 39,9 % eine Telefonnummer. Diese Prozentsätze sind umso erschreckender, weil 89 % aller Profile unter dem realen Namen der Person liefen. In diesen Fällen können also ganz leicht die persönlichen Daten auf die Person zurückgeführt werden.

Neben diesem Trend zur Selbstoffenbarung konstatieren Gross und Acquisti, dass die Mitglieder von Facebook nur spärlich davon Gebrauch machen, die Privatsphäre-Einstellungen zu ändern. Die meisten nehmen sich nicht die Zeit, die Settings zu überprüfen und zu personalisieren, sondern belassen es bei den Voreinstellungen, die von Facebook vorgeschlagen werden. Somit werden die von Facebook veranschlagten Standard-Einstellungen umso wichtiger.

Und wie sieht es aus bei den Entscheidungsträgern von Facebook? Wird die Rolle des Datenschützers ernst genommen? Kritische Stimmen beantworten diese Frage mit einem klaren „Nein“. Auf Facebook gibt es ständig Neuerungen, das System wird weiterentwickelt und gleichzeitig ändert sich damit die Situation der Privatsphäre-Einstellungen. In welche Richtung diese Veränderungen weisen, scheint eindeutig: Die Datensammlung soll immer größer und umfangreicher werden. Der Chaos Computer Club, die größte deutsche Hacker-Vereinigung, nennt Facebook eine „Datenkrake“: „Wenn man erstmal drin ist, ist es eine Krake, die sich alles von den Nutzern holt.“ (CCC-Sprecher Rosengart in: Der Standard online, 6.4.2010)

Die Entwicklung zur Datenkrake

Im September 2006 änderte Facebook das Layout der Startseite. Seit damals wird jedes Mitglied auf Facebook nach dem Einloggen von einem **News Feed** begrüßt. Dieser News Feed listet auf, was Personen aus der Freundesliste in letzter Zeit auf Facebook gemacht haben, was sie gepostet haben, welche Fotos online gestellt wurden, welchen Gruppen sie beigetreten oder mit wem sie neu befreundet sind. All diese Informationen waren auch schon vorher auf Facebook öffentlich, sie waren jedoch um einiges weniger übersichtlich dargestellt. Was man vorher durch viele Klicks auf unterschiedlichen Facebook-Seiten erfahren konnte, wird fortan auf einen Blick von Facebook zusammengefasst. Facebook verstößt damit nicht gegen das Datenschutzgesetz. Trotzdem waren viele Mitglieder empört. Sie fühlten sich bloßgestellt, weil ihre Informationen mit einem Schlag um vieles sichtbarer waren als zuvor. (Boyd 2008, S.13f)

Im November 2009 kündigte Facebook an, eine strukturelle Änderung vorzunehmen. Auf Grund des beständigen Wachsens der Plattform wurden die **regionalen Netzwerke abgeschafft**. Mark Zuckerberg schrieb dazu in einem offenen Brief an alle Facebook-Mitglieder:

> Wir planen, „regionale Netzwerke ganz abzuschaffen und ein einfacheres Modell zur Kontrolle der Privatsphäre zu entwerfen. In diesem kannst du Inhalte dann ausschließlich für „Freunde“, „Freunde von Freunden“ oder „Alle“ sichtbar machen.“ (Zuckerberg 2009)

Zuckerberg hat also ein hehres Ziel: ein „einfacheres Modell zur Kontrolle der Privatsphäre“ zu generieren. Im Dezember 2009 wurden schließlich die **Privatsphäre-Settings** erneuert und im Zuge der Neuerung wurden alle alten Privatsphäre-Einstellungen nichtig. Alle Mitglieder mussten die Einstellungen neu eingeben. Und wer das nicht aktiv tat, wurde auf die Einstellungen zurückgesetzt, die Facebook als Standard deklarierte: Alle können alles sehen. Die Mitglieder wurden beim ersten Einloggen nach der Umstellung auf das neue System hingewiesen und konnten einem Link folgen, der zu den Sicherheitseinstellungen führte. Folgte man dem Link, wurde man gefragt, ob man die bisher vorgenommenen Einstellungen behalten wolle, oder ob alle Inhalte für alle sichtbar sein sollen. Die Voreinstellung war „alle“. Bei jedem, der dem Link also nicht folgte, wurden alle Einstellungen auf die von Facebook vorgeschlagene Option gesetzt, dass alle alles sehen können, ungeachtet der in der Vergangenheit getroffenen Einstellungen des Facebook-Mitglieds.

Kurze Zeit nach dem Einführen der neuen Sicherheitseinstellungen erklärte Facebook stolz, dass bereits 35 % der Nutzerinnen und Nutzer die Privatsphäre-Einstellungen geändert hätten. Das bedeutet gleichzeitig, dass **65 % aller Nutzerinnen und Nutzer** ihre Einstellungen nicht geändert und somit auf **„öffentlich“** festgelegt haben. (Boyd 2010) Als Erfolg von Zuckerberg als Ritter der Privatsphäre kann das wohl kaum verbucht werden. Ob es allerdings für Facebook selbst ein Erfolg ist, aus der Perspektive des Anzeigenplatz-Verkäufers oder des Datensammlers, das sei dahingestellt. Fakt ist, dass die Privatsphäre-Einstellungen weiterhin ein Dschungel blieben, in dem manche Punkte so versteckt waren, dass man sie erst nach langem Suchen fand. Zuckerberg wollte

allerdings dem Image eines Datenschutz-Gefährders nicht nachgeben. Er beharrte stets darauf, alles für die Facebook-Mitglieder zu tun, um deren Privatsphäre zu schützen.

Im April 2010 folgte die nächste Neuerung: Während bisher Facebook-Mitglieder „Fans" von Seiten, Gruppen, Filmen etc. werden konnten, kann eine Vorliebe von nun an durch ein einfaches Klicken auf den **„Gefällt mir"-Button** ausgedrückt werden. Facebook Manager Alex Li hofft, dass diese Aktion leichter fällt, als das Beitreten zu einer Seite als Fan. So soll der Umfang der Verknüpfungen auf den Seiten steigen. (Li in: Lischka 2010)

Künftig müssen Facebook-Mitglieder also nicht mehr eine Seite aufsuchen und ihr als Fan beitreten, wenn sie von etwas angetan sind, sondern sie klicken auf „Gefällt mir" und schon ist das, was ihnen zusagt, im eigenen Profil abgespeichert. Ein Spiegel-Redakteur urteilt kritisch:

> „Mit jedem Klick auf Dinge, die sie (Anm.: die Nutzerinnen und Nutzer) mögen, verfeinern sie ihr öffentliches Interessenprofil, das Facebooks Werbekunden zur Feinabstimmung von Anzeigen nutzen können." (Lischka 2010)

Diese Umstellung von einem „Fan"- auf einen „Gefällt mir"-Button war nur der Vorbote für ein viel größeres Projekt: Wenige Tage nach der Änderung wurde auf der Facebook Entwicklerkonferenz f8 der sogenannte „Open Graph" vorgestellt, eine Technologie, die es Facebook erlaubt, jede andere Webseite zu infiltrieren. In der Praxis bedeutet das, dass es den „I-like"- bzw. **„Gefällt mir"-Button in Zukunft auch außerhalb von Facebook** gibt. Im ganzen Internet können von nun an Inhalte wie Musik, Videos, Texte, Nachrichten aber auch Marken und Firmen mit dem Symbol des erhobenen Daumens bewertet werden. Worauf Facebook mit dieser Neuerung abzielt, ist klar: Es will auf jede Webseite. Mit jedem Klick auf fremden Internet-Seiten erfasst Facebook, was einem gefällt, speichert es als Profil-Information ab und lässt es in den eigenen Facebook-Stream einfließen. Somit ist eine ständige Verbindung zu Facebook gegeben, auch wenn die Plattform selbst nicht aufgesucht wird. Durch das Bewerten während des Internet-Surfens, liefern Userinnen und User wertvolle Daten, zum Beispiel welche Seiten beliebt sind und welche nicht. Damit erhält Facebook eine völlig neue Funktion – nämlich die einer Suchmaschine. Es kann von nun an seinen Mitgliedern Tipps geben und beliebte Restaurants, Events oder Autos vorschlagen. Die "Open Graph"-Technologie bringt Facebook eine unglaubliche Datenmenge zur Auswertung und Weitergabe. Webseiten-Betreiber erhalten im Gegenzug Zugang zur weltweit größten Online-Community und mit Web-Analytics-Tools auch Einsichten in das Benutzerverhalten ihrer Besucherinnnen und Besucher. (Steinschaden 2010, S.16 / Kapeller 2010 / Weigert 2010)

Facebook hat es also erneut geschafft, etwas zu generieren, das den Datenfluss auf der Plattform erhöht und den Wert auf dem Werbemarkt steigert.

All diese Entwicklungen weisen in dieselbe Richtung: Facebook soll größer werden, es sollen mehr und mehr Daten gesammelt werden und immer mehr Userinnen und User sollen immer mehr Inhalte immer öffentlicher machen. Die Mitglieder der Plattform lassen es weitgehend mit sich geschehen. Facebook ist noch immer im Wachsen und auch wenn die Medien auf Missstände aufmerksam machen, Datenschützer den Zeigefinger erheben und so manches Mitglied wachgerüttelt wird, schwimmt die breite Masse mit Facebook und nicht dagegen. Oder doch nicht?

Proteste … und Verbesserungen?

Fast jede Neuerung auf Facebook brachte eine Protestwelle mit sich. Einige klein und überschaubar, andere schon etwas größer. Das Thema Privatsphäre und Datenschutz wurde in letzter Zeit immer mehr von den Medien aufgegriffen. Allen voran natürlich die neuen Medien. So wird beispielsweise auf Blogs die Entwicklung von Social Network Sites verfolgt und Blog-Schreiberinnen und –Schreiber tun ihre Meinung kund, kritisieren und geben Ratschläge. Auf dem Blog SpreeSee wurde bereits im Juli 2009 eine Gebrauchsanleitung für Facebook gepostet, die genau beschreibt, wie man Profil-Informationen sicher verwalten kann. Die Anleitung wurde seit der Veröffentlichung nach jeder Entwicklung von Facebook aktualisiert. (SpreeSee 2009) Auch Hutter (2010) veröffentlichte in seinem Blog zu Social Media einen Leitfaden zur Facebook-Privatsphäre. Dies sind nur zwei Beispiele von vielen aus der virtuellen Welt.

Die Printmedien folgten dem Beispiel mit etwas Verzögerung. Der Spiegel brachte im Dezember 2009 eine Schritt-für-Schritt-Anleitung zur sicheren Verwaltung der Privatsphäre-Einstellungen (Lischka 2009). Außerdem sorgten Artikel wie das Testergebnis zu Sozialen Online-Netzwerken der Stiftung Warentest (2010) oder Beiträge im Wochenmagazin News oder in den Tageszeitungen Kurier, Der Standard und Die Presse für Aufmerksamkeit.

Neben dieser eher alltäglichen Berichterstattung provozierte Facebooks Umgang mit personenbezogenen Daten aber auch ganz andere Aktionen. So wurde beispielsweise die Plattform **We're quitting Facebook** ins Leben gerufen. Die Initiative forderte auf, kollektiv Facebook am 31. Mai 2010 zu verlassen und damit ein Zeichen zu setzen. Als Grund für die Protest-Aktion werden die unfairen Bestimmungen und der Umgang mit Daten von Facebook genannt:

> „Facebook gives you choices about how to manage your data, but they aren't fair choices, and while the onus is on the individual to manage these choices, Facebook makes it damn difficult for the average user to understand or manage this. We also don't think Facebook has much respect for you or your data, especially in the context of the future." (quitfacebookday.com)

Die Aktion sollte Facebook einen ordentlichen Hieb versetzen und schaffte es auch, einiges an Aufsehen in den Medien zu generieren. Bis 31. Mai hatten sich dann aber doch nur magere 34.425 Facebook-Mitglieder auf quitfacebookday.com registriert, um der Plattform kollektiv adieu zu

sagen. Nicht einmal jedes 10.000ste Mitglied wollte Facebook den Rücken zukehren. Bei den aktuellen Wachstumszahlen von Facebook kompensieren die Ausstiege am Quit Facebook Day wahrscheinlich gerade einmal die neuen Registrierungen des Tages.

Ob dergleichen Aktionen der größten Social Network Seite auf Dauer schaden können, wird sich weisen. Klar ist, dass Facebook eine harte Linie bezüglich der Datenschutzbestimmungen verfolgt und dass damit Proteste vorprogrammiert sind.

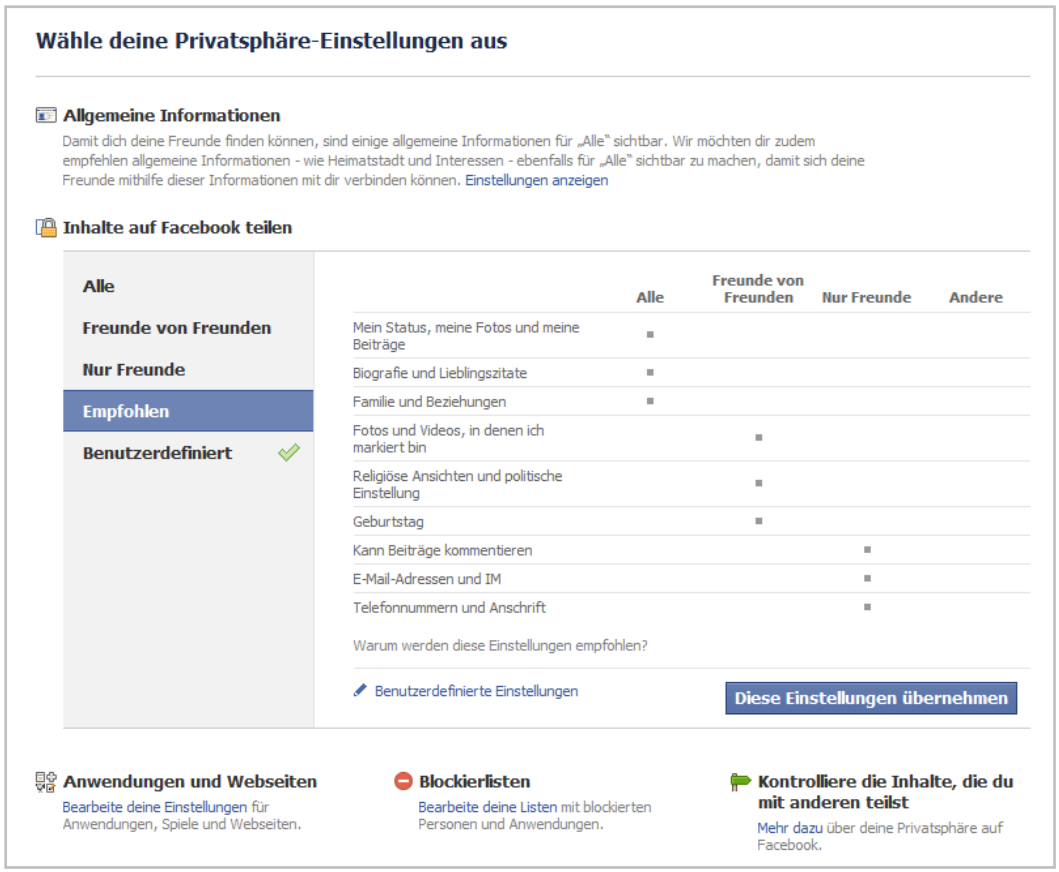
Vielleicht war es ja die Summe all dieser Proteste, die Facebook-Gründer Mark Zuckerberg dazu veranlasste, sich die Privatsphäre-Einstellungen nochmal durch den Kopf gehen zu lassen. Nachdem er gebetsmühlenartig wieder und wieder betont hatte, er wolle alles tun, um die Privatsphäre der Userinnen und User zu schützen, entschloss er sich schließlich dazu, den Bereich der Privatsphäre-Einstellungen auf Facebook neu zu gestalten. Offensichtlich war ihm der negative Tenor in den Medien doch zu laut geworden und er ging in die Offensive, um sein Image als Datenschützer zurückzuerobern. "The big takeaway is, don't mess with the privacy stuff for a long time." (Der Standard online, 27.5.2010) soll Zuckerberg zu einem Reporter gesagt haben und gesteht damit durchaus das Wissen ein, dass er die Facebook-Gemeinde ein wenig an der Nase herumgeführt hatte, was die Privatsphäre-Einstellungen betrifft. Doch nun wollte er ausziehen, um den Mitgliedern die volle Kontrolle über ihre Daten zu geben:

Nachdem er die Neuerung ein paar Tage vorher angekündigt hatte, wurde am 28. Mai 2010 der Privatsphäre-Bereich auf Facebook geändert – er wurde übersichtlicher und einfacher. Einstellungen, die man zuvor auf verschiedenen Seiten suchen musste, wurden zusammengefasst und auf einer umfassenden Seite gebündelt präsentiert. Inhaltlich änderte sich wenig an den Einstellungsoptionen. Der einzige inhaltliche Punkt bezog sich auf Seiten, von denen man Fan ist: Während zuvor diese Seiten als öffentliche Information gehandhabt wurden und immer sichtbar waren, kann man nun frei wählen, wer diese Seiten sehen darf. Ansonsten bleibt die Optionsauswahl in allen Punkten gleich, nur die Überschaubarkeit wird um ein Vielfaches verbessert. Übersichtlich auf einer Seite zusammengefasst, kann jedes Facebook-Mitglied nun mit wenigen Klicks alle Einstellungen in kurzer Zeit regeln. Expertinnen und Experten geht diese Maßnahme allerdings nicht weit genug und auch die Medien ätzen, dass die Änderung nicht das Werk eines wohltätigen Datenschützers sei, sondern dass es nur die Ausführung einer längst nötigen Vereinfachung wäre. Facebook behandelt weiter standardmäßig Informationen als öffentlich – daran ändern auch vereinfachte Optionen nichts. (Spiegel online, 26.5.2010)

Abbildung 6 zeigt, welche Einstellung Facebook seinen Mitgliedern empfiehlt. Ändert man seine Privatsphäre-Settings nicht manuell, können „alle" den eigenen Status, die erstellten Fotoalben und alle Beiträge sehen. Das führt soweit, dass Personen, die einem eine Freundschaftsanfrage geschickt haben, fortan den eigenen Status auf ihrer Startseite angezeigt bekommen. Auch wenn man die Freundschaftsanfrage noch nicht beantwortet hat. Manche Inhalte empfiehlt Facebook nur Freunde sowie Freunde von Freunden sehen zu lassen. Unter anderem fallen darunter sensible personenbezogene Daten wie religiöse Ansichten und die politische Einstellung. Belässt man es für

diese Inhalte bei Facebooks Standard-Einstellung „Freunde von Freunden“, können bei durchschnittlichen Freundeslisten von 130 Kontakten mit einem Schlag zigtausende Personen die eigenen Daten sehen. Nur bei E-Mail-Adresse, Telefonnummer und Anschrift hat Facebook standardmäßig eingestellt, dass diese nur Freunde sehen dürfen. Außerdem empfiehlt Facebook, dass nur Freunde Beiträge kommentieren können.

Abbildung 6: **Menü für Privatsphäre-Einstellungen auf Facebook**



Quelle: http://www.facebook.com/home.php?#!/settings/?tab=privacy&ref=mb

5.3.3. Facebooks Rechte

Facebook stellt eine riesige Datensammlung dar. Das Volumen dieser Daten ist nicht zu unterschätzen. Auf den Profilen finden sich E-Mail-Adressen, Geburtsdaten, Fotos, Hobbies, Gruppen-Mitgliedschaften, die Interessen dokumentieren, … und das ganze meistens unter dem eigenen Namen, sodass zu all den Informationen gleich die eigene Identität mitgeliefert wird.

Wie in Kapitel 4.3.2 dargelegt, besteht laut österreichischem Datenschutzgesetz kein schutzwürdiges Interesse mehr für sensible Daten, wenn diese offensichtlich selbst veröffentlicht wurden. Für Facebook bedeutet das, dass alle Mitglieder freiwillig auf Datenschutz verzichten, wenn sie persönliche Inhalte online stellen und diese „allen“ zugänglich machen.

Neben diesen gesetzlichen Regelungen sorgt auch Facebook selbst dafür, dass den Mitgliedern die Kontrolle über die Daten weitgehend abgenommen wird. Wie oben beschrieben gibt es zwar Privatsphäre-Einstellungen, in denen die Mitglieder verwalten können, wer ihre Inhalte sehen kann und wer nicht. Gleichzeitig erklärt man sich aber mit so mancherlei einverstanden, wenn man einen Facebook-Account erstellt. Man kann dies nämlich nur tun, indem man den AGBs zustimmt. Diese enthalten durchaus kritische Punkte. Im Folgenden werden einige Stellen aus den **Datenschutzrichtlinien** (Stand 28.4.2010) sowie aus der **Erklärung der Rechte und Pflichten** (Stand 28.4.2010) zitiert.

In der Erklärung der Rechte und Pflichten stellt Facebook klar, dass man der Plattform jegliche Rechte auf alle Inhalte überträgt:

> „Du erteilst uns eine einfache, übertragbare, unterlizenzierbare, unentgeltliche, weltweite Lizenz für die Nutzung aller IP-Inhalte, die du auf oder im Zusammenhang mit Facebook postest („IP-Lizenz"). Diese IP-Lizenz endet, wenn du deine IP-Inhalte oder dein Konto löscht, außer deine Inhalte wurden mit anderen Nutzern geteilt und diese haben sie nicht gelöscht."

Außerdem sollten sich Mitglieder bewusst sein, dass andere Facebook-Mitglieder die eigenen Daten benutzen können:

> „Dir ist bewusst, dass Informationen möglicherweise von anderen Nutzern kopiert oder weitergegeben werden können."

Wenn Facebook-Mitglieder Inhalte „allen" zur Verfügung stellen, wie es für viele Inhalte von Facebook vorgeschlagen und standardmäßig eingestellt wird, dann können diese Daten auch wirklich von **allen** eingesehen werden, nicht nur von anderen Facebook-Mitgliedern:

> „Wenn du die Einstellung „Alle" bei der Veröffentlichung von Inhalten oder Informationen verwendest, können alle Personen, einschließlich solcher, die Facebook nicht verwenden, auf diese Informationen zugreifen und sie verwenden und sie mit dir (d. h. deinem Namen und Profilbild) assoziieren."

In den Datenschutzbestimmungen wird der Punkt noch genauer ausgeführt:

> „Für „Alle" zugänglich gemachte Informationen sind öffentlich verfügbare Daten wie zum Beispiel dein Name, Profilbild und deine Verbindungen. Auf derartige Informationen kann beispielsweise jedermann im Internet zugreifen (auch Personen, die nicht bei Facebook angemeldet sind). Außerdem können diese Daten von Suchmaschinen Dritter indexiert sowie von uns und anderen ohne datenschutzbezogene Einschränkungen importiert, exportiert, weitergegeben und erneut weitergeleitet werden. Diese Informationen, einschließlich deines Namens und Profilbilds, können auch außerhalb von Facebook mit dir in Verbindung gebracht werden (…)."

Besonders kritisch zu betrachten ist die Tatsache, dass Facebook-Mitglieder ihre Daten frei zugänglich machen, wenn sie Anwendungen nutzen. Beteiligt man sich beispielsweise an einem

Spiel, lässt man sich ein Horoskop erstellen, oder nimmt man an einem Quiz teil, fließen die eigenen Daten ungestört an die Betreiberinnen und Betreiber der Anwendung:

> „Wie oben bereits erwähnt, sind die Anwendungen oder Webseiten, welche die Facebook-Plattform verwenden, weder Eigentum von Facebook noch werden sie von Facebook betrieben. Das bedeutet, dass du deine Facebook-Informationen für Personen außerhalb von Facebook verfügbar machst, indem du diese Anwendungen und Webseiten benutzt."

Damit nicht genug. Anwendungen können nicht nur auf die eigenen Informationen zugreifen, sondern auch auf die von Freunden:

> „Wenn du eine Verbindung zu einer Anwendung oder Webseite herstellst, wird dieser der Zugang auf allgemeine Informationen über dich gestattet. Der Begriff „Allgemeine Informationen" umfasst folgende Informationen von dir und deinen Freunden: Name, Profilbild, Geschlecht, Nutzerkennnummer, Verbindungen sowie alle Inhalte, die unter Verwendung der Privatsphäre-Einstellung „Alle" mit anderen geteilt werden. Wir können zudem Informationen über den Standort deines Computers oder Zugangsgeräts und dein Alter Anwendungen und Webseiten zur Verfügung stellen (…)"

Und natürlich kann Facebook nicht für das Verhalten von Anwendungen garantieren:

> „Du solltest dich immer gut über die Richtlinien von Anwendungen und Webseiten Dritter informieren, um sicher zu sein, dass du mit deren Nutzungsmöglichkeiten deiner Informationen einverstanden bist. Wir können nicht garantieren, dass sie unseren Richtlinien folgen."

Die Datenschutzrichtlinien, nach denen Facebook operiert, beinhalten die Erlaubnis personalisierter Werbung:

> „Wir geben Werbern die Möglichkeit, die Eigenschaften der Nutzer zu bestimmen, die ihre Werbeanzeigen sehen sollen. Wir dürfen die von uns erfassten nicht personenbezogenen Attribute (dazu gehören u. a. Informationen, die anderen Nutzern aufgrund deiner Entscheidung nicht angezeigt werden sollen, wie z.B. dein Geburtsdatum und andere sensible persönliche Informationen sowie Vorlieben) zur Auswahl der geeigneten Zielgruppe für derartige Werbung verwenden."

Zur Sammlung von Transaktionsdaten schreibt Facebook folgendes:

> „Gegebenenfalls speichern wird [sic!] die Einzelheiten über von dir auf Facebook durchgeführte Transaktionen oder Zahlungen."

Ein Stück weiter unten wird genauer ausgeführt, welche Informationen während der Interaktionen gesammelt werden:

> „**Informationen über Verhalten auf der Webseite.** Wir verfolgen einige deiner Handlungen auf Facebook, beispielsweise, wenn du Verbindungen hinzufügst (auch wenn du einer Gruppe beitrittst oder einen Freund/eine Freundin hinzufügst), ein Fotoalbum erstellst, ein

> Geschenk verschenkst, einen anderen Nutzer anstupst, zu erkennen gibst, dass dir ein Beitrag „gefällt“, an einer Veranstaltung teilnimmst oder eine Anwendung autorisierst. In manchen Fällen gilt es auch als Aktivität, wenn du uns Informationen oder Inhalte übermittelst. Wenn du zum Beispiel ein Video mit anderen teilst, dann kann es geschehen, dass wir zusätzlich zur Speicherung des tatsächlich hochgeladenen Inhalts auch die Tatsache protokollieren, dass du das Video mit anderen geteilt hast.
>
> **Zugriff auf Informationen von Zugangsgeräten und Browsern.** Wenn du über einen Computer, ein Handy oder ein anderes Gerät Zugriff auf Facebook zugreifst, sammeln wir u. U. von diesem Gerät Informationen über deinen Browsertyp, deinen Standort, deine IP-Adresse und die Seiten, die du besuchst.
>
> **Cookie-Informationen.** Wir verwenden „Cookies“ (kleine Dateneinheiten, die wir für eine längere Zeitspanne auf deinem Computer, Handy oder anderen Geräten speichern), um die Nutzung von Facebook zu vereinfachen, unsere Werbung zu optimieren und dich sowie auch Facebook selbst zu schützen. So speichern wir beispielsweise mithilfe von Cookies deine Anmeldekennnummer (aber unter keinen Umständen dein Passwort), um dir die nächste Anmeldung bei Facebook zu erleichtern. Außerdem verwenden wir Cookies, um zu verifizieren, dass du bei Facebook angemeldet bist, und um zu wissen, wann du mit Anwendungen und Webseiten der Facebook-Plattform, unseren Widgets und „Teilen“-Schaltflächen sowie unseren Werbeanzeigen interagierst. Du kannst die Cookies über deine Browsereinstellungen entfernen oder blockieren, aber in manchen Fällen kann dies die Nutzungsmöglichkeiten von Facebook einschränken.“

An anderer Stelle weist man auf die Risiken beim Informationsaustausch hin und stellt präventiv klar, dass Facebook nicht zur Verantwortung gezogen werden kann:

> „Obwohl wir dir die Möglichkeit bieten, den Zugriff auf deine Informationen über die Privatsphäre-Einstellungen einzuschränken, solltest du dir darüber im Klaren sein, dass keine Sicherheitsmaßnahme perfekt oder unüberwindbar ist. Wir haben keine Kontrolle über die Handlungen von anderen Nutzern, mit denen du deine Informationen austauschst. Wir können nicht garantieren, dass nur befugte Personen deine Informationen ansehen. Wir können nicht gewährleisten, dass Informationen, die du auf Facebook austauschst, nicht öffentlich zugänglich werden. Wir übernehmen keine Haftung, wenn Dritte Privatsphäre-Einstellungen oder Sicherheitsmechanismen auf Facebook umgehen.“

Dass es erlaubt ist, Inhalte auch außerhalb von Facebook zu verwenden, hält die Richtlinie zum Exportieren von Information fest:

> „Du (sowie alle, denen du Informationen zur Verfügung stellst) kannst mithilfe von Werkzeugen wie RSS-Feeds, Handy-Adressbüchern oder Funktionen zum Kopieren und Einfügen Informationen von Facebook sammeln und exportieren (und in einigen Fällen importieren), darunter auch deine Informationen sowie Informationen über dich.“

Wie schwer die eigenen Privatsphäre-Einstellungen tatsächlich zu kontrollieren sind, zeigt dieser Absatz der Datenschutzrichtlinien:

> „Wenn du Informationen in dem Profil eines anderen Nutzers veröffentlichst oder Beiträge von anderen Nutzern kommentierst, unterliegen diese Informationen den Privatsphäre-Einstellungen des anderen Nutzers."

Komisch mutet auch an, dass Daten ganz selbstverständlich an die USA weitergegeben werden.

> „Durch die Verwendung von Facebook stimmst du der Übertragung und Verarbeitung deiner persönlichen Daten in die bzw. den USA zu."

Die Geschäftsbedingungen und Datenschutzrichtlinien von Facebook sind lang und für den Laien fast undurchschaubar. So schön sie formuliert sein mögen, sie machen doch eine sehr unschöne Tatsache deutlich. Nämlich, dass jedes Facebook-Mitglied mit der Sekunde der Anmeldung die eigenen Daten der Öffentlichkeit preisgibt. Und zwar der totalen Öffentlichkeit. Nicht nur dem eigenen Netzwerk, das man sich auf der Plattform aufbaut, sondern buchstäblich jedem, der sich für die Daten interessiert. Die Privatsphäre-Einstellungen, die jeder Nutzer und jede Nutzerin personalisieren kann, sehen zwar schön aus und mögen auch eine gewisse Verbesserung zum einst ungeregelten Zustand sein. Die Datenschutzrichtlinien beinhalten aber, dass auch diese Einstellungen nicht vor Daten-Export und dergleichen schützen.

Jeder einzelne Nutzer und jede einzelne Nutzerin stimmt mit der Account-Erstellung den Facebook-eigenen Richtlinien zu und gibt somit die eigenen Daten frei. Auf die Rechte an den eigenen Daten wird durch die Einwilligung des angehenden Mitglieds freiwillig verzichtet.

Schaar weist darauf hin, dass echte Freiwilligkeit nur dann gegeben ist, wenn es wirkliche Alternativen gibt (2007, S.223). Will ein User oder eine Userin das Risiko nicht eingehen, dass Facebook die persönlichen Informationen weiterverwertet, dann gibt es nur eine Alternative: nicht Mitglied im Netzwerk werden. Das ist es wohl nicht, was Schaar mit einer „wirklichen Alternative" meint.

Der einzig wahre Schutz der Daten kann nur durch eines erreicht werden: das Vermeiden von öffentlichen Aufritten im Internet, **keine** Veröffentlichung von persönlichen Daten, **keine** Mitgliedschaft bei Facebook.

Der Blick in die Geschäftsbedingungen und die Datenschutzrichtlinien von Facebook machten deutlich, dass alles, was User und Userinnen auf Facebook über sich preisgeben, frei verwendet werden kann – sei es von Facebook selbst, von Anwendungen, die auf Facebook laufen, von anderen Facebook-Mitgliedern oder sogar von externen Personen, die mit Facebook nichts zu tun

haben. Es gibt kaum etwas, das Facebook nicht erlaubt ist, wenn es um die Verwertung der Mitgliederdaten geht.

Die Tatsache, dass Facebook-Mitglieder durch die Veröffentlichung ihrer Daten auf Datenschutz verzichten, öffnet der Wirtschaft Tür und Tor. Aus all den veröffentlichten Informationen können Wirtschafts-Füchse mögliche Zielgruppen erstellen, herauslesen, was die Vorlieben der Nutzer und Nutzerinnen sind und beispielsweise personalisierte Werbung verschicken. Personenbezogene Daten bekommen eine immer größere wirtschaftliche Bedeutung: Viele Marketingstrategien bauen darauf, die Kundschaft zu kennen und den Massenmarkt wieder zu individualisieren. Mit Hilfe der fortschreitenden Digitalisierung können leicht Daten aus dem Internet, Daten aus dem elektronischen Telefonverzeichnis oder Kundendaten von vorangegangenen Bestellungen verknüpft und umfassende Persönlichkeitsprofile angelegt werden. (Schaar 2007, S.188ff)

Aber nicht nur wirtschaftliche Unternehmen können von leichtfertig veröffentlichten Daten profitieren. Jeder, der sich ein Profil auf Facebook zulegt, kann frei über alle veröffentlichten Daten verfügen. So kann ein geübter Computernutzer eine Person ausfindig machen, die sowohl ihre E-Mail-Adresse als auch ihre Hobbies und vielleicht sogar ihre Telefonnummer online gestellt hat. Diese Daten können dann mehr als leicht missbräuchlich verwendet werden. Sie können aber auch ganz legal weiterverwendet werden. Etwa zum Erstellen von Statistiken oder um sie in eine Datenbank eingepflegt weiterzuverkaufen. Im Prinzip ist vom Gesetz her fast alles erlaubt: Der Profilbesitzer bzw. die Profilbesitzerin hat die Daten ja freiwillig veröffentlicht.

Zusammenfassung

Im Theorieteil der Arbeit wurden Konzepte vorgestellt, die wissenschaftlich relevant sind, wenn man sich dem Untersuchungsgegenstand Facebook widmet.

Das Web2.0 lieferte die technischen Voraussetzungen für das Entstehen von Social Network Sites wie Facebook. Es zeichnet sich dadurch aus, dass Userinnen und User Inhalte nicht mehr nur rezipieren, sondern auch selbst produzieren können. Auf Facebook, einer typischen Web2.0-Anwendung, ist genau das der Fall: Die Mitglieder speisen die Plattform mit Inhalten und bauen die Seiten quasi selbst auf. Sie tun das, um von den Gratifikationen der Teilnahme zu profitieren: Sie können mit Freunden und Bekannten in Kontakt bleiben, sich vernetzen und Beziehungen leichter pflegen, als es in dieser Fülle offline möglich wäre. Um das alles zu tun, legt man sich auf Facebook ein Profil an und präsentiert sich darauf selbst.

Der Mensch will naturgemäß von anderen positiv wahrgenommen werden und achtet bei der Selbstdarstellung darauf, im rechten Licht zu erscheinen. Das ist auch auf Facebook nicht anders. Jeder versucht, sich möglichst so darzustellen, wie er gerne gesehen werden möchte. Und zwar mittels computervermittelter Kommunikation, die sich in einigen wesentlichen Punkten von Face-

to-Face-Kommunikation unterscheidet. Beim Versuch, sich selbst bestmöglich zu präsentieren, vergessen viele Facebook-Mitglieder alles andere um sich herum. Inklusive der Privatsphäre, die sie mit ihrer Anmeldung bei Facebook auf's Spiel setzen.

Die Privatsphäre ist ein altes, viel umkämpftes Konstrukt, das den Menschen Privatheit und informationelle Selbstbestimmung gewährt. Gesetzlich verankert ist das Recht auf Privatsphäre im Datenschutzgesetz. In Österreich regelt das DSG 2000 den Datenschutz im Sinne des europäischen Rechtes. Doch die gesetzlichen Regelungen hinken an mancher Stelle den Entwicklungen hinterher und die Privatsphäre ist durch verschiedene Faktoren bedroht: durch den technischen Fortschritt, wirtschaftliche Interessen, staatliche Kontrolllust und nicht zuletzt durch die Freizügigkeit der Menschen. Auf Facebook kommt diese Freizügigkeit besonders zu tragen. Die Plattform baut förmlich darauf auf, dass Userinnen und User etwas über sich preisgeben und das unter ihrem richtigen Namen.

Facebook hat sich über die Jahre zur weltweit größten Social Network Seite entwickelt, hat 400 Millionen Mitglieder und stellt demnach eine riesige Datensammlung dar. Alle Entwicklungsschritte in den letzten Jahren gingen in dieselbe Richtung: Das Netzwerk wird größer und größer und mit ihm wächst die Datenbank. Für diese Datenbank nimmt sich Facebook alle Rechte heraus, die man sich nur vorstellen kann. Während zwischen Facebook-Mitgliedern die Frage der Rechtszuständigkeit zu klären ist, gilt im Bezug auf Facebook auf alle Fälle immer amerikanisches Recht, was es den Facebook-Betreibern leicht macht, mit den Daten große Gewinne zu machen.

Das Thema der Arbeit liegt am Puls der Zeit. Während der Literatur-Recherche und der Durchführung der Studie gab es ständig neue Medienberichte zum Thema, Aufschreie von Datenschutzorganisationen aber auch Neuerungen auf Facebook selbst. Die Arbeit wurde in einer Zeit verfasst, in der das Thema Facebook beinahe omnipräsent war und sich Medien sowie Gesellschaft in einem Prozess der Bewusstwerdung befanden. Bücher zum Thema Überwachungsstaat und Datenschutz erschienen, in Fernsehdiskussionen wurde über die Gefahr von Online-Netzwerken debattiert, Zeitschriften druckten Leitfäden für den Dschungel der Privatsphäre-Einstellungen, und Facebook verlautbarte fast im Monatstakt Neuerungen: Die Datenschutzbestimmungen wurden geändert, der Open Graph wurde vorgestellt und die Privatsphäre-Einstellungen wurden übersichtlicher gestaltet. Zur Zeit der Studie befand sich Facebook also einerseits im Kreuzfeuer der Aufmerksamkeit, andererseits in einer Phase des Umbruches. Es stellte eine große Herausforderung dar, alle aktuellen Geschehnisse ständig in die Arbeit einfließen zu lassen. Die Arbeit wurde so lange wie möglich aktualisiert und dokumentiert den Status Quo vom 7. Juni 2010.

EMPIRIE

6. Forschungsdesign

Die vorliegende Arbeit hat das Ziel, das Wissen über Datenschutz sowie das Selbstdarstellungs- und Privatsphäre-Verhalten von Facebook-Nutzerinnen und –Nutzern zu untersuchen. Die Beschäftigung mit der Literatur und dem aktuellen Forschungsstand brachte die Erkenntnis, dass das Konzept der Privatsphäre mit Web2.0-Anwendungen wie Facebook völliges Neuland betritt. Genauso erfährt das Konzept der Selbstdarstellung eine Erschütterung. Das Internet bietet Userinnen und Usern ungeahnte Möglichkeiten, was die Selbst-Präsentation betrifft. Aus diesem brisanten Themenkomplex sollen einige Details am Beispiel Facebook empirisch untersucht werden: Wie gut wissen Facebook-Mitglieder über Datenschutz Bescheid? Gibt es einen Zusammenhang zwischen Datenschutz-Wissen und der Freizügigkeit, mit der man sich auf Facebook präsentiert? Und beeinflusst das Wissen, das man über Datenschutz hat, wie man seine Privatsphäre-Einstellungen wählt? Auf diese Fragen sollen mit Hilfe eines dreistufigen Studien-Designs Antworten gefunden werden.

6.1. Forschungsstand

In den letzten Jahren wurden viele Studien veröffentlicht, die sich auf die eine oder andere Weise mit Social Network Sites befassen. Zu erforschen gibt es vieles: Gründe und Art der Nutzung, Auswirkungen von Social Network Sites auf zwischenmenschliche Beziehungen[10] oder die wirtschaftlichen Aspekte von Online-Netzwerken – um nur einige Ansatzpunkte für Studien zu nennen. In den Theorieteil der Arbeit flossen bereits an mehreren Stellen empirische Ergebnisse ein. Es wird nun ergänzend auf drei relevante Untersuchungen etwas näher eingegangen: auf die Studie „Social Networking Sites And The Surveillance Society“ von Christian Fuchs, Dozent an der Universität Salzburg; auf eine Studie von Sophos, in der auf Facebook 200 Freundschaftsanfragen an fremde Personen verschickt wurden; und auf eine aktuelle Oekonsult-Umfrage, die repräsentativ in Österreich zum Thema Datenschutz durchgeführt wurde.

[10] Den Beziehungen in Netzwerken widmet sich die Netzwerkforschung, die mittels Netzwerkanalyse soziale Netzwerke untersucht. (siehe z.B. Schenk 1995 oder Zerfaß 2008)

Fuchs 2009

Unter dem Titel "Social Networking Sites And The Surveillance Society" führte Fuchs im Zeitraum von Oktober bis Dezember 2008 eine Studie unter Salzburger Studentinnen und Studenten durch, die die Nutzung von StudiVZ, Facebook und MySpace im Zusammenhang mit elektronischer Überwachung untersuchte. (Fuchs 2009)

Die **forschungsleitenden Fragen** lauteten dabei:

1. What do students consider as the greatest opportunities of ISNS?
2. What do students consider as the greatest risks of ISNS?
3. How knowledgeable are students of the rise of a surveillance society?
4. How critical are students of the rise of a surveillance society?
5. How does the degree of knowledge about surveillance and the degree of critical consciousness on surveillance influence the usage of social networking sites?

Auf diese Fragen wurden mit Hilfe einer Online-Befragung Antworten gesucht. Es wurden 35 Fragen gestellt und unter anderem ein Index für das Wissen zum Thema Überwachung generiert. Die Studie brachte folgende Ergebnisse:

- Geschlecht, Klassenzugehörigkeit und Wohnsitz (in der Stadt oder im ländlichen Raum) beeinflussen das Wissen über Überwachung.
- Die Umfrage-Teilnehmerinnen stehen der Überwachung kritischer gegenüber als die Teilnehmer.
- Während die Befragten durchwegs kritisch gegenüber Bewachung eingestellt sind, ist ihr Wissen über das Thema eher gering.
- Je mehr Wissen Studierende zur Überwachung haben, desto kritischer stehen sie ihr gegenüber.
- Kommunikation ist der größte Nutzen, den Social Network Sites bringen: 59,1 % der Befragten nennen als größten Vorteil das Kontakthalten mit Freunden und der Familie. 29,8 % geben an, neue Kontakte zu knüpfen sei wichtig und 19,9 % nennen als größten Vorteil das Finden und Erneuern von alten Kontakten und Freundschaften.
- Als größte Gefahr bei der Nutzung von Social Network Sites sehen 55,7 % der Befragten die politische, ökonomische oder persönliche Überwachung als Folge von Datenmissbrauch, -weitergabe oder das Fehlen von Datenschutz.
- Studierende, die Social Network Sites oft benutzen, nehmen das Risiko der Überwachung in Kauf, obwohl sie sich der Gefahr bewusst sind. Die Vorteile scheinen die möglichen Nachteile zu übertreffen.

Die vorliegende Arbeit baut auf diese Ergebnisse auf. Fuchs' Resultate zum Wissen über Überwachung dienen als Grundlage für die Untersuchung des Wissens über Datenschutz. Anders als in Fuchs' Studie werden in der vorliegenden Arbeit nicht nur Studentinnen und Studenten

befragt, sondern ganz allgemein Facebook-Nutzerinnen und –Nutzer ohne berufliche Einschränkung.

Sophos 2007

Das internationale Unternehmen Sophos ist führend im Bereich der IT-Sicherheit und -Kontrolle. Es entwickelt und vertreibt Sicherheits-Software für Virenschutz, Datenschutz, Verschlüsselung, sowie Software gegen Spams, Phishing, Spyware und dergleichen mehr. (Sophos)

2007 führte Sophos eine Studie auf Facebook durch. Es sollte herausgefunden werden, wie viele Userinnen und User die Freundschaftsanfrage einer fremden Person bestätigen und dieser somit die eigenen Profildaten zugänglich machen.

Es wurde ein Facebook-Profil unter dem Namen „Freddi Staur“ erstellt – ein Anagramm für „ID Fraudster“ (auf Deutsch: ID-Betrüger). Die Profil-Seite wurde mit sehr spärlichen Angaben zur Person und dem Foto eines kleinen, grünen Frosches versehen (Abbildung 7). Mit diesem Profil wurde eine Freundschaftsanfrage an 200 Facebook-Mitglieder verschickt, die weltweit zufällig ausgewählt wurden. Im Anschluss wurde untersucht, wie viele Personen die Anfrage bestätigten und welche Informationen sie mit dem neuen „Freund“ teilten.

Abbildung 7
Quelle: www.sophos.com/pressoffice/news/articles/2007/08/facebook.html

Die Ergebnisse der Studie zeigen deutlich, wie freizügig Facebook-Mitglieder mit ihren Daten umgehen:

- 41 % der 200 Versuchspersonen akzeptierten Freddis Anfrage und gaben personenbezogene Daten preis.
- 72 % von Freddis neuen „Freunden“ veröffentlichten mindestens eine E-Mail-Adresse auf ihrem Profil.
- 84 % gaben ihren vollen Namen sowie ihr Geburtsdatum an.
- 87 % teilten Informationen über Ausbildung und Arbeitsplatz.
- 78 % gaben ihren derzeitigen Wohnort an.
- 23 % veröffentlichten ihre Telefonnummer.

Außerdem bekam Freddi im Großteil der Fälle Zugang zu den Fotos der Testpersonen sowie zu ihren Vorlieben und Hobbies.

Mit diesem Berg von Informationen können leicht personalisierte Werbe-Mails verschickt werden, oder schlimmer: Es können gezielte Phishing-Mails kreiert werden, um Passwörter von Personen auszuspionieren. Die wenigsten der Testpersonen würden die eigenen personenbezogenen Daten

wohl einem x-beliebigen Fremden auf der Straße geben. Freddi auf Facebook jedoch hatte keine Probleme, von 41 % der Stichprobe Zugriff auf die Daten zu bekommen.

Seit 2007 hat sich viel verändert auf Facebook. Nicht nur die Plattform selbst hat Neuerungen hinter sich. Auch die Diskussion rund um Facebook hat sich weiterentwickelt. Social Nework Sites werden nicht mehr nur als Segen gefeiert, sondern aufmerksam reflektiert. Datenschutz-Gremien zeigen Gefahren auf, Medien berichten kritisch. Es stellt sich die Frage, ob es dadurch zu einer Änderung im Bewusstsein der Nutzerinnen und Nutzer kam. Drei Jahre nachdem Freddi seine Fühler nach den Daten von Facebook-Mitgliedern ausstreckte, wird mit der vorliegenden Arbeit ein ähnlicher Versuch gestartet. Eine Studie soll zeigen, ob es noch immer so leicht ist wie 2007, sich auf Facebook mit fremden Personen anzufreunden.

Oekonsult 2010

Das Beratungsunternehmen Oekonsult führte im Auftrag der Austria Presseagentur österreichweit eine repräsentative Studie zum Thema Datenschutz durch (Oekonsult 2010). Bei der Umfrage wurde den Teilnehmerinnen und Teilnehmern zur Beantwortung jeder Frage eine sechsstufige Skala vorgelegt. Diese reichte von „völlige, uneingeschränkte Zustimmung zum vorgelegten Statement“ bis zu „absolute, zweifelsfreie Ablehnung des angeführten Statements“. Dazwischen lagen abgeschwächte Antwortmöglichkeiten wie „sehr hohe Zustimmung“ oder „tendenzielle Zurückweisung“. In Summe waren die ersten drei Antwortoptionen auf der Skala zustimmend, die letzten drei Möglichkeiten waren ablehnend. Bei der nun folgenden Präsentation der Ergebnisse beziehen sich die Prozentzahlen immer auf die Summe der drei Kategorien. Heißt es beispielsweise 81,2 % aller Befragten stimmen einer Aussage zu, dann bedeutet das, dass 81,2 % völlig, sehr oder zumindest tendenziell zustimmen.

Die wichtigsten Ergebnisse für die vorliegende Arbeit:

- 91,6 % messen einem wirksamen Schutz der Daten eine außerordentlich hohe Bedeutung bei in einer Zeit, in der Computer und elektronischer Datenverkehr eine große Rolle spielen.
- 89,6 % fordern harte, wirksame und abschreckende Sanktionen für große Firmen, die unrechtmäßig Personendaten erlangt oder verarbeitet haben.
- 85 % sehen sich selbst ziemlich machtlos, wenn es um die Durchsetzung des individuellen Datenschutzes gegenüber Großunternehmen geht.
- 81,6 % gestehen ein, nicht genau zu wissen, wer aller über die eigenen personenbezogenen Daten verfügt.
- 76,7 % denken nicht, dass sie alles in ihrer Macht stehende tun, um die eigenen Personendaten wirksam zu schützen.
- 92,7 % wünschen sich, dass AGBs in Zukunft verständlicher formuliert werden.

- 82,1 % stimmen der Aussage zu, dass Soziale Netzwerke im Internet (wie Facebook) nicht vorrangig das Ziel haben, Nutzen und Unterhaltung zu bringen, sondern dass das primäre Ziel die Erlangung der Nutzerdaten zu kommerziellen Zwecken ist.
- 57,7 % geben an, die Datenschutz-Materie sei einfach zu kompliziert und wollen sich damit nicht belasten.
- Am knappsten geht die Entscheidung zum Thema Google aus: Der Aussage „Mir persönlich ist es gleichgültig, wenn Google für die kostenlose Nutzung seiner Dienste gleichzeitig möglichst viele meiner Personen- und Verhaltensdaten sammelt." stimmen 54,9 % zu, 44,8 % widersprechen ihr.

91,6 % aller Befragten halten Datenschutz also für wichtig. Es stellt sich unweigerlich die Frage, warum die restlichen 8,4 % dies nicht tun. Außerdem erschreckt die Zahl derer, die selbstkritisch eingestehen, nicht genug für den Schutz der eigenen Daten zu tun. Der Großteil der Befragten gibt sich zwar aufgeklärt, weiß, dass Social Network Seiten nur Datensammeln im Sinn haben, will Sanktionen für Groß-Unternehmen, die Daten verwenden und fordert verständlichere AGBs. Trotz alldem schützen sie die eigenen Daten nicht ausreichend und wissen das auch. Vielleicht hängt es mit der gefühlten Machtlosigkeit zusammen. Oder mit der Komplexität des Themas. Immerhin 57,7 % gaben ja an, sich mit der Sache nicht belasten zu wollen.

Die Studie zeigt deutlich, dass Handlungsbedarf besteht. Einerseits sind sich die Österreicherinnen und Österreicher der Bedrohungen bewusst. Andererseits fühlen sie sich machtlos, haben keinen Überblick, wer auf die eigenen personenbezogenen Daten aller zugreifen kann und wollen sich dem Problem Datenschutz nicht stellen.

Diese Ergebnisse können als Grundlage für die vorliegende Studie dienen, in der das Datenschutz-Wissen von Facebook-Nutzerinnen- und Nutzer ermittelt wird.

6.2. Forschungsfragen und Hypothesen

Aus der bearbeiteten Theorie werden drei zentrale Forschungsfragen abgeleitet und Hypothesen gebildet.

F1: Wie gut kennen Facebook-Nutzerinnen und -Nutzer die datenschutzbezogenen Rechte, die bei einer Facebook-Mitgliedschaft zum Tragen kommen?

Forschungsfrage 1 befasst sich mit dem Datenschutz-Wissen von Facebook-Mitgliedern. Wie in Kapitel 5.3.1 dargestellt, gibt es im Zusammenhang mit Facebook unterschiedliche Rechtszuständigkeiten. Die Hypothesen werden darum differenziert für das österreichische Datenschutzgesetz und die Datenschutzbestimmungen von Facebook formuliert.

H1.1: Weniger als die Hälfte aller Facebook-Mitglieder kennt die Grundlagen des österreichischen Datenschutzgesetzes.

H1.2: Weniger als die Hälfte aller Facebook-Mitglieder kennt die Datenschutzbestimmungen, denen sie auf Facebook zustimmt.

F2: Gibt es einen Zusammenhang zwischen Wissen über Datenschutz und den Faktoren Privatsphäre-Sorgfalt und Selbstoffenbarung?

Forschungsfrage 2 zielt ab auf eine mögliche Abhängigkeit des Privatsphäre- und Selbstdarstellungsverhaltens vom Datenschutz-Wissen. Es wurden vier spezifische Faktoren definiert, die als abhängige Variablen der unabhängigen Variable „Datenschutz-Wissen" gegenübergestellt werden sollen.

H2.1: Je besser Userinnen und User über Datenschutz Bescheid wissen, desto sorgfältiger gehen sie mit den Privatsphäre-Einstellungen auf Facebook um.

H2.2: Je besser Userinnen und User über Datenschutz Bescheid wissen, desto weniger geben sie über sich selbst auf ihrem Facebook-Profil preis.

H2.3: Je besser Userinnen und User über Datenschutz Bescheid wissen, desto weniger häufig setzen sie Aktionen auf Facebook.

H2.4: Je besser Userinnen und User über Datenschutz Bescheid wissen, desto weniger Inhalte machen sie „allen" zugänglich.

F3: Wie großzügig geben Facebook-Mitglieder ihre Daten Personen preis, mit denen sie nicht befreundet sind?

Forschungsfrage 3 fragt nach dem Verhalten von Facebook-Mitgliedern gegenüber fremden Personen auf Facebook.

H3.1: Nicht alle Facebook-Mitglieder regulieren ihre Privatsphäre-Einstellungen so, dass nur Freunde ihre Profil-Inhalte sehen können.

H3.2: Viele Facebook-Mitglieder geben ihre Daten großzügig preis, indem sie Freundschaftsanfragen bestätigen, auch wenn sie eine Person nicht kennen.

6.3. Untersuchungsgegenstand

Untersuchungsgegenstand der Studie ist die Social Network Seite Facebook. Sie bietet ihren Mitgliedern die Möglichkeit, Beziehungen zu pflegen und mit Freunden und Bekannten Kontakt zu halten. Im Rahmen der Selbstdarstellung auf Facebook geben die Nutzerinnen und Nutzer oft sehr Persönliches von sich preis. Dabei gerät leicht in Vergessenheit, dass das Internet keinem Kaffeekränzchen gleicht. In der vorliegenden Studie wird das Verhalten von Facebook-Mitgliedern bezüglich der Selbstdarstellung und des Privatsphäre-Verhaltens untersucht. Der Untersuchungsgegenstand Facebook wurde in Kapitel 5 ausgiebig beschrieben.

6.4. Grundgesamtheit und Stichprobe

Grundgesamtheit

Für die Untersuchung relevant sind alle Facebook-Mitglieder, für die das österreichische Datenschutzgesetz gilt – demnach alle Personen, die ein Facebook-Profil haben und in Österreich leben. Da es zur Registrierung auf Facebook nicht nötig ist, seinen Lebensmittelpunkt anzugeben, ist diese Grundgesamtheit schwer zu beziffern. Einen Anhaltspunkt liefert die Zahl der österreichischen Facebook-Mitglieder: Am 21. April 2010 nutzten 1.982.120 Österreicherinnen und Österreicher Facebook (digitalaffairs.at).

Stichprobe

Da es sich bei der Grundgesamtheit um eine besondere Population handelt, die nicht genau fassbar und durchnummerierbar ist, konnte keine Zufallsstichprobe gezogen werden.

Untersucht wurde eine **Ad-hoc-Stichprobe**, auch genannt Gelegenheitsstichprobe (Bortz/Döring 2002, S.261). Die Teilnehmerinnen und Teilnehmer wurden auf verschiedenen Wegen zur Teilnahme an der Studie animiert: durch Nachrichten auf Facebook, durch E-Mails sowie durch diverse Foren.

Da Facebook darauf abzielt, sehr viele und unterschiedliche Menschen zu erreichen, wurde auch in der Stichprobe eine möglichst große Vielfalt angestrebt. Es sollte ein Querschnitt mit Männern und Frauen, Menschen in allen Altersklassen, Personen mit unterschiedlichen Bildungsniveaus und unterschiedlichen Heimatorten gebildet werden. Um dies zu gewährleisten, wurde ein **geschichtetes Schneeballprinzip** in Gang gesetzt. Zwölf Personen wurden nach demographischen Schichtungsmerkmalen ausgesucht. Sie wurden als Eckpunkte des Schneeballverfahrens kontaktiert und um die Verbreitung der Umfrage gebeten. Die Merkmalsaufteilung unter den zwölf Personen ist in Tabelle 5 zusammengefasst.

Tabelle 5: **Demographie der 12 Startpersonen für die Umfrage**

Geschlecht		Alter		Ausbildung	
Weiblich	6	bis 20	3	Pflichtschule	1
Männlich	6	21 bis 30	4	Lehre	3
		31 bis 40	4	Matura	4
		41 bis 50	3	College	1
		51 bis 60	1	Hochschule	3

6.5. Dreistufiges Studiendesign

Um die aufgestellten Hypothesen überprüfen zu können, wurde ein Methoden-Mix angewandt.

Im ersten Schritt wurde ein standardisierter **Online-Fragebogen** eingesetzt um herauszufinden, was Facebook-Nutzerinnen und –Nutzer über ihre Rechte und die österreichischen Datenschutzbestimmungen wissen und wie sie mit der Privatsphäre auf Facebook umgehen.

Im Anschluss wurden die Facebook-Profile der befragten Userinnen und User einer **Inhaltsanalyse** unterzogen, die aufzeigte, welche Inhalte die Facebook-Mitglieder ohne Einschränkung öffentlich zugänglich machen.

Zuletzt wurde mit einem **Experiment** erhoben, wie leicht oder schwierig es ist, an die Daten von unbekannten Personen zu kommen: An die untersuchten Profile wurde mit einem eigens erstellten Profil eine Freundschaftsanfrage geschickt und erhoben, wie viele Personen eine Fremde in die Freundes-Liste aufnehmen und ihr somit Zutritt zu den eigenen Profil-Inhalten gewähren.

6.5.1. Online-Fragebogen

Die Online-Befragung ist eine Erhebung, bei der „die Befragten den bei einem Server abgelegten Fragebogen im Internet online ausfüllen“ (Atteslander 2008, S.156). Sie kann nur zur Befragung von Personen eingesetzt werden, die elektronisch erreichbar und im Umgang mit dem Internet geübt sind, ist aber ansonsten mit anderen Arten der Befragung vergleichbar.

Wie bei der schriftlichen Befragung muss auch der Online-Fragebogen sorgfältig ausgearbeitet und präzise formuliert werden. Die Teilnehmerinnen und Teilnehmer müssen informiert werden, wer für die Befragung verantwortlich ist, welchen Zweck die Untersuchung verfolgt und dass alle Daten vertraulich behandelt werden. Die Fragen müssen dem Zweck entsprechend gewählt und verständlich und eindeutig formuliert werden, da die Befragten keine Möglichkeit haben, nachzufragen. (Atteslander 2008, S.136ff)

Für die vorliegende Untersuchung wurde ein Fragebogen mit hauptsächlich geschlossenen Fragen erarbeitet, da diese besser vergleichbare Antworten liefern. Der Fragebogen wurde bewusst auf die wesentlichen Fragen reduziert, um die Abbruchrate gering zu halten. Er umfasste in der finalen Version 31 Fragen, für deren Beantwortung knappe zehn Minuten nötig waren. Dafür waren die meisten Fragen als Pflichtfragen konzipiert, um vollständige Datensätze zu gewährleisten.

Facebook stellt einen sehr dynamischen, sich ständig verändernden Untersuchungsgegenstand dar. Der Fragebogen ging am 12. Mai 2010 online und bezieht sich darum auf den Stand von Facebook im Mai 2010.

Die Umfrage wurde mittels LimeSurvey online gestellt, einem freien Anbieter für Online-Umfragen (LimeSurvey). Sie war mit einem Gewinnspiel gekoppelt, das einen Anreiz zum Mitmachen bieten sollte. Alle Teilnehmerinnen und Teilnehmer hatten am Schluss des Fragebogens die Möglichkeit, ihren Facebook-Namen bekannt zu geben, um an der Verlosung eines 50 € Niedermeyer- und eines 30 € dm-Gutscheines teilzunehmen.

Fragebogen-Aufbau

Der Fragebogen diente dazu, die ersten beiden Forschungsfragen zu beantworten. Die **Operationalisierung** der Forschungsfragen sah folgendermaßen aus:

F1: Wie gut kennen Facebook-Nutzerinnen und -Nutzer die datenschutzbezogenen Rechte, die bei einer Facebook-Mitgliedschaft zum Tragen kommen?

Zur Beantwortung von F1 wurde in Anlehnung an Fuchs (2009) ein **Datenschutz-Index** erstellt: Es wurden **acht Datenschutz-Fragen** formuliert. Für jede gab es drei Antwortmöglichkeiten von denen eine korrekt war. Die richtige Antwort wurde mit 1 codiert, die beiden falschen Antworten jeweils mit 0. Außerdem hatten die Teilnehmerinnen und Teilnehmer die Möglichkeit, „Ich habe absolut keine Ahnung." auszuwählen, wenn sie die Frage nicht beantworten konnten. Diese Antwortmöglichkeit wurde ebenfalls mit 0 codiert.

Der Datenschutz-Index hatte somit eine **Skala von 0 bis 8**: 0 stand für Personen, die über gar kein Wissen zum Thema Datenschutz verfügten und alle Fragen falsch beantworteten. Den Maximal-Wert von 8 erreichten Personen, die alle Datenschutz-Fragen korrekt beantworten konnten.

Der Inhalt und die Formulierung der Fragen wurden mit einem Juristen sowie mit der Datenschutz-Expertin der AK Wien abgeklärt.

Für wie öffentlich hältst du deine Daten auf Facebook?

- □ Was ich auf Facebook veröffentliche, kann nur innerhalb von Facebook gesehen werden.
- □ Was ich auf Facebook veröffentliche, kann überall im Internet auftauchen.
- ✓ Was ich auf Facebook veröffentliche, kann im Internet sowie außerhalb des Internets auftauchen.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Schützt das österreichische Datenschutzgesetzt deine Daten auf Facebook?

- □ Das österreichische Datenschutzgesetz besagt, dass meine auf Facebook veröffentlichten Daten geschützt sind.
- ✓ Das österreichische Datenschutzgesetz schützt Daten, die ich auf Facebook nur begrenzten Personenkreisen zugänglich mache.
- □ Nach den Bedingungen des österreichischen Datenschutzgesetzes sind Daten, die ich auf Facebook stelle, nicht geschützt.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Diese Frage war eine der kniffligsten, da schwer einzuschätzen ist, was vor dem Gesetz als „begrenzter Personenkreis“ gilt und ab wann eine Gruppe von Leuten zu groß ist, um als begrenzt zu zählen. Es gibt bis jetzt keinen ausjudizierten Fall, in dem ein Facebook-Mitglied sein Recht auf Datenschutz eingeklagt hat mit dem Argument, seine Daten nur Facebook-Freunden zugänglich gemacht zu haben. Ob es vor dem Gesetz als Veröffentlichung gilt, wenn man seine Inhalte 200 Freunden zeigt, oder ob in diesem Fall noch immer von einem begrenzten Personenkreis zu sprechen ist, wird man erst mit Gewissheit sagen können, wenn es einen Präzedenzfall gibt. Nach derzeitigem Wissen und der Einschätzung der Datenschutz-Expertin Zimmer gilt die Freundesliste auf Facebook als beschränkter Personenkreis, egal wie viele Mitglieder sie enthält. Darum ist bei der oben genannten Frage Antwort 2 richtig und nicht Antwort 3.

Welche deiner Daten dürfen von Facebook weiterverwendet werden?

- ✓ Facebook darf alle Daten, die ich auf Facebook stelle, verwenden.
- □ Facebook darf die Daten weiterverwenden, die ich "allen" zugänglich mache, nicht aber Daten, deren Privatsphäre-Einstellungen ich beschränke.
- □ Facebook darf nur meine allgemein verfügbaren Daten weiterverwenden (= Name, Profilbild, Verbindungen).
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Darfst du laut österreichischem Datenschutzgesetz die Daten anderer Facebook-Mitglieder verwenden?

□ Ich mache mich strafbar, wenn ich Daten weiterverwende, die von anderen auf Facebook veröffentlicht wurden.
✓ Die Daten auf Facebook werden von den Mitgliedern freiwillig veröffentlicht, darum darf ich sie kopieren und verwenden.
□ Daten, die von anderen auf Facebook veröffentlicht wurden, darf ich laut österreichischem Datenschutzgesetz nur verwenden, wenn ich vorher den Urheber gefragt habe.
□ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Was passiert mit deinen Daten, wenn du deinen Facebook-Account löschst?

□ Wenn ich mich von Facebook abmelde, werden meine Daten automatisch gelöscht.
□ Wenn ich mich von Facebook abmelde, kann ich beantragen, dass meine Daten gelöscht werden.
✓ Wenn ich mich von Facebook abmelde, bleiben meine Daten gespeichert.
□ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Welche deiner Daten dürfen von befreundeten Facebook-Mitgliedern verwendet werden?

✓ "Facebook-Freunde" dürfen nur Daten weiterverwenden, die ich "allen" zeige.
□ "Facebook-Freunde" dürfen keine meiner Daten weiterverwenden.
□ "Facebook-Freunde" dürfen die Daten, die ich ihnen auf meinem Profil zeige, weiterverwenden.
□ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Welche deiner Daten dürfen von Dritten (= Personen, mit denen du nicht auf Facebook befreundet bist) weiterverwendet werden?

✓ Dritte dürfen Daten verwenden, die ich "allen" zugänglich mache.
□ Dritte müssen mich vorher fragen, bevor sie meine Daten verwenden.
□ Dritte dürfen meine Daten nicht weiterverwenden.
□ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Welche Daten speichert Facebook von dir?

□ Facebook speichert die Inhalte, die ich veröffentliche (Fotos, Kommentare, Links, etc.)
□ Facebook speichert meine Verbindungsdaten (wann ich welche Aktion setze, von welcher IP-Adresse ich mich einlogge, etc.).
✓ Facebook speichert beides: die veröffentlichten Daten und die Verbindungsdaten.
□ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

F2: Gibt es einen Zusammenhang zwischen Wissen über Datenschutz und den Faktoren Privatsphäre-Sorgfalt und Selbstoffenbarung?

Für die Beantwortung von F2 wurde als unabhängige Variable der eben dargestellte Datenschutz-Index verwendet. Dieser wurde mit den abhängigen Variablen **Privatsphäre-Index**, **Selbstoffenbarungsintensität** und **Selbstoffenbarungshäufigkeit** in Verbindung gebracht.

Privatsphäre-Index

Für die Variable „Privatsphäre-Sorgfalt" wurde ein Index ähnlich dem Datenschutz-Index generiert. Die Umfrage enthielt sechs Fragen zum Privatsphäre-Verhalten auf Facebook. Die Antwortmöglichkeiten waren von 0 (für besonders leichtsinniges Verhalten) bis 2 (für große Sorgfalt) codiert. Wusste jemand nicht, wie er seine Privatsphäre-Einstellungen geregelt hatte, wurde dies als Desinteresse bewertet und ebenfalls mit 0 codiert. Der Privatsphäre-Index hatte somit eine **Skala von 0 bis 12**.

Selbstoffenbarung

Für die **Selbstoffenbarungsintensität** wurde abgefragt, in welchen Kategorien auf dem Profil Informationen eingetragen wurden.

	Ja, in dieser Kategorie stehen Angaben.	**Nein, in dieser Kategorie steht nichts.**
Derzeitiger Wohnort	□	□
Heimatstadt	□	□
Beziehungsstatus	□	□
Interesse an (Männern, Frauen)	□	□
Auf der Suche nach (Freundschaft, Verabredungen,…)	□	□
Politische Einstellung	□	□
Religiöse Ansichten	□	□
Interessen	□	□
Anschrift	□	□
Handy-Nummer	□	□

„Ja" wurde mit 1 codiert, „nein" mit 0. Das ergab eine **Skala von 0 bis 10**.

Für die **Selbstoffenbarungshäufigkeit** wurde abgefragt, welche Anwendungen auf Facebook wie oft genutzt werden.

Anwendung	sehr oft	häufig	manchmal	selten	nie
Ich aktualisiere meinen Status	□	□	□	□	□
Ich schreibe auf die Pinnwand anderer	□	□	□	□	□
Ich veröffentliche Fotos	□	□	□	□	□
Ich poste Links	□	□	□	□	□
Ich kommentiere etwas durch den „Gefällt mir"-Button	□	□	□	□	□
Ich nutze Applikationen (Quiz, Glücksnuss, FarmVille, etc.)	□	□	□	□	□

Pro Anwendung wurde die Häufigkeit von 0 (nie) bis 4 (sehr oft) codiert. Das ergab eine **Skala von 0 bis 24**.

Neben diesen Indizes für Datenschutz-Wissen, Privatsphäre-Sorgfalt und Selbstoffenbarung wurden im Fragebogen außerdem einige allgemeine Daten zur Facebook-Nutzung erhoben, die deskriptiv ausgewertet wurden, sowie auch soziodemographische Angaben zur Stichprobenbeschreibung.

Durchführung

Der Fragebogen wurde durch einen Pre-Test von 15 Personen hinsichtlich Verständlichkeit und Vollständigkeit der Antwortmöglichkeiten geprüft. Nach einigen Verbesserungen und Ergänzungen ging die Umfrage online und war **von 12. Mai bis 4. Juni 2010** abrufbar unter dem Link: http://www.unet.univie.ac.at/~a0406572/umfragen/index.php?sid=79131&lang=de-informal.

In diesem Zeitraum nahmen **451 Personen** an der Umfrage teil. 37 brachen den Fragebogen vorzeitig ab. 414 Datensätze waren vollständig.

Von den 414 Personen gaben 30 an, kein Facebook-Profil zu haben. 3 hatten ihren Lebensmittelpunkt nicht in Österreich.

Die verbleibenden **381 Datensätze** wurden herangezogen, um die Hypothesen zu überprüfen.

6.5.2. Inhaltsanalyse

> „Die Inhaltsanalyse ist eine empirische Methode zur systematischen, intersubjektiv nachvollziehbaren Beschreibung inhaltlicher und formaler Merkmale von Mitteilungen, meist mit dem Ziel einer darauf gestützten interpretativen Inferenz auf mitteilungsexterne Sachverhalte." (Früh 2007, S.27)

Diese Definition nach Früh kann auf die geplante Inhaltsanalyse umgelegt werden: Die zu untersuchenden „Mitteilungen“ fanden sich auf Facebook-Profilen, untersucht wurden sie auf formale Merkmale hin – nämlich innerhalb welches Facebook-Bereiches sie veröffentlicht wurden.

Die Inhaltsanalyse wurde als nonreaktive Querschnittsstudie durchgeführt (Döring 2003, S.209f), in der erfasst wurde, welche Inhalte Userinnen und User allen anderen Registrierten auf Facebook uneingeschränkt zugänglich machen. Analyseeinheiten waren die einzelnen Facebook-Profile der Stichprobe. Bei diesem formal-deskriptiven Ansatz (Früh 2007, S.44) ging es nicht um den veröffentlichten Inhalt selbst, sondern nur um die Gattung des Inhaltes. Es wurde beispielsweise erfasst, ob auf einem untersuchten Profil die Pinnwand-Einträge sichtbar sind, nicht aber, *was* auf der Pinnwand steht.

Wie im Theorieteil erörtert (Kapitel 4.3.2 & 5.3.2), ist es auf Facebook besonders heikel, Daten online zu stellen ohne zu beschränken, wer die Inhalte sehen kann. Alle Daten, von denen man in den Privatsphäre-Einstellungen festgelegt hat, dass sie von „allen“ eingesehen werden können, sind unbeschränkt für jedermann zugänglich. Es können sowohl andere Facebook-Mitglieder darauf zugreifen, als auch Anwendungen, die man benutzt und sogar teilweise Personen, die nicht auf Facebook aktiv sind. Problematisch ist dabei, dass Facebook standardmäßig alle Inhalte „allen“ zugänglich macht. Erst wenn man sich durch die Privatsphäre-Einstellungen klickt, kann man manuell die Zugänge ändern und beschränken.

Mit Hilfe der Inhaltsanalyse wurde in der vorliegenden Studie erhoben, welche Inhalte die Umfrage-Teilnehmerinnen und –Teilnehmer öffentlich zugänglich machen. Die Ergebnisse wurden mit einer Häufigkeitsanalyse (Bortz/Döring 2002, S.151) ausgewertet und dienen der **Überprüfung von H3.1**: „Nicht alle Facebook-Mitglieder regulieren ihre Privatsphäre-Einstellungen so, dass nur Freunde ihre Profil-Inhalte sehen können.“

Die Kategorien zur Untersuchung ergaben sich aus den Kategorien, in denen man auf Facebook Inhalte veröffentlichen kann. Eine Kategorie wurde mit 1 codiert, wenn sie Inhalte aufwies. 0 wurde codiert, wenn die Kategorie nicht sichtbar war.

In Anlehnung an Gross und Acquisti (2005, S.6) wurde für die Codierung der Fotos eine Unterscheidung hinsichtlich der Erkennbarkeit der Person getroffen.

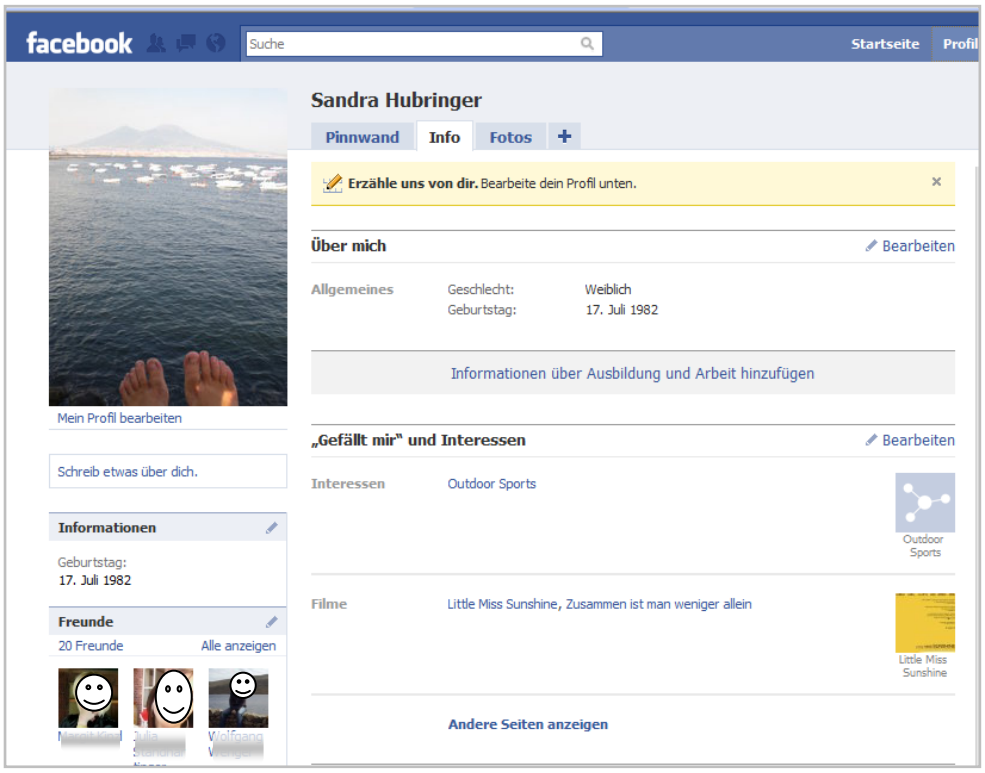
0 – kein Foto
1 – Foto, auf dem die Person eindeutig zu identifizieren ist
2 – Foto, auf dem eine Person zu sehen aber nicht eindeutig erkennbar ist
3 – Gruppenfoto, auf dem mehrere Personen als Profil-Inhaber in Frage kommen
4 – kein personenbezogenes Foto (Comic, Gegenstand, etc.)

Durchführung

Um am **Gewinnspiel** teilzunehmen, konnten die Umfrage-Teilnehmerinnen und –Teilnehmer am Ende des Fragebogens ihren Facebook-Namen hinterlassen. Diese Namen wurden herangezogen, um die Profile zu untersuchen. Von den 188 Namen, die angegeben wurden, konnten 154 auf Facebook eindeutig identifiziert werden.

Um herauszufinden, welche Inhalte auf den untersuchten Profilen für „alle" sichtbar sind, wurde ein **Fake-Profil** erstellt: Als Name für die imaginäre Profil-Besitzerin wurde *Sandra Hubringer* gewählt – ein Name, zu dem auf Facebook kein Profil gefunden wurde, Google keine Ergebnisse lieferte und es auf gmx.at noch keine Mail-Adresse gab. Als Profilfoto diente eine Landschaftsaufnahme, auf der nur die Zehen einer Person zu sehen sind. In den Kategorien Aktivitäten und Interessen wurden einige wenige Informationen angegeben. (siehe Abbildung 8)

Abbildung 8: **Fake-Profil von Sandra Hubringer**



Quelle: http://www.facebook.com/home.php?

Da sie zu Beginn noch mit niemandem auf Facebook befreundet war, konnte Sandra als „fremdes" Facebook-Mitglied die Profile der Versuchspersonen aufsuchen und nachsehen, welche Inhalte öffentlich zugänglich sind.

Von den 154 Profilen wurden 126 mit der Suchfunktion gefunden. 28 Personen hatten ihre Privatsphäre-Einstellungen so konfiguriert, dass ihr Profil in der Trefferliste nicht auftaucht.

Die **126 Profile**, die mit der Suchfunktion gefunden werden konnten, wurden der Inhaltsanalyse unterzogen.

6.5.3. Experiment

Die dritte Phase der Untersuchung wird als „Experiment“ bezeichnet, auch wenn es sich nur um ein sehr einfaches Exemplar seiner Art handelt. Ein Experiment ist laut Atteslander eine bestimmte Untersuchungsanordnung.

> Ein Experiment ist eine „Überprüfung von bereits vorher theoretisch festgelegten Aussagen nach festgelegten Bedingungen.“ (Atteslander 2008, S.165)

Untersucht wird mit einem Experiment immer eine soziale Situation, in der ein verursachender Faktor (unabhängige Variable) auf eine Person wirkt und damit ihr soziales Verhalten beeinflusst. Das soziale Verhalten ist der bewirkte Faktor (abhängige Variable).

Im vorliegenden Untersuchungsdesign sind die Personen in der sozialen Situation Facebook-Mitglieder, deren Profile bereits einer Inhaltsanalyse unterzogen wurden. Als verursachender Faktor wurde diesen Facebook-Mitgliedern eine Freundschaftseinladung von einer fremden Person geschickt. Als abhängige Variable wurde beobachtet, ob die Facebook-Mitglieder die Freundschaftseinladung akzeptierten oder nicht.

Das Experiment wird als Feldexperiment durchgeführt – der zu untersuchende Gegenstand wird nicht aus der natürlichen Umgebung herausgelöst. (Atteslander 2008, S.167ff)

Dieses Experiment sollte eine **Antwort auf Hypothese 3.2** geben: „Viele Facebook-Mitglieder geben ihre Daten großzügig preis, indem sie Freundschaftsanfragen bestätigen, auch wenn sie eine Person nicht kennen.“ Dabei wurde wie folgt codiert:

0 – Die Person hat die Freundschaftsanfrage-Funktion deaktiviert.
1 – Die Freundschaftsanfrage wurde bestätigt.
2 – Es wurde eine Nachricht geschrieben.
3 – Es wurde bestätigt UND eine Nachricht geschrieben.

Durchführung

Das Experiment wurde mit Hilfe des Fake-Profiles durchgeführt, das oben beschrieben wurde. Sandra Hubringer sandte an die 126 Personen, deren Profil inhaltsanalytisch untersucht wurde, eine Freundschaftsanfrage. Es wurde codiert, wie die Versuchspersonen auf diese Anfrage einer Fremden innerhalb von zwei Wochen reagierten.

7. Ergebnisse & Interpretation

7.1. Stichprobenbeschreibung

Von den 414 Personen, die an der Umfrage teilnahmen, hatten 3 ihren Lebensmittelpunkt nicht in Österreich und entsprachen somit nicht der Stichprobe. 30 Personen gaben an, kein Facebook-Profil zu besitzen. Es blieben **381 Facebook-Mitglieder**, deren Antworten zur Auswertung herangezogen wurden.

Von den 381 Personen sind 67 % weiblich und 33 % männlich.

12 % sind unter 21 Jahre; 69 % sind 21 bis 30 Jahre; 13 % sind 31 bis 40 Jahre; 5 % sind 41 bis 50 und 1 % ist über 50 Jahre alt. (Tabelle 6)

Dass fast 70 % der Befragten zwischen 21 und 30 Jahre alt sind, überrascht nicht. Facebook startete 2004 als Plattform für Studierende. In den sechs Jahren seines Bestehens öffnete sich das Netzwerk für alle Berufsgruppen und wurde für jedermann ab 13 Jahren zugänglich. Es verbreitete sich daraufhin schnell auch außerhalb der Gruppe der Studierenden. Trotzdem stellen Tweens noch immer die Haupt-Usergruppe dar. In andere Altersgruppen dringt Facebook erst langsam vor.

44 % geben als höchste abgeschlossene Ausbildung die Matura an, 32 % haben einen Hochschulabschluss, 7 % haben eine Lehre und jeweils unter 4 % aller Befragten haben entweder einen Pflichtschulabschluss oder gehen noch zur Schule. (Tabelle 7)

Die Beschäftigung der Befragten teilt sich im Wesentlichen auf zwei große Gruppen auf: 39 % stehen in einem Angestellten-Verhältnis und 37 % studieren. 4 % sind Führungskräfte und weitere 4 % selbstständig. (Tabelle 8)

Tabelle 6: **Verteilung Alter**

Alter	Anzahl	%
unter 21	44	11,5
21-30	264	69,3
31-40	49	12,9
41-50	20	5,2
über 50	4	1,0
Summe	**381**	**100,0**

Tabelle 7: **Verteilung Ausbildung**

Ausbildung	Anzahl	%
noch in der Schule	13	3,4
Pflichtschule	15	3,9
Lehre	28	7,3
Fachschule	18	4,7
Matura	167	43,8
College / Akademie	18	4,7
Hochschulabschluss	122	32,0
Summe	**381**	**100,0**

Tabelle 8: **Verteilung Beruf**

Beschäftigung	Anzahl	%
AngestellteR	150	39,4
ArbeiterIn	12	3,1
Führungskraft	14	3,7
selbstständig	16	4,2
StudentIn	141	37,0
SchülerIn	21	5,5
auf Job-Suche	9	2,4
Hausfrau/Hausmann	5	1,3
Sonstiges	13	3,4
Summe	**381**	**100,0**

7.2. Facebook-Nutzung

42 % aller Befragten haben ihr Facebook-Profil seit 1-2 Jahren. 17 % sind seit 2-3 Jahren Mitglied auf der Plattform und nur 8 % sind schon über 3 Jahre dabei. 33 % haben ihren Account im letzten Jahr erstellt. (Abbildung 10) Dieses Ergebnis geht konform mit den offiziellen Zahlen von Facebook, die besagen, dass die Plattform stetig wächst und sich laufend neue Mitglieder anmelden.

Sehr eindeutig ist das Ergebnis zu den Profilnamen: 90 % aller Befragten nutzen auf Facebook ihren eigenen Namen. Nur 15 Personen (4 %) haben ihren Vor- oder Nachnamen abgekürzt, 22 Personen (6 %) benutzen ein Pseudonym. Dass der Großteil der Mitglieder das Facebook-Profil unter dem echten Namen führt, entspricht dem Konzept von Facebook. Es ist für die Privatsphäre besonders relevant, da alle auf dem Profil veröffentlichten Daten einer Person direkt zuordenbar werden.

Von den 381 Befragten melden sich 23 % im Schnitt einmal pro Tag bei ihrem Facebook-Profil an, 49 % sogar mehrmals täglich. (Abbildung 9) Diese 72 % übersteigen die offiziellen Zahlen von Facebook, laut denen sich 50 % aller Mitglieder mindestens einmal täglich anmelden. Es deutet darauf hin, dass an der Umfrage vor allem Leute teilnahmen, die Facebook sehr aktiv nutzen.

74 % der Befragten sind auf Fotos verlinkt. Von diesen 280 Personen gehen die meisten sehr verantwortungsbewusst mit ihren Verlinkungen um: 64 % kontrollieren alle Fotos, auf denen sie verlinkt werden. 6 % akzeptieren alle Verlinkungen, mit denen sie auf Fotos markiert werden, 3 % gaben an, sich die Fotos nicht immer anzusehen, auf denen Links gesetzt wurden. 7 % aller Befragten sind auf keinem Foto markiert, weil sie alle Verlinkungen gelöscht haben. Das ist der sicherste Weg, um dem Missbrauch von Bildern zu entgehen. Es widerspricht allerdings der Leit-Idee von Facebook und nur wenige wählen diese Option. 11 % hingegen zeigen völlige Gleichgültigkeit gegenüber der Thematik: Sie wissen nicht, ob sie auf einem Foto verlinkt sind.

Der Open Graph, der es Facebook-Nutzerinnen und –Nutzern seit April 2010 ermöglicht, auch außerhalb von Facebook den „Gefällt mir“-Button zu drücken, wurde bisher von den Befragten noch nicht ins Nutzungsverhalten aufgenommen. Nur 9 % haben den Button schon einmal betätigt, obwohl es sich bei den Befragten um äußerst aktive Facebookerinnen und Facebooker handelt.

Abb.9: **Dauer der Facebook-Mitgliedschaft, N=381**

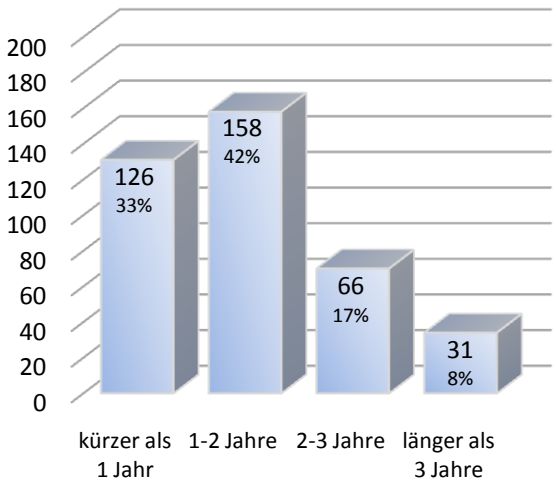
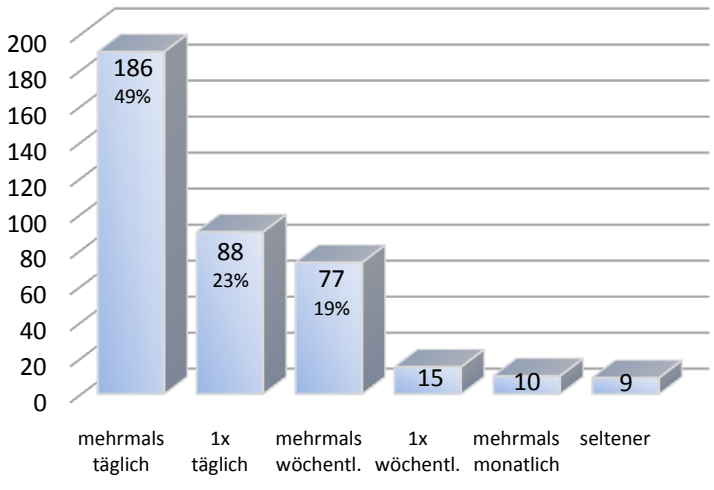


Abb.10: **Einlogg-Häufigkeit auf Facebook, N=381**



Der Fragebogen wurde für Facebook-Mitglieder konzipiert. Darum wurde gleich zu Beginn die Frage gestellt: „Hast du ein Facebook-Profil?“ Wenn eine Person „Nein“ als Antwort wählte, hatte sie die Möglichkeit, einen Grund dafür anzugeben. Dann war die Umfrage beendet.

Von 30 Personen, die an der Umfrage teilnahmen und kein Facebook-Profil hatten, gaben 13 einen Grund an, der etwas mit **Datenschutz oder Privatsphäre** zu tun hat. Sie schrieben etwa:

- mangelnder Schutz der Privatsphäre hat mich gestört
- will mich nicht öffentlich präsentieren
- keine Privatsphäre, viele negative Gerüchte
- vermeide alles, was du über dich persönlich ins Internet schreibst
- Facebook ist unsicher

Der zweithäufigste Ablehnungsgrund ist **mangelndes Interesse**:

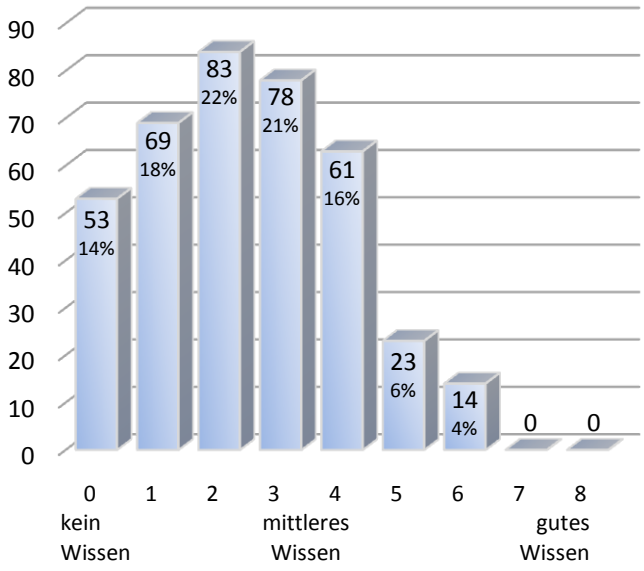
- interessiert mich nicht
- wird nur Blödsinn reingeschrieben
- wüsste nicht wofür ich das brauche
- keine Lust

7.3. Datenschutz-Wissen, Selbstdarstellung & Privatsphäre

7.3.1. Datenschutz-Wissen

Die Auswertung der Datenschutz-Fragen ergab, dass das Wissen der Befragten auf diesem Gebiet große Lücken aufweist. Keine einzige der 381 Personen konnte alle 8 Datenschutz-Fragen richtig beantworten. Ebenso hatte niemand 7 richtige Antworten. Das Datenschutz-Wissen der Befragten bewegt sich zwischen 0 und 6, wobei das durchschnittliche Wissen 2,4 beträgt – ein erschreckend niedriger Wert bei 8 möglichen Punkten. (Abbildung 11)

Abb.11: **Datenschutz-Index, N=381**



Am sichersten sind sich die Testpersonen bei der Frage, welche Daten Facebook speichere. 62 % wählten die richtige Antwort, dass Facebook sowohl die Verbindungsdaten als auch alle Transaktionsdaten der Mitglieder archiviert. (Abbildung 19)

Außerdem weiß über die Hälfte aller Befragten, was mit ihren Daten passiert, wenn sie ihren Facebook-Account löschen. 52 % antworten: „Wenn ich mich von Facebook abmelde, bleiben meine Daten gespeichert." (Abbildung 17) Es herrscht also ein hohes Bewusstsein dafür, dass Facebook nicht nur eine Plattform zum Austausch, sondern auch eine große Datensammlung ist.

Bei den restlichen 6 Fragen wählte die Mehrheit eine der falschen Antworten. Die wenigsten richtigen Antworten wurden auf die Frage gegeben, welche der eigenen Daten Facebook-Freunde verwenden dürfen. Nur 8 % wissen, dass befreundete Facebook-Mitglieder nur die Daten weiterverwenden dürfen, die man „allen" zeigt. 19 % glauben, Facebook-Freunde dürfen gar keine der eigenen Daten verwenden, 34 % denken, sie dürfen alles verwenden, was sie ihnen auf der Profil-Seite zeigen. Die Mehrheit von 39 % gibt an, keine Ahnung zu haben. (Abbildung 16)

Bei der Frage, ob das österreichische Datenschutzgesetz die eigenen Inhalte auf Facebook schütze, schätzt ein Großteil der Befragten die Wirkung des DSG 2000 geringer ein als sie tatsächlich ist. 39 % glauben, dass auf Facebook gestellte Inhalte nicht vom österreichischen DSG geschützt sind. 10 % gaben die richtige Antwort, dass das DSG die Daten schützt, die man nur einem begrenzten Personenkreis zugänglich macht. (Abbildung 12) Wie in Kapitel 6.5.1 beschrieben, ist diese Frage schwer zu beantworten, da es in der Justiz keinen Präzedenzfall gibt, der absolute Klarheit schaffen würde. Es verwundert daher nicht, dass die Befragten mit ihren Antworten unsicher sind.

Erschreckend ist, wie oft die Befragten keine Meinung zu einer Frage haben und auf Antwort 4 ausweichen: „Ich hab absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten." Bei 4 von 8 Fragen stellt diese Ausweich-Option die Top-Antwort dar. Das deutet darauf hin, dass sich viele Personen noch keine Gedanken zum Thema Datenschutz auf Facebook gemacht haben.

Für die Diagramme wurden Fragen und Antworten zur besseren Darstellung verkürzt. Die detaillierte Auswertung der Datenschutz-Fragen findet sich im Anhang.

Abb.13: **Wo können Daten auftauchen, die du auf Facebook veröffentlichst? N=381**

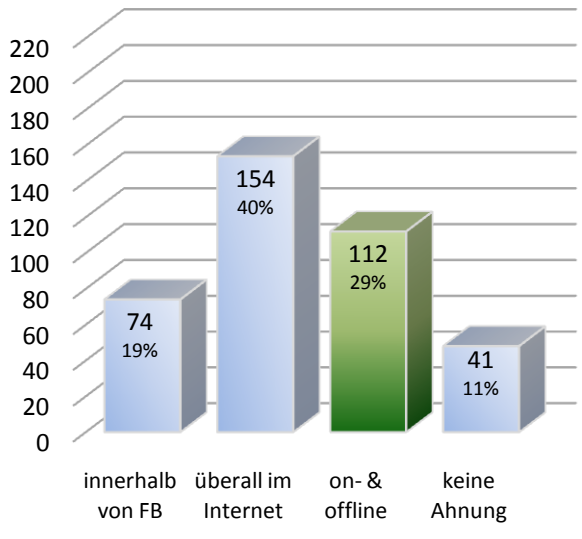


Abb.12: **Schützt das österreichische Datenschutzgesetz deine Daten auf Facebook? N=381**

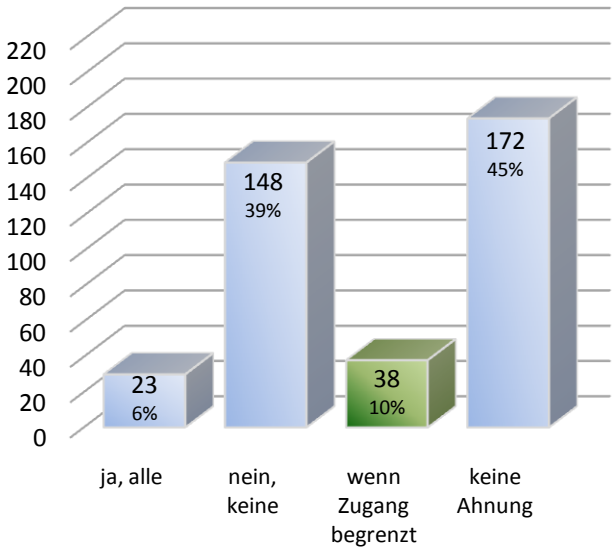


Abb.15: **Welche deiner Daten dürfen von Facebook weiterverwendet werden? N=381**

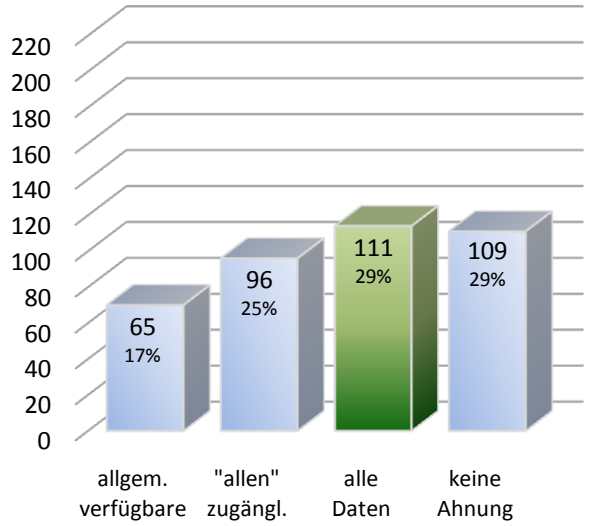


Abb.14: **Darfst du laut österr. DSG die Daten anderer Facebook-Mitglieder verwenden? N=381**

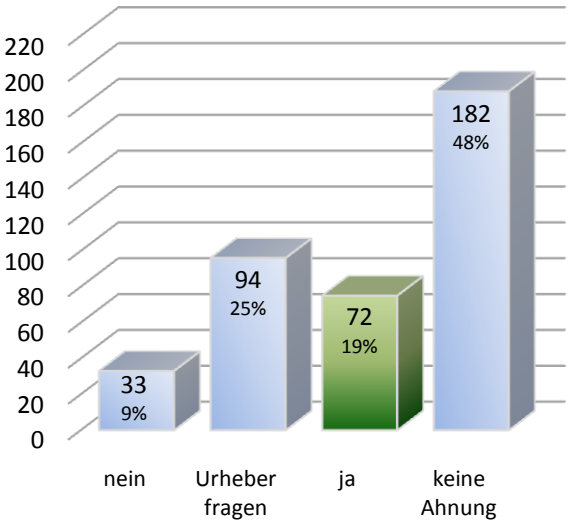


Abb.17: **Was passiert mit deinen Daten, wenn du deinen Facebook-Account löschst? N=381**

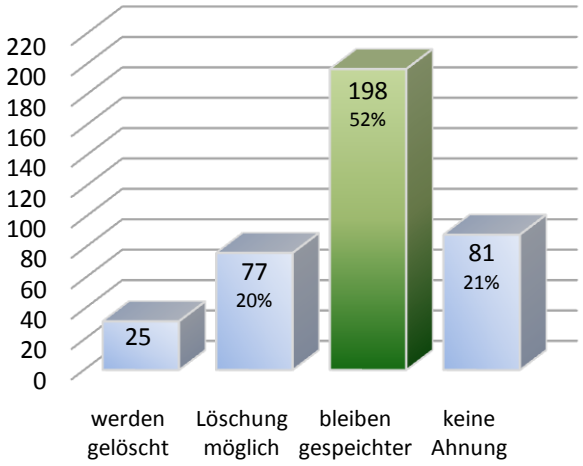


Abb.16: **Welche deiner Daten dürfen von Facebook-Freunden verwendet werden? N=381**

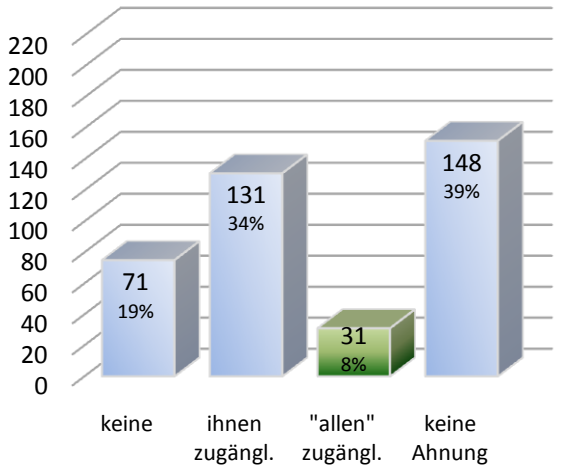


Abb.19: **Welche deiner Daten dürfen von Dritten weiterverwendet werden? N=381**

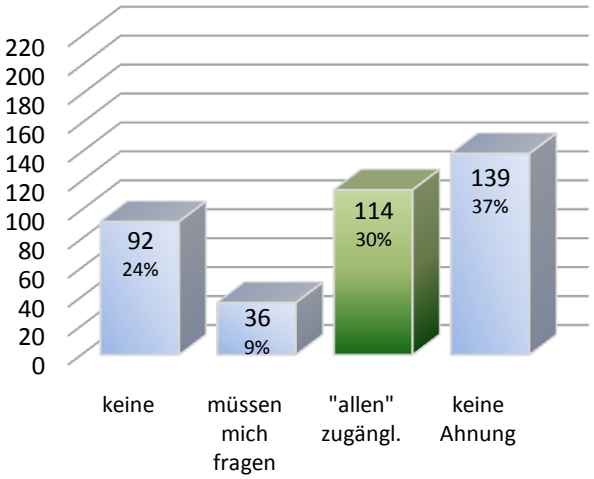
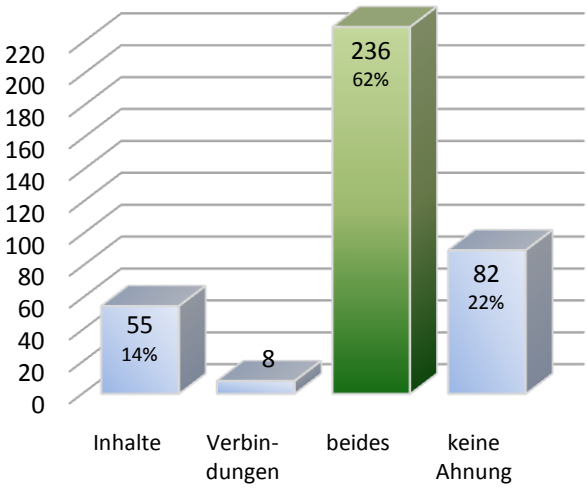


Abb.18: **Welche Daten speichert Facebook? N=381**



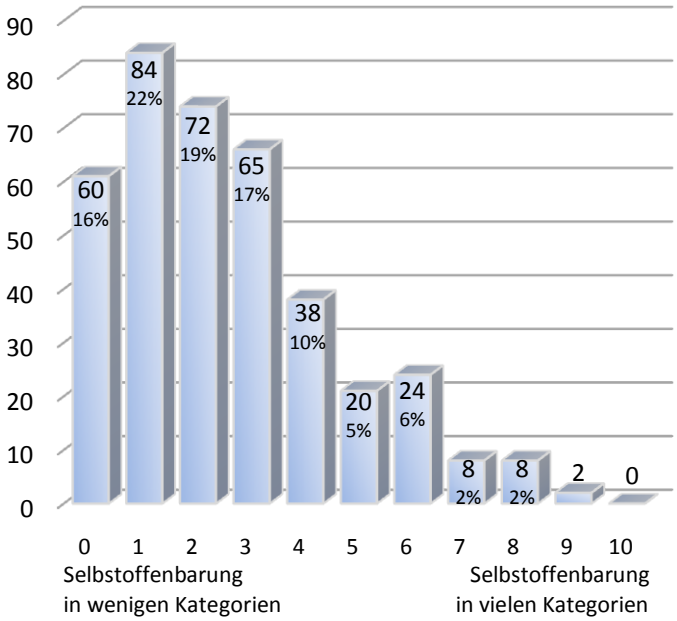
Werden die acht Datenschutz-Fragen getrennt ausgewertet nach Fragen zum österreichischen Datenschutzgesetz und Fragen zu Facebooks Datenschutzbestimmungen, erhält man das Ergebnis, dass die Probanden besser über Facebooks Rechte als über ihre eigenen Bescheid wissen. 55 % aller Befragten können von den vier Fragen zum DSG keine einzige richtig beantworten. Bei den vier Fragen zu Facebooks Datenschutzbestimmungen liegt der Anteil der völlig Ahnungslosen immerhin bei nur 19 %. Alle vier Fragen richtig hat zum Thema DSG keine einzige Person, bei den Facebook-Fragen schaffen 9 % (34 Personen) vier Richtige. Dementsprechend fallen die Mittelwerte aus: Bei einer Skala von 0 bis 4 erreichten die Probanden zum Thema DSG im Schnitt 0,7 Punkte und zum Thema Facebook einen ganzen Punkt mehr, nämlich 1,7 Punkte.

7.3.2. Selbstdarstellung

Selbstoffenbarungsintensität

Für den Index der Selbstoffenbarungsintensität wurde abgefragt, in welchen Kategorien die Probanden Angaben über sich auf ihrem Profil machen. Die Auswertung ergab, dass die Mehrheit der 381 Befragten (57 %) in höchstens 2 der 10 abgefragten Kategorien Daten zu ihrer Person angeben. Keine einzige der Testpersonen gibt in allen Kategorien etwas über sich preis, nur 2 stellen in 9 von 10 Kategorien Daten online. (Abbildung 20) Der Mittelwert des Index liegt bei 2,5 von 10 möglichen Punkten. Dass die Index-Werte eher niedrig ausfallen, weist darauf hin, dass viele Facebook-Mitglieder zurückhaltend sind, was das Online-Stellen von persönlichen Informationen angeht.

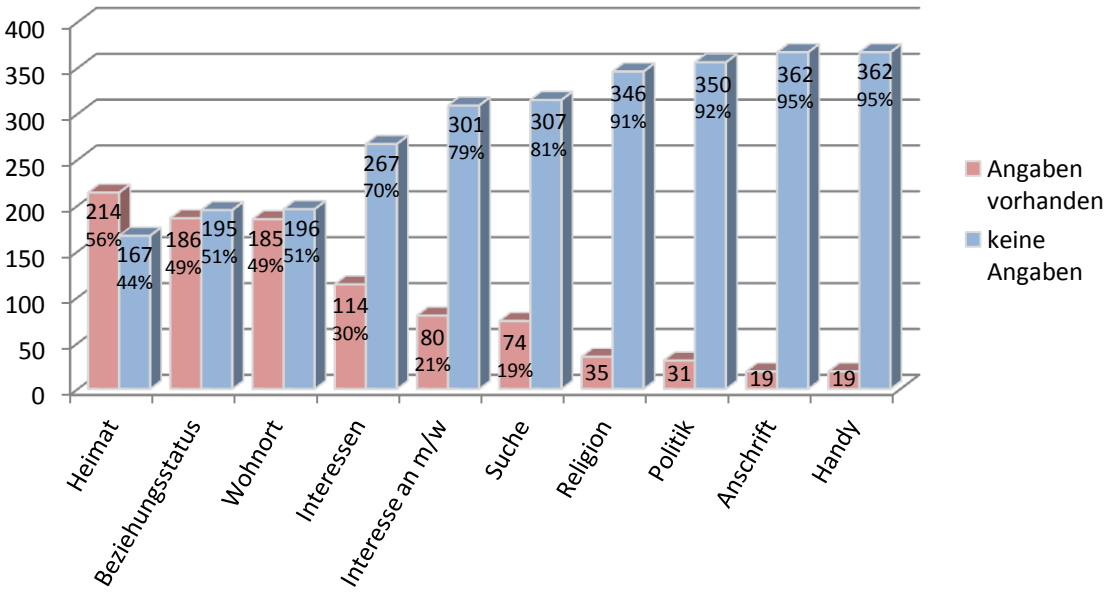
Abb.20: **Index Selbstoffenbarungsintensität, N=381**



Ein genaueres Bild erhält man, wenn man sich die einzelnen abgefragten Kategorien ansieht. (Abbildung 21) Der Heimatort ist die einzige Kategorie, in der über 50 % der Befragten eine Angabe machen. Mit 49 % folgen Beziehungsstatus sowie Wohnort. 30 % geben ihre Interessen auf Facebook an, 21 % geben bekannt, ob sie an Frauen oder Männern interessiert sind und 19 % schreiben auf ihr Profil, wonach sie auf der Suche sind (Freundschaft, feste Beziehung, etc.). Richtig zurückhaltend werden die Befragten, wenn es um die religiöse Einstellung, die politische Gesinnung oder um Anschrift und Handy-Nummer geht. Diese persönlichen Daten teilen nur die Wenigsten auf Facebook mit anderen.

Auf die Frage, warum sie in manchen Kategorien nichts über sich schreiben, antworten 90 % aller Befragten: „Ich wollte nicht zu viel über mich preisgeben." Die Befragten sind also durchaus aufmerksam, was ihre Selbstdarstellung auf Facebook betrifft und differenzieren zwischen allgemeinen und intimen Informationen.

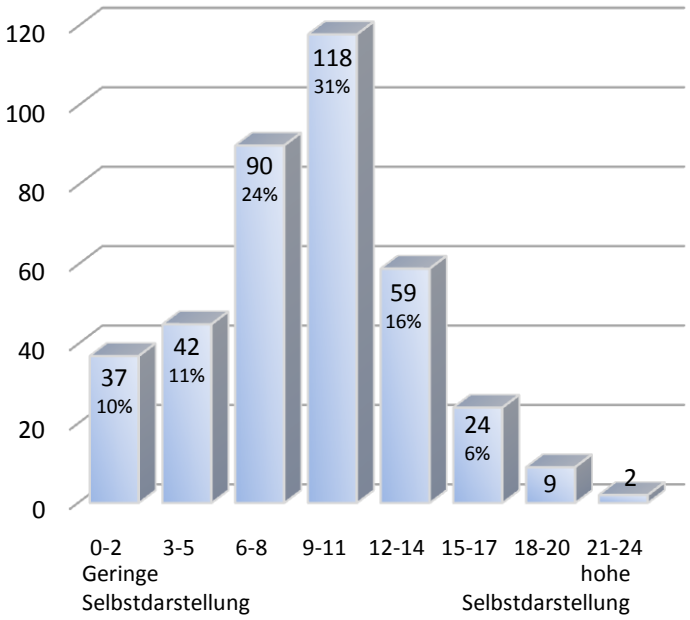
Abb.21: **Personenbezogene Angaben in den einzelnen Kategorien, N=381**



Selbstoffenbarungshäufigkeit

Mit sechs Fragen zur Nutzung von verschiedenen Facebook-Anwendungen wurde der Index der Selbstoffenbarungshäufigkeit ermittelt. Bei einer Skala von 0 bis 24 hat er einen Mittelwert von 8,9. Die höchsten Spitzen erreicht der Index im mittleren Bereich: 31 % aller Befragten haben einen Index-Wert von 9, 10 oder 11 Punkten. 44 % verteilen sich auf die 9 Kategorien darunter, 25 % erzielen einen höheren Wert. Es kann der Trend abgelesen werden, dass die Befragten die Anwendungen auf Facebook eher gemäßigt als inflationär benutzen. Abbildung 22 zeigt die Index-Werte gebündelt in 8 Gruppen zu je 3 Index-Punkten.

Abb.22: **Index Selbstoffenbarungshäufigkeit in 8 Gruppen, N=381**

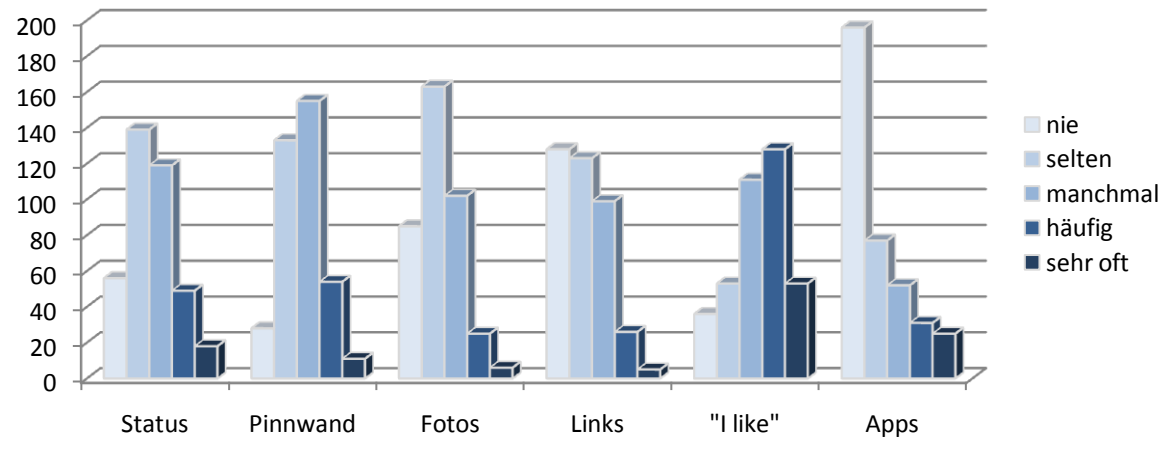


Betrachtet man die sechs abgefragten Anwendungen einzeln (Abbildung 23), wird deutlich, in welchen Bereichen die 381 Befragten am häufigsten Selbstdarstellung auf Facebook betreiben. 48 % betätigen häufig oder sehr oft den „I like“-Button. 18 % ändern häufig oder sehr oft ihren Status. Und 17 % hinterlassen häufig oder sehr oft Nachrichten auf den Pinnwänden anderer.

Am zurückhaltendsten sind die Befragten bei der Nutzung von Applikationen. 72 % geben an, selten oder nie Anwendungen von externen Anbietern zu verwenden.

Diese Prozentsätze werden durch die Mittelwerte der einzelnen Anwendungen bestätigt: Bei einer Skala von 0 bis 4 erreicht der „Gefällt mir“-Button den höchsten Mittelwert mit 2,3. Das Schreiben auf fremde Pinnwände hat einen durchschnittlichen Index-Wert von 1,7 während Status-Meldungen im Schnitt auf 1,6 Punkte im Index kommen. Es folgt das Hochladen von Fotos mit 1,2 Index-Punkten und das Posten von Links mit einem Index-Wert von 1,1. Mit einem durchschnittlichen Index von 1 bildet das Verwenden von Applikationen eindeutig das Schlusslicht.

Abb.23: **6 Fragen zur Selbstdarstellungs-Häufigkeit:**
Wie oft werden Anwendungen benutzt? N=381

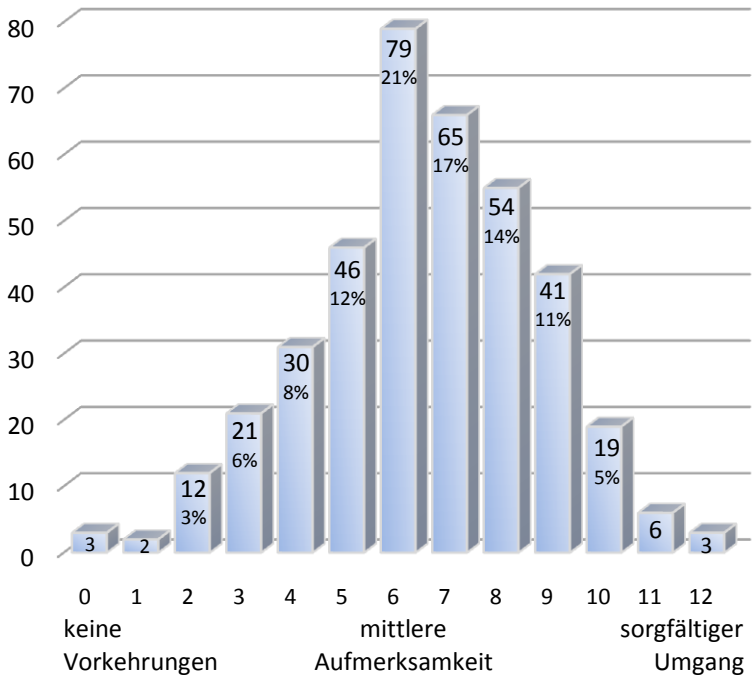


7.3.3. Privatsphäre

In den sechs Fragen zu den Privatsphäre-Einstellungen konnten die Befragten 0 bis 12 Punkte erreichen. Einen Indexwert von 0 haben Personen, die ihre Privatsphäre-Einstellungen noch nie kontrolliert und geändert hatten. Wer einen Wert von 12 erreicht, legt ein verantwortungsbewusstes Privatsphäre-Verhalten an den Tag.

Beim Privatsphäre-Verhalten geht der Trend zur Mitte: Die mittleren drei Kategorien (5, 6 und 7 Index-Punkte) ergeben gemeinsam 50 %, der Mittelwert beträgt 6,5. Die Hälfte der Befragten kümmert sich also durchschnittlich um die eigene Privatsphäre – zwar nicht äußerst penibel, aber auch nicht grob fahrlässig. 18 % der befragten Userinnen und User gehen bedenkenloser mit ihrer Privatsphäre um als der Durchschnitt. 32 % legen ein überdurchschnittliches Privatsphäre-Verhalten an den Tag und sind in allen abgefragten Bereichen wachsam. (Abbildung 24)

Abb.24: **Privatsphäre-Index, N=381**



Kontrolle der Privatsphäre-Einstellungen

47 % der Befragten haben ihre Privatsphäre-Einstellungen gleich nach der Registrierung auf Facebook kontrolliert, 45 % haben dies im Laufe ihrer Facebook-Mitgliedschaft getan. Das deutet darauf hin, dass das Bewusstsein für die Relevanz der Privatsphäre-Einstellungen gestiegen ist. Durch die kritische Berichterstattung in den Medien, Testberichte sowie die Warnungen von Datenschutz-Organisationen scheinen immer mehr Leute auf die Notwenigkeit gut gepflegter Privatsphäre-Einstellungen aufmerksam zu werden. 8 % der Befragten waren trotzdem noch nie auf der Seite der Privatsphäre-Einstellungen oder können sich nicht mehr erinnern, ob sie schon einmal nachgeschaut haben. (Abbildung 24)

Änderung von Privatsphäre-Einstellungen

Von den 349 Personen, die ihre Privatsphäre-Settings kontrollierten, gaben 41 % an, jeden Punkt einzeln reguliert zu haben. 44 % änderten zumindest manche Punkte. 7 % ließen alles so eingestellt, wie es von Facebook vorgeschlagen war. In Summe haben 15 % der Stichprobe ihre Privatsphäre-Einstellungen auf Facebook nicht reguliert. Sie haben entweder alle Voreinstellungen von Facebook übernommen oder die Seite der Settings noch gar nie aufgesucht.

Inhalte beschränkt zugänglich machen

Wenn es darum geht, einzuschränken, wer die eigenen Inhalte sehen darf und wer nicht, gibt es eine klare Tendenz unter den Befragten: 71 % geben an, dass nur ihre Freunde auf Facebook ihre Inhalte sehen können. Weitere 13 % regeln sogar ganz spezifisch, wer was sehen darf – etwa durch die Unterteilung von Freunden in verschiedene Gruppen. 16 % machen die eigenen Inhalte mehr Personen als nur dem Freundeskreis zugänglich. Sie zeigen ihre Daten auch Freunden von Freunden oder sogar „allen“. (Abbildung 25)

Hinter diesem Ergebnis verbirgt sich der Knackpunkt zum österreichischen Datenschutzgesetz (siehe Kapitel 4.3.2). Laut Datenschutz-Expertin Zimmer macht es einen großen Unterschied, ob man Inhalte im Internet nur mit Freunden teilt oder sie allen zugänglich macht. In letzterem Fall spricht man von einer Veröffentlichung. Liegt diese vor, sind Daten nicht mehr durch das DSG geschützt. Dass 84 % der Stichprobe gut regulieren, wer Inhalte sehen kann und wer nicht und es 16 % nicht so genau nehmen mit dem Schutz der eigenen Daten, mag als guter Schnitt erscheinen. In Anbetracht der Tatsache, dass von der Regelung der Privatsphäre-Einstellungen sehr viel abhängt, sind aber auch 16 % an leichtfertigen Mitgliedern noch zu viel. Ziel sollte es sein, dass alle Mitglieder die Bedeutung der Privatsphäre-Einstellungen erkennen und sie dementsprechend auf dem eigenen Profil kontrollieren.

Umgang mit Freundschaftsanfragen

Eine Freundschaftsanfrage von einer fremden Person lehnen 53 % aller Befragten ab. 11 % schreiben der betreffenden Person eine Nachricht und fragen, woher sie sie kennen. 27 % besuchen das Profil des oder der Fremden und entscheiden dann, ob sie die Person als Freund akzeptieren. Und 2 % akzeptieren alle Anfragen.

Abb.26: **Wann wurden die Privatsphäre-Einstellungen kontrolliert? N=381**

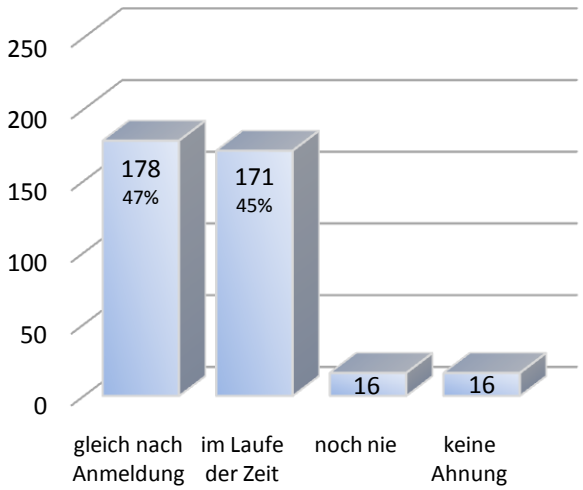
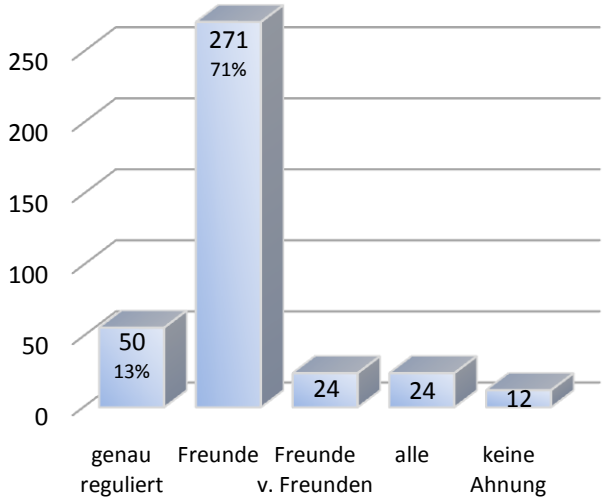


Abb.25: **Wer darf eigene Inhalte sehen? N=381**



7.3.4. Zusammenhänge der Indizes

Mit den vier Indizes **Datenschutz-Wissen**, **Selbstdarstellungsintensität**, **Selbstdarstellungs-häufigkeit** und **Privatsphäre-Verhalten** wurden **Korrelationen** nach Pearson gerechnet. Dabei zeigten sich bei Vorgabe einer Irrtumswahrscheinlichkeit von α=0,05 drei signifikant positive Zusammenhänge:

1. **Datenschutz-Wissen & Privatsphäre-Sorgfalt**

Der Datenschutz-Index korreliert signifikant positiv mit dem Privatsphäre-Index (p=.000, r=.182). Das bedeutet, je höher das Datenschutz-Wissen der Befragten ist, desto sorgfältiger gehen sie mit ihren Privatsphäre-Einstellungen um.

2. **Privatsphäre-Sorgfalt & Selbstdarstellungshäufigkeit**

Der Privatsphäre-Index korreliert außerdem signifikant mit der Selbstdarstellungshäufigkeit (p=.000, r=.228). Personen, die ihre Privatsphäre-Einstellungen sorgfältig reguliert haben, verwenden Facebooks Anwendungen häufiger als andere. Oder umgekehrt ausgedrückt: Je öfter Facebook-Mitglieder verschiedene Aktionen auf der Plattform setzen, desto strikter regulieren sie ihre Privatsphäre-Settings.

3. **Selbstdarstellungsintensität & Selbstdarstellungshäufigkeit**

Und es besteht ein signifikanter Zusammenhang zwischen den beiden Selbstdarstellungs-indizes (p=.000, r=.365). Je mehr jemand auf dem eigenen Profil über sich offenbart, desto öfter nutzt er Facebooks verschiedene Angebote.

Aus der Literatur und dem aktuellen Forschungsstand wurde eine Hypothese zur ersten Korrelation abgeleitet. Das Ergebnis überrascht nicht, der Zusammenhang weist in die erwartete Richtung. Für die beiden anderen Korrelationen wurden keine Hypothesen gebildet. Dass die unabhängigen Variablen untereinander Zusammenhänge aufweisen, ist ein interessantes Ergebnis, muss an dieser Stelle aber rein als empirisches Resultat angesehen werden, das in der vorliegenden Arbeit nicht theoretisch untermauert wurde. Dass Selbstdarstellungsintensität und –häufigkeit positiv korrelieren, erscheint auf den ersten Blick logisch. Je freizügiger Userinnen und User auf ihrem Profil mit Informationen sind, desto häufiger nutzen sie auch Anwendungen. Wie der Zusammenhang jedoch zwischen Privatsphäre-Verhalten und Selbstdarstellung verläuft, kann an dieser Stelle nicht weiter interpretiert werden. Es wäre sicher interessant, in einer weiterführenden Studie zu prüfen, welche der beiden Variablen die andere beeinflusst.

Die Korrelationen zwischen Datenschutz-Wissen und den beiden Selbstdarstellungs-Indizes sind beide nicht signifikant, weisen aber in die Richtung, die in den Hypothesen vorausgesagt wurde.

Die Korrelations-Tabelle findet sich im Anhang.

Die Zusammenhänge zwischen der unabhängigen Variable Datenschutz-Wissen und den drei abhängigen Variablen wurden mit einer **Regression** überprüft. Sie bestätigte das Ergebnis: Es

besteht ein Zusammenhang zwischen dem Datenschutz-Wissen einer Person und der Privatsphäre-Sorgfalt mit einer Signifikanz von p=.001. Die beiden unabhängigen Variablen zur Selbstdarstellung korrelieren nicht signifikant mit dem Datenschutz-Wissen.

7.3.5. Inhaltsanalyse

Für die Inhaltsanalyse wurden 154 Profile in die Suchfunktion eingegeben. 28 Personen hatten ihre Privatsphäre-Einstellungen so strikt reguliert, dass ihr Profil in der Trefferliste nicht auftaucht. **126** konnten gefunden und mit Hilfe des Profils von Sandra Hubringer analysiert werden. Die folgenden Ergebnisse dokumentieren, welche Inhalte diese Facebook-Mitglieder „allen“ zugänglich machen.

Von den 126 untersuchten Profil-Seiten enthalten 85 % ein Foto, auf dem der Profil-Besitzer bzw. die Besitzerin eindeutig erkennbar ist. 79 % zeigen ihre Freundeslisten an, 76 % machen allen die Seiten zugänglich, von denen sie Fan sind und 48 % veröffentlichen ihre Lieblings-Musik. Welche weiteren Bereiche die Probanden „allen“ zugänglich machen, zeigt Abbildung 28. Es sind nicht alle Kategorien gelistet, in denen Inhalte gefunden wurden. In Summe fanden sich in 31 verschiedenen Kategorien Daten. In manchen von ihnen jedoch nur bei vereinzelten Probanden. So ist beispielsweise auf einem Profil unter dem Punkt „Eltern“ ein anderes Facebook-Mitglied verlinkt, 5 Probanden geben die Namen ihrer Kinder an, 3 veröffentlichen ihren Jahrestag und 6 zitieren auf ihrem Profil ihren Lieblings-Spruch. Im Durchschnitt machen die Testpersonen Angaben in 7 Kategorien. Die freizügigste Person veröffentlicht Inhalte in 20 Kategorien. Bei 55 % aller Probanden finden sich in bis zu 6 Kategorien Angaben. 36 % veröffentlichen Inhalte in 7 bis 12 Kategorien. (Abbildung 27) Diesen Ergebnissen steht die Antwort der Probanden auf eine Privatsphäre-Frage gegenüber. Die Frage „Wem zeigst du deine Inhalte auf Facebook?“ in der Umfrage beantworteten 74 % der 126 Probanden mit „Nur Freunden.“ Eine Fehleinschätzung, wie die Inhaltsanalyse beweist. Bei keinem einzigen der untersuchten Profile waren alle Daten versteckt und somit Freunden vorbehalten, 78 % geben Daten in mehr als 3 Bereichen preis. Das beweist, dass Facebook-Mitglieder oft nicht genau wissen, was sie wem zeigen.

Abb.28: **„allen“ zugängliche Informationen, N=126**

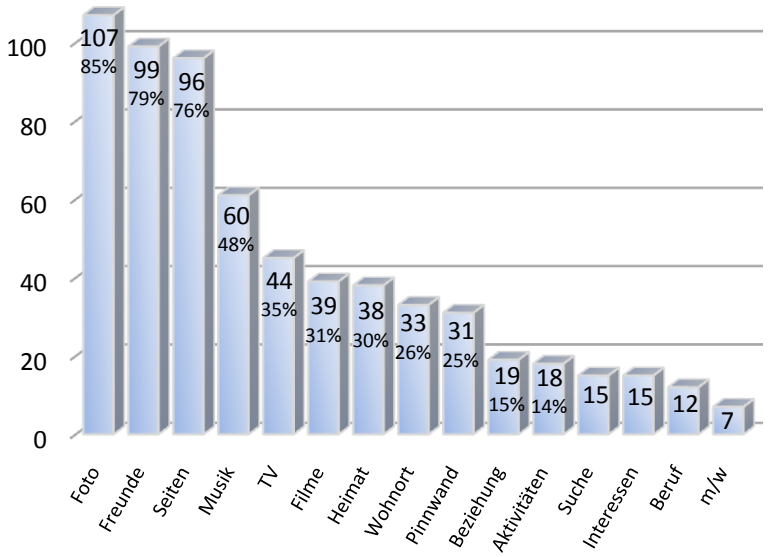
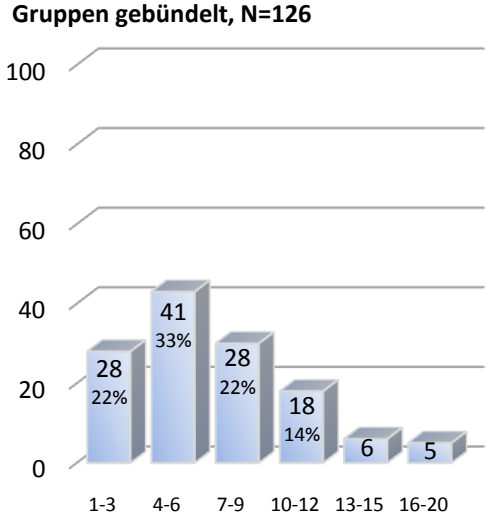


Abb.27: **veröffentlichte Kategorien in 3er-Gruppen gebündelt, N=126**

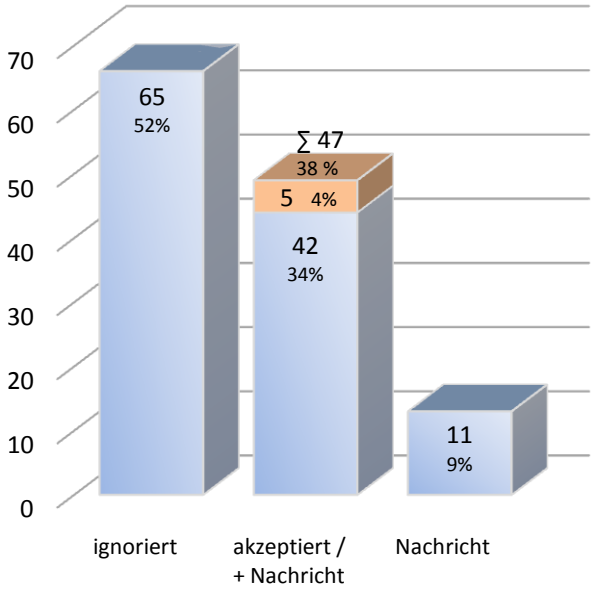


Die Ergebnisse der Inhaltsanalyse wurden mit dem Datenschutz-Index korreliert in einer Korrelation nach Pearson. Die Berechnung ergab jedoch keinen signifikanten Zusammenhang. Es kann also keine Aussage darüber getroffen werden, ob das Datenschutz-Wissen beeinflusst, wie viele Inhalte man auf Facebook „allen“ zugänglich macht.

7.3.6. Experiment

Nachdem die Inhaltsanalyse abgeschlossen war, schickte die imaginäre Sandra Hubringer an **123** Probanden eine Freundschaftseinladung. (3 Personen hatten ihr Profil so eingestellt, dass ihnen Fremde keine Freundschaftsanfragen schicken können.) Innerhalb von zwei Wochen hatte Sandra 47 Freunde auf Facebook. 34 % der 123 Testpersonen akzeptierten die Anfrage, 9 % schrieben eine Nachricht mit Inhalten wie „Kennen wir uns?“ oder „Wer bist du?“ und 4 % schrieben Sandra zwar eine fragende Nachricht, bestätigten die Freundschaft aber schon einmal pro forma. In Summe hatten also 38 % die Anfrage bestätigt, 52 % reagierten innerhalb der zwei Versuchswochen nicht darauf. (Abbildung 29) Nachdem es sich bei der Stichprobe um eher aktive Facebook-Mitglieder handelt, ist davon auszugehen, dass sich alle in den 14 Tagen, in denen der Versuch lief, mindestens einmal auf ihrem Profil eingeloggt haben. Dass Sandras Anfrage nicht bestätigt wurde, kann also als bewusste Ablehnung der Freundschaftsanfrage gewertet werden.

Abb.29: **Reaktion auf Freundschaftsanfrage, N=123**



Bemerkenswert ist, dass 12 von Sandras 47 neuen Freunden (26 %) im Fragebogen angaben, Freundschaftsanfragen von fremden Personen abzulehnen. Das deutet darauf hin, dass manche Leute sehr wohl wissen, dass es ratsam wäre, fremde Personen nicht in die Freundesliste aufzunehmen. In der Realität verhalten sie sich aber nicht diesem Wissen entsprechend. Denkbar sind dafür zwei Erklärungen: Entweder, die Befragten sind sich ihrer Handlungsweise bewusst und machten in der Umfrage falsche Angaben im Sinne der sozialen Erwünschtheit. Sie kreuzten an,

Fremde nicht als Freunde zu akzeptieren, weil sie das für die „bessere“ Antwort hielten. Oder aber die Befragten antworteten in der Umfrage unwissentlich fehlerhaft. Sie glauben in der Theorie, fremde Personen auf Facebook nicht anzufreunden. Wenn dann aber eine unbekannte Freundschaftsanfrage hereinkommt, wird sie doch unvorsichtigerweise akzeptiert. Vielleicht glauben die Probanden, die Person entfernt zu kennen, oder vermuten, sie einmal wo getroffen zu haben und sich nicht mehr zu erinnern. Vielleicht wäre es ihnen peinlich, die Anfrage nicht zu akzeptieren. Oder sie machen sich in der konkreten Situation wenig Gedanken darüber und klicken schneller auf den „Akzeptieren“-Button, als sich Sorgen um die Privatsphäre breit machen können.

Kritisch ist das Akzeptieren von fremden Freundschaftsanfragen auch insbesondere, weil Personen mit der Aufnahme von Fremden in Freundeslisten nicht nur die eigenen Daten großzügig preisgeben. Sie ermöglichen dadurch oft den Zugang zu Daten von Freunden. Viele Facebook-Mitglieder stellen ihre Privatsphäre-Settings so ein, dass die meisten Inhalte Freunde von Freunden sehen können. Gehen ihre Freunde nicht gewissenhaft mit Freundschaftsanfragen um, haben schnell tausende Personen Zugriff auf ihre Daten. Dieses Phänomen trat auch beim vorliegenden Experiment auf. Bei der Inhaltsanalyse konnte Sandra Hubringer nur auf sehr beschränkte Daten der Versuchspersonen zugreifen. Wurde sie allerdings in die Freundesliste einer Person aufgenommen, hatte sie plötzlich Zugang zu einem unüberschaubar großen Datenvolumen. Sie konnte sich durch Fotoalben klicken, den Status der neuen Freunde verfolgen und sie konnte nicht nur die Kontakte der eigenen Freundesliste ausspionieren, sondern auch die Freunde ihrer Freunde. Sie erhielt Zugang zu unzähligen Fotos, Profil-Daten, Pinnwänden und Links.

Das dreistufige Untersuchungsverfahren fand mit diesem Experiment seinen Abschluss. Eine weitere Inhaltsanalyse darüber, welche Daten Sandra Hubringer im Endeffekt zugänglich waren, wäre sicher interessant, hätte aber den Rahmen der Arbeit gesprengt.

7.3.7. Zusammenfassung der Ergebnisse

Die Stichproben von 381 Probanden stellte eine gute Basis für umfangreiche Auswertungen dar. Sie umfasste Personen in verschiedenen Altersgruppen und mit unterschiedlichem Bildungsniveau. Leute zwischen 20 und 30 Jahren waren überdurchschnittlich in der Stichprobe vertreten, was aber der Grundgesamtheit durchaus gerecht werden dürfte. Auch der größere Anteil von Studierenden und Angestellten spiegelt Literatur-Recherchen zufolge die Realität wider. Mit einem Anteil von 72 % an Täglich-Usern sind die Befragten im Schnitt aktiver auf der Plattform, als die Grundgesamtheit der Facebook-Gemeinde. Diese Tatsache muss in die Interpretation der Ergebnisse mit einfließen.

Das Datenschutz-Wissen der Befragten wurde als mangelhaft festgestellt. Im Schnitt erreichte die Stichprobe einen Index-Wert von 2,4 bei einer Skala von 0 bis 8. Keine einzige der Testpersonen konnte alle 8 Datenschutz-Fragen richtig beantworten.

Mit der direkten Selbstdarstellung auf Facebook sind die Befragten eher zurückhaltend. 57 % der Befragten stellen in höchstens 2 der 10 abgefragten Kategorien Informationen über sich auf ihr Facebook-Profil. Die Hauptbegründung, viele Kategorien nicht zu füllen, ist der Widerwille, zu viel über sich preiszugeben.

Freizügiger sind die Probanden bei der Nutzung der vielen angebotenen Anwendungen auf Facebook. Sie verwenden auch diese nicht gerade inflationär, bewegen sich aber mit den Index-Werten durchwegs im mittleren Bereich. Besonders häufig wird der „Gefällt mir"-Button gedrückt, der eigene Status aktualisiert und eine Nachricht auf einer anderen Pinnwand hinterlassen.

Bezüglich des Selbstdarstellungs-Verhalten lässt sich also folgendes über die Stichprobe sagen: Auf den Profil-Seiten werden im Durchschnitt nicht allzu viele Angaben zur eigenen Person gemacht. Viel mehr Daten geben die Probanden von sich preis, indem sie aktiv am Facebook-Geschehen teilnehmen.

Das Privatsphäre-Verhalten der Befragten zeigte sich als relativ verantwortungsbewusst. 50 % schenken der Privatsphäre auf Facebook mittlere Aufmerksamkeit, 32 % gehen überdurchschnittlich sorgfältig mit ihren Einstellungen um. Die Tendenz dürfte weiter steigend sein. 45 % kontrollierten die Seite der Privatsphäre-Einstellungen nicht gleich nach ihrer Registrierung, sondern erst im Laufe der Mitgliedschaft. Das deutet darauf hin, dass das Bewusstsein zum Thema steigt. Dass die Wichtigkeit gut geregelter Privatsphäre-Settings noch nicht zu allen durchgedrungen ist, zeigen die 15 % der Stichprobe, die ihre Einstellungen nicht reguliert haben. Ihr Profil läuft mit den Voreinstellungen, die Facebook getroffen hat.

Zwischen dem Wissen über Datenschutz und der Sorgfalt gegenüber der Privatsphäre besteht ein signifikanter Zusammenhang. Dieser lässt darauf schließen, dass Facebook-Mitglieder besonders aufmerksam auf ihre Privatsphäre achtgeben, wenn sie über die Grundlagen des Datenschutzes Bescheid wissen.

Zusammenfassend hat die Umfrage ergeben, dass die Stichprobe zwar nur ein geringes Datenschutz-Wissen an den Tag legt, sich aber offensichtlich trotzdem über die Relevanz des Privatsphäre-Schutzes bewusst ist. Auf den Profil-Seiten wird allzu ausführliche Selbstdarstellung vermieden. Weniger aufmerksam ist man allerdings bei den Daten, die man durch diverse Handlungen auf Facebook von sich preisgibt. Wahrscheinlich ist die Tatsache, dass jede gesetzte Aktion auf Facebook gleichzeitig eine Information für das Unternehmen bedeutet, nicht in den Köpfen der Userinnen und User präsent.

Die Ergebnisse gehen konform mit der theoretischen Fundierung des Themas. Dennoch ist eine Verallgemeinerung mit Vorsicht zu genießen, da die Stichprobe auf Grund der Beschaffenheit von Facebook nicht zufällig gezogen werden konnte.

Die Inhaltsanalyse und das Experiment konnten nur bei einem Teil der Stichprobe durchgeführt werden, nämlich bei allen Personen, die am Gewinnspiel teilnahmen. Dass diese Probanden im

Gegensatz zu den anderen Umfrage-Teilnehmerinnen und –Teilnehmern ihren Namen für ein Gewinnspiel zur Verfügung stellten, könnte darauf hinweisen, dass sie der freizügigere Teil der Gruppe sind. Die Ergebnisse von Inhaltsanalyse und Experiment sind sehr interessant und in vielerlei Hinsicht auch vielsagend. Sie können aber nicht auf die Grundgesamtheit umgelegt werden.

Auf allen 126 Profilen, die der Inhaltsanalyse unterzogen wurden, waren Teile der Inhalte für „alle" zugänglich. Besonders mit dem Profil-Foto, der Freundesliste und den Seiten, an denen sie Interesse haben, gehen die Probanden freizügig um. Dieses Ergebnis widerlegt manche Aussagen der Umfrage, in der sich viele Befragte verschlossener darstellten. In der Praxis macht es einen großen Unterschied, ob man Daten nur begrenzten Personengruppen oder „allen" zugänglich macht. Diese Tatsache verleiht dem Resultat besondere Relevanz.

Das Experiment, das mit 123 Profil-Besitzerinnen und -Besitzern durchgeführt wurde, brachte das erschreckende Ergebnis, dass 38 % aller Probanden Freundschaftanfragen von fremden Personen annehmen. Dieses Resultat ist etwas niedriger als die Rate von 41 %, die bei einem ähnlichen Experiment im Jahr 2007 herausgefunden wurde (vgl. Kapitel 6.1). Welche Inhalte durch die Bestätigung der Freundschaftsanfrage zugänglich wurden, wurde nicht erhoben. Dass es aber ein enormes Datenvolumen war, das die vertrauensseligen Probanden veröffentlichten, war klar ersichtlich.

Es lässt sich also zusammenfassen, dass unter Facebook-Mitgliedern das Bewusstsein für Privatsphäre zwar teilweise vorhanden ist, das Datenschutz-Wissen und die tatsächliche Kontrolle über die eigenen Daten aber noch immer hinterher hinken. Facebook-Mitglieder haben keinen guten Überblick über ihre Profil-Situation. Sie würden ihre Privatsphäre gerne schützen, gehen aber trotzdem viel zu leichtfertig mit ihren Daten um. Mit diesen Ergebnissen werden nun die Hypothesen überprüft.

7.4. Hypothesen-Prüfung

F1: Wie gut kennen Facebook-Nutzerinnen und -Nutzer die datenschutzbezogenen Rechte, die bei einer Facebook-Mitgliedschaft zum Tragen kommen?

Die Hypothesen-Prüfung zeigt, dass Facebook-Mitglieder die eigenen Rechte schlechter kennen als die Rechte, die sich Facebook bezüglich der Mitglieder-Daten herausnimmt:

H1.1: Weniger als die Hälfte aller Facebook-Mitglieder kennt die Grundlagen des österreichischen Datenschutzgesetzes.

Vier der acht Datenschutz-Fragen in der Umfrage bezogen sich auf das österreichische Datenschutzgesetz. Ihre Auswertung ergab, dass 55 % der Probanden keine davon beantworten

konnten, weitere 25 % gaben nur bei einer der vier Fragen die korrekte Antwort. Keine einzige der 381 Personen wählte bei allen vier Fragen die richtige Antwort. Mit diesem Ergebnis von 80 % an mangelndem Wissen, 20 % des mittelmäßigen Wissens und 0 % an umfassendem Wissen kann **H1.1 bestätigt** werden.

H1.2: Weniger als die Hälfte aller Facebook-Mitglieder kennt die Datenschutzbestimmungen, denen sie auf Facebook zustimmt.

Die Auswertung der vier Fragen zu Facebooks Datenschutzbestimmungen zeigen, dass 19 % der Probanden kein Wissen zum Thema und 26 % ein sehr geringes Wissen haben. 46 % beweisen mit zwei oder drei richtigen Antworten einen mittelmäßigen Wissensstand und 9 % konnten mit ihrem umfassenden Wissen alle vier Fragen korrekt beantworten. Mit 45 % an mangelndem Wissen und 55 % an mittelmäßigem bis gutem Wissen, kann **H1.2 nicht bestätigt** werden. Weniger als die Hälfte der Probanden weisen grobe Wissenslücken auf, was die Datenschutzbestimmung von Facebook betrifft.

F2: Gibt es einen Zusammenhang zwischen Wissen über Datenschutz und den Faktoren Privatsphäre-Sorgfalt und Selbstoffenbarung?

Nur eine der Variablen hängt signifikant vom Datenschutz-Wissen ab:

H2.1: Je besser Userinnen und User über Datenschutz Bescheid wissen, desto sorgfältiger gehen sie mit den Privatsphäre-Einstellungen auf Facebook um.

Diese Hypothese kann **mit einer Signifikanz von p=.000 bestätigt** werden. Eine Korrelation nach Pearson ergab einen positiven Zusammenhang der Variablen Datenschutz-Wissen und Privatsphäre-Sorgfalt (r=.182). Eine Regression bestätigte das Ergebnis mit einer Signifikanz von p=.001.

H2.2: Je besser Userinnen und User über Datenschutz Bescheid wissen, desto weniger geben sie über sich selbst auf ihrem Facebook-Profil preis.

Die Korrelation nach Pearson zeigte zwischen den Variablen Datenschutz-Wissen und Selbstdarstellungsintensität keinen signifikanten Zusammenhang. Die Korrelation verläuft zwar negativ (r=-.031), wie angenommen, das Ergebnis ist jedoch nicht signifikant (p=.545). Somit wird **H2.2 nicht bestätigt**.

H2.3: Je besser Userinnen und User über Datenschutz Bescheid wissen, desto weniger häufig setzen sie Aktionen auf Facebook.

Auch für die Variablen Datenschutz-Wissen und Selbstdarstellungshäufigkeit zeigte die Korrelation nach Pearson einen Zusammenhang in der angenommenen Richtung (r=-.056), jedoch ebenfalls ohne Signifikanz (p=.276). **H2.3 wird nicht bestätigt.**

H2.4: Je besser Userinnen und User über Datenschutz Bescheid wissen, desto weniger Inhalte machen sie „allen" zugänglich.

Eine Korrelation der Ergebnisse der Inhaltsanalyse mit dem Index zum Datenschutz zeigte keinen signifikanten Zusammenhang zwischen den Variablen (p=.552). **H2.4** kann **nicht bestätigt** werden.

F3: Wie großzügig geben Facebook-Mitglieder ihre Daten Personen preis, mit denen sie nicht befreundet sind?

Die Hypothesen-Prüfung zeigt deutlich, dass Facebook-Mitglieder durchwegs freizügig sind, was die Veröffentlichung ihrer eigenen Daten angeht:

H3.1: Nicht alle Facebook-Mitglieder regulieren ihre Privatsphäre-Einstellungen so, dass nur Freunde ihre Profil-Inhalte sehen können.

Alle mittels Inhaltsanalyse untersuchten Profile machten in mindestens einer Kategorie auf Facebook Inhalte der Öffentlichkeit zugänglich. Somit kann **H3.1 eindeutig bestätigt** werden.

H3.2: Viele Facebook-Mitglieder geben ihre Daten großzügig preis, indem sie Freundschaftsanfragen bestätigen, auch wenn sie eine Person nicht kennen.

Im Experiment akzeptierten 38 % der Probanden die Freundschaftsanfrage einer fremden Person. Mit über einem Drittel an bestätigten Anfragen wird **H3.2 bestätigt**.

Die Hypothesen konnten zur Hälfte bestätigt werden, die andere Hälfte wurde verworfen. Besonders interessant erscheint H2.1, die mit hoher Signifikanz bestätigt wurde. Ebenfalls spannend und durch und durch mit der theoretischen Fundierung konform sind die Ergebnisse von H3.1 und H3.2, die beide zeigen, dass Facebook-Mitglieder sehr großzügig mit der Veröffentlichung ihrer Daten umgehen.

7.5. Resumée und Ausblick

Die vorliegende Arbeit beschäftigt sich mit dem Spannungsfeld zwischen Selbstdarstellung und dem Schutz der Privatsphäre im virtuellen Raum. Auf Social Network Seiten wie Facebook findet tagtäglich eine Gratwanderung zwischen den beiden Extremen statt: Einerseits funktioniert ein System wie Facebook nur, wenn die Mitglieder Informationen über sich preisgeben und Inhalte generieren. Andererseits geht damit ein Stück wertvoller Privatsphäre verloren. Userinnen und User können nur dann einen Nutzen aus der Plattform ziehen, wenn sie das Spiel mitspielen: Um vernetzt zu sein, Beziehungen zu pflegen und mit anderen Kontakt zu halten, zahlen sie den Preis des Privatsphäre-Verzichts. Dass das Web2.0 mit all seinen Besonderheiten geradezu geschaffen ist zur freizügigen Selbstdarstellung, wurde in Kapitel 2 beschrieben. Das Web2.0 ist interaktiv – wer online ist, kann mitmachen. Und so werden Inhalte generiert, Meinungen ausgetauscht, Blogs geschrieben, Videos hochgeladen, Social Network Seiten genutzt, und die Userinnen und User werden von Nutzenden zu Produzierenden.

Mit jeder Handlung im Internet geht eine gewisse Selbstdarstellung einher. Und wenn man sich schon einmal selbstdarstellt, will man das meistens auch gut machen. Es liegt in der Natur des Menschen, die eigene Erscheinung ins rechte Licht zu rücken und den Eindruck, den man erweckt, nicht dem Zufall zu überlassen. So betreiben viele im Web2.0 ganz bewusste Selbstdarstellung und präsentieren sich online mit Hilfe von computervermittelter Kommunikation. Darauf wurde in Kapitel 3 ausführlich eingegangen.

Während die Facebook-Gemeinde, Blogger oder eifrige Forum-Mitglieder noch dabei sind, am eigenen Auftritt im Web2.0 zu basteln und durch gezielte Selbstoffenbarung einen gewünschten Eindruck zu hinterlassen, werden im Hintergrund im Internet all ihre Handlungen ausgewertet und als Daten abgespeichert. Das Web2.0 stellt eine riesige Daten-Maschinerie dar, die von vielen Einzelpersonen betrieben wird, deren Profit aber einige wenige Groß-Unternehmen einstreifen. Expertinnen und Experten warnen daher vor allzu freizügiger Mitarbeit am Social Web. Sie plädieren für mehr Datenschutz sowie besseren Schutz der Privatsphäre. Bis die rechtlichen Bestimmungen den stetigen Entwicklungen angepasst werden, obliegt es jeder Person selbst, die eigene Privatsphäre zu wahren. Details zur aktuellen Situation wurden in Kapitel 4 beleuchtet.

Auf Facebook wagen jeden Tag Millionen von Mitgliedern den Spagat zwischen Selbstdarstellung und Privatsphäre. Darum wurde das Soziale Online-Netzwerk als Untersuchungsgegenstand ausgewählt und hinsichtlich der vorgestellten Aspekte erforscht. Es wurde eine dreistufige Studie durchgeführt: Eine Online-Umfrage, eine Inhaltsanalyse von Profilen und ein Experiment sollten Aufschluss über das Datenschutz-Wissen sowie das Selbstdarstellungs- und Privatsphäre-Verhalten der Userinnen und User geben.

Die durchgeführte Studie ergab, dass in der Facebook-Gemeinde ein Mangel an Datenschutz-Wissen herrscht. Die Nutzerinnen und Nutzer wissen also manchmal gar nicht, welches Risiko sie mit der Veröffentlichung von Daten auf Facebook eingehen. Ein Großteil der Probanden zeigte in

der Studie zwar ein Verständnis für die Wichtigkeit der Privatsphäre-Einstellungen, viele von ihnen handeln aber in der Realität nicht gemäß diesem Bewusstsein. Es zeigte sich, dass viele Facebook-Mitglieder sehr freizügig mit den eigenen Daten umgehen. Auf 78 % aller inhaltsanalytisch untersuchten Profile (N=126) waren mehr als drei personenbezogene Daten veröffentlicht. 38 % aller Probanden des Experiments (N=123) bestätigten die Freundschaftsanfrage einer Fremden und zeigten so alle Inhalte, die normalerweise Freunden vorbehalten sind, einer unbekannten Person. Zusätzlich ermöglichten sie dieser Person die Inhalte zu durchstöbern, die die eigenen Freunde „Freunden von Freunden" zugänglich machen. Und 90 % aller Befragten (N=381) verwenden auf Facebook den vollständigen eigenen Namen, was es leicht macht, die personenbezogenen Daten der jeweiligen Person zuzuordnen.

Facebook wird durch die Freizügigkeit der Mitglieder zu einem riesigen Datenkonstrukt. Die Gratifikationen erzielen damit nicht nur die Userinnen und User, die die Plattform für ihre Vernetzung schätzen, sondern vor allem die Macher von Facebook. In letzter Zeit wurde vermehrt Kritik diesbezüglich laut, und Proteste gegen Datenmissbrauch drangen an die Medien und wurden ausgiebig kommuniziert. Die Bestandsaufnahme durch die vorliegende Studie zeigt, dass die Relevanz von Privatsphäre trotzdem noch nicht bis zum letzten Facebook-Mitglied vorgedrungen ist. Noch immer können unzählige ungeschützte Daten aus Facebook gezogen werden, die Mitglieder unter Verzicht auf Datenschutz freizügig veröffentlichen.

Die Freizügigkeit der Facebook-Gemeinde erschreckt, sie überrascht jedoch nicht. Die Ergebnisse gehen mit der theoretischen Fundierung des Themas überein und bestätigen den aktuellen Forschungsstand. Obwohl die Resultate nicht gerade erbaulich sind, gibt es Hoffnung. Einerseits scheint das Bewusstsein für Privatsphäre zu steigen: Nach und nach beginnen Facebook-Mitglieder, ihre Privatsphäre-Einstellungen zu überprüfen und somit die Verantwortung für die eigenen Daten zu übernehmen. Und andererseits liefert die vorliegende Arbeit ein relevantes Ergebnis für Verbesserungen: Die Studie zeigte einen signifikant positiven Zusammenhang (p=.000) zwischen dem Wissen über Datenschutz und der Sorgfalt, mit der man Privatsphäre-Einstellungen reguliert. Der Schlüssel zu verantwortungsbewussteren Facebook-Mitgliedern liegt also in gezielter Aufklärung und der Verbesserung des Datenschutz-Wissens.

Die durchgeführte Untersuchung stellt eine Momentaufnahme dar. Sie bildet ab, welches Datenschutz-Wissen Facebook-Userinnen und –User zum gegebenen Zeitpunkt haben und wie sie sich auf Facebook verhalten unter den Bedingungen, die zur Zeit der Erhebung herrschten. Da Facebook ein sehr dynamischer Untersuchungsgegenstand ist, ändern sich diese Bedingungen laufend und mit ihnen ändert sich vielleicht auch das Verhalten der Mitglieder. Facebook entwickelt sich ständig weiter, die Medien greifen das Thema immer kritischer auf, und Datenschutzorganisationen sind bemüht um strengere Regelungen. Das eröffnet einige spannende neue Forschungsfelder. Ändern Facebook-Mitglieder ihren Umgang mit den eigenen Privatsphäre-Einstellungen? Erhöht sich ihr Wissen zum Thema Datenschutz? Wie beschrieben, besteht ein signifikanter Zusammenhang zwischen Datenschutz-Wissen und Privatsphäre-Sorgfalt. Es kann also davon ausgegangen werden, dass Facebook-Mitglieder verantwortungsbewusster mit ihren Daten

umgehen, wenn sie erst einmal das nötige Wissen über Datenschutz haben. Ziel ist es darum, das Wissen der Userinnen und User sowohl über Datenschutz als auch über die Relevanz der Privatsphäre zu verstärken. Die vorliegende Arbeit sieht sich als Teil einer großen Bewusstseins-Kampagne im Kampf gegen den Abbau der Privatsphäre. Es bleibt zu hoffen, dass viele weitere Arbeiten zum Thema folgen und das Web2.0 neben all den Gratifikationen, die es der Anhängerschaft bringt, auch bald mit Daten-Sicherheit dienen kann.

QUELLENVERZEICHNIS

Literatur

Atteslander, Peter (2008): Methoden der empirischen Sozialforschung. 12., durchgesehene Auflage. Berlin: Erich Schmidt Verlag GmbH & Co.

Bahl, Anke (2002): Zwischen On- und Offline. Identität und Selbstdarstellung im Internet. München: KoPäd Verlag.

Barth, Josef (2007): www.anonymitaet.ade. In: Profil Nr. 37. 10. September 2007. S.110-116

Bayersburg, Frédéric (2009): Selbstdarstellung auf Social-Network-Plattformen am Beispiel MySpace. Magisterarbeit, Universität Wien.

Benesch, Thomas (2008): Anschauliche und verständliche Datenbeschreibung. Methoden der deskriptiven Statistik. 4., überarbeitete Auflage. Wien: Neuer wissenschaftlicher Verlag.

Berners-Lee, Tim/Hendler, James/Lassila, Ora (2001): The Semantic Web. A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities. In: Scientific American Magazine, May 2001, Issue 5, S.34-43

Bortz, Jürgen/Döring, Nicola (2002): Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler. 3. Überarbeitete Auflage. Berlin, Heidelberg: Springer.

Boyd, Danah (2008): Facebook's Privacy Trainwreck. Exposure, Invasion, and Social Convergence. In: Convergence 2008, Vol. 14(1), S.13-20. Online: http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf abgerufen am 13.2.2010

Boyd, Danah (2010): "Making Sense of Privacy and Publicity". Vortrag auf dem SXSW (South by Southwest Festival) am 13. März 2010. Online: http://www.danah.org/papers/talks/2010/SXSW2010.html abgerufen am 10.06.2010

Boyd, D. M./Ellison, N. B. (Hg.) (2007): Social Network Sites: Definition, History and Scholarship. In: Journal of Computer-Mediated Communication, Vol. 13, Issue 1, October 2007. Online: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html abgerufen am 13.2.2010

Bruns, Axel (2007): Produsage: Towards a Broader Framework for User-Led Content Creation. Online: http://snurb.info/files/Produsage%20(Creativity%20and%20Cognition%202007).pdf abgerufen am 13.2.2010

Bucher, Hans-Jürgen/Erlhofer, Sebastian/Kallass, Kerstin/Leibert, Wolf-Andreas (2008): Netzwerkkommunikation und Internet-Diskurse: Grundlagen eines netzwerkorientierten Kommunikationsbegriffs. In: Zerfaß, Ansgar/Welker, Martin/ Schmidt, Jan (Hg.): Kommunikation, Partizipation und Wirkungen im Social Web. Band 1: Grundlagen und Methoden: Von der Gesellschaft zum Individuum. Aus der Reihe: Neue Schriften zur Online Forschung, herausgegeben von der Deutschen Gesellschaft für Online-Forschung (DGOF). Köln: Herbert von Halem Verlag. S.41-61

Buffardi, Laura E./Campbell, W. Keith (2008): Narcissism and Social Networking Web Sites. In: Personality and Social Psychology Bulletin, 2008, Vol. 34, S.1303-1315.

Cassidy, John (2006): Me Media. How hanging out on the Internet became big business. In: The New Yorker. 15. May 2006. Online: http://www.newyorker.com/archive/2006/05/15/060515fa_fact_cassidy abgerufen am 12.4.2010

Chester, Andrea/Bretherton, Di (2007): Impression management and identity online. In: Joinson, Adam/McKenna, Katelyn/Postmes, Tom/Reips, Ulf-Dietrich (Hg.): The Oxford Handbook of Internet Psychology. New York: Oxford University Press 2007. S.223-236

Der Standard: Facebook kündigt Regler für Privatsphäre an. Netzwerk gibt Druck wegen Datenweitergabe nach. 28.5.2010. S.20

Der Standard: Österreicher nehmen Schutz persönlicher Daten nicht genau. 25.5.2010. S.8

Diaz-Bone, Rainer (2006): Eine kurze Einführung in die sozialwissenschaftliche Netzwerkanalyse. Mitteilungen aus dem Schwerpunktbereich Methodenlehre Nr. 57. Berlin: Institut für Soziologie, Freie Universität Berlin. Online: http://www.rainer-diaz-bone.de/Diaz-Bone_Netzwerkanalyse.pdf abgerufen am 13.5.2010

Döring, Nicola (2008): Freunde zum Anklicken. Nutzen und Gefahren von Online-Netzwerken. In: Psychologie Heute, 2008, Vol 35, S.28-31

Döring, Nicola (2003): Sozialpsychologie des Internet. Die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen. 2., völlig überarbeitete und erweiterte Auflage. Aus der Reihe: Internet und Psychologie. Neue Medien in der Psychologie. Herausgegeben von Dr. Bernad Batinic. Band 2. Göttingen: Hogrefe-Verlag GmbH &Co. KG.

Drobesch, Heinz/Grosinger, Walter (2000): Das neue österreichische Datenschutzgesetz. Datenschutzgesetz 2000. Wien: Juridica Verlag GmbH.

Duden. Band 5. Das Fremdwörterbuch. 7., neu bearbeitete und erweiterte Auflage. Mannheim: Dudenverlag 2001

Ebersbach, Anja/Glaser, Markus/Heigl, Richard (2008): Social Web. Stuttgart: UVK VerlagsgesmbH.

Etzioni Amitai/Etzioni, Oren (1999): Face-to-Face and Computer-Mediated Communities, a Comparative Analysis. In: The Information Society Vol. 15, No. 4. S.241-248. Online: http://www.gwu.edu/~ccps/etzioni/E31.html abgerufen am 10.6.2010

Früh, Werner (2007): Inhaltsanalyse. Theorie und Praxis. 6., überarbeitete Auflage. Konstanz: UVK VerlagsgmbH.

Fuchs, Christian (2009): Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance. Salzburg/Vienna: Forschungsgruppe UTI. Online: http://fuchs.icts.sbg.ac.at/SNS_Surveillance_Fuchs.pdf abgerufen am 10.6.2010

Gerhards, Maria/Klingler, Walter/Trump, Thilo (2008): Das Social Web aus Rezipientensicht: Motivation, Nutzung und Nutzertypen. In: Zerfaß, Ansgar/Welker, Martin/ Schmidt, Jan (Hg.): Kommunikation, Partizipation und Wirkungen im Social Web. Band 1: Grundlagen und Methoden: Von der Gesellschaft zum Individuum. Aus der Reihe: Neue Schriften zur Online Forschung, herausgegeben von der Deutschen Gesellschaft für Online-Forschung (DGOF). Köln: Herbert von Halem Verlag. S.129-148

Ghazal, Nadya (2010): Schutz der Persönlichkeit im Internet. In: Jaksch-Ratajczak (Hg.): Aktuelle Rechtsfragen der Internetnutzung. Wien: facultas.wuv

Goffman, Erving (2007): Wir alle spielen Theater. Die Selbstdarstellung im Alltag. 5. Auflage. München: Piper Verlag.

Götzenbrucker, Gerit (2008): Beyond Impression. Kommunikationskultur und soziale Praxis auf Social Network Sites am Beispiel von StudiVZ. Online: http://user.uni-frankfurt.de/~chris/Stuttgart-Symposium/Gerit_Goetzenbrucker.pdf abgerufen am 24.3.2010

Gross, Ralph/Acquisti, Alessandro (2005): Information Revelation and Privacy in Online Social Networks (The Facebook case). Pittsburgh: Carnegie Mellon University. Online: http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf abgerufen am 16.6.2010

Haythornthwaite, Caroline (2007): Social networks and online community. In: Joinson, Adam/McKenna, Katelyn/Postmes, Tom/Reips, Ulf-Dietrich (Hg.): The Oxford Handbook of Internet Psychology. New York: Oxford University Press. S.121-137

Hecht, Judith: Große Wirkung im Web2.0. In: Der Standard, Album. 22.5.2010. K18

Herbold, Astrid (2009): Das große Rauschen. Die Lebenslügen der digitalen Gesellschaft. München: Droemer.

Hippner, Hajo (2006): Bedeutung, Anwendung und Einsatzpotenziale von Social Software. In: Hildebrand, Knut/Hofmann, Josephine (Hg.): Social Software. Aus der Reihe: HMD – Praxis der Wirtschaftsinformatik. Heft 252, Dezember 2006. Heidelberg: dpunkt.verlag GmbH.

Janisch, Sonja/Mader, Peter (2006): E-Business. 3. neu bearbeitete und erweiterte Auflage. Aus der Reihe: Praxis-Rechtsskripten. Wien: LexisNexis Verlag

Jansen, Dorothea (2006): Einführung in die Netzwerkanalyse. Grundlagen, Methoden, Forschungsbeispiele. 3., überarbeitete Auflage. Wiesbaden: VS Verlag

Joinson, Adam N./Paine, Carina B. (2007): Self-disclosure, privacy and the Internet. In: Joinson, Adam/McKenna, Katelyn/Postmes, Tom/Reips, Ulf-Dietrich (Hg.): The Oxford Handbook of Internet Psychology. New York: Oxford University Press. S.237-252

Kuhlen, Rainer (2004): Informationsethik. Umgang mit Wissen und Information in elektronischen Räumen. Konstanz: UVK Verlagsgesellschaft mbH.

Marwick, Alice (2005): “I’m a Lot More Interesting than a Friendster Profile”: Identity Presentation, Authenticity and Power in Social Networking Services. Chicago. Online: http://www.tiara.org/papers/ abgerufen am 17.4.2010

Mayer-Schönberger, Viktor / Brandl, Ernst O. (2006): Datenschutzgesetz. Grundsätze und europarechtliche Rahmenbedingungen. Gesetzestext mit Materialien. Datenschutz-Verordnungen und Richtlinien im Anhang. 2., überarbeitete Auflage. Wien: Linde Verlag

McKenna, Katelyn Y.A. (2007): Through the Internet looking glass: expressing and validating the true self. In: Joinson, Adam/McKenna, Katelyn/Postmes, Tom/Reips, Ulf-Dietrich (Hg.): The Oxford Handbook of Internet Psychology. New York: Oxford University Press. S.205-221

Michel, Ulrike: .DATENSCHUTZGESETZ 2000. Datenschutz geht und alle an. Was ist EKIS? Eine Broschüre der Republik Österreich. Bundesministerium für Inneres. Online: http://www.bmi.gv.at/cms/BMI_Datenschutz/Datenschutzgesetz2000_Broschuere.pdf abgerufen am 27.1.2010 abgerufen am 6.4.2010

Misoch, Sabina (2006): Online-Kommunikation. Konstanz: UVK Verlagsgesellschaft mbH.

Misoch, Sabina (2004): Identitäten im Internet. Selbstdarstellung auf privaten Homepages. Konstanz: UVK Verlagsgesellschaft mbH.

Musser, John/O'Reilly Tim (2006): Web 2.0 Principles and Best Practices. O'Reilly Radar. Executive Summary Online: http://oreilly.com/catalog/web2report/chapter/web20_report_excerpt.pdf abgerufen am 12.12.2009

Nagl, Johannes (2008): Datenschutz und Informationssicherheit in Social Communities. Klosterneuburg. Diplomarbeit, Fachhochschule Technikum Wien. Online: http://johannes.nagl.name/publications/2008/DatenschutzInformationssicherheitSocialCommunities.pdf abgerufen am 15.6.2010

Oekonsult (2010): Datenhunger und Überwachungswahn. Bundesweite, repräsentative OEKONSULT Umfrage unter 1100 Personen. Mai 2010. Online: http://www.oekonsult.eu/datenhunger_final.pdf abgerufen am 1.6.2010

O'Reilly, Tim (2005): What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software. O'Reilly Verlag.

O'Reilly, Tim/Battelle, John (2009): Web Squared: Web 2.0 Five Years On. Web2.0 summit. O'Reilly Media.

Öffentliche Sicherheit. Das Magazin des Innenministeriums. Nr.11-12/2001. Lattacher, Siegbert: Lauschangriff und Rasterfahndung. Unverzichtbares Instrument. Online: http://www.bmi.gv.at/cms/BMI_OeffentlicheSicherheit/2001/11_12/Artikel_04.aspx abgerufen am 7.3.2010

Öffentliche Sicherheit. Das Magazin des Innenministeriums. Nr.1-2/2008. S 51. Waffengleichheit herstellen. Online: http://www.bmi.gv.at/cms/BMI_OeffentlicheSicherheit/2008/01_02/files/Online_Durchsuchung.pdf abgerufen am 7.3.2010

Reinecke, Leonard/Trepte, Sabine (2008): Privatsphäre 2.0: Konzepte von Privatheit, Intimsphäre und Werten im Umgang mit „user-generated-content“. In: Zerfaß, Ansgar/Welker, Martin/ Schmidt, Jan (Hg.): Kommunikation, Partizipation und Wirkungen im Social Web. Band 1: Grundlagen und Methoden: Von der Gesellschaft zum Individuum. Aus der Reihe: Neue Schriften zur Online Forschung, herausgegeben von der Deutschen Gesellschaft für Online-Forschung (DGOF). Köln: Herbert von Halem Verlag. S.205-228

Rosenblat, Tanya S./Mobius, Markus M. (2004): Getting Closer or Drifting Apart? In: Quarterly Journal of Economics, August 2004, Vol. 119, S 971–1009.

Schaar, Peter (2007): Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft. München: C.Bertelsmann.

Schenk, Michael (1984): Soziale Netzwerke und Kommunikation. Tübingen: J. C. B. Mohr.

Schenk, Michael (1995): Soziale Netzwerke und Massenmedien. Untersuchungen zum Einfluß der persönlichen Kommunikation. Tübingen: J. C. B. Mohr.

Schmidt, Jan (2008): Was ist neu im Social Web? Soziologische und kommunikationswissenschaftliche Grundlagen. In: Zerfaß, Ansgar/Welker, Martin/ Schmidt, Jan (Hg.): Kommunikation, Partizipation und Wirkungen im Social Web. Band 1: Grundlagen und Methoden: Von der Gesellschaft zum Individuum. Aus der Reihe: Neue Schriften zur Online Forschung, herausgegeben von der Deutschen Gesellschaft für Online-Forschung (DGOF). Köln: Herbert von Halem Verlag. S.18-40

Schneider, Roman (2008): Web 3.0 ante portas? Integration von Social Web und Semantic Web. In: Zerfaß, Ansgar/Welker, Martin/ Schmidt, Jan (Hg.): Kommunikation, Partizipation und Wirkungen im Social Web. Band 1: Grundlagen und Methoden: Von der Gesellschaft zum Individuum. Aus der Reihe: Neue Schriften zur Online Forschung, herausgegeben von der Deutschen Gesellschaft für Online-Forschung (DGOF). Köln: Herbert von Halem Verlag. S.112-128

Semrad E./Siebert N./Pesendorfer D. (2010): So gefährlich sind facebook & Co. Die Internet-Falle. Kick, Mobbing, Datenklau: Wie wir unsere Privatsphäre im Netz aufs Spiel setzen. In: News Nr.18. 6.Mai 2010. S.32-38

Spudich, Helmut (2010a): Facebook-Exitstrategien. In: Der Standard. 27.5.2010. S.16

Spudich, Helmut (2010b): Das Unbehagen mit der Veröffentlichungskultur. In: Der Standard. 22.5.2010. S.3

Stegbauer, Christian (Hg.) (2008): Netzwerkanalyse und Netzwerktheorie. Ein neues Paradigma in den Sozialwissenschaften. Aus der Reihe: Netzwerkforschung. Band 1. Wiesbaden: VS Verlag für Sozialwissenschaften.

Stegbauer, Christian (2008): Wikipedia und die Bedeutung der sozialen Netzwerke. Netzwerkanalyse liefert Einblicke, wie soziale Prozesse das Handeln Einzelner bestimmen. In: Forschung Frankfurt 2/2008, S.12-18

Steinschaden, Jakob (2010): Facebook greift nach der Internet-Herrschaft. In: Kurier, 1. Ausgabe, Nr.112, 23. April 2010, S.16-17.

Sterbik-Lamina, Jaro et al. (2009): Privatsphäre 2.0. Beeinträchtigung der Privatsphäre in Österreich. Neue Herausforderungen für den Datenschutz. Endbericht. Studie im Auftrag der Bundesarbeitskammer. Wien.

Szugat, Martin/Gewehr, Jan Erik/Lochmann, Cordula (2006): Social Software. Blogs, Wikis & Co. entwickler.press.

Testbericht der Stiftung Warentest (2010): Datenschutz bei Onlinenetzwerken: Ungeschützt. In: test. Das Magazin der Stiftung Warentest 4/2010. S.40-45

Trojanow, Ilija/Zeh, Juli (2009): Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau der bürgerlichen Rechte. München: Carl Hanser Verlag.

Tzschentke, Karin (2010): Österreich stoppt Google Street View. In: Der Standard. Net Business. 28.5.2010. S.20

Westerhoff, Nikolas (2008): Geborgenheit oder Einengung: Wie wichtig sind soziale Netze? In: Psychologie Heute, 2008, Vol 35, S.21-25

Westerhoff, Nikolas (2008): „Im Durchschnitt unterhält ein Mensch elf Beziehungen“ Interview mit Dr.Sören Petermann. In: Psychologie Heute, 2008, Vol 35, S.26-27

Weyer, Johannes (2000): Soziale Netzwerke. Konzepte und Methoden der sozialwissenschaftlichen Netzwerkforschung. Aus der Reihe: Lehr- und Handbücher der Soziologie. München: Oldenbourg Wissenschaftsverlag.

Zeger, Hans G. (2008): Mensch.Nummer.Datensatz: Unsere Lust an totaler Kontrolle. St. Pölten: Residenz Verlag.

Zeger, Hans G. (2009): Paralleluniversum Web 2.0. Wie Online-Netzwerke unsere Gesellschaft verändern. Wien: Kremayr & Scheriau.

Zimmer, Daniela (2009): Facebook, MySpace & Co. Soziale Netzwerke im Internet, Analyse und Tipps. Ratgeber der AK Wien.

Online-Quellen

Die Abrufungs-Daten beziehen sich auf den letzten Zeitpunkt, zu dem ein Link kontrolliert wurde.

Aichinger, Philipp (2009): Keine Chance gegen Facebook-Spionage. 2.3.2009. Auf: Die Presse online: http://diepresse.com/home/recht/rechtallgemein/457150/index.do abgerufen am 28.5.2010

Alexa – The Web Information Company: http://www.alexa.com/topsites abgerufen am 16.6.2010
Alexa analysiert 4,5 Milliarden Webseiten weltweit und erstellt Traffic-Rankings.

Amtsblatt der Europäischen Gemeinschaften 2000/C 364/01: Charta der Grundrechte der europäischen Union: www.europarl.europa.eu/charter/pdf/text_de.pdf abgerufen am 5.3.2010

ARD-ZDF Onlinestudie: www.ard-zdf-onlinestudie.de/ abgerufen am 27.11.2009

ARGE DATEN – Österreichische Gesellschaft für Datenschutz: www.argedaten.at abgerufen am 16.6.2010

ARGE DATEN (2010): Österreichische Datenschutzkommission verbietet Googles Street View. 28.5.2010: http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=63497usw abgerufen am 28.5.2010

ARGE DATEN (2009): Grauslichkeiten2.0 – Europäischer Datenschutztag in Österreich. 30.1.2009: http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=57754cvx abgerufen am 28.5.2010

Berger, Anette (2007): Mitmach-Web als Millionärsgarantie. Verkauf von Facebook-Anteilen. 26.10.2007. Auf: Stern online: http://www.stern.de/digital/online/verkauf-von-facebook-anteilen-mitmach-web-als-millionaersgarantie-601046.html abgerufen am 28.5.2010

Bundesministerium für Inneres: Kriminalstatistik 2009: http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/files/2009/Jahresstatistik_2009_1.pdf abgerufen am 18.5.2010

Bundesministerium für Inneres: Presseaussendung vom 13.5.1998: Schlögl informiert Plenum über Letztstand der Briefbombenermittlungen http://www.parlament.gv.at/PG/PR/JAHR_1998/PK0317/PK0317.shtml abgerufen am 18.5.2010

Der Standard online: Facebook reagiert und bessert bei Privacy-Einstellungen nach. 27.5.2010: http://derstandard.at/1271377565799/Kritik-Facebook-reagiert-und-bessert-bei-Privacy-Einstellungen-nach abgerufen am 27.5.2010

Der Standard online: Immer mehr Nutzer wollen Facebook-Profil löschen. 11.5.2010: http://derstandard.at/1271376425782/Ausstieg-Immer-mehr-Nutzer-wollen-Facebook-Profil-loeschen abgerufen am 13.5.2010

Der Standard online: Chaos Computer Club warnt vor der „Datenkrake“ Facebook. 6.4.2010: http://derstandard.at/1269449004008/Chaos-Computer-Club-warnt-vor-der-Datenkrake-Facebook abgerufen am 13.5.2010

Der Standard online: Ab 2010 werden alle Telefon- und Internet-Verbindungen gespeichert. 6.11.2009: http://derstandard.at/1256744163647/Ueberwachung-20-Ab-2010-werden-alle-Telefon--und-Internet-Verbindungen-gespeichert abgerufen am 13.5.2010

Die Presse online: „Quit Facbook Day“ interessierte kaum jemanden. 1.6.2010: http://diepresse.com/home/techscience/internet/570463/index.do?_vl_backlink=/home/techscience/index.do abgerufen am 1.6.2010

Die Presse online: Facebook schaltet schlanke "Lite"-Version ab. 21.4.2010: http://diepresse.com/home/techscience/internet/559719/index.do?_vl_backlink=/home/techscience/internet/index.do abgerufen am 13.5.2010

Digital Affairs: http://digitalaffairs.at abgerufen am 6.6.2010
Digtial Affairs ist eine Social Media Agentur. Im Blog der Homepage werden täglich die neuesten Userzahlen zu Facebook und netlog veröffentlicht. Diese Zahlen sind kein Geheimnis, sie werden in den Werbeplanungstools von Facebook und netlog immer aktuell angezeigt. Das Team von Digital Affairs hat eine Methode entwickelt, die Userzahlen täglich nach Altersgruppen und Geschlecht zu erheben.

Facebook – Datenschutzrichtlinien (Stand 22. April 2010):
http://www.facebook.com/terms.php?ref=pf#/policy.php abgerufen am 28.5.2010

Facebook – Erklärung der Rechte und Pflichten (Stand 22. April 2010):
http://www.facebook.com/terms.php?ref=pf# abgerufen am 28.5.2010

Facebook – Pressebereich: www.facebook.com/press.php abgerufen am 21.4.2010

Facebook – Privatsphäre-Einstellungen:
http://www.facebook.com/settings/?tab=privacy#/settings/?tab=privacy abgerufen am 16.6.2010

GfK Austria – Online Monitor:
http://www.gfk.at/sectors_and_markets/media/media_research/mediasub/002820/index.de.html abgerufen am 28.5.2010

Google Street View: http://www.google.de/help/maps/streetview/behind-the-scenes.html abgerufen am 28.5.2010

Hack, Günther (2009): EuGH bestätigt Vorratsdatenspeicherung. 10.2.2009. Auf: ORF Futurezone:
http://futurezone.orf.at/stories/1502409/ abgerufen am 23.3.2010

Hutter, Thomas (2010): Facebook: Der ultimative Facebook Privatsphäre Leitfaden. 12.5.2010 Auf: thomashutter.com – Blog zu Social Media, Facebook, Twitter, Online-Marketing:
http://www.thomashutter.com/index.php/2010/05/facebook-der-ultimative-facebook-privatsphaere-leitfaden/ abgerufen am 21.5.2010

Kapeller, Reiner (2010): Facebook macht den nächsten Schritt. 23.4.2010. Auf: digitalaffairs.at:
http://networkedblogs.com/3bVgH abgerufen am 28.4.2010

Lime Survey: www.limesurvey.org abgerufen am 2.6.2010

Lischka, Konrad (2010): Neue Regeln. Facebook macht mehr öffentlich. 20.4.2010. Auf: Spiegel online: http://www.spiegel.de/netzwelt/web/0,1518,689990,00.html abgerufen am 20.4.2010

Lischka, Konrad (2009): Schritt für Schritt. So schotten Sie ihr Facebook-Profil ab. 17.12.2009. Auf: Spiegel online: http://www.spiegel.de/netzwelt/web/0,1518,667331,00.html abgerufen am 21.5.2010

Österreichische Datenschutzkommission: www.dsk.gv.at abgerufen am 15.6.2010

Österreichische Datenschutzkommission: Google Street View. Mai 2010:
http://www.dsk.gv.at/site/6733/default.aspx abgerufen am 28.5.2010

QuitFacebookDay: Plattform zum kollektiven Facebook-Austritt am 31. Mai 2010:
http://www.quitfacebookday.com/ abgerufen am 2.6.2010

Rechtsinformationssystem des Bundeskanzleramts (RIS BKA) – Bundesrecht: Gesamte Rechtsvorschrift für Datenschutzgesetz 2000, Fassung vom 30.05.2010: http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597 abgerufen am 30.5.2010

Reißmann, Ole (2010): Facebook-Chef zeigt neue Datenschutz-Optionen. Auf: Spiegel online. 26.5.2010: http://www.spiegel.de/netzwelt/web/0,1518,696956,00.html abgerufen am 27.5.2010

ReputationDefender. Der zuverlässige Schutz für Ihren Ruf und Ihre Privatsphäre im Internet: http://www.reputationdefender.com/ abgerufen am 12.2.2010

Saubere Weste. Wir verteidigen Ihr Image im Internet: http://www.sauberereweste.de/ abgerufen am 12.2.2010

Sophos – Unternehmen für Antiviren- und Antispam-Software. Unternehmens-Profil: http://www.sophos.de/companyinfo/ abgerufen am 1.6.2010

Sophos: Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. 14.8.2007: http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html abgerufen am 4.6.2010

SpreeSee –Blog. Facebook Gebrauchsanleitung. 8.7.2009: http://spreesee.com/2009/07/08/facebook-gebrauchsanleitung/ abgerufen am 21.5.2010

Statistik Austria – Bevölkerung Österreich 1. Quartal 2010: http://www.statistik.at/web_de/statistiken/bevoelkerung/bevoelkerungsstand_und_veraenderung/bevoelkerung_zu_jahres-_quartalsanfang/index.html abgerufen am 1.6.2010

SXSW – South by Southwest: www.sxsw.com abgerufen am 15.6.2010

Weigert, Martin (2008): Die Ära der Facebook-Applikationen ist vorbei. 14.12.2008. Auf: netzwertig.com: http://netzwertig.com/2008/12/14/die-aera-der-facebook-applikationen-ist-vorbei abgerufen am 12.1.2010
netzwertig.com ist lt. eigener Definition ein Blog der Blogwerk AG über die Internet-Ökonomie. Seit Mai 2008 wird über Entwicklungen in der Internet-Wirtschaft, ihre Auswirkungen international und insbesondere auf den deutschen Sprachraum berichtet.

Weigert, Martin (2010): Facebook übernimmt das Netz. 21.4.2010. Auf: netzwertig.com: http://netzwertig.com/2010/04/21/f8-facebook-uebernimmt-das-netz/ abgerufen am 28.4.2010

Wikipedia – Über Wikipedia: http://de.wikipedia.org/wiki/Wikipedia:%C3%9Cber_Wikipedia abgerufen am 3.1.2010

Homepage des World Wide Web Consortium (W3C): http://www.w3.org/ abgerufen am 4.1.2010
Das World Wide Web Consortium (W3C) ist nach eigener Definition eine internationale Vereinigung zur Entwicklung von Standards, die das langfristige Wachstum des Webs sicherstellen soll.

Yarow, Jay/Angelova, Kamelia (2010): CHART OF THE DAY: Almost Half Of You Are Checking Facebook As Soon As You Wake Up. 24.3.2010. Auf: businessinsider.com: http://www.businessinsider.com/chart-of-the-day-twitter-facebook-updates-in-the-morning-2010-3?utm_source=Triggermail&utm_medium=email&utm_campaign=SAI_COTD_032410 abgerufen am 28.4.2010

YouTube – „At My Wedding Twitterring and Facebooking at the Altar": http://www.youtube.com/watch?v=VSkT5XykJzo abgerufen am 14.1.2010

Zeger, Hans G. (2010): Vorratsdatenspeicherung ist Beginn präventivstaatlicher Maßnahmen. 6.5.2010: http://www2.argedaten.at/php/cms_monitor.php?q=AD-NEWS-LAST abgerufen am 28.5.2010

Zsolt, Wilhelm (2010): „Facebook gerät außer Kontrolle": Zeit sich zu wehren. 10.5.2010. Auf: Der Standard online: http://derstandard.at/1271376317644/Aufschrei-Facebook-geraet-ausser-Kontrolle-Zeit-sich-zu-wehren abgerufen am 15.5.2010

Andere Quellen

Club2: Macht uns das Internet dumm? 5.5.2010 um 23:30 auf ORF2. Es diskutierten bei Corinna Milborn: Frank Schirrmacher, Angelika Hager, Luca Hammer, Hubert Poppe, Daniela Zimmer, Helmut Spudich. Online: http://tvthek.orf.at/programs/1283-Club-2/episodes/1381972-CLUB-2--Macht-uns-das-Internet-dumm-/1385641-CLUB-2 abgerufen am 6.5.2010

OGH Entscheidung: 3.9.2002, 11 Os 109/01. Online: http://www.ris.bka.gv.at/Dokumente/Justiz/JJR_20020903_OGH0002_0110OS00109_0100000_001/JJR_20020903_OGH0002_0110OS00109_0100000_001.html abgerufen am 12.5.2010

Telefonat mit Frau Mag. Zimmer, Datenschutz-Expertin der Arbeiterkammer Wien, am 17. Mai 2010.

Zuckerberg, Mark (2009): Offener Brief an alle Facebook-Mitglieder.

ABBILDUNGS- & TABELLENVERZEICHNIS

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

ANHANG

Online-Fragebogen

Hallo,
danke, dass du dem Link gefolgt bist!
Für meine Magisterarbeit an der Uni Wien untersuche ich Zusammenhänge zwischen Facebook und Datenschutz. Ich freue mich, wenn du dazu ein paar Fragen beantwortest. Es wird ca. 5 Minuten dauern.
Deine Daten werden streng vertraulich behandelt und absolut anonym ausgewertet.
Als Dankeschön für deine Teilnahme gibt es am Ende des Fragebogens ein Gewinnspiel. Unter allen Teilnehmerinnen und Teilnehmern werden ein 50 € Niedermeyer-Gutschein ein 30 € dm-Gutschein verlost.
Falls du Fragen und/oder Anregungen hast, kannst du mich gerne kontaktieren:
christine.weilhartner@gmail.com

Demographie:

Geschlecht

- □ Weiblich
- □ Männlich

Wie alt bist du?

- □ Unter 21
- □ 21 – 30
- □ 31 – 40
- □ 41 – 50
- □ 51 – 60
- □ Über 60

Was ist deine höchste abgeschlossene Ausbildung?

- □ Noch in der Schule
- □ Pflichtschul-Abschluss
- □ Lehre
- □ Fachschule / Berufsbildende mittlere Schule
- □ Matura / Meisterprüfung
- □ College / Akademie
- □ Hochschulabschluss (Uni, FH)

Derzeit bin ich hauptberuflich

- □ AngestellteR
- □ ArbeiterIn
- □ Führungskraft
- □ selbständig
- □ StudentIn
- □ Schülerin
- □ Auf Job-Suche
- □ Hausfrau/Hausmann
- □ Sonstiges:

Ich habe meinen Lebensmittelpunkt derzeit …

- □ in Österreich
- □ in einem anderen europäischen Land als Österreich
- □ außerhalb von Europa

Facebook-Nutzung allgemein:

Hast du ein Facebook-Profil?

- □ ja
- □ nein

Wenn ja: weiter

Wenn nein: Aus welchem Grund hast du kein Profil auf Facebook? [Textfeld] → **Ende Fragebogen**

Seit wann hast du dein Profil auf Facebook?

- □ Kürzer als 1 Jahr
- □ 1-2 Jahre
- □ 2-3 Jahre
- □ länger als 3 Jahre

Unter welchem Namen läuft dein Profil?

- □ Vor- und Nachname
- □ Nach- und Vorname
- □ Vor- und/oder Nachname abgekürzt
- □ Pseudonym, das etwas mit meinem Namen zu tun hat
- □ Pseudonym, das nichts mit meinem Namen zu tun hat
- □ Sonstiges:

Wie oft meldest du dich im Normalfall bei deinem Profil an?

- □ mehrmals täglich
- □ 1x täglich
- □ mehrmals wöchentlich
- □ 1x wöchentlich
- □ mehrmals wöchentlich
- □ 1x monatlich
- □ seltener als monatlich

Facebook Nutzung:

Wie oft nutzt du die folgenden Anwendungen auf Facebook?

Anwendung	Sehr oft	häufig	manchmal	selten	nie
Ich aktualisiere meinen Status	□	□	□	□	□
Ich schreibe auf die Pinnwand anderer	□	□	□	□	□
Ich veröffentliche Fotos	□	□	□	□	□
Ich poste Links	□	□	□	□	□
Ich kommentiere etwas durch den „Gefällt mir“-Button	□	□	□	□	□
Ich nutze Applikationen (Quiz, Glücksnuss, FarmVille, etc.)	□	□	□	□	□

Seit Kurzem findet man den "Gefällt mir"-Button nicht mehr nur auf Facebook, sondern im ganzen Internet: auf Unternehmens-Homepages, auf Blogs etc.Hast du schon mal außerhalb von Facebook auf den "Gefällt mir"-Button geklickt?

- □ Ja
- □ Nein

Bist du auf Fotos verlinkt?

- □ Ja, auf bis zu 50 Fotos.
- □ Ja, auf bis zu 100 Fotos.
- □ Ja, auf über 100 Fotos.
- □ Nein, ich wurde bis jetzt auf keinem Foto verlinkt.
- □ Nein, ich habe alle Verlinkungen gelöscht.
- □ Ich weiß nicht, ob ich auf Fotos verlinkt bin.

Wenn Ja:
Wie gehst du mit Verlinkungen auf Fotos um?

- □ Ich akzeptiere alle Verlinkungen, mit denen mich jemand auf Fotos markiert.
- □ Ich kontrolliere Fotos, auf denen ich verlinkt werde, und lösche die Markierung, wenn mir das Foto nicht gefällt.
- □ Ich sehe mir die Fotos gar nicht immer an, auf denen ich verlinkt werde.

Hast du auf deinem Facebook-Profil Informationen über dich in folgenden Kategorien eingetragen?(kann auf Facebook nachgesehen werden unter "Profil" - Karteireiter "Info")

	Ja, in dieser Kategorie stehen Angaben.	**Nein, in dieser Kategorie steht nichts.**
Derzeitiger Wohnort	□	□
Heimatstadt	□	□
Beziehungsstatus	□	□
Interesse an (Männern, Frauen)	□	□
Auf der Suche nach (Freundschaft, Verabredungen,…)	□	□
Politische Einstellung	□	□
Religiöse Ansichten	□	□
Interessen	□	□
Anschrift	□	□
Handy-Nummer	□	□

Wenn mindestens 1x nein:
Warum hast du in manchen Kategorien nichts angegeben?

- □ Das Ausfüllen dauerte mir zu lange.
- □ Ich habe noch gar nicht gesehen, dass man das alles ausfüllen kann.
- □ Ich wollte nicht zu viel über mich preisgeben.
- □ Ich fand die Kategorien uninteressant.
- □ Ich wusste nicht, was ich über mich schreiben soll.
- □ Sonstiges:

Privatsphäre:

Priv1: Hast du auf Facebook schon einmal deine Privatsphäre-Einstellungen gecheckt?

- □ Ja, ich habe mir die Einstellungen gleich nach meiner Registrierung angesehen.
- □ Ja, ich habe mir die Einstellungen im Laufe meiner Facebook-Mitgliedschaft angesehen.
- □ Nein, ich war noch nie auf der Seite der Privatsphäre-Einstellungen.
- □ Ich kann mich nicht erinnern, ob ich schon mal auf der Seite der Privatsphäre-Einstellungen war.

Priv2: Hast du etwas an deinen Privatsphäre-Einstellungen verändert?

- □ Nein, ich habe alles so gelassen, wie es vorgeschlagen war.
- □ Ja, ich habe manche Punkte geändert.
- □ Ja, ich habe jeden Punkt einzeln reguliert.
- □ Ich weiß nicht, ob ich etwas geändert habe.

Priv6: Hast du deine "Freunde" auf Facebook in Gruppen unterteilt?

- □ Nein, meine Facebook-Kontakte sind nicht in Gruppen gegliedert.
- □ Ja, meine Facebook-Kontakte sind in 2-3 Gruppen sortiert.
- □ Ja, meine Facebook-Kontakte sind auf mehr als 3 unterschiedliche Gruppen aufgeteilt.
- □ Ich weiß nicht, ob ich meine "Freunde" in Gruppen eingeteilt habe.

Priv3: Wem zeigst du deine Inhalte auf Facebook?

- □ Jeder kann meine Inhalte sehen.
- □ Ich zeige meine Inhalte Freunden.
- □ Ich zeige meine Inhalte Freunden sowie Freunden von Freunden.
- □ Ich habe spezifisch reguliert, welche Personen welche Inhalte sehen können. (Durch unterschiedliche Gruppen oder Auswahl von bestimmten Personen)
- □ Ich weiß es nicht.

Priv4: Wie gehst du mit Freundschaftsanfragen von fremden Personen um?

- □ Ich lehne sie ab.
- □ Ich akzeptiere sie.
- □ Ich sehe mir das Profil der Person an und entscheide dann, ob ich die Anfrage akzeptiere.
- □ Ich schreibe der Person eine Nachricht und frage, woher sie mich kennt.
- □ Ich weiß es nicht. / Ich reagiere unterschiedlich.

Priv5: Wie gehst du mit Freundschaftsanfragen von Personen um, die du nicht magst?

- □ Ich akzeptiere sie vorerst und lösche sie dann wieder.
- □ Ich lehne sie ab.
- □ Ich akzeptiere sie.
- □ Ich weiß es nicht. / Ich reagiere unterschiedlich.

Datenschutz:

Dat1: Für wie öffentlich hältst du deine Daten auf Facebook?

- □ Was ich auf Facebook veröffentliche, kann nur innerhalb von Facebook gesehen werden.
- □ Was ich auf Facebook veröffentliche, kann überall im Internet auftauchen.
- □ Was ich auf Facebook veröffentliche, kann im Internet sowie außerhalb des Internets auftauchen.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Dat3: Schützt das österreichische Datenschutzgesetzt deine Daten auf Facebook?

- □ Das österreichische Datenschutzgesetz besagt, dass meine auf Facebook veröffentlichten Daten geschützt sind.
- □ Das österreichische Datenschutzgesetz schützt Daten, die ich auf Facebook nur begrenzten Personenkreisen zugänglich mache.
- □ Nach den Bedingungen des österreichischen Datenschutzgesetzes sind Daten, die ich auf Facebook stelle, nicht geschützt.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Dat6: Welche deiner Daten dürfen von Facebook weiterverwendet werden?

- □ Facebook darf alle Daten, die ich auf Facebook stelle, verwenden.
- □ Facebook darf die Daten weiterverwenden, die ich "allen" zugänglich mache, nicht aber Daten, deren Privatsphäre-Einstellungen ich beschränke.
- □ Facebook darf nur meine allgemein verfügbaren Daten weiterverwenden (= Name, Profilbild, Verbindungen)
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Dat2: Darfst du laut österreichischem Datenschutzgesetz die Daten anderer Facebook-Mitglieder verwenden?

- □ Ich mache mich strafbar, wenn ich Daten weiterverwende, die von anderen auf Facebook veröffentlicht wurden.
- □ Die Daten auf Facebook werden von den Mitgliedern freiwillig veröffentlicht, darum darf ich sie kopieren und verwenden.
- □ Daten, die von anderen auf Facebook veröffentlicht wurden, darf ich laut österreichischem Datenschutzgesetz nur verwenden, wenn ich vorher den Urheber gefragt habe.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Dat4: Was passiert mit deinen Daten, wenn du deinen Facebook-Account löschst?

- □ Wenn ich mich von Facebook abmelde, werden meine Daten automatisch gelöscht.
- □ Wenn ich mich von Facebook abmelde, kann ich beantragen, dass meine Daten gelöscht werden.
- □ Wenn ich mich von Facebook abmelde, bleiben meine Daten gespeichert.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Dat7: Welche deiner Daten dürfen von befreundeten Facebook-Mitgliedern verwendet werden?

- □ "Facebook-Freunde" dürfen nur Daten weiterverwenden, die ich "allen" zeige.
- □ "Facebook-Freunde" dürfen keine meiner Daten weiterverwenden.
- □ "Facebook-Freunde" dürfen die Daten, die ich ihnen auf meinem Profil zeige, weiterverwenden.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Dat8: Welche deiner Daten dürfen von Dritten (= Personen, mit denen du nicht auf Facebook befreundet bist) weiterverwendet werden?

- □ Dritte dürfen Daten verwenden, die ich "allen" zugänglich mache.
- □ Dritte müssen mich vorher fragen, bevor sie meine Daten verwenden.
- □ Dritte dürfen meine Daten nicht weiterverwenden.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Dat5: Welche Daten speichert Facebook von dir?

- □ Facebook speichert die Inhalte, die ich veröffentliche (Fotos, Kommentare, Links, etc.)
- □ Facebook speichert meine Verbindungsdaten (wann ich welche Aktion setze, von welcher IP-Adresse ich mich einlogge, etc.)
- □ Facebook speichert beides: die veröffentlichten Daten und die Verbindungsdaten.
- □ Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.

Juchui, das war's! Es bleibt nur eine Frage:
Willst du am Gewinnspiel teilnehmen?
Es werden ein 50 € Niedermeyer- und ein 30 € dm-Gutschein verlost. Die Gewinner werden über Facebook verständigt. Wenn du teilnehmen möchtest, gib bitte deinen Facebook-Namen an:

Vielen Dank für's Mitmachen!

Wenn du Interesse an den Ergebnissen meiner Studie hast, lasse ich sie dir gerne zukommen. Gib mir einfach Bescheid:
christine.weilhartner@gmail.com

SPSS Auswertungstabellen

Für wie öffentlich hältst du deine Daten auf Facebook?

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Was ich auf Facebook veröffentliche, kann nur innerhalb von Facebook gesehen werden.	74	19,4	19,4	19,4
	Was ich auf Facebook veröffentliche, kann überall im Internet auftauchen.	154	40,4	40,4	59,8
	Was ich auf Facebook veröffentliche, kann im Internet sowie außerhalb des Internets auftauchen.	112	29,4	29,4	89,2
	Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.	41	10,8	10,8	100,0
	Gesamt	381	100,0	100,0	

Schützt das österreichische Datenschutzgesetz deine Daten auf Facebook?

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Das österreichische Datenschutzgesetz besagt, dass meine auf Facebook veröffentlichten Daten geschützt sind.	23	6,0	6,0	6,0
	Nach den Bedingungen des österreichischen Datenschutzgesetzes sind Daten, die ich auf Facebook stelle, nicht geschützt	148	38,8	38,8	44,9
	Das österreichische Datenschutzgesetz schützt Daten, die ich auf Facebook nur begrenzten Personenkreisen zugänglich mache.	38	10,0	10,0	54,9
	Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.	172	45,1	45,1	100,0
	Gesamt	381	100,0	100,0	

Welche deiner Daten dürfen von Facebook weiterverwendet werden?

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Facebook darf nur meine allgemein verfügbaren Daten verwenden (=Name, Profilbild, Verbindungen).	65	17,1	17,1	17,1
	Facebook darf die Daten weiterverwenden, die ich „allen“ zugänglich mache, nicht aber Daten, deren Privatsphäre-Einstellungen ich beschränke.	96	25,2	25,2	42,3
	Facebook darf alle Daten, die ich auf Facebook stelle, verwenden.	111	29,1	29,1	71,4
	Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.	109	28,6	28,6	100,0
	Gesamt	381	100,0	100,0	

Darfst du laut österreichischem Datenschutzgesetz die Daten anderer Facebook-Mitglieder verwenden?

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Ich mache mich strafbar, wenn ich Daten weiterverwende, die von anderen auf Facebook veröffentlicht wurden.	33	8,7	8,7	8,7
	Daten, die von anderen auf Facebook veröffentlicht wurden, darf ich laut österreichischem Datenschutzgesetz nur verwenden, wenn ich vorher den Urheber gefragt habe.	94	24,7	24,7	33,3
	Die Daten auf Facebook werden von den Mitgliedern freiwillig veröffentlicht, darum darf ich sie kopieren und verwenden.	72	18,9	18,9	52,2
	Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.	182	47,8	47,8	100,0
	Gesamt	381	100,0	100,0	

Was passiert mit deinen Daten, wenn du deinen Facebook-Account löschst?

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Wenn ich mich von Facebook abmelde, werden meine Daten automatisch gelöscht.	25	6,6	6,6	6,6
	Wenn ich mich von Facebook abmelde, kann ich beantragen, dass meine Daten gelöscht werden.	77	20,2	20,2	26,8
	Wenn ich mich von Facebook abmelde, bleiben meine Daten gespeichert.	198	52,0	52,0	78,7
	Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.	81	21,3	21,3	100,0
	Gesamt	381	100,0	100,0	

Welche deiner Daten dürfen von befreundeten Facebook-Mitgliedern verwendet werden?

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	„Facebook-Freunde“ dürfen nur Daten weiterverwenden, die ich „allen“ zeige.	31	8,1	8,1	8,1
	„Facebook-Freunde“ dürfen keine meiner Daten weiterverwenden.	71	18,6	18,6	26,8
	„Facebook-Freunde“ dürfen die Daten, die ich ihnen auf meinem Profil zeige, weiterverwenden.	131	34,4	34,4	61,2
	Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.	148	38,8	38,8	100,0
	Gesamt	381	100,0	100,0	

Welche deiner Daten dürfen von Dritten (= Personen, mit denen du nicht auf Facebook befreundet bist) weiterverwendet werden?

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Dritte dürfen meine Daten nicht weiterverwenden.	92	24,1	24,1	24,1
	Dritte müssen mich vorher fragen, bevor sie meine Daten verwenden.	36	9,4	9,4	33,6
	Dritte dürfen Daten verwenden, die ich „allen“ zugänglich mache.	114	29,9	29,9	63,5
	Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.	139	36,5	36,5	100,0
	Gesamt	381	100,0	100,0	

Welche Daten speichert Facebook von dir?

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Facebook speichert die Inhalte, die ich veröffentliche (Fotos, Kommentare, Links, etc.)	55	14,4	14,4	14,4
	Facebook speichert meine Verbindungsdaten (wann ich welche Aktion setze, von welcher IP-Adresse ich mich einlogge, etc.)	8	2,1	2,1	16,5
	Facebook speichert beides: die veröffentlichten Daten und die Verbindungsdaten.	236	61,9	61,9	78,5
	Ich habe absolut keine Ahnung und auch keine Tendenz zu einer der 3 Antworten.	82	21,5	21,5	100,0
	Gesamt	381	100,0	100,0	

Korrelationen

		Datenschutz	Privatsphäre Summe	SelbstHäuf	SelbstProfil
Datenschutz	Korrelation nach Pearson	1	,182**	-,056	-,031
	Signifikanz (2-seitig)		,000	,276	,545
	N	381	381	381	381
PrivatsphäreSumme	Korrelation nach Pearson	,182**	1	,228**	,011
	Signifikanz (2-seitig)	,000		,000	,825
	N	381	381	381	381
SelbstHäuf	Korrelation nach Pearson	-,056	,228**	1	,365**
	Signifikanz (2-seitig)	,276	,000		,000
	N	381	381	381	381
SelbstProfil	Korrelation nach Pearson	-,031	,011	,365**	1
	Signifikanz (2-seitig)	,545	,825	,000	
	N	381	381	381	381

**. Die Korrelation ist auf dem Niveau von 0,01 (2-seitig) signifikant.

Lebenslauf

Christine Weilhartner

Zur Person

Geburtsdaten	10. September 1983 in Ried im Innkreis (OÖ)
Staatsbürgerschaft	österreichisch
Kontakt	christine.weilhartner@gmail.com

Studium

seit Okt 2007	Magisterstudium Publizistik in Wien
Feb – Juli 2009	Erasmus: Auslandssemester in Rom
Okt 2004 – Aug 2007	Bakkalaureatsstudium Publizistik in Wien Schwerpunkt: Werbung, PR, Markt- & Meinungsforschung

Schule

Mai 2003	BHS-Matura mit Ausgezeichnetem Erfolg
1998 – 2003	Höhere Bundeslehranstalt für wirtschaftliche Berufe in Ried i. I.
1994 – 1998	Bundesgymnasium in Ried i. I.

Praktika und Berufserfahrung

Sep 2008 – Jän 2009	Assistentin der PR Ecker & Partner in Wien
Sep 2006 – Aug 2007	Praktikantin im Marketing Robert Bosch AG Wien
Juli 2003 – Mai 2004	Servierkraft & Hostess Hotel du Vin – Tunbridge Wells, England

Kenntnisse

Deutsch – Muttersprache

Englisch – fließend in Wort und Schrift

Italienisch – fließend in Wort und Schrift

Maschinschreiben & Textverarbeitung

Microsoft Office

SPSS

21. Juni 2010

ABSTRACT

Mit der Entwicklung zum Web2.0 wurde das Internet zu einem kollektiven Projekt: Alle können mitmachen, Inhalte generieren und sich selbst im Netz präsentieren. Dieser Fortschritt eröffnet ein heikles Spannungsfeld zwischen Selbstdarstellung und Privatsphäre. Im Web2.0 machen immer mehr Menschen immer mehr persönliche Informationen immer mehr Fremden zugänglich. Sie veröffentlichen personenbezogene Daten und verzichten damit auf den gesetzlich gewährten Datenschutz. Ein solch leichtfertiges Verhalten im Netz kann schnell zu kritischen Situationen führen. Denn das Internet vergisst nichts. Die vorliegende Arbeit beleuchtet das Gegensatzpaar Selbstdarstellung und Privatsphäre am Untersuchungsgegenstand Facebook.

Social Network Seiten wie Facebook funktionieren nur durch die Selbstdarstellung ihrer Mitglieder. Userinnen und User produzieren Inhalte, teilen Informationen mit anderen und genießen es, mit ihrem Freundeskreis vernetzt zu sein. Kontakthalten wird im Web2.0 leicht gemacht – und je mehr Personen bei einem Sozialen Online-Netzwerk mitmachen, desto größer ist der Nutzen für die Mitglieder. Aber die Veröffentlichung von personenbezogenen Daten hat einen Haken: Um die Gratifikationen von Facebook zu nutzen, zahlen die Mitglieder den Preis des Privatsphäre-Verzichts. Das Problem dabei ist, dass sie dies nicht immer wissentlich tun, sondern sich der Konsequenzen ihres Handelns oft nicht bewusst sind. Die durchgeführte Studie ergab, dass in der Facebook-Gemeinde ein Mangel an Datenschutz-Wissen herrscht. Die Nutzerinnen und Nutzer realisieren manchmal nicht, welches Risiko sie mit der Veröffentlichung von Daten auf Facebook eingehen. Ein Großteil der Probanden zeigte in der Studie zwar ein Verständnis für die Wichtigkeit der Privatsphäre-Einstellungen, viele von ihnen handeln aber in der Realität nicht gemäß diesem Bewusstsein. Es zeigte sich, dass viele Facebook-Mitglieder sehr freizügig mit den eigenen Daten umgehen. Auf 78 % aller inhaltsanalytisch untersuchten Profile (N=126) waren mehr als drei personenbezogene Daten Fremden zugänglich. 38 % warfen im Experiment (N=123) jegliche Vorsicht über Bord und akzeptierten fremde Freundschaftsanfragen. Damit gewährten sie einer unbekannten Person Zugriff auf alle Daten, die normalerweise Freunden vorbehalten sind. Und 90 % aller Befragten (N=381) verwenden auf Facebook den vollständigen eigenen Namen, was es leicht macht, die personenbezogenen Daten der jeweiligen Person zuzuordnen.

Die Freizügigkeit der Facebook-Gemeinde erschreckt, sie überrascht jedoch nicht. Die Ergebnisse bestätigen den aktuellen Forschungsstand. Obwohl die Resultate nicht gerade erbaulich sind, gibt es Hoffnung. Einerseits scheint das Bewusstsein für Privatsphäre zu steigen: Nach und nach beginnen Facebook-Mitglieder, ihre Privatsphäre-Einstellungen zu überprüfen und somit die Verantwortung für die eigenen Daten zu übernehmen. Und andererseits liefert die vorliegende Arbeit ein relevantes Ergebnis für Verbesserungen: Die Studie zeigte einen signifikant positiven Zusammenhang (p=.000) zwischen dem Wissen über Datenschutz und der Sorgfalt, mit der man Privatsphäre-Einstellungen reguliert. Der Schlüssel zu verantwortungsbewussteren Facebook-Mitgliedern liegt also in gezielter Aufklärung und der Verbesserung des Datenschutz-Wissens.

ABSTRACT

With its change to Web2.0 the internet became a collective project: everybody can participate, generate content and present oneself online. This development generates a conflict between self disclosure and privacy. By using Web2.0 more and more people pass more and more information to more and more strangers. They publish their personal data, and therefore waive their right of data protection. Such careless behaviour can lead to critical situations – because the internet never forgets. The study at hand explores the antagonistic issues of self disclosure and privacy with an analysis of the social network site Facebook.

Social network sites like Facebook only work if their members present themselves. Users generate content, share information with others and benefit from being connected with friends. To keep in touch is easy with Web2.0 and the more people join a social online-network, the greater the benefits of their members are. But there is a catch to it: Members pay the price of privacy for benefiting from Facebook. The main problem is that not all the users are aware of this fact. The study revealed, that Facebook members have a lack of data protection knowledge. Users do not realise what risk they take by publishing their data on Facebook. Although many participants have shown comprehension for the importance of privacy settings, lots of them do not act like this in real life. A lot of Facbook members are very generous with their personal data. 78 % publish data in more than three categories, enabling strangers to see it. 38 % accept friend requests from a complete stranger thus making all their usally disclosed information available. And 90 % of all participants use Facebook under their full name which makes it easy to trace all their data directly back to them.

The openness of Facebook members may be alarming but it is not surprising. The results confirm recent studies performed on this subject. Although the findings are not very positive there is reason for hope. On the one hand, the awareness of the importance of privacy seems to increase: Slowly but surely Facebook members start to check on their privacy settings and in doing so they take responsibility for their own data. On the other hand the study shows a relevant result for possible improvements: There is a significant positive correlation (p=.000) between data protection knowledge and the care one takes in regulating one's privacy settings. The more people know about data protection, the better they take care of their privacy. This means the key to more responsible Facebook members lies within the generation of a better understanding for data protection.