FERNUNIVERSITÄT

IN HAGEN

FACHBEREICH RECHTSWISSENSCHAFT

Datenschutz in sozialen Netzwerken

Seminar/Übung : Rechtliche Fallstricke im Internet
bei : Prof. Dr. Ulrich Wackerbarth

Name, Vorname : Mayer, Hubert

Inhaltsverzeichnis

Literaturverzeichnis

Arlt, Christian

Datenschutzrechtliche Betrachtung von Onlineangeboten zum Erwerb digitaler Inhalte

MMR 2007, S. 683 ff.

Bauer, Stefan

Personalisierte Werbung auf Social Community-Websites – Datenschutzrechtliche Zulässigkeit der Verwendung von Bestandsdaten und Nutzungsprofilen

MMR 2008, S. 435 ff.

Däubler/Klebe/Wedde/Weichert

Bundesdatenschutzgesetz - Kompaktkommentar zum BDSG (zitiert „Kompaktkommentar)“

3. Auflage, Frankfurt/Main, 2010

Dieterich, Thomas

Erfurter Kommentar zum Arbeitsrecht

11. Auflage, München 2011

Gola/Schomerus

Bundesdatenschutzgesetz

10. Auflage, München 2010

Hoeren, Thomas

Skript Internetrecht

Münster, Stand September 2010

Hoeren/Sieber

Handbuch Multimediarecht

25. Ergänzungslieferung, München 2010

Hoeren/Vossen

Die Rolle des Rechts in einer durch das Web 2.0 dominierten Welt

DuD (Datenschutz und Datensicherheit) 2010, S. 463 ff.

Joecks/Miebach
Münchner Kommentar zum Strafgesetzbuch (zitiert: MüKo StGB)
1. Auflage, München 2010 (Onlineausgabe)

Jotzo, Florian
Gilt deutsches Datenschutzrecht auch für Google, Facebook & Co. bei grenzüberschreitenden Datenverkehr?
MMR 2009, S. 232 ff.

Mainusch/Burtchen
Kontrolle über eigene Daten in sozialen Netzwerken
DuD (Datenschutz und Datensicherheit) 2010, S. 448 ff.

Meyerdierks, Per
Sind IP-Adressen personenbezogene Daten?
MMR 2009, S. 8 ff.

Roßnagel, Alexander
Handbuch Datenschutzrecht
1. Auflage, München 2003

Roßnagel/Scholz
Datenschutz durch Anonymität und Pseudonymität
MMR 2000, S. 721 ff.

Schonbeck, Oliver
Auf das Timing kommt es an
Datenschutz Praxis 10/2008, S. 6 f.

Simitis, Spiros
Bundesdatenschutzgesetz
6. Auflage, Baden-Baden 2006

Spindler/Schuster
Recht der elektronischen Medien
1. Auflage, München 2008

Taeger/Gabel

Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG (zitiert: „TG“)

1. Auflage, Frankfurt/Main, 2010

Tinnefeld/Ehmann/Gerling

Einführung in das Datenschutzrecht (zitiert „TEG“)

4. Auflage, München, Wien 2005

Wandtke/Bullinger

Praxiskommentar zum Urheberrecht

3. Auflage, München 2009

Zscherpe, Kerstin A.

Anforderungen an die datenschutzrechtliche Einwilligung im Internet

MMR 2004, S. 723 ff.

A. Einleitung

„vzbv reicht Klage gegen Facebook ein.“[1] Diese Pressemitteilung veröffentlichte der Verbraucherzentrale Bundesverband am 30.11.2011. Vorangegangen war eine Abmahnung des Bundesverbandes aufgrund von durch Facebook verwendeter Klauseln in den Allgemeinen Geschäftsbedingungen sowie betreffend die Datenschutzerklärung von Facebook.

Doch neben Facebook stehen auch andere soziale Netzwerke regelmäßig im Blick verschiedener Institutionen, so beschäftigen sich das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV)[2], die Stiftung Warentest[3] oder auch zahlreiche Blogs immer wieder mit diesen.

Diese Arbeit stellt im Folgenden dar, was solche sozialen Netzwerke sind, über die berichtet wird, was Grundbelange des Datenschutzes in diesem Zusammenhang sind und wo die gesetzlichen Regelungen hierfür statuiert sind. Methodisch wird dies entlang eines typischen Verlaufes einer Mitgliedschaft in einem sozialen Netzwerk dargestellt. Das bereits genannte Netzwerk Facebook wurde hierfür ausgewählt, weil dieses nicht nur das soziale Netzwerk mit den meisten Nutzern in Deutschland und auch weltweit ist (s. auch B. I.), sondern da hier auch augenscheinlich die höchste Dichte an Datenschutzproblemfeldern in der Öffentlichkeit diskutiert wird. Eine Google-Suche (begrenzt auf „Seiten auf Deutsch“), durchgeführt am 30.11.2010 mit den Suchbegriffen Datenschutz und der jeweiligen Verknüpfung mit den Namen der größeren in Deutschland aktiven Netzwerken (s. auch B. I.) LinkedIn[4], StudiVZ[5], Xing[6] und Wer-kennt-wen[7] zeigte klare Ergebnisse: Facebook 19.100.000, LinkedIn 7.400.000, StudiVZ 3.770.000, Xing 3.450.000 und Wer-kennt-wen 1.700.000 (ca-Werte lt. google).

Auf diese zahlreichen weiteren Netzwerke wird jedoch vereinzelt verwiesen werden, insbesondere dort, wo sich zeigt, wie ein datenschutzkonformes Verhalten innerhalb des deutschen Rechts besser gemacht werden kann. Auch hier liegt jedoch eine weitere Grenze dieser Arbeit – es wird mit guten Gründen[8] unterstellt, dass deutsches Datenschutzrecht auch maßgeblich ist. Für Facebook ergibt sich das insbesondere aus dem Niederlassungsprinzip des § 1 V BDSG

---

[1] http://www.surfer-haben-rechte.de/cps/rde/xchg/ls_digitalerechte/hs.xsl/75_1164.htm (aufgerufen am 30.11.2010)
[2] http://www.bmelv.de/cln_172/SharedDocs/Standardartikel/Verbraucherschutz/Internet-Telekommunikation/Umgang-Persoenliche-Daten.html (aufgerufen am 30.11.2010)
[3] Test 4/2010, 40 ff.
[4] http://de.LinkedIn.com/
[5] http://www.studivz.net/
[6] https://www.xing.com/
[7] http://www.wer-kennt-wen.de/
[8] *Jotzo*, MMR 2009, 232 ff.

(Bundesdatenschutzgesetz), da Facebook seit Februar 2010 eine Niederlassung in Hamburg hat[9].

Anhand einzelner ausgewählter Lebenssachverhalte werden datenschutzrechtlich problematische Punkte bei Facebook identifiziert und dargestellt. Soweit möglich sollen an einzelnen Punkten auch Verbesserungsmöglichkeiten dargestellt werden– teilweise dergestalt, wie sie von den Mitbewerbern auf dem Markt bereits angeboten werden. An diese Punkte anschließen werden sich einzelne weitere Problemfelder des Datenschutzes in sozialen Netzwerken und ein kurzes Fazit.

Doch was sind soziale Netzwerke, die nun bereits mehrfach genannt wurden, überhaupt?

B. Begriffsbestimmungen

I. Soziale Netzwerke

Der Begriff taucht in verschiedenen Zusammenhängen[10], so zum Beispiel in der Betriebswirtschaft, der Systemtheorie, der Soziologie und in Verbindung mit dem uns hier interessierenden Bereich Internet auf. Im Blog „fieser-admin.de“ wird folgende Definition für ein Soziales Netzwerk verwendet: „Kurz gefasst: Ein soziales Netzwerk ist eine Plattform auf der profilierungsgeile Idioten mit Mitteilungsbedürfnis sich selbst darstellen können.“[11] Ernsthafter ist jedoch die Definition, wie sie Wikipedia vorstellt: „Soziale Netzwerke im Sinne der Informatik sind Netzgemeinschaften bzw. Webdienste, die Netzgemeinschaften beherbergen.“[12] Diese Definition soll dann auch der Maßstab für die kommenden Ausführungen sein.

Übliche Funktionen eines sozialen Netzwerkes sind: die Möglichkeit, ein Profil zu erstellen mit unterschiedlich umfangreichen persönlichen Daten, die Möglichkeit, Nachrichten zu versenden und teilweise eine Chatfunktionalität. Auch das Teilen von Dateien wie beispielsweise Filmen, Bildern oder Musik findet sich häufig. Dies kann man in der Regel entweder öffentlich sichtbar in seinem Profil mit unterschiedlichen Abstufungen, wer was sehen darf – hierzu wird ein „Adressbuch“ verwendet, dass in den verschiedenen Netzwerken unterschiedliche Namen trägt – seien es „Kontakte“ bei Xing und LinkedIn, „Freunde“ bei Facebook, StudiVZ und wer-kennt-wen.

---

[9] http://www.heise.de/newsticker/meldung/Facebook-eroeffnet-erste-deutsche-Niederlassung-928403.html (aufgerufen am 30.11.2010)
[10] http://de.wikipedia.org/wiki/Soziale_Netzwerke (aufgerufen am 01.12.2010)
[11] http://fieser-admin.de/2008/soziale-netzwerke-teil-1-definition/ (aufgerufen am 01.12.2010)
[12] http://de.wikipedia.org/wiki/Soziales_Netzwerk_(Internet) (aufgerufen am 01.12.2010)

In diesen Netzwerken sind zwischenzeitlich eine Vielzahl von Menschen – teilweise mehrfach – registriert: Die Zeitschrift test 4/2010[13] nennt weltweit 10,4 Mio. Nutzer für StudiVZ (inkl. meinVZ), 7,7 Mio. Nutzer für wer-kennt-wen.de, 8,3 Mio. Nutzer für Xing, 400 Mio. für Facebook und rund 60 Mio. Nutzer bei LinkedIn. Aktuell (Stand 30.11.2010) sind es bei Facebook alleine in Deutschland 13.392.500 Nutzer.[14] Weltweit gibt Facebook selbst „More than 500 million active users“[15] an.

II. Datenschutz

§ 1 I BDSG lautet: „Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.“ Es geht hierbei um den vorbeugenden Schutz des Einzelnen vor einem zweckwidrigen und missbräuchlichen Umgang mit seinen personenbezogenen Daten.[16] Schutzobjekt des Bundesdatenschutzgesetzes sind personenbezogene Daten jeder natürlichen Person, unabhängig von Ihrer Staatsangehörigkeit oder Ihrem Aufenthaltsort.[17]

Wichtig ist zu verstehen, dass das Bundesdatenschutzgesetz nach § 1 III BDSG nur subsidiär anzuwenden ist. Hier ist festgelegt, dass wenn andere Rechtsvorschriften des Bundes auf personenbezogene Daten anzuwenden sind, diese dem Bundesdatenschutzgesetz vorgehen. Dies gilt jedoch nur, wenn die speziellere Regelung inhaltlich einen Regelungsgegenstand des Bundesdatenschutzgesetzes erfasst. Ansonsten bleibt das Bundesdatenschutzgesetz insofern lückenfüllend anwendbar.[18] Wichtigste Rechtsquelle ist im Zusammenhang mit dieser Arbeit das seit 01.03.2007 in Kraft getretene Telemediengesetz, welches das Teledienstgesetz (TDG), das Teledienstedatenschutzgesetz (TDDSG) und den Mediendienste-Staatsvertrag (MDStV; Aufhebung erfolgte durch die Länder) abgelöst hat. Hierbei wurde auch die schwer abgrenzbare Unterscheidung zwischen „Teledienst“ und „Mediendienst“ aufgehoben und ein zusammenfassender Begriff „Telemedien“ eingeführt. Dieser umfasst nach § 1 I 1 TMG „alle elektronischen Informations- und Kommunikationsdienste“ und nimmt davon im Weiteren nur Rundfunkdienste und reine Telekommunikation aus.

§ 3 BDSG sieht zahlreiche Begriffsbestimmungen vor, von denen hier zunächst nur auf Absatz 1, die personenbezogenen Daten, eingegangen werden soll. Per-

[13] a.a.O.
[14] http://facebookmarketing.de/userdata/ (aufgerufen am 01.12.2010)
[15] http://www.facebook.com/press/info.php?statistics (aufgerufen am 01.12.2010)
[16] Erfurter Kommentar/*Wank*, § 1 BDSG, Rn. 1
[17] TEG, S. 225
[18] Kompaktkommentar/*Weichert*, § 1 BDSG, Rn. 13

sonenbezogene Daten sind demnach „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“. Diese Einzelangaben werden sehr weit gefasst, so werden unter persönliche Verhältnisse Angaben zu dem Betroffenen selbst, seine Identifizierung und Charakterisierung (z.B. Name, Anschrift, Familienstand, Geburtsdatum, Staatsangehörigkeit, Konfession, Beruf, Erscheinungsbild, Eigenschaften, Aussehen, Gesundheitszustand, Überzeugungen) angesehen[19], unter sächlichen Angaben hingegen Angaben über einen auf den Betroffenen beziehbaren Sachverhalt, wie z.B. seinen Grundbesitz.[20] Bestimmbar ist eine Person, wenn der Nutzer nicht durch seine Angaben selbst, aber durch zusätzliche Kenntnisse identifizierbar ist.[21]

Obwohl das Gesetz den Begriff durchweg in der Mehrzahl verwendet, besteht kein Zweifel, dass die Regelungen auch bezüglich eines einzelnen Datums anzuwenden sind.[22] Ob die IP-Adresse[23] (Zahlencode, der zwischen vernetzten Rechnern wie eine postalische Adresse wirkt[24]) ein personenbezogenes Datum ist, ist streitig.[25] Dagegen spricht, dass diese im derzeit noch verwendeten IPv4-Adressraum aufgrund der Begrenztheit der Adressen von den Accessprovidern dynamisch vergeben wird, was bedeutet, dass mit jeder Einwahl eine neue IP-Adresse vergeben wird. Der Access-Provider hat die Möglichkeit, bei Angabe der Nutzungszeit einen Personenbezug herzustellen.[26] Die IP-Adresse kann daher temporär auch als Pseudonym gesehen werden (hierzu später detaillierter unter D.I.).[27] Eine eindeutige Zuordnung zu einer Person ist damit bei dynamischen IP-Adressen nur begrenzt möglich. So beispielsweise das Amtsgericht München in seiner Entscheidung vom 30.09.2008.[28] Auch bezeichnet diese IP-Adresse nur den Rechner, der sich gerade eingewählt hat, nicht jedoch den einzelnen tatsächlichen Nutzer.

Anderer Ansicht ist hier u.a. das Amtsgericht Berlin Mitte in seiner früheren Entscheidung vom 27.03.2007, das IP-Adressen in Verbindung mit weiteren von der Beklagten ursprünglich gespeicherten Daten als personenbezogene Daten im Sinne des § 15 TMG sieht, da es sich um Einzelangaben über bestimmbare natürliche Personen im Sinne des § 3 1 BDSG handle.[29] Das hier in Frage gestellte

[19] Gola/Schomerus, § 3, Rn. 6
[20] Gola/Schomerus, § 3, Rn. 7
[21] Roßnagel, Kapitel 7.9, Rn. 50
[22] Simitis/*Dammann*, § 3 BDSG, Rn. 3
[23] http://de.wikipedia.org/wiki/IP-Adresse (aufgerufen am 26.12.2010)
[24] TEG, S. 284
[25] TG/*Moos*, § 12 TMG, Rn. 7 f.
[26] Kompaktkommentar/Weichert, § 3 BDSG Rn. 14 mit zahlreichen weiteren Nachweisen
[27] *Roßnagel/Scholz*, MMR 2000, 721, 725
[28] BeckRS 2008, 23037
[29] BeckRS 2007, 18728

Portal war das des Bundesjustizministeriums. Der Ansicht, dass es sich bei einer IP-Adresse i.d.R. um ein personenbezogenes Datum handelt, hat sich neben den Datenschutzbehörden (Beschluss des Düsseldorfer Kreises am 26./27.11.2009 in Stralsund)[30] auch ein Teil der Literatur angeschlossen.[31] *Zscherpe* macht die Qualifizierung der IP-Adresse als personenbezogenes Datum wiederum von der Art des Diensteanbieters abhängig.[32]

Wenngleich auch die Argumente gegen das Ansehen einer IP-Adresse als personenbezogenes Datum überwiegen, muss derzeit wohl zur Vermeidung von Nachteilen die Ansicht der Datenschutzbehörden zumindest zur Kenntnis genommen werden. Spannend bleibt abzuwarten, ob durch die Verbreitung des neuen Adressraumes IPv6 die Internetanbieter dazu übergehen, nur mehr statische IP-Adressen zu vergeben.

C. „A life in Facebook" – konkrete Datenschutzprobleme von Beginn bis Ende einer Mitgliedschaft in einem sozialen Netzwerk am Beispiel Facebook

Im Folgenden werden einige der konkret vorhandenen Datenschutzaspekte, die im Zusammenhang mit sozialen Netzwerken problematisch werden können, am Beispiel eines typischen Verlaufs der Mitgliedschaft in einem sozialen Netzwerk, hier am Beispiel Facebook, aufgezeigt werden. Eine vollständige Darstellung ist im Rahmen dieser Arbeit nicht möglich.

I. Anmeldung

1. Erforderliche Anmeldedaten

Für die Nutzung eines sozialen Netzwerkes sind grundsätzliche Anmeldedaten erforderlich. Als Mindestdaten, um ein soziales Netzwerk zu betreiben, wären ein Nutzername und ein Passwort zu erwägen. Grundsätzlich würden diese zunächst ausreichen, um einen entsprechenden Dienst zu nutzen. Diese Daten, die zur Begründung eines Vertragsverhältnisses und zur inhaltlichen Ausgestaltung erhoben werden, nennt § 14 I TMG Bestandsdaten. Diese dürfen nur erhoben werden, soweit sie für die Nutzung des Dienstes erforderlich sind. *Zscherpe* will aufgrund des Wortlautes die Anwendbarkeit des § 14 I TMG ablehnen für Telemediendienste, die unentgeltlich erbracht werden, da hier keine vertragliche Beziehung zwischen Diensteanbieter und Nutzer erforderlich sei.[33] Diese Ansicht ist

[30] http://www.lfd.m-v.de/dschutz/beschlue/Analyse.pdf (aufgerufen am 01.12.2010)
[31] u.a. *Bohne* in Wandtke/Bullinger UrhG §101 Rn. 34; mit Einschränkung Simitis/*Hammam*, § 3 BDSG, Rn. 63; a.A. z.B. *Schmittmann* in Hoeren/Sieber Teil 9 Rn. 107, *Meyerdierks*, MMR 2009, 8, 13 f., TG/*Moos*, § 12 TMG, Rn. 8
[32] TG/*Zscherpe*, § 15 TMG, Rn 18 ff.
[33] TG/*Zscherpe*, § 14 TMG, Rn. 11

jedoch abzulehnen. Bei § 14 I TMG handelt es sich bereits um eine abschliessende Regelung, so dass ein Rückgriff auf andere Erlaubnistatbestände wie das Bundesdatenschutzgesetz nicht möglich ist.[34]

Über den vorgenannten Benutzernamen und das Passwort hinaus werden regelmäßig weitere Daten abgefragt, so bspw. bei Facebook die E-Mailadresse, das Geschlecht und das Geburtsdatum als Pflichtangaben zur Anmeldung. Wie ist das mit § 14 I TMG zu vereinbaren? Dem Wortlaut dieses Absatzes folgend dürfen personenbezogene Daten eines Nutzers erhoben werden, die für Begründung, inhaltliche Ausgestaltung und Änderung des Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Es handelt sich hierbei also um einen konkreten Vertrag zwischen zwei Parteien. Die Erfassung einer E-Mailadresse zur Kommunikation zwischen Anbieter und Nutzer kann für die konkrete Nutzung dieses Dienstes erforderlich sein, da in sozialen Netzwerken regelmäßig auch der Nutzer informiert werden soll, wenn seine Kontakte/Freunde (im Folgenden nur mehr „Freunde“ als Begrifflichkeit von Facebook) Informationen mit ihm teilen möchten. Auch zur Information über Änderungen des Angebots des Anbieters, zum Erhalt eines neuen Passwortes im Falle des Vergessens des bisherigen und zur Identifizierung eines Nutzers, wenn mit Einwilligung desselben (s. 2.) weitere personenbezogene Daten eingestellt werden, erscheint die E-Mailadresse als erforderlich gelten zu dürfen. Für die zwingende Erforderlichkeit des Geschlechts und des Geburtsdatums ist jedoch keine rechtliche Grundlage zu erkennen. Facebook benennt jedoch zumindest für das Erheben des Geburtsdatums einen plausiblen Grund: „Facebook fordert von allen Nutzern, dass sie ihr richtiges Geburtsdatum angeben. Dadurch soll die Authentizität der Seite und der Zugang zu altersgerechten Inhalten gewährt werden.“ Erforderlich wird dies dadurch jedoch nicht. Dürfen diese personenbezogenen Daten dennoch aufgrund einer Einwilligung des Nutzers erhoben werden?

2. Einwilligung zur Speicherung von personenbezogenen Daten

Nach § 12 I 2. Alt. TMG darf der Anbieter personenbezogene Daten zur Bereitstellung der Telemedien auch verwenden, wenn der Nutzer eingewilligt hat. Hierbei handelt es sich also um ein Verbot mit Erlaubnisvorbehalt, wonach nur dann, wenn ein gesetzlicher Erlaubnistatbestand oder die Einwilligung des Nutzers vorliegt, die Erhebung oder Verwendung von personenbezogenen Daten erlaubt ist.[35] Da es sich um eine Einwilligung handelt, muss diese der Datenverarbeitung

[34] Spindler/*Nink*, § 14 TMG, Rn. 1
[35] Spindler/*Nink*, § 13 TMG, Rn. 2

vorangehen. Die Form der Einwilligung ist im Telemediengesetz nicht unmittelbar vorgegeben. Sie richtet sich daher nach den Vorschriften des Bundesdatenschutzgesetzes.[36] Dort ist nach § 4a Absatz 1 ein Schriftformerfordernis festgehalten, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Dieses Schriftformerfordernis ist eine Schutzvorkehrung zugunsten der Betroffenen.[37] Diese andere, aufgrund der Umstände sicher angemessene Form, stellt im Falle der Nutzung von sozialen Netzwerken wie Facebook vor allem die elektronische Einwilligung dar, die unter den in § 13 II TMG genannten Voraussetzungen auch zulässig ist.[38] Dies ist auch sinnvoll, da eine schriftliche Einwilligung die Vorteile einer schnellen und vor allem medienbruchlosen elektronischen Kommunikation eines Onlinedienstes erheblich mindern würde.[39] Die elektronische Form der Einwilligung darf also verwendet werden, wenn der Diensteanbieter zunächst sicherstellt, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt (§ 13 II Nr. 1 TMG). Hierdurch soll der Schutz der Nutzer vor einer übereilten Einwilligung, die beispielsweise durch unbewusste Erklärung beim Anklicken einer Schaltfläche gegeben werden kann, gewährleistet werden.[40] Weiter ist erforderlich, das diese Einwilligung protokolliert wird (§ 13 II Nr. 2 TMG), der Nutzer den Inhalt der Vereinbarung jederzeit abrufen kann (§ 13 II Nr. 3 TMG) und der Nutzer die Einwilligung auch jederzeit mit Wirkung für die Zukunft widerrufen kann (§ 13 II Nr. 4 TMG). Ergänzend hierzu wird gefordert, dass die Einwilligung freiwillig, ohne jeden Druck, erteilt wird.[41]

Fraglich ist bei Facebook jedoch schon, inwieweit die Einwilligung bewusst und eindeutig erteilt wird. Nachdem die unter C.I.1. genannten Angaben auf der Anmeldeseite von Facebook gemacht wurden, verlangt Facebook auf der Folgeseite neben einem sog. CAPTCHA[42] zur „Sicherheitskontrolle“ nur noch den Klick auf den Button „Registrieren“. Deutlich kleiner darunter steht „Indem Du auf „Registrieren“ klickst, bestätigst Du, dass Du die Nutzungsbedingungen und Datenschutzrichtlinien gelesen hast und diesen zustimmst“. Diese Nutzungsbedingungen und die Datenschutzrichtlinien sind jedoch nicht unmittelbar auf dieser Seite dargestellt, es wird nur auf diese verlinkt.

Die Vorschrift des § 13 II TMG deckt sich im Wortlaut der Nr. 1-3 nahezu mit § 4 II TDDSG. Hierzu hat OLG Brandenburg[43] es für ausreichend erachtet, wenn ein Kontrollkästchen mit dem Text „Ich willige in die Verarbeitung und Nutzung mei-

[36] TG/*Moos*, § 12 TMG, Rn. 18
[37] Simitis, § 4a BDSG, Rn. 33
[38] Hoeren, Skript Internetrecht 9.2010, 415
[39] Roßnagel/*Sonntag*, Kapitel 4.8, Rn. 85
[40] TG/*Moos*, § 13 TMG, Rn. 17
[41] Spindler/*Nink*, § 13 TMG, Rn. 6
[42] http://de.wikipedia.org/wiki/CAPTCHA (aufgerufen am 26.12.2010)
[43] MMR 2006, 405, 406

ner personenbezogenen Daten gemäß der vorstehenden Datenschutzerklärung ein“ aktiviert und anschließend ein Schaltfeld mit Text „Ich akzeptiere und willige ein“ aktivieren muss. Auch in der Gesetzesbegründung[44] zu § 3 VII TDDSG findet sich dies sinngemäß wieder wenn es heißt „In diesem Sinne autorisiert ist eine Einwilligung zum Beispiel durch eine bestätigende Wiederholung des Übermittlungsbefehls, während gleichzeitig die Einwilligungserklärung mindestens auszugsweise auf dem Bildschirm dargestellt wird.“ Hier zeigt sich, dass die Art der Einwilligung in der Erhebung und Verwendung von personenbezogenen Daten bei Facebook nicht ausreichend sein kann. Die Vorgaben, wie sie das OLG Brandenburg[45] im Einklang mit der Gesetzesbegründung[46] zu § 3 VII TDDSG gemacht hat, werden hier nicht einmal ansatzweise eingehalten, da weder der Text auch nur auszugsweise gleichzeitig angezeigt wird, noch ein explizites Feld für eine Einwilligung, beispielsweise eine nicht vorbelegte Checkbox vorhanden ist und auch keine erneute Bestätigung dessen aktiviert werden muss. Bewusst im Sinne der vorgenannten Vorgaben erfolgt hierbei demzufolge keine Einwilligung.

Inwieweit Facebook diese so erteilte „Einwilligung“ protokolliert, kann ohne Kenntnisse der Prozesse bei Facebook nicht beurteilt werden. Der Abruf des Inhalts dieser Einwilligung ist innerhalb und außerhalb von Facebook möglich.[47] Einen nach § 13 III TMG erforderlichen Hinweis vor der Erklärung der Einwilligung auf die Möglichkeit des Widerrufs der Einwilligungserklärung nach § 13 II Nr. 4 TMG findet sich bei Facebook weder auf der Anmeldeseite noch in der Datenschutzerklärung. Ob die nach § 13 I 1 TMG erforderliche Unterrichtung des Nutzers zu Beginn des Nutzungsvorganges über Art, Umfang und Zweck der Erhebung und Verwendung personenbezogener Daten durch die Möglichkeit der Kenntnisnahme der Datenschutzerklärung im Schritt 2 des dargestellten Anmeldeprozesses rechtssicher erfolgt, soll hier nur der Vollständigkeit wegen kurz andiskutiert werden. Konkrete Angaben, in welcher Form diese Unterrichtung stattfinden muss, sind im Gesetz zumindest nicht enthalten. *Nink*[48] nennt hier verschiedene Möglichkeiten, so zum Beispiel die Einbindung in den Nutzungsvorgang in einer Form, die den Nutzer zwangsläufig mit den Informationen in Berührung kommen lassen soll. U.a. nennt er dabei die Verwendung eines Popups und übersieht hierbei wohl, dass zahlreiche Nutzer Popups durch den Browser bzw. entsprechende Plugins ausblenden oder unterdrücken. Als weitere Möglichkeiten nennt er hier die Einbindung eines Hyperlinks. Die Verlinkung zu der Datenschutzerklärung sollte daher für die Art der Unterrichtung ausreichend sein.

---

[44] BR-Drucksache 966/96, 25
[45] a.a.O.
[46] a.a.O.
[47] http://www.facebook.com/policy.php
[48] Spindler/*Nink*, § 13 TMG, Rn. 5 mit weiteren Nachweisen

Ob die erforderlichen Informationen dort vollständig sind, soll an dieser Stelle jedoch nicht weiter untersucht werden.

Abschließend lässt sich festhalten, dass im Rahmen des Anmeldeprozesses bei Facebook keine Einwilligung im Sinne des § 12 I TMG erteilt wird, da insbesondere diese an der Bewusstheit und der Eindeutigkeit der Erteilung scheitert. Die Beweislast für eine wirksame Einwilligung liegt beim Diensteanbieter.[49] Ein wenig besser ist diese Problematik seitens des (Business-) Networks XING gelöst. Hier sind zur Anmeldung nur Vorname, Nachname, E-Mailadresse und Passwort einzutragen. Zur Annahme der Datenschutzbestimmungen und der AGB (beide jedoch ebenfalls „nur" verlinkt"; es erfolgt jedoch der Hinweis, dass die E-Mailadresse ausschließlich von XING verwendet und nicht weitergeben wird) muss aktiv ein Kästchen angekreuzt werden, bevor der Button „Jetzt registrieren" angeklickt werden kann. Dies kommt den gesetzlichen Vorgaben zumindest näher als die Lösung von Facebook.

Bezüglich der elektronischen Einwilligung zeigen sich jedoch derzeit interessante Entwicklungen, hat doch die vom Bundestag eingesetzte Enquete Internet und digitale Gesellschaft in Ihrer Arbeitsgruppe Datenschutz und Persönlichkeitsrechte am 13.12.2010 entschieden, dass auch die Bürger an der Frage beteiligt werden sollen, welche Voraussetzungen es geben muss, damit die Einwilligung des Nutzers in die Verwendung seiner Daten rechtlich wirksam ist und wie diese möglichst einfach und praktikabel, gerade in Bezug auf soziale Netzwerke, gegeben werden kann. Die Arbeitsgruppe stellt dabei insbesondere die Frage, ob der Staat uns wirklich vor uns selbst schützen muss.[50] Die Impulse der Forendiskussion sollen in die nächste Sitzung der Projektgruppe Datenschutz am 17.01.2011 einfließen. Vielleicht ändern sich daher künftig die Voraussetzungen für eine elektronische Einwilligung.

II. Während der Mitgliedschaft

Auch während der Mitgliedschaft bei Facebook (und anderen Netzwerken) treten zahlreiche datenschutzrechtliche Problemstellungen auf, von denen im Folgenden nur einige wesentliche angerissen werden sollen.

1. Vorschläge von „Freunden"

[49] *Zscherpe*, MMR 2004, 723, 725

[50] http://www.bundestag.de/internetenquete/Datenschutz_PG_Datenschutz__Sachverstand_der_Buergerinnen_und_Buerger_gefragt/index.jsp (aufgerufen am 15.12.2010)

Mit Abschluss der Registrierung und auch während der Vertragsdauer schlägt Facebook dem Nutzer vor, mithilfe eines sog. „Freundefinders“ bestehende reale oder virtuelle Kontakte anhand verschiedener Möglichkeiten zu finden. Mit diesem Freundefinder werden die gespeicherten Daten von Kontakten bei verschiedenen Anbietern wie bspw. GMX[51], Skype[52] oder auch die eigene Kontaktdatei aus Outlook ausgelesen und mit den bei Facebook bereits vorhandenen Daten abgeglichen. Finden sich ein oder mehrere Treffer, werden diese als Freunde vorgeschlagen. Die hochgeladenen Datensätze werden von Facebook anschließend jedoch nicht gelöscht, sondern weiter vorgehalten und für zwei Zwecke verwendet. Zum Einen, um bei einer späteren Anmeldung einer so gespeicherten Person diesen als Freund vorzuschlagen, zum Anderen, um diese Daten mit den gespeicherten Daten anderer abzugleichen. Findet sich nun ein und die selbe Person in dem Datensatz, den man selbst hochgeladen hat und in dem eines Dritten, schlägt Facebook auch diesen Dritten vor – denn bei einem gemeinsamen Bekannten besteht ja auch die Möglichkeit, dass man einander bereits kennt. Diese Art der Verwendung der Daten findet sich in der Privacy Policy[53] unter Nr. 5. („Verwendung deiner Informationen durch uns“) „Zur Unterbreitung von Vorschlägen“. Die Person, die beide kennen, wird jedoch nicht angezeigt. Desweiteren kann die hochgeladene E-Mail-Adresse dazu genutzt werden, diese Personen zu Facebook einzuladen. Gegen diese Nutzung hat die Verbraucherzentrale Bundesverband laut einer Pressemitteilung[54] vom 29.11.2010 Klage erhoben. Der Inhalt der Klageschrift wurde dem Verfasser leider auf Anfrage nicht zugänglich gemacht.

Ein möglicher Verstoß könnte hier gegen § 13 I TMG vorliegen. Denn hiernach hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorganges über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Die Unterrichtung würde also gleichzeitig zum Zeitpunkt der Erhebung der Daten ausreichen.[55] Zweifeln könnte man allerdings, ob denn der o.g. Dritte überhaupt Nutzer ist. Doch es genügt auch die unfreiwillige Nutzung, z.B. als Adressat eines Pushdienstes[56], somit auch als „Eingeladener“ zu Facebook. Hier erfährt der Nutzer erst mit der Einladungsmail, dass Facebook personenbezogene Daten wie die E-Mailadresse verarbeitet. Diese Einladungsmail bietet immerhin dann die Option, sich von weiteren Facebook-Kontakver-

[51] http://www.gmx.net/
[52] http://www.skype.com/intl/de/home
[53] s. Fußnote 47
[54] http://www.vzbv.de/go/presse/1423 (aufgerufen am 09.12.2010)
[55] TG/*Moos*, § 13 TMG, Rn. 9
[56] MüKo StGB/*Altenhain*, § 2 TMG, Rn. 13

suchen auszusperren – gegen den Preis des Belassens der E-Mail-Adresse bei Facebook, da nur so ein neuer Kontaktversuch verhindert werden kann.[57]

2. Sichtbarkeit der Daten

Spannend ist in diesem Zusammenhang auch die Frage, welche personenbezogenen Daten von Nutzern Dritten angezeigt werden, sei es der Eingeladene, solange dieser nicht bei Facebook registriert ist, sei es ein Personalleiter, der sich über einen Bewerber genauer informieren möchte, oder sei es jemand, der selbst bereits bei Facebook registriert ist, als Freund oder (noch) nicht Freund.

a) Außerhalb von Facebook

Sucht man beispielsweise in der erweiterten Suche bei Google nach „Hubert Mayer“ auf der Seite „Facebook.com“, so findet sich dort ein Profil[58] mit Bild und der Angabe von acht „Freunden“, ebenfalls mit Bild. Für den vorgenannten Personalleiter, der sich über einen Bewerber informieren möchte, ergibt sich unter Umständen schon an dieser Stelle ein interessantes Bild (ohne, dass dieser selbst bei Facebook registriert sein muss, dazu mehr unter b)), können sich doch auch Institutionen als „Person“ registrieren und der Nutzer diese als „Freunde“ hinzufügen. Hier taucht beispielsweise als „Freund“ der „Stadtjugendring Stuttgart“ auf, ein wohl eher unverfängliches Beispiel. Unangenehmer kann das möglicherweise für den Bewerber werden, wenn dort – ohne hier eine Wertung vornehmen zu wollen - ein Freund wie die NPD Mainfranken[59] oder eine Gewerkschaft, bspw. der DGB[60], auftaucht. Je nach Fasson eines Personalleiters/Arbeitgebers könnte bereits daran eine Bewerbung, unabhängig von der Qualifikation des Bewerbers, scheitern.

An dieser Stelle muss in aller Kürze auf die verschiedenen Datenarten des Bundesdatenschutzgesetzes eingegangen werden. Bestandsdaten sind nach § 14 I TMG personenbezogene Daten eines Nutzers, die dieser erhebt und verwendet, um das Vertragsverhältnis zwischen Nutzer und Diensteanbieter zu begründen, inhaltlich auszugestalten oder zu ändern, also beispielsweise Name, Geburtsdatum und E-Mailadresse des Nutzers. Nutzungsdaten hingegen sind nach § 15 I TMG personenbezogene Daten, die erforderlich sind, das Telemedium zu nutzen und abzurechnen, also beispielsweise die IP-Adresse, Beginn und Ende einer Nutzung, besuchte Unterseiten oder auch die

[57] http://www.zeit.de/digital/datenschutz/2010-02/facebook-sammelt-emailadressen (aufgerufen am 09.12.2010)
[58] http://www.facebook.com/hubert.mayer (aufgerufen am 11.12.2010)
[59] http://www.facebook.com/profile.php?id=100001730980858 (aufgerufen am 26.12.2010)
[60] http://www.facebook.com/profile.php?id=737886394 (aufgerufen am 26.12.2010)

Mitgliedschaft in verschiedenen Gruppen[61]. Zu beachten ist hier, dass die Aufzählungen in § 15 I 2 Nr. 1-3 TMG nicht abschließend sind, da hier ein „insbesondere“ vorangestellt ist.

Strittig ist, als welche Art von Daten weitere persönliche Daten anzusehen sind, die ein Nutzer freiwillig eingibt, wie z.B. Angaben über Geschlecht, Wohnort, Lieblingsfilme, Hobbys und unzählige mehr. Diese werden üblicherweise als Inhaltsdaten bezeichnet.[62] Solche Daten werden teilweise als Unterfall von Nutzungsdaten behandelt, teilweise werden sie aber als nicht vom Telemediengesetz erfasste Daten angesehen und nach § 27 ff. BDSG bemessen.[63] Da das Zeigen von Bildern, die Auffindbarkeit mittels ergänzender Angaben zu Interessen, Beziehungsstatus u.ä. gerade den Nutzen von sozialen Netzwerken wie Facebook ausmacht, erscheint es nur interessengerecht, diese Daten in diesem Zusammenhang als Unterfall der Nutzungsdaten zu qualifizieren.[64]

Wenn diese Daten als Nutzungsdaten qualifiziert sind, dann bedeutet dies, dass der Diensteanbieter diese Daten nur verwenden darf, wenn dies erforderlich ist (s.o.). Die Anzeige von Bild und Namen außerhalb einer Mitgliedschaft von Facebook lässt hieran jedoch erste Zweifel aufkommen. Möglicherweise kann die Nutzung jedoch zulässig sein, wenn der Nutzer in diese eingewilligt hat. Da jedoch bei Facebook bereits die Einwilligung zur Nutzung von personenbezogenen Daten (außerhalb der gesetzlich erlaubten Nutzung von Bestands- und Nutzungsdaten) bei Beitritt in das Netzwerk nicht rechtmäßig erfolgte, kann hiervon keine Rede sein.

b) Innerhalb von Facebook

Innerhalb von Facebook (als Mitglied) sieht man neben dem Namen und dem Bild des Nutzers und den ausgewählten „Freunden“, abhängig von den Einstellungen, die der Nutzer vorgenommen hat, zahlreiche weitere, oben als sog. Inhaltsdaten teilweise erwähnte, Daten. Die einsehbaren Daten können sich unterscheiden, je nach dem, ob der Betrachter ein „Freund“ des Nutzers ist, ein „Freund eines Freundes“ oder ein „Fremder“, also jemand ohne ersichtliche Verknüpfung zu dem Nutzer (Sichtbarkeit für „Alle“ in den Facebook Privacy Einstellungen).

[61] *Bauer*, MMR 2008, 435, 436
[62] Spindler/*Nink*, § 15 TMG, Rn. 3
[63] *Bauer*, MMR 2008, 435, 436
[64] a.a.O.

Bei diesen möglichen Angaben finden sich teilweise auch Angaben über politische Meinungen und Religion. Hierbei handelt es sich nach § 3 IX BGSG um besondere Arten personenbezogener Daten. Dies sind Daten, die grundsätzlich unzugänglich sein sollten.[65] Das Telemediengesetz trifft zu diesen besonderen personenbezogenen Daten keine eigenen Regelungen. Es ist daher § 4a III BDSG zu beachten, der nach dem Vorbild der EG-Datenschutzrichtlinie (s. Fußnote 45) eine Verwendung dieser Daten zulässt, sofern der Betroffene sich einverstanden erklärt und sich die Einwilligung explizit auf diese Daten beziehen muss.[66] Hiernach muss zur Erhebung, Verarbeitung oder Nutzung derselben die Einwilligung über die allgemeine Einwilligung des § 4a I BDSG hinaus ausdrücklich auf diese Daten beziehen. Es genügt also nicht, dass die Einwilligung auf der freiwilligen Entscheidung des Betroffenen beruht und dieser auf den Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen wurde. Blankoeinwilligungen oder pauschal gehaltene Erklärungen, die dem Betroffenen die Möglichkeit nehmen, die Tragweite seines Einverständnisses zu überblicken, sind daher mit § 4a I BDSG unvereinbar.[67] Nachdem jedoch, wie bereits unter C.I.2. dargelegt, bereits der Hinweis auf den Zweck der Erhebung, Verarbeitung oder Nutzung unterblieben ist, fehlt quasi folgerichtig seitens Facebook auch ein entsprechender Hinweis, der eine entsprechende ausdrückliche Einwilligung für diese besonderen personenbezogenen Daten ermöglichen könnte.

3. Voreinstellungen

Kurz angesprochen werden soll in diesem Zusammenhang auch die Frage, welche Voreinstellungen zur Sichtbarkeit der personenbezogenen Daten inkl. der Inhaltsdaten bei Facebook festgelegt sind. Diese Voreinstellungen werden dort auch mit „Empfohlen“ gekennzeichnet; es sollte daher angenommen werden können, dass diese Datenschutzbelange ausreichend berücksichtigen. Dem ist jedoch nicht so. Grundsätzlich ist alles, was erfasst wird auch sichtbar – in unterschiedlichen Abstufungen: Alle Mitglieder von Facebook, die die Seite des Nutzers, der die Voreinstellungen übernommen hat, aufrufen, können Fotos, Biographie und Familie und Beziehungen sehen. Leicht eingeschränkt für „Freunde von Freunden“ ist die Anzeige von Fotos und Videos auf denen der Nutzer markiert wurde, der Geburtstag und – trotz der besonderen Schutzwürdigkeit, s. vorangegangener Abschnitt, die besonderen personenbezogenen Daten „Religiöse Ansichten“ und „politische Einstellungen“. Lediglich Orte, die der Nutzer besucht hat und die Kontaktinformationen sind in den Voreinstellungen auf die „Freunde“ limitiert.

[65] Art. 8 Abs. 1 EG-Richtlinie 95/46/EG
[66] Simitis, § 4a BDSG, Rn86
[67] Simitis, § 4a BDSG, Rn77

Besser macht es hier zumindest teilweise das (Business-) Netzwerk XING. Dort sind innerhalb des Netzwerkes zwar auch Name und die beruflichen Daten (Arbeitgeber, beruflicher Werdegang) sowie Interessen sichtbar, jegliche Kontaktdaten sind jedoch in den Voreinstellungen als nicht sichtbar definiert – und auch gegenüber seinen „Kontakten“ müssen diese explizit frei geschalten werden. Letzteres ist auch sehr detailliert möglich, so dass jede einzelne Kontaktinformation auf Wunsch dem Kontakt zur Ansicht freigegeben werden kann, während bei Facebook alle Kontaktdaten, die eingegeben wurden, sichtbar sind für die „Freunde“.

Festzuhalten bleibt daher, dass wer sich um die Verbreitung seiner personenbezogenen Daten sorgt, diese bei Facebook besser gar nicht erst erfasst – oder besser bei überhaupt keinem sozialen Netzwerk.

4. Werbeeinblendungen

Durch die vielfältigen personenbezogenen Daten, die die Nutzer von sozialen Netzwerken von sich selbst erfassen, bietet sich den Betreibern der Netzwerke die Möglichkeit, Werbung konkret auf die Interessen des einzelnen Nutzers zuzuschneiden.[68] Facebook weist darauf explizit in seinen Privacy Policies unter „5. Verwendung deiner Informationen durch uns“ beim Unterpunkt „Zur Platzierung individuell abgestimmter Werbung“ hin. Interessant ist in diesem Zusammenhang die Verkennung seitens Facebook, was personenbezogene Daten sind. So findet sich in dem genannten Abschnitt der Privacy Policy folgender Hinweis: „Wir dürfen die von uns erfassten nicht personenbezogenen Attribute (dazugehören u.a. Informationen, die anderen Nutzern aufgrund deiner Entscheidung nicht angezeigt werden sollen, z.B. dein Geburtsdatum [sic!] und andere sensible persönliche Informationen sowie Vorlieben) zur Auswahl der geeigneten Zielgruppe für derartige Werbung verwenden.“

a) gesetzliche Ermächtigung

Nach § 15 III 1 1. Alt. TMG darf der Anbieter Nutzungsprofile bei Verwendung von Pseudonymen zum Zwecke der Werbung erstellen, sofern der Nutzer nicht widerspricht. Was Nutzungsprofile sind, ist im Telemediengesetz nicht definiert. Ein Nutzungsprofil ist, vereinfacht dargestellt, die systematische Zusammenstellung von Nutzungsdaten.[69] Voraussetzung für diese Nutzung ist, dass dem

[68] *Bauer*, MMR 2008, 435, 435
[69] *Bauer*, MMR 2008, 435, 437

Nutzer ein Widerspruchsrecht eingeräumt wird und er zu Beginn des Nutzungsvorganges auf dieses hingewiesen wird. Nicht ganz klar ist, was mit dem Beginn gemeint ist, also die Registrierung auf der Plattform oder das jeweilige neue Erstellen eines Nutzungsprofils. *Arlt*[70] kommt mit guten Gründen zu dem Schluss, dass mit dem Hinweis zum Zeitpunkt der erstmaligen Registrierung dem Informationsinteresse eines mündigen Nutzers genüge getan ist, u.a. weil eine wiederholt gleichlautende Information höchstens beim ersten Mal mit der entsprechenden Sorgfalt wahrgenommen und gelesen wird. Auch kann der Diensteanbieter so lange pseudonymisierte Nutzungsprofile erstellen, bis der Nutzer erklärt, hiermit zukünftig nicht mehr einverstanden zu sein.[71] Facebook weist hierauf jedoch nicht hin und stellt auch keine Möglichkeit zur Verfügung, dieser Art der Nutzung zu widersprechen. Die Zweifel von *Bauer*[72], ob denn die Erstellung von Nutzungsprofilen bei einer Social Community (=Social Network) unter Verwendung von Pseudonymen überhaupt zu bewirken ist, brauchen daher nicht weiter beleuchtet werden.

b) Einwilligung des Nutzers in die Nutzung der Daten zu Zwecken der Werbung

Die Einschränkungen des § 15 III TMG gelten nur, wenn der Nutzer keine Einwilligung in die Erstellung von Nutzungsprofilen zu Zwecken der Werbung erteilt hat.[73] Hierfür muss der Nutzer nicht nur über die geplante Datennutzung unterrichtet werden (§ 13 I TMG), sondern ihm muss auch die Möglichkeit eingeräumt werden, dieser Art der Datennutzung durch Widerruf seiner Einwilligung zu widersprechen.[74] Wie bereits dargestellt, wird seitens Facebook bereits die Einwilligung nicht rechtskonform eingeholt. Auch besteht keine Möglichkeit des Widerspruches. Facebook dürfte also keine Nutzungsprofile erstellen.

III. Beendigung der Mitgliedschaft

Nachdem der Nutzer nun ausführlich feststellen konnte, dass Facebook unter Datenschutzaspekten nicht unmittelbar eine positive Leuchtturmstellung einnimmt, kann er sich entscheiden, ob er weiter das Netzwerk nutzen möchte oder die Mitgliedschaft freiwillig beenden möchte.

1. Kündigung

[70] *Arlt*, MMR 2007, 683, 685
[71] TG/*Zscherpe*, § 15 TMG, Rn. 56
[72] *Bauer*, MMR 2008, 435, 437
[73] *Bauer*, MMR 2008, 435, 438
[74] a.a.O.

Gegebenenfalls entscheidet sich der Nutzer aufgrund der bislang dargestellten Problematik für eine Beendigung der Mitgliedschaft. Hierzu geht der Nutzer unter „Konto“ zu „Kontoeinstellungen“ und findet unter „Einstellungen“ die Option „Konto deaktivieren“. Ein Klick darauf führt aber nicht unmittelbar zur Abmeldung, sondern zu einer Seite, die überschrieben wird mit „Bist du sicher, dass du dein Konto deaktivieren willst? Durch die Deaktivierung wird dein Profil gesperrt. Außerdem werden dein Name und dein Bild von allen Inhalten entfernt, die du auf Facebook geteilt hast.“ Quasi garniert wird dies mit fünf großformatigen Bildern der Freunde des Nutzers mit dem jeweiligen Hinweis, dass diese(r) Dich vermissen wird. Ergänzend hierzu muss man einen Grund für den Austritt angeben; es bestehen verschiedene Auswahlmöglichkeiten. Damit ist es jedoch ebenfalls noch nicht getan – es folgt eine weitere Checkbox zum Markieren, wenn man künftig keine E-Mails mehr von Facebook mehr erhalten mag, weil Freunde einen weiterhin (also nach der Abmeldung) auf Bildern markieren und zu Gruppen einladen können! Im Hilfebereich erfährt man ergänzend, dass Facebook mitnichten hier eine Löschung vornimmt, sondern trotzdem weiterhin alle Inhalte speichert. Denn die Nutzer würden bei einer Wiederkehr erwarten, dass Ihre Inhalte noch da seien.[75] Ergänzend hierzu gibt es auf der Hilfeseite noch den Hinweis, wie man sein Konto ganz löschen könne – doch Vorsicht! Wer sich innerhalb von zwei Wochen mit den bisherigen Zugangsdaten einloggt, macht seine Löschung wieder rückgängig.

Betrachtet man nun an dieser Stelle § 13 IV Nr. 1 und Nr. 2 TMG, so wird man schnell erneut Zweifel haben dürfen, an einer rechtskonformen Vorgehensweise seitens Facebook. Denn hier ist unter Nr. 1 geregelt, dass der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherstellen muss, dass der Nutzer die Nutzung des Dienstes jederzeit beenden kann. Beenden meint hier den Abbruch des konkreten Nutzungsvorganges und kann somit durch einfaches Schließen des Browsers vollzogen werden, ohne dass es hierfür besonderer Vorkehrungen des Diensteanbieters bedarf.[76] Unter Nr. 2 ist ergänzend hierzu geregelt, dass die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar gelöscht oder ggf. nach Satz 2 gesperrt werden müssen. Diese Regelungen entsprechen inhaltlich – bis auf erforderliche redaktionelle Anpassungen – den bisherigen § 4 IV Nr. 1 TDDSG und dem § 18 IV Nr. 1 MDStV.[77] Ausweislich der Gesetzbegründung[78] des Teledienstendatenschutzgesetzes konkretisiert die Regelung des § 4 IV TDDSG (ursprünglich Absatz 2) die in § 3 TDDSG festgelegen Grundsätze des System-

[75] http://www.facebook.com/help/?search=how%20do%20i%20delete%20my%20account (aufgerufen am 26.12.2010)
[76] TG/*Moos*, § 13 TMG, Rn. 29
[77] BT-Drucksache 16/3078, 15
[78] BR-Drucksache 966/96, 25

datenschutzes und der Datenvermeidung. Der Nutzer soll zum einen jederzeit seinen Nutzungsvorgang abbrechen können, zum anderen soll der Dienste-anbieter verpflichtet werden, die technischen und organisatorischen Vorkehrungen zu treffen, damit die personenbezogenen Daten über die Anspruchnahme der Dienste unmittelbar gelöscht werden.

Klar zu erkennen ist an dieser Stelle, dass die Vorgehensweise von Facebook, die Daten auch weiterhin zu speichern und nur teilweise zu sperren, nicht konform mit den Datenschutzbestimmungen ist. Dabei soll die Sperrung anstelle der Löschung nach § 13 IV Satz 2 TMG nur dann gelten, wenn einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegen stehen. Dies sind beispielsweise die gesetzlichen Aufbewahrungsfristen nach § 257 HGB[79].

2. Tod

Neben dem freiwilligen Beenden einer Mitgliedschaft bei Facebook stellt sich auch die Frage, was eigentlich passiert, wenn ein Nutzer verstirbt? Was passiert dann mit den Inhalten, die dieser eingestellt hat?

Die Möglichkeit, Facebook über ein hierfür vorgesehenes Formular[80] über den Tod eines Nutzers zu informieren, ist nur schwer zu finden. Über dieses Formular können nahe Angehörige das Profil des Nutzers „entfernen“ lassen – oder die Seite in einem „Gedenkzustand“ aufrecht erhalten. Dann gilt „ Hierdurch werden bestimmte sensible Informationen wie Statusmeldungen entfernt und der Zugang zum Profil nur für bestätigte Freunde zugelassen.“[81]

Doch wie sieht hier die rechtliche Situation aus? Nach § 2 Nr. 3 TMG ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen. In § 3 I BDSG werden personenbezogene Daten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) definiert. Beiden Absätzen gemein ist die natürliche Person. Das sind lebendige Menschen.[82] Eine ausdrückliche Regelung für Verstorbene hingegen fehlt.[83] Ziel des Bundesdatenschutzgesetz (und anderer datenschutzrechtlicher Regelungen) ist es, die freie Entfaltung der Persönlichkeit des Einzelnen zu

[79] **Schonbec**k, Datenschutzpraxis 10/08, 6, 7; TG/Moos, § 13 TMG, Rn. 31
[80] http://www.facebook.com/help/contact.php?show_form=deceased (aufgerufen am 15.12.2010)
[81] http://www.facebook.com/help/?faq=13941&ref_query=verstorbe (aufgerufen am 15.12.2010)
[82] Simitis/*Dammann*, § 3 BDSG, Rn. 17
[83] a.a.O.

schützen, es werden daher lebendige Personen vorausgesetzt.[84] Der Schutz von Verstorbenen wird ganz überwiegend abgelehnt.[85] Eine entsprechende gesetzliche Anspruchsgrundlage besteht daher nicht.

Ein Anspruch kann jedoch den gesetzlichen Erben, die nach § 1922 BGB in Rechtsstellung des Erblassers eintreten, zustehen. Die Erben treten auch in die bestehenden Nutzungsverträge mit dem sozialen Netzwerk ein.[86] Diese können dann den Vertrag entsprechend beenden oder Inhalte löschen, die nicht mehr veröffentlicht sein sollen. Aus praktischen Erwägungen heraus wäre es jedoch sinnvoll, die Nutzungsdaten der sozialen Netzwerke so aufzubewahren, dass im Todesfall die Erben darauf direkt zugreifen können. Ein entsprechendes Testament über den digitalen Nachlass wäre daher sinnvoll.[87]

3. Allgemeines zur Beendigung

Im Zusammenhang mit der Beendigung der Mitgliedschaft in sozialen Netzwerken bekommt auch die Forderung der für die Bereiche Justiz, Grundrechte und Bürgerschaft zuständigen EU-Kommissarin *Viviane Reding*[88], dass die Privatsphäre auch das Recht, wieder vergessen zu werden, einschließen muss, eine besondere Bedeutung.[89] Konkrete Gesetzesvorschläge will die EU im kommenden Frühjahr vorlegen.[90]

D. Weitere Problemfelder

Unter Punkt C. wurden bereits viele der datenschutzrechtlich relevanten Aspekte bzw. Schwierigkeiten während einer Mitgliedschaft bei Facebook angesprochen. Im Folgenden werden noch einige weitere Punkte beleuchtet, die für alle sozialen Netzwerke gleichermaßen gelten. Diese Darstellungen erheben jedoch ebensowenig wie die unter C. angesprochenen Punkte einen Anspruch auf Vollständigkeit.

I. Anonyme Nutzung der Netzwerke

---

[84] a.a.O.
[85] TG/Buchner, § 3 BDSG, Rn. 9 mit weiteren Nachweisen
[86] http://www.rechtzweinull.de/index.php?/archives/134-Datenschutz-endet-mit-dem-Tod-Rechtlicher-Umgang-mit-dem-digitalen-Nachlass.html (aufgerufen am 17.12.2010)
[87] a.a.O.
[88] http://de.wikipedia.org/wiki/Viviane_Reding (aufgerufen am 26.12.2010)
[89] http://www.stern.de/digital/online/datenschutz-in-sozialen-netzwerken-eu-fordert-ein-recht-vergessen-zu-werden-1620643.html (aufgerufen am 17.12.2010)
[90] a.a.O.

Einige Netzwerke schreiben in Ihren Nutzungsbedingungen fest, dass diese nur mit dem realen Namen genutzt werden dürfen. Insbesondere bei Businessnetzwerken wie XING ist dies häufiger zu finden, hier bspw. in den AGB unter 4.1.1.[91] Diese für ein Businessnetzwerk sicher sinnvolle Regelung muss jedoch aufgrund der Regelung des § 13 VI TMG kritisch hinterfragt werden. Dort ist festgelegt, dass der Diensteanbieter die Nutzung von Telemedien anonym oder unter Pseudonym zu ermöglichen hat. Voraussetzung ist, dass dies technisch möglich und zumutbar ist. Der Nutzer muss zudem über diese Möglichkeit informiert werden. Entsprechende Regelungen waren auch schon in den Vorgängern des Telemediengesetz, namentlich in § 4 I 2 TDDSG und § 13 I 2 MDStV enthalten.

Zunächst muss unterschieden werden zwischen der Anonymität[92] und einem Pseudonym.[93] Anonymität bedeutet im Zusammenhang mit personenbezogenen Daten allgemein ausgedrückt, dass die Person, zu der die Daten gehören, nicht identifiziert werden kann bzw. die Wahrscheinlichkeit, dass die Daten einer Person zugeordnet werden können, so gering ist, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet.[94]. Eine Legaldefinition des Anonymisierens findet sich in § 3 VI BDSG. Bei einem Pseudonym wird hingegen ein fingierter Name mit den Daten verbunden. Je nach Art des Pseudonyms[95] ist die Zuordnung der Daten zu dem Betroffenen/Nutzer unterschiedlich schwierig, also von grundsätzlich unmöglich bis mit einfachen Mitteln erreichbar. Eine Legaldefinition des Pseudonymisierens ist in § 3 VIa BDSG niedergelegt. Ein solches Pseudonym kann auch ein sog. Nickname sein, der aus sich heraus die Identität des Nutzers nicht preisgibt (der Diensteanbieter selbst kann jedoch anhand der Referenzliste dieses zuordnen).[96]

Es sind grundsätzlich drei Arten der Pseudonymisierung zu unterscheiden:

- Der Betroffene wählt sein Pseudonym selbst aus und verfügt allein über die Zuordnungsregel.
- Ein vertrauenswürdiger Dritter verwaltet die Zuordnungsregel.
- Der Datenverarbeiter vergibt und verwaltet das Pseudonym.[97]

Durch die anonyme Nutzung bzw. die Nutzung unter einem Pseudonym soll die Entstehung personenbezogener Daten verhindert werden und ist daher als Konkretisierung des Datenvermeidungsgebotes in § 3a BDSG zu sehen.[98]

---

[91] https://www.xing.com/app/user?op=tandc#4 (aufgerufen am 26.12.2010)
[92] http://de.wikipedia.org/wiki/Anonymit%C3%A4t (aufgerufen am 18.12.2010)
[93] http://de.wikipedia.org/wiki/Pseudonym (aufgerufen am 18.12.2010)
[94] Roßnagel/*Scholz*, MMR 2000, 721, 724
[95] Vgl. *Roßnagel/Scholz*, MMR 2000, 721, 725
[96] TG/*Moos*, § 13 TMG, Rn. 42
[97] Simitis/*Bizer*, § 3 BDSG, Rn. 219, Roßnagel/Scholz, MMR 2000, 721, 725
[98] Spindler/*Nink*, § 13 TMG, Rn. 10 mit Verweis auf weitere Nachweise

Freizeitnetzwerke wie StudiVZ verbieten eine Nutzung unter einem Pseudonym nicht. Der Name ist bei StudiVZ frei veränderbar, so dass die Plattform grundsätzlich auch während der Mitgliedschaft unter einem Pseudonym genutzt werden kann. Die Plattform weist jedoch nicht ausdrücklich, wie in § 13 VI TMG gefordert, auf diese Art der Nutzung hin. Facebook hingegen trifft hierzu in den Privacy Policies[99] keine Regelung – das Verbot der Verwendung der Nutzung des Dienstes unter falschem Namen findet sich erst in der „Erklärung der Rechte und Pflichten“[100] unter Nummer 4: „Facebook-Nutzer geben Ihre tatsächliche Namen und Daten an [...]. 1. Du wirst keine falschen persönlichen Informationen auf Facebook bereitstellen oder ohne Erlaubnis ein Profil für jemand anders erstellen“. Zu berücksichtigen ist, dass praktisch betrachtet, alle Angaben frei gewählt werden können. Auch beim Netzwerk Xing ist der Name änderbar (was aufgrund der tatsächlichen Möglichkeiten einer Namensänderung auch nötig ist), jedoch schließen die AGB (s.o.) eine Nutzung des Netzwerkes unter einem anderen als dem realen Namen aus. Diese Regelung verstößt somit gegen § 13 VI TMG. Da jedoch die technische Möglichkeit besteht, den Namen zu ändern, könnte noch fraglich sein, ob die Nutzung unter einem Pseudonym oder die anonyme Nutzung dem Anbieter zumutbar ist. Hierbei soll vermieden werden, dass ein Anbieter jede abstrakt mögliche, technische Lösung zur Anonymisierung realisieren muss. Die Zumutbarkeit ist anbieterbezogen und auch unter Berücksichtigung der Größe und Leistungsfähigkeit des Diensteanbieters zu beurteilen.[101] Hier könnte eine Unterscheidung darin liegen, dass XING eine normale, kostenfreie Mitgliedschaft und eine kostenpflichtige Premiummitgliedschaft anbietet. Bei der kostenfreien Mitgliedschaft ist nicht erkennbar, weswegen es Xing nicht zumutbar sein soll, eine anonyme Nutzung bzw. die Nutzung mit Pseudonym zu erlauben. Bei der kostenpflichtigen Nutzung sollte aus technischer Sicht zumindest die Nutzung unter einem Pseudonym, das vom Anbieter verwaltet wird, auch keine unzumutbare Möglichkeit darstellen. Die Sinnhaftigkeit einer derartigen anonymen oder pseudonymisierten Nutzung eines Businessnetzwerkes kann jedoch in Frage gestellt werden. Den Verstoß gegen § 13 VI TMG betrifft dies jedoch nicht.

Ausführlich mit Gefahren, die sich bei der Nutzung von insbesondere Pseudonymen, teilweise im Nachhinein, beispielsweise durch Zusammenführung von Daten oder versehentlichem Aufdecken der wahren Identität des Nutzers, erge-

[99] a.a.O.
[100] http://www.facebook.com/terms.php (aufgerufen am 04.01.2011)
[101] TG/*Moos*, § 13 TMG, Rn. 46

ben können, beschäftigen sich *Roßnagel* und *Scholz* bereits im Jahr 2000 zu den Regelungen des TDDSG und des MDStV.[102]

II. Downloadmöglichkeit der Daten

Soziale Netzwerke leben davon, dass die Nutzer dort Inhalte jeglicher Art austauschen, seien es Kontaktdaten oder Inhalte wie Bilder oder Videos. Grundsätzlich besteht immer die Möglichkeit, alles was von einem anderen an Daten/ Inhalten sichtbar ist, in irgendeiner Weise selbst zu speichern. Teilweise werden von den verschiedenen Plattformen auch entsprechende Exportfunktionen angeboten. Bei der Nutzung dieser Daten ist zu unterscheiden zwischen der privaten und der gewerblichen Nutzung dieser Daten/Inhalte.

1. Private Nutzung

Wer die Kontaktdaten und Inhalte seiner Freunde/Kontakte über ein soziales Netzwerk herunter lädt, stellt sich vielleicht die Frage, ob er die Daten denn beispielsweise in Outlook überhaupt speichern darf oder ob es hierzu möglicherweise der Einwilligung des jeweiligen Kontaktes/Freundes bedarf. Das Telemediengesetz normiert nur Pflichten des Diensteanbieters, nicht jedoch solche für den Nutzer. Eine entsprechende Verpflichtung könnte dennoch im subsidiär geltenden Bundesdatenschutzgesetz normiert sein. Hier stellt jedoch § 1 II Nr. 3 BDSG klar, dass das Bundesdatenschutzgesetz zwar auch für nicht-öffentliche Stellen gilt, schränkt dies aber wieder ein, durch die Ausnahme, wenn es heisst: „die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten“. Dies wird auch im dritten Abschnitt des Bundesdatenschutzgesetzes nochmals klar unter § 27 I 2 BDSG festgelegt.

Was hierbei als persönlich bzw. familiär anzusehen ist, richtet sich nach der Verkehranschauung.[103] Eine Nutzung der Kontaktdaten für Hobbys, Urlaub, Sport und ähnliches fällt unzweifelhaft unter diese Ausnahmeregelung. Die Nutzung für einen Verein überschreitet jedoch bereits die Grenze der persönlichen/familiären Nutzung.[104] Kritisch ist daher auch die Nutzung der Kontaktdaten zu sehen, wenn beispielsweise bei XING Kontakte zu anderen Nutzern im beruflichen Umfeld bei einem anderen Unternehmen aufgenommen, deren Kontaktdaten heruntergeladen und gespeichert werden und anschließend Kontakt zu diesen Personen aufgenommen wird, um sich für eine Stelle dort zu empfehlen. Diese vereinzelte

[102] *Roßnagel/Scholz*, MMR 2000, 721 ff.
[103] Simitis/*Dammann*, § 1 BDSG, Rn. 151, TG/Schmidt, § 1 BDSG, Rn. 20
[104] Gola/Schomerus, § 27 BDSG, Rn. 12

Nutzung ansonsten für persönliche Zwecke genutzter Daten ist aufgrund des klaren Wortlautes der gesetzlichen Regelung unzulässig.[105]

Die Speicherung und Nutzung von Daten und Inhalten ist somit für den dargestellten rein persönlichen und familiären Gebrauch zulässig. Dies gilt ebenso für die besonderen personenbezogenen Daten.[106] Risiken, bestehen jedoch bei der Nutzung dieser Daten im Grenzbereich zwischen privater und beruflicher Natur.

2. Gewerbliche Nutzung

Anders sieht dies demnach bei einer gewerblichen Nutzung der Daten aus. Wenn bereits die eben dargestellte berufliche Nutzung von Daten problematisch ist, so gilt das Bundesdatenschutzgesetz in vollem Umfang für die gewerbliche Nutzung. Die dem Verfasser häufig begegnete Praxis, ihn als Nutzer von Xing in der Firma mit Einladungen zu Seminaren und Werbungen für Bücher nahezu zu überhäufen, ist zwar einerseits interessant, da einigermaßen zielgerichtet, jedoch nicht zulässig. Hier werden die Daten der Namen, des Arbeitsgebers und der beruflichen Tätigkeit miteinander verknüpft und zu Werbezwecken verarbeitet, ohne dass eine Einwilligung des Betroffenen vorliegt oder eine Rechtsvorschrift dies erlaubt. Auch wenn § 4 II 2 Nr. 2 a BDSG die Erhebung nicht beim Betroffenen, sondern bei anderen Stellen zulassen würde, sofern der Geschäftszweck dies erforderlich macht, so ist diese Vorschrift hier nicht anwendbar. Zunächst ist Voraussetzung, dass die Daten nicht beim Betroffenen direkt erhoben werden können. Denn dass die Daten grundsätzlich beim Betroffenen erhoben werden sollen, ist unmittelbarer Ausfluss des Volkszählungsurteils[107] und des Rechts auf informationelle Selbstbestimmung.[108] Dieser Ausnahmetatbestand ist jedoch eng auszulegen.[109] Die Erhebung muss erforderlich sein, damit der Geschäftszweck erfüllt werden kann. Nicht ausreichend ist daher, dass dieser nur erleichtert wird. Dies gilt auch für § 4 II Nr. 2 b BDSG, der die Erhebung bei anderen Stellen als dem Betroffenen selbst davon abhängig macht, dass die Erhebung bei Betroffenen selbst einen unverhältnismäßig hohen Aufwand erfordern würde. Diese Ausnahme darf jedoch nicht bei jeder beliebigen Arbeits- oder Kostenersparnis greifen.[110] Diese Ausnahmemöglichkeiten dürfen nur herangezogen werden, wenn keine Anhaltspunkte bestehen, dass überwiegend schutzwürdige Interessen des Betroffenen beeinträchtigt werden (Abwägungsvorbehalt).[111]

---

[105] TG/*Schmidt*, § 1 BDSG, Rn. 28; a.A. Bergmann/Möhrle/Herb, § 1 BDSG, Rn. 22
[106] Simitis/*Dammann*, § 1 BDSG, Rn. 149
[107] BVerfGE 65, 1, 43 ff.
[108] Gola/Schommerus, § 4 BDSG, Rn. 21
[109] Simitis/*Sokol*, § 4 BDSG, Rn. 34
[110] Simitis/*Sokol*, § 4 BDSG, Rn. 35
[111] TG/*Taeger* § 4 BDSG, Rn. 66

Diese Art des, lapidar ausgedrückt, „Abgreifens“ von personenbezogenen Daten zu gewerblichen Zwecken ist also nicht zulässig.

E. Fazit/Ausblick

Auch wenn in dieser Arbeit der Großteil der Kritik am Beispiel Facebook dargestellt wurde, kann nicht übersehen werden, dass die meisten problematischen Punkte auch bei den anderen Anbietern sozialer Netzwerke in mehr oder minder deutlicher Form gleichfalls vorhanden sind. Die Zeitschrift „test“ titelte nicht ohne Grund bereits in ihrer Ausgabe 8/2008 „Daten außer Kontrolle“.[112] Auch später hat test das Thema erneut aufgegriffen und stellt fest, dass alle getesteten sozialen Netzwerke Mängel beim Datenschutz sowie bei der Datensicherheit haben.[113]

Auch konnten nicht alle datenschutzrechtlichen Probleme in dem Umfang dargestellt werden, wie sie hätten dargestellt werden können. Allein die Fragestellung der Einwilligung kann, insbesondere durch die ausführliche Kommentierungen zu § 4a BDSG, in einem weit größeren Rahmen dargestellt werden, als diese Arbeit dies bieten kann. Auch weitere bekannte Problemfelder wurden hier nicht thematisiert, wie beispielsweise der „Like-Button“ von Facebook oder der Zugriff auf personenbezogene Daten durch „Anwendungen“/“Apps“, da hier zusätzlich zu den rechtlichen Fallstricken auch ausführliche technische Darstellungen hätten gemacht werden müssen.

Die vorangegangene grobe Darstellung von datenschutzrechtlichen Problemstellungen bei der Nutzung sozialer Netzwerke zeigt, dass das Datenschutzrecht und die technische Entwicklung immer stärker auseinanderdriften. Je detaillierter eine datenschutzrechtliche Regelung gefasst wird, desto mehr Fälle werden von ihr nicht erfasst, die zum Zeitpunkt der Erstellung der Vorschrift noch nicht absehbar waren. Eine zu offene Regelung würde die Telemediendienstebetreiber hingegen auch vor große Risiken stellen, da es schwer wird, die Auslegung seitens der Gerichtsbarkeit zu diesen Fragen im Voraus zu erahnen. Ein rechtssicheres Vorgehen wäre dabei dann allen Unternehmen, die in diesem Bereich agieren, nur schwer möglich, selbst wenn sie den Willen dazu hätten.

Dies scheint auch der derzeitige Bundesinnenminister, Herr *Dr. Thomas de Maizière*, so zu sehen, wenn er am 01.12.2010 in einen Gesetzesentwurf des BMI zum Schutz vor besonders schweren Eingriffen in das Persönlichkeitsrecht unter Nr. III darauf hinweist, dass es sein zentraler Gedanke ist, die

[112] test 8/2008, 38 ff.
[113] Test 4/2010, 40, 41

Rechtsordnung mit Augenmaß weiterzuentwickeln und dann darauf verweist, dass wir – soweit möglich – auf das bestehende Recht zurückgreifen sollten und die Selbstregulierungskräfte stärken. Zentral erscheint hierbei das anschließende Zitat: „Bei der darüber hinaus notwendigen Weiterentwicklung des Rechts ist darauf zu achten, dass die Rechtsordnung entwicklungsoffen für Innovation und Fortschritt bleibt.“[114]

In der Beschlussempfehlung und Bericht[115] des Innenausschusses (4. Ausschuss) vom 14.12.2010 zum Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit – 22. Tätigkeitsbericht – wird unter anderem unter 1. festgestellt, dass gesetzliche Vorgaben verpflichtend und technikneutral die Schutzziele [des Datenschutzes] bestimmen sollen, damit der Datenschutz auch bei weiterem technologischen Fortschritt gewährleistet und bereits im Entwicklungsstadium von neuen Produkten und Geschäftsmodellen berücksichtig wird. Unter Nr. 4 werden u.a. die Aufklärung und technisches Knowhow als wichtige datenschutzpolitische Ziele empfohlen.

Auch *Hoeren* und *Vossen* stellen heraus, dass es ein riesiges Spektrum an Fragen bezüglicher rechtlicher Probleme im Web 2.0 gibt, so zum Beispiel die fehlende Sensibilität der Nutzer, was die Privatsphäre und den Datenschutz gerade auch in sozialen Netzwerken betrifft und die korrespondierende Mißachtung der Privatsphäre und des Datenschutzes auf Seiten der Betreiber der sozialen Netzwerke.[116] Fraglich ist jedoch, ob und was seitens des Gesetzgebers diesbezüglich getan werden kann. Seitens der Europäischen Union kommen zahlreiche Richtlinien, die nicht sorgfältig genug ausgearbeitet wurden. So wollen *Hoeren* und *Vossen* mehr als 20 technische Fehler in der EU Software-Richtlinie ausfindig gemacht haben.[117] Vollkommen zu Recht stellen sie heraus, dass zur Lösung dieser Fragen Menschen aus verschiedenen Bereichen wie Computerwissenschaften, Wirtschaft, Recht und Politik zusammenarbeiten müssen.[118]

Schwierig wird das ganze auch deswegen, weil man auf schwierig miteinander zu vereinbarende Bedürfnisse der Nutzer, nämlich einerseits das Bedürfnis nach Privatsphäre und Datenschutz, anderseits der Wunsch nach öffentlicher Selbstdarstellung, trifft.[119] Dieses Spannungsfeld sieht auch die Bundesregierung und hat bezüglich einer Teilgruppe der Menschen, den Arbeitnehmern, einen Vor-

---

[114] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/rote_linie.pdf%3F__blob%3DpublicationFile (aufgerufen am 20.12.2010)

[115] BT-Drucksache 17/4179

[116] *Hoeren/Vossen*, DuD 7/2010, 463, 464

[117] *Hoeren/Vossen*, DuD 7/2010, 463, 465

[118] *Hoeren/Vossen*, DuD 7/2010, 463, 466

[119] *Mainusch/Burtchen*, DuD 7/2010, 448

schlag gemacht, wie ein Lösungsversuch aussehen könne. Dieser Gesetzesentwurf zur Regelung des Beschäftigtendatenschutzes[120] vom 25.08.2010 sieht u.a. die Ersetzung des bisherigen § 32 BDSG vor durch eine Vielzahl von Unterparagraphen. Interessant ist der dort geplante § 32 VI BDSG: *„Beschäftigtendaten sind unmittelbar bei dem Beschäftigten zu erheben. Wenn der Arbeitgeber den Beschäftigten vor der Erhebung hierauf hingewiesen hat, darf der Arbeitgeber allgemein zugängliche Daten ohne Mitwirkung des Beschäftigten erheben, es sei denn, dass das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung das berechtigte Interesse des Arbeitgebers überwiegt. Bei Daten aus sozialen Netzwerken, die der elektronischen Kommunikation dienen, überwiegt das schutzwürdige Interesse des Beschäftigten; dies gilt nicht für soziale Netzwerke, die zur Darstellung der beruflichen Qualifikation ihrer Mitglieder bestimmt sind. Mit Einwilligung des Beschäftigten darf der Arbeitgeber auch bei sonstigen Dritten personenbezogene Daten des Beschäftigten erheben; dem Beschäftigten ist auf Verlangen über den Inhalt der erhobenen Daten Auskunft zu erteilen. Die Absätze 1 bis 5 sowie § 32a bleiben unberührt.“* Dieser Absatz ist beispielsweise auch beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD)[121] auf deutliche Kritik gestoßen, welches dieser Regelung ein erfolgloses Bemühen um eine differenzierte Regelung von Internetrecherchen durch den Arbeitgeber attestiert. Eine Unterscheidung zwischen sozialen Netzwerken, die der Regelung von rein privaten Beziehungen und der Darstellung der beruflichen Qualifikation dienen, wird zutreffend als in der Praxis nicht möglich festgestellt.[122]

Insgesamt zeigt sich, dass der Gesetzgeber sich grundsätzlich seiner Verantwortung bewusst ist, ein modernes und zukunftsoffenes Datenschutzrecht zu schaffen. Dennoch schießt er immer wieder über das gebotene Maß der Vernunft hinaus. Entscheidend scheint aber nicht das Maß der Regulierung zu sein, sondern der Erfolg der Aufklärung der Nutzer über den Umgang mit personenbezogenen Daten. Nur wer das Recht auf informationelle Selbstbestimmung für sich verinnerlicht hat, kann eine bewusste Entscheidung treffen, welche Daten er dem Netz, hier besonders den sozialen Netzwerken, anvertraut und welche Sicherheitseinstellungen/-vorkehrungen er nutzt. Jeder ist zunächst selbst verantwortlich, welche Daten er von sich preisgibt.

---

120 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_Beschaeftigtendatenschutz.pdf

121 https://www.datenschutzzentrum.de/

122 https://www.datenschutzzentrum.de/arbeitnehmer/20101012-stellungnahme.html (aufgerufen am 26.12.2010)