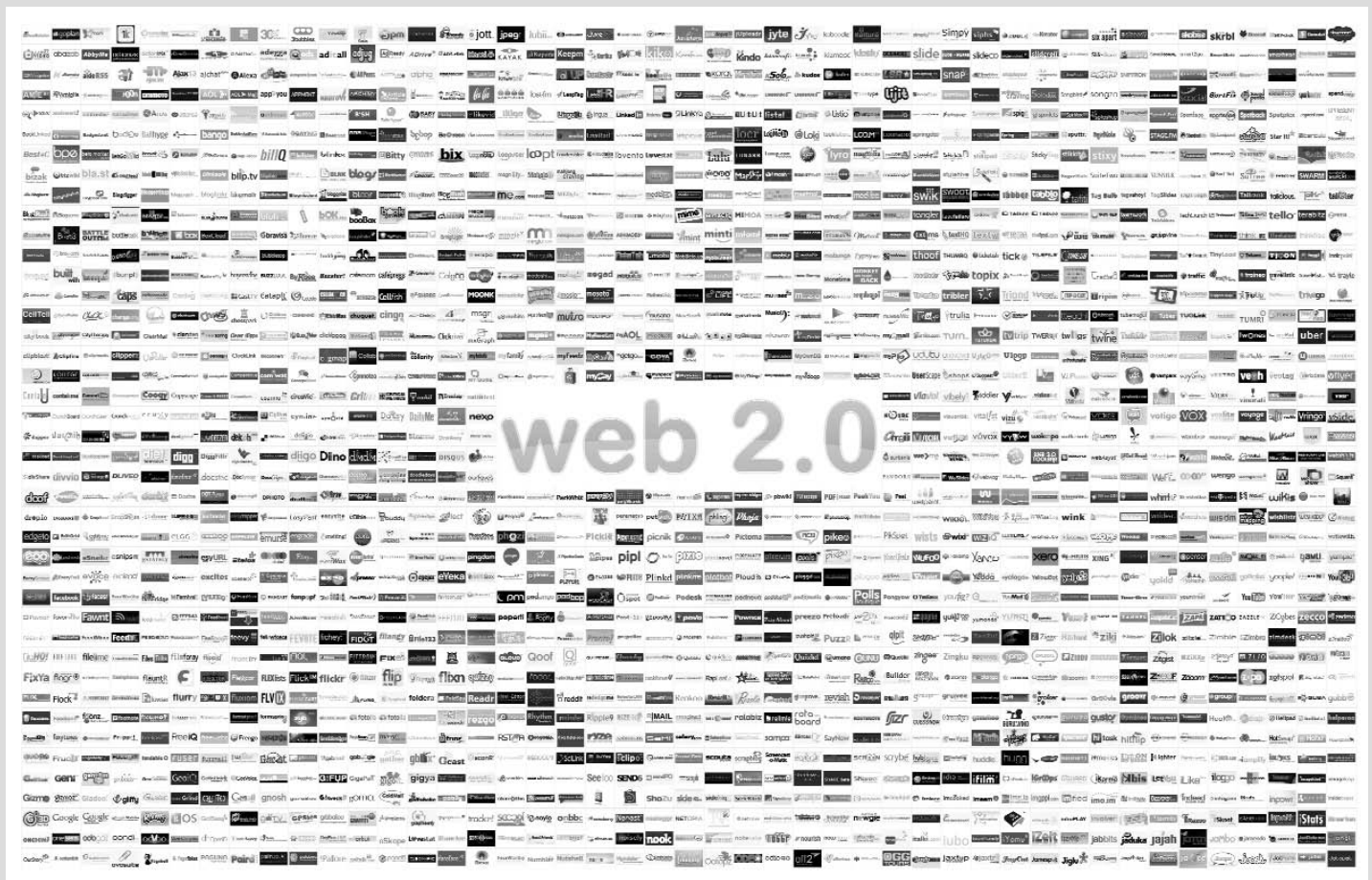


Mein Name sei hase123

Chancen, Risiken und digitales Identitätsmanagement in sozialen Netzwerken

Uwe Spoerl

Sie haben noch keinen Führerschein, sie dürfen noch zu keiner Wahl gehen, im Urlaub können sie oft sogar gratis mit ihren Eltern ans Frühstücksbuffet treten. Aber als Medienproduzenten sind sie längst publizistisch tätig. Denn kaum sitzen Jugendliche vor ihrem Computer, scheinen alle Altersgrenzen zu fallen. Soziale Netzwerke üben gerade auf die jüngsten Nutzer die unwiderstehliche Faszination aus, dass sie sich hier endlich einmal ganz selbstverständlich selbstbestimmt bewegen dürfen, frei von den Fesseln der sonst im Alltag allgegenwärtigen Reglementierungen. So wird das Internet zum *Global Playground*. Man ist ganz unter sich – auch wenn alle Welt zuschauen kann. Guckt ja doch keiner hin, oder?



Online ist cool, die aktive Teilnahme an der sozialen Community im Netz steht für Freiheit, sorgt für Selbstbestätigung. Beim intuitiv technischen Know-how im Umgang mit dem Internet sind sie ihren eigenen Eltern meist haushoch überlegen, doch im contentbezogenen Bewusstsein tun sich gewaltige Defizite auf. Wie soll auch jemand über inhaltliche, geschweige denn juristische Medienkompetenz verfügen, der im Bildungswesen kaum die Hürde der mittleren Reife übersprungen hat?

Populäre Umschreibungen wie „Mitmach-Internet“ untertreiben die Realität. Bloggen, Twittern, Posten, Kommentieren, Hochladen von Fotos, ja schon das Ausfüllen von Formularen mit persönlichen Daten, all das bedeutet im Vergleich zu jeder passiven Mediennutzung einen exponentiellen Zuwachs an Verantwortung. Die klassische Trennung zwischen Produzenten eines Mediums und seinen Nutzern verschwindet. Gerade *dass* diese Grenze fällt, macht ja das Wesen und letztlich den Reiz jeder Community aus. Gleichzeitig entsteht aber bei den Mitgliedern der fatale Irrtum, hier quasi *unter sich* zu sein. Zwar ist der Zugang zu den Communitys mit Namen und Passwörtern geschützt, aber nicht nur kann hier jeder Mitglied im virtuellen Club werden, auch die Suchmaschinen haben einen anonymen, mehr oder weniger eingeschränkten Zugriff auf die Inhalte. Außerdem ist es gar kein Problem, sich notfalls parallel mit mehreren Identitäten verdeckt Zutritt zu verschaffen. Für den Missbrauch fehlt der vernetzten Welt das Unrechtsbewusstsein. Was im wirklichen Leben als Voyeurismus oder Schnüffelei geächtet oder als Hausfriedensbruch strafrechtlich verfolgt wird, gilt nur als clevere Nutzung eines Tools. Die realen ethischen Wertesysteme hinken bestenfalls weit hinter der Entwicklung im virtuellen Raum her, eher erleben sie vor dem Hintergrund der neu gewonnenen systemischen Offenheit einen grundlegenden Wandel.

Für Lehrer und Erziehungsberechtigte bedeutet das die Verpflichtung, Kinder so früh wie möglich nicht nur für den Straßenverkehr fit zu machen, sondern auch für den Datenverkehr. Verbote sind jedenfalls gar keine Lösung, eine Verweigerung ist ebenso unmöglich wie unrealistisch.

Stasi hatte weniger Datenhunger

Allzu klar liegen die Vorteile von Netzwerken auf der Hand – beschenken sie doch dem ganzen WWW das rheinische Klüngelmotto: „Man trifft sich, man kennt sich, man hilft sich“. Insgesamt sind die virtuellen Treffpunkte so unterschiedlich wie die Interessen, die sie bedienen. Die Bandbreite reicht von schülerVZ und Spickmich über mediale Plattformen wie MySpace sowie last.fm für Musik, flickr für Fotos, YouTube und sevenload für Videos, Social Bookmarking zur Orientierung im Internet selbst

sowie Suchmaschinen für ehemalige Schulfreunde, vergriffene Bücher, gegenwärtige Kommilitonen oder künftige Lebensgefährten bis hin zu virtuellen Berufsseilschaften bei Xing und LinkedIn. Bei allen Unterschieden ist eine Eigenschaft allen gemeinsam: der Datenhunger. Denn erst wer genug übereinander weiß, findet passende Kontakte. Prof. Hendrik Speck¹ vom Lehrstuhl für Interaktive Medien der Fachhochschule Kaiserslautern nannte gegenüber der Nachrichtenagentur Associated Press (AP) pro Nutzer sozialer Netzwerke nicht weniger als 120 ermittelte Einzeldaten (Vor-/Nachname, Wohnort, Geburtstag, Familienstand, Lieblingsmusik plus 114 weitere Rubriken), während die 1987 heftig umstrittene deutsche Volkszählung gerade einmal 18 Datenfelder umfasst habe. Informatiker Speck: „Soziale Netzwerke sind der feuchte Traum jedes Nachrichtendienstes. Selbst die Stasi brachte es in ihrem Erfassungsbeleg nur auf 48 Punkte.“

Drin sein oder nicht drin sein, das ist längst keine Frage mehr. Onlinepräsenz ist viel wichtiger als der Eintrag im Telefonbuch. Das betrifft praktisch alle intellektuell kommunizierenden Altersklassen, für die Pflege privater Kontakte ebenso wie für den Erfolg im Beruf. Und es gilt für die Mediennutzung ganz allgemein. Laut *ARD/ZDF-Onlinestudie 2009*² bewegen sich 67,1 % der Deutschen regelmäßig im Internet, in der Altersgruppe von 14 bis 29 Jahren liegt die Quote bei schwindelerregenden 96,1 %. Die 14- bis 19-Jährigen haben nach ZDF-Berechnungen im letzten Jahr bei ihrer täglichen Nutzungsdauer mit dem Internet (120 Minuten) erstmals Radio und Fernsehen (je knapp 100 Minuten) klar überholt. Insgesamt sank der TV-Konsum dieser Zielgruppe während der letzten fünf Jahre um durchaus dramatische 20 %. Beliebteste Applikationen – hier unterscheiden sich Teenager kaum von der Gesamtheit aller Onliner – sind Suchmaschinen und Dialog-Kommunikation (Instant Messaging, E-Mails). Je jünger die Beteiligten, desto höher ihre Affinität zum Social Networking, stellte die ZDF-Medienforscherin Beate Frees zum Europäischen Datenschutztag 2009 fest: „Drei Viertel der jugendlichen Internetnutzer haben persönliche Informationen, Vorlieben oder Hobbys online gestellt.“³

Den Mut zur Lücke stärken

Wer sich freilich irgendwo online *verewigt*, tut das tatsächlich für eine sehr lange, jedenfalls unabsehbare Zeit. Der harmlose Begriff „Posten“ für das Abschicken von Inhalten aller Art ist gleichbedeutend damit, Rechte aller Art aus der Hand zu geben. Jeder „Poster“ erteilt gleichzeitig sein Einverständnis zu Allgemeinen Geschäftsbedingungen des Informationsverarbeiters. Das geschieht normalerweise nur einmal gleich zu Beginn der Mitgliedschaft mit einem „Ja“-Klick auf das AGB-Fenster; dahin-

Anmerkungen:

1 Frankfurter Rundschau, Januar 2009. Abrufbar unter: www.fr-online.de/in_und_ausland/multimedia/aktuell/?em_cnt=1275827
www.hendrikspeck.com

2 Vorab veröffentlichte Teilergebnisse Ende Mai 2009, ausführliche Ergebnisse ab August 2009 abrufbar unter: www.ard-zdf-online-studie.de

3 Vortrag auf dem Symposium „Ach wie gut, dass jeder weiß – Neues zum Datenuiting von Heranwachsenden in Netz-Communitys“ am 28. Januar 2009 im ZDF-Konferenzzentrum Mainz

4

Vgl. Anm. 3

5

Hansen, M./Meissner, S. (Hrsg.): *Verkettung digitaler Identitäten*. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und Technische Universität Dresden, Kiel 2007. In: www.datenschutz-zentrum.de/projekte/verkettung

6

Die komplette Fraunhofer-SIT-Studie Privatsphärenschutz in Soziale-Netzwerke-Plattformen (Planung und Durchführung: Andreas Poller, www.sit.fraunhofer.de, Darmstadt, September 2008) ist als pdf-Datei abrufbar unter: <http://tiny-url.com/4ttc7o>

ter verbirgt sich eine Fülle von für die Betroffenen vielfach schwer verständlichem Text, den folglich kaum jemand liest – und das durchaus im doppelten Wortsinn zu Unrecht. Marktführer Facebook (über 200 Millionen Mitglieder, darunter allein 2 Millionen Deutsche) versuchte Anfang 2009 neue Regeln einzuführen, darunter: „Mit dem Posten von Benutzerinhalt auf einem beliebigen Teil der Site erteilst du dem Unternehmen automatisch eine *unwiderrufliche, zeitlich unbegrenzte*, nicht ausschließliche, übertragbare, vollständig bezahlte, *weltweite* Lizenz (mit dem Recht zur Vergabe von Unterlizenzen) für das Verwenden, Kopieren, öffentliche Aufführen, öffentliche Darstellen, Umformatieren, Übersetzen, Anfertigen von Auszügen (vollständig oder teilweise) und Weitergeben solcher Benutzerinhalte für kommerzielle, Werbe- oder sonstige Zwecke.“

Eine heftige kontroverse Debatte um die Sittenwidrigkeit oder Zulässigkeit derart weitreichender Claims bewog das kalifornische Unternehmen zum Zurückrudern, es veranstaltete bis Ende April 2009 eine Art elektronisches Volksbegehren und teilte als Ergebnis im offiziellen Facebook-Blog mit, von 665.654 teilnehmenden Mitgliedern hätten knapp 75 % den neuen AGB zugestimmt. Diese Wahlbeteiligung von 0,3 (!) % deutet freilich auf kein ausgeprägtes Problembewusstsein innerhalb der Community selbst. Das daraufhin geänderte Kleingedruckte wandelt Unwiderruflichkeit und Ewigkeits-Vorbehalt in halbherzige Absichtserklärungen um, enthält einige Sprachkosmetik und juristische Mäander um Präzisierungen. Weiterverarbeitung und andere Stolpersteine werden zwar nicht mehr erwähnt, aber auch nicht ausdrücklich ausgeschlossen. Auch die AGB deutscher Communitys sind noch meilenweit entfernt von der Forderung des Medienrechtlers Prof. Dr. Alexander Roßnagel, neben der Verpflichtung zu sofortiger Löschung bei Missbrauch bindende *Verfallsdaten* für nutzergenerierten Content zwingend festzulegen: „Hier geht es vor allem um technische Regeln für den Datenschutz, die bisher fehlen.“⁴ Wobei Datenschutz ausnahmsweise das genaue Gegenteil von geschützten Daten bedeutet, also Persönlichkeitsschutz z. B. durch *Zweckbindung* und eine Art *Vergesslichkeits-Automatik*. Intelligente Löschnachweise ist in Roßnagels Augen nicht nur eleganter, sondern auch effektiver, weil sich normative Einschränkungen durch Gesetze lediglich auf nationaler oder allenfalls auf europäischer Ebene durchsetzen ließen. „Datenschutzgerechte Standardeinstellungen“ aller Community-Tools seien dringend notwendig, sagt Roßnagel, der an der Universität Kassel die Projektgruppe verfassungsverträgliche Technikgestaltung (*provet*) und als wissenschaftlicher Direktor das Saarbrücker Institut für Europäisches Medienrecht (EMR) leitet. Es sei ein nicht hinzunehmender Missstand, dass Anbieter mit dem niedrigsten Level ausgerechnet daraus den größten Wettbewerbsvorteil

ziehen könnten. Das bestätigte auch Thorsten Feldmann als Anwalt des Lehrerbewertungsportals Spickmich, das sich inzwischen als eine „Bravo 2.0“ für Teenager begreift, auf dem ZDF-Symposium zum „Datenouting in Netz-Communitys“: „Der Anbieter verhält sich juristisch am sichersten, wenn er die Daten *nicht* überprüft.“ Für den Nutzer bedeutet es bei Auskünften zur eigenen Person: Datensparsamkeit ist oberstes Gebot, innerhalb wie außerhalb der Community im Internet braucht es beim Ausfüllen aller Formulare Mut zur Lücke.

Biometrische Suche beendet die Anonymität

Um nicht zum gläsernen Menschen zu werden, ist die Voraussetzung für optimiertes, effektives Haushalten mit Daten ein bewusstes *digitales Identitätsmanagement*, das Datenschützer unter dem Label IDM diskutieren. Das bedeutet, nur immer jene Daten preiszugeben, die für den Zweck der jeweiligen Community relevant sind. Beispielsweise kann die Information darüber, dass der User Mitglied einer politischen Partei ist, im Profil seines Job-Netzwerks ausgesprochen kontraproduktiv wirken, es gehört ebenso wenig in den virtuellen Fotoclub. Auch dass jemand in seiner Freizeit Motorsport treibt, geht den Rechercheur einer Versicherung gar nichts an. Standardeinstellungen der Betreiber zum Datenschutz sollten Datenvermeidung und restriktive Sichtbarkeit vorsehen, fordert die stellvertretende schleswig-holsteinische Datenschutzbeauftragte Marit Hansen⁵. Dazu gehört etwa die Blockierung persönlicher Profile für Personen-Suchmaschinen, die auf Umwegen dann doch wieder unerwünschte Verknüpfungen herstellen können.

Doch um das zu erreichen, sind häufig besondere Einstellungen in der Standardkonfiguration des jeweiligen Accounts nötig, zu denen sich neue Nutzer im Anmeldeprozess zur Community erst zeitraubend hindurchklicken müssen. Andreas Poller vom Fraunhofer-Institut für Sichere Informationstechnologie SIT rät, die Zugriffskontrolle in den Profil-Einstellungen bei bestehenden Mitgliedschaften so weit wie möglich zu verschärfen, möglichst aber vor entsprechenden Absicherungen gar nicht erst mit der Eingabe persönlicher Daten zu beginnen. Mindestens jedoch sollte Geschäftliches von Privatem generell getrennt werden. „Sonst ist jeder ganz schnell drin bei einer Rasterfahndung. Denn die Sicherheitsmechanismen sind generell überhaupt noch nicht ausgereift,“ stellte Poller bei einer umfangreichen Untersuchung zum „Privatsphärenschutz in Soziale-Netzwerke-Plattformen“⁶ fest. Auf den SIT-Prüfstand kamen die größten Anbieter mit mindestens 1 Million Mitgliedern in Deutschland: MySpace, Facebook, studiVZ, wer-kennt-wen, lokalisten sowie die Business-Netze Xing und LinkedIn. „Die Prüfung lieferte ein sehr ambivalentes Bild: Einzelne Schwächen der einen Plattform decken sich vielfach genau mit

den Stärken einer anderen“, berichtet Poller. Einen Test-sieger gab es nicht, auch wenn Xing als einziger Dienst jede Nutzersitzung mit einer vollständigen Verschlüsselung zumindest technisch gegen Lauschangriffe absichert. Bei einigen anderen Plattformen waren zumindest Anmeldevorgang und Konfigurationsseiten verschlüsselt, sodass Nutzernamen oder Passwort nicht mitgelesen werden können. In der Standardkonfiguration schnitten alle Anbieter mangelhaft ab. Insgesamt empfiehlt Poller ein IDM mit möglichst unterschiedlichen Teil-Identitäten, jeweils neuen Nutzernamen und sehr unterschiedlichen E-Mail-Adressen, die sich nicht mehr *depseudonymisieren* lassen. Wer in einem politischen Forum als hase123 auftritt, sollte nirgendwo sonst, erst recht in keinem Netzwerk, eine E-Mail-Adresse wie hase123@...de registrieren. Auch beim vermeintlich anonymisierten Hochladen von Bildern ins Internet ist große Vorsicht angebracht. Schon jetzt hat die Foto-Gesichtserkennung biometrischer Such-Software eine technische Qualität erreicht, die sich selbst gut informierte Laien gar nicht vorstellen können und Datenschützern im Hinblick auf künftige Diskurse die Haare zu Berge stehen lässt.

Keine Sünde ist auch keine Lösung

Damit droht auch dem Cyber-Mobbing eine ganz neue Qualität. Schon jetzt werden vor allem Jugendliche massenhaft mit unvorteilhaften, *doofen Pics* drangsaliert, die z. T. anonym oder sogar unter gefälschten Identitäten der geschmähten Opfer ins Netz gestellt werden. So erging es Chantal aus Opladen, in deren Namen kurz vor dem Abitur mehrmals rechtsradikale Slogans mit Hitlerfotos bei schülerVZ tagelang abrufbar waren. Erst nach hartnäckiger Beschwerde wurde das Material gelöscht. Chantal war fassungslos, als sie die museumsreifen Computer auf der Polizeiwache sah: „Das Beweismaterial hatte ich auf einem Datenstick mitgebracht, aber die hatten noch nicht einmal einen USB-Anschluss.“

Ihre Anzeige verlief im Sande, der Täter blieb unbekannt. Fremde oder „Freunde“? In der vernetzten Welt verschwimmen die Grenzen ohnehin. 300 „Freunde“ sind hier keine Seltenheit, im echten Leben wären sie undenkbar. Und wie leicht es ist, einer zu werden! ZDF-Redakteur Philipp Müller beispielsweise. Zur Recherche hatte sich der 36-Jährige als angeblicher Fünftklässler bei Spickmich eingeloggt. Im Nu schloss er dort Freundschaft mit Vanessa, 11 Jahre alt. Wenig später wusste er Details aus ihrem Familienleben, Hobbys, Vanessas Schulweg und ihren Lieblingsfilm – ja sogar, dass sie gerade verliebt ist. Vanessa hatte keine Ahnung, dass ihr unbekannter neuer Freund ein erwachsener Mann war.

Doch was tun? Immer nur fremdeln? Vor lauter Angst, dass man eines Tages im Vorstellungsgespräch mit einer hase123-Polemik konfrontiert wird, die digitale Welt mei-

den? Wenn ein Personalchef über einen Kandidaten *gar keine* Spuren in Suchmaschinen findet, ist das inzwischen viel schlimmer als die Entdeckung einer Jugendsünde.

Uwe Spoerl lebt und arbeitet als freiberuflicher Medienfachjournalist in Köln.

