klicksafe Datenschutz Dossier

safer internet day

der internationale Aktionstag für mehr Sicherheit im Internet

Meinungen und Perspektiven zum Thema „Datenschutz und Persönlichkeitsrechte im Web"

klicksafe.de

SAFER INTERNET DAY 2010

Co-funded by the European Union

Inhaltsverzeichnis

Vorwort

Datenschutz und Persönlichkeitsrechte im Internet – nicht gerade ein einfaches Thema, kaum auf den Punkt zu bringen, weit gefasst mit verschiedensten Problembereichen. Viele unterschiedliche Sichtweisen, Ängste, Ansprüche. Längst ist Datenschutz im Internet kein rein „technisches" Thema mehr, erschöpft sich nicht in Diskussionen über Vorratsdatenspeicherung, Cookies und IP-Adressen. Schon lange ist das Thema nicht mehr nur für politisch interessierte und engagierte Mitbürger von Relevanz, sondern für jeden Einzelnen von uns, jeden Internetnutzer, jeden, der einen E-Mail-Account hat, jeden mit einem Profil bei einem Sozialen Netzwerk, jeden, der online einkauft. Spätestens seit Etablierung des so genannten Web 2.0, des „Mitmachnetzes", geht es nicht mehr nur um Daten, die jemand über uns sammelt – zunehmend geht es auch und gerade um die Daten, die wir selbst über uns, über andere ins Netz stellen.

So unüberschaubar das Thema auf den ersten Blick ist, so groß ist die Vielzahl der Institutionen und Personen, die sich zu der Thematik Datenschutz und Persönlichkeitsrechte im Internet mit berechtigtem Interesse äußern. Die einen prophezeien den gläsernen Menschen und warnen, das Internet vergesse nichts; die anderen betonen die Vorteile für Kommunikation und Interaktion. Die Diskussion um Datenschutz und Persönlichkeitsrechte ist, wenig überraschend, immer auch die alte Diskussion um die Abwägung von Freiheit und Sicherheit. Hier wird der Ruf nach mehr und strengeren Gesetzen laut, dort werden die Möglichkeiten zur freien Entfaltung der Persönlichkeit verteidigt.

Wer steht in der Verantwortung? Der Staat, der für die entsprechenden Gesetze zu sorgen hat? Die Anbieter von Webseiten und Portalen? Die Nutzer selbst? Was aber, wenn diese Nutzer Minderjährige sind, Kinder und Jugendliche, welche die langfristigen Konsequenzen ihres Handelns, nicht nur im Internet, häufig noch nicht absehen und einschätzen können? Sind hier dann alleine die Eltern gefragt? Die Erzieher, die Lehrer, die Pädagogen?

Vor diesem Hintergrund veröffentlicht klicksafe zum Safer Internet Day 2010 das vorliegende Dossier zum Thema Datenschutz und Persönlichkeitsrechte im Internet. Dieses Dossier soll als Basis für die weitere Diskussion dienen, als disziplinübergreifende und durchaus auch kontroverse Auseinandersetzung mit dem Thema. Ziel war es, verschiedensten Institutionen und Autoren die Möglichkeit zu geben, ihren Standpunkten und Meinungen Ausdruck zu verleihen. Autorinnen und Autoren aus unterschiedlichen Bereichen, aus Politik, Wirtschaft, Jugendschutz, Gesellschaft, haben daher mit Artikeln und ihren Perspektiven zu diesem Dossier beigetragen. Die einzelnen Beiträge geben die Meinung des jeweiligen Verfassers wieder – entstanden ist eine spannende Sammlung der aktuellen Sichtweisen und auch Forderungen zum Thema. Wir hoffen, damit die aktuelle Diskussion bereichern zu können und werden den weiteren Prozess, die weiteren Entwicklungen und Debatten mit großem Interesse verfolgen.

Wir bedanken uns ausdrücklich bei allen Autorinnen und Autoren für ihre Artikel und die Beiträge zur Diskussion und wünschen allen Lesern eine spannende Lektüre.

Ihr klicksafe-Team

Datenschutz und Persönlichkeitsrechte im Web 2.0

Frank Ackermann,
eco—Verband der deutschen Internetwirtschaft e. V.

Entwicklung zum Web 2.0

Vor 15 Jahren war das Internet eher eine Sache von Experten, es wurde vor allem beruflich genutzt. Für Unternehmen ging um es dabei um Wissen, Organisation und Datenaustausch, der wesentliche Effekt war die Rationalisierung von Arbeitsabläufen. Mit der technischen Weiterentwicklung nutzten immer mehr Menschen das Internet, auch für private Zwecke. Sie interessierten sich für Informationen, Downloads oder Spiele. Durch Werbung und den einsetzenden Internethandel konnten Unternehmen ihre Kundschaft im Netz erreichen.

Web 2.0 aus Verbrauchersicht

Der technische Fortschritt verbesserte die Zugangsmöglichkeiten, unter anderem durch das mobile Internet, und die Geschwindigkeit bei der Datenübertragung. Ab 2004 entwickelte sich das Web 2.0, das sich vor allem durch interaktive Techniken und Dienste auszeichnet. Beispiele hierfür sind Wikis, Tauschbörsen, Podcasting oder Social Networks. Im Fokus stehen Meinungsbildung und soziale Beziehungen, u.a. von Verbraucher zu Verbraucher. Zunehmend ist zu beobachten, dass sich durch das Web 2.0 auch die Sozialisierung verändert. Kinder und Jugendliche pflegen weiterhin soziale Kontakte, aber auf ganz andere Art und Weise: Statt auf der Straße zu spielen, treffen sie sich im Internet.

Es gibt inzwischen unzählige Online-Communities, viele von ihnen verzeichnen weiterhin steigende Mitgliederzahlen. Zu den größten Communities zählen MySpace und Facebook mit jeweils rund 200 Millionen Mitgliedern. Auf Geschäftskontakte spezialisiert sind zum Beispiel LinkedIn, das weltweit größte Business-Network mit mehr als 41 Millionen Mitgliedern, und Xing, mit mehr als 7,5 Millionen Mitgliedern das größte deutsche Business-Network.

Frank Ackermann

ist Leiter des Bereichs Selbstregulierung und Jugendschutz im eco – Verband der deutschen Internetwirtschaft e. V. und Vizepräsident des International Network of Internet Hotlines (INHOPE). Nach dem Jura-Studium in Bonn und Gießen war er für die International Organisation for Migration (IOM) im Repatriation Programme Bosnien und Kosovo tätig. 1998 und 2002 arbeitete Frank Ackermann für eine deutsche politische Stiftung und eine international tätige Kanzlei in Sofia / Bulgarien. Seit 2003 ist er als Rechtsanwalt in Bonn niedergelassen.

Marktführer der Sozialen Netzwerke in Deutschland sind schülerVZ, wer-kennt-wen.de und studiVZ. Zusammen verzeichnen sie monatlich über 13 Milliarden Page Impressions. Beeindruckend sind auch die Zahlen von StayFriends: neun Millionen Mitglieder von 70.000 Schulen und 11.000 aus dem Netzwerk resultierende Klassentreffen (Stand: Oktober 2009).

Von Gefahren, denen die Nutzer sozialer Netzwerke ausgesetzt sind, wird in den Medien immer wieder berichtet. Dazu gehören

- Sogenannte Drive-By-Infektionen mit Schadsoftware (Spyware, Keylogger, Backdoor-Trojaner, etc.), deren Installation häufig durch den Besuch einer Internet-Präsenz ausgelöst wird, die durch Widgets (Zusatzfunktionen oder Spiele) von Drittanbietern beworben werden. Web 2.0-Plattformen eignen sich bestens für die Schadsoftware-Verbreitung, da sie ohnehin User-Generated-Content enthalten und wegen der häufig erforderlichen aktiven

Browser-Komponenten oder Plug-Ins viele Angriffsmöglichkeiten bieten. Dabei sorgen die Nutzer selbst für eine zügige Verbreitung der Inhalte, insbesondere durch Einladung anderer Nutzer.

- Informationen/Profile in Sozialen Netzwerken können Kriminelle nutzen, um Verbrechen zu planen. Zum Beispiel erfahren sie, wann Menschen im Urlaub sind oder ob eine oder mehrere Personen zum Haushalt gehören. Auch Adressen sind leicht herauszufinden.
- Scheinbar gelöschte Daten tauchen immer wieder, auch noch nach vielen Jahren, im Netz auf.
- Manche Netzwerke sammeln personenbezogene Daten der Nutzer und behalten sich in ihren AGB das Recht vor, die Daten zu verkaufen, wenn das Unternehmen den Eigentümer wechselt.
- Personenbezogene Daten von Web-2.0-Dienstenutzern werden immer noch oft rechtswidrig für werbliche Zwecke verwendet oder sogar an Dritte übermittelt.

Problematisch ist allerdings auch die Leichtfertigkeit, mit der Nutzer ihre Daten hergeben. Das zeigt zum Beispiel ein Experiment der Firma Sophus. Eine fingierte Single-Frau, Natalie, suchte über eine Internetseite Kontakte. Innerhalb von wenigen Minuten erhielt sie 19 sofort bestätigte Kontakte, 27 E-Mails mit Kontaktanfragen sowie 48 Nachrichten und damit freien Zugang zu den persönlichen Daten der anderen Mitglieder.

Datenschutzverstöße und -spionage in Social Networks werden sicher weiter zunehmen, ebenso wie die Angriffe und kriminellen Handlungen, die mithilfe dieser Daten erfolgen.

Herausforderungen für die Wirtschaft

Von den in der Internetwirtschaft tätigen Unternehmen verlangt das Web 2.0 eine hohe Flexibilität. Um konkurrenzfähig zu bleiben, müssen sie unkonventionell denken und schnell auf neue Trends reagieren. Erforderlich ist außerdem eine kontinuierliche, intensive Marktbeobachtung und die Präsenz bei Blogs, Podcasts und Community-Sites.

Unternehmen, die nicht im Web 2.0 aktiv sind, haben schlechte Karten. Haben Mitarbeiter kein Profil auf Xing oder LinkedIn, wird nicht getwittert oder gebloggt, gehen wertvolle Kontakte und Synergieffekte verloren. Während Marketing- und PR-Abteilungen immer mehr auf Social Media setzen, haben Sicherheitsverantwortliche häufig Bedenken. Doch gerade diese sollten sich intensiv mit den Möglichkeiten und Gefahren Sozialer Medien befassen, um die Aktivitäten des Unternehmens im Web 2.0 technisch, aber auch unternehmenspolitisch abzusichern.

Ziel sollte ein verantwortungsvoller, sinnvoller Umgang mit Social Media sein. Policies zur Nutzung von Social Media im Unternehmenskontext helfen, die Nutzung für die Mitarbeiter leichter und sicherer zu machen und auch das Unternehmen selbst gegen Schäden abzusichern. Die Struktur einer solchen Policy sollte dabei vom Zweck über den Geltungsbereich und die Regeln hin zu Konsequenzen bei Nichtbeachtung führen. Bei der strategischen Planung von Web 2.0-Aktivitäten sollten die Unternehmensbereiche Information Security, Corporate Communications, PR, Marketing sowie Compliance- und Risk-Management einbezogen werden.

Eine weitere Aufgabe der Wirtschaft ist es, bei den Nutzern das Vertrauen zu schaffen, dass ihre Daten vertraulich behandelt werden. Dazu gehören Maßnahmen zum Datenschutz und deren transparente Darstellung. Ebenso wichtig ist es, die Internetnutzer dafür zu sensibilisieren, vorsichtig mit ihren Daten umzugehen. Ein wichtiger Schritt hierzu ist die Aus- bzw. Fortbildung von Nutzern und Multiplikatoren. In diesem Zusammenhang kooperiert eco mit der lonet GmbH und bietet Veranstaltungen zur Lehrerfortbildung an Schulen an.

Der eco Arbeitskreis Sicherheit hat im Oktober 2009 eine Umfrage zur erwarteten Entwicklung der Internet-Sicherheit durchgeführt, an der 264 Personen teilgenommen haben. 82% der Befragten halten die

allgemeine Bedrohungslage bei der Internet-Sicherheit für wachsend oder sogar stark wachsend. Nur 3% rechnen für 2010 mit sinkenden Sicherheitsausgaben. Anwender und Anbieter unter den Befragten haben zwar eine recht ähnliche Sicht, was wichtige und weniger wichtige Themen sein werden, es wird aber deutlich, dass die Anbieter alle Themen in ihrer Wichtigkeit höher bewerten, und dies teilweise erheblich. Natürlich gehen die Anbieter auch deutlich stärker davon aus, dass die Auslagerung von Sicherheitsthemen zunehmen wird: 58% zu 35% der Antworten. Eine ähnliche Differenzierung wird auch zwischen den budgetverantwortlichen Managern und den Mitarbeitern sichtbar: 47% zu 35% erwarten das Outsourcing wachsend.

Organisatorische Sicherheitsthemen erhalten auch 2010 eine höhere Aufmerksamkeit als technische.

An erster Stelle wurde der Datenschutz genannt, der möglicherweise aufgrund der gravierenden Übertretungen in jüngster Vergangenheit einerseits und den signifikanten politisch-gesetzlichen Aktionen andererseits in den Vordergrund des Interesses gerückt ist.

Der Schutz vor Schadsoftware im Web ist mit Abstand das am wichtigsten bewertete technische Thema.

Die Sicherheit sozialer Netze bildet für die Teilnehmer der Umfrage dagegen das Schlusslicht. Sie ist thematisch bei den Unternehmen mit bis zu 50 Computerarbeitsplätzen schon angekommen. Ihre Bedeutung muss aber in Zukunft wesentlich an Präsenz in den Köpfen der Nutzer gewinnen, denn gerade in den neuen Anwendungen des Web 2.0 verwirklichen sich alte Sicherheitsrisiken.

Damit meins meins bleibt:

Persönlichkeitsrechte und Datenschutz im Netz stärken

Ilse Aigner, Bundesministerin für Ernährung, Landwirtschaft und Verbraucherschutz

Früher hat man nach der Schule am Telefon mit Freunden geplaudert, um sich zu verabreden. Heute stellt man eine kurze Nachricht ins Netz und schon hat man jede Menge Optionen für den Nachmittag. Das ist auch eine neue Form der Freiheit.

Das Internet ist das freiheitlichste, globalste und gleichzeitig effizienteste Informations- und Kommunikationsmedium, das wir bisher kannten. Die Offenheit und der relativ leichte Zugang stellen unseren Umgang mit persönlichen Informationen vor neue Herausforderungen. So leicht es ist, etwas von sich preis zu geben, die Kontrolle über ihre Daten muss weiterhin bei den Menschen selbst liegen. Immerhin geben zwei Drittel der Nutzer an, dass sie über die Verwendung ihrer Daten selbst bestimmen wollen.

Verbraucherschutz in der digitalen Welt bedeutet für mich, die Verbraucherinnen und Verbraucher so zu stärken, dass sie die Freiheit des Internets verantwortungsbewusst und selbstbestimmt wahrnehmen können. Informationen und Sicherheit sind die Leitplanken für die Nutzer.

Meine „Kompetenzoffensive digitale Welt" setzt genau hier an: Was muss ich dafür tun, um sicher zu surfen? Was sind meine Rechte? Antworten auf diese Fragen geben unter anderem die beiden Informationsportale www.surfer-haben-rechte.de und www.verbraucher-sicher-online.de.

Besonders wichtig ist die Unterstützung Jugendlicher bei der Nutzung des Internet. Die heutige Jugend ist quasi mit dem Internet aufgewachsen; sie betrachten es als Teil des sozialen Lebens. So haben 70 Prozent der 12-19-jährigen mehrmals pro Woche über soziale Netzwerke Kontakt mit anderen. Was den Schutz ihrer persönlichen Angaben angeht, sind sie weniger vorsichtig. Nicht einmal die Hälfte der jungen Nutzer haben die Sichtbarkeit ihres Profils auf bestimmte Personen beschränkt. Ihnen ist nicht bewusst, dass sie sich hier nicht nur mit Freunden austauschen. Das peinliche Foto von der letzten Party kann auch den Eltern, Lehrern oder dem Arbeitgeber auf den Bildschirm kommen. Was man von sich ins Netz stellt, kann sogar für kriminelle Absichten genutzt werden. Dafür muss ein Bewusstsein geschaffen werden.

Jeder sollte sich überlegen, für welche privaten Informationen das Internet das geeignete Me-dium ist. So sind in manchen sozialen Netzwerken die Profile auch über Suchmaschinen auf-findbar oder es ist Hackern gelungen, Daten zu kopieren, die nur für „Freunde" sichtbar sein sollten. Was einmal im Netz

Ilse Aigner

Bild: BMELV/BILDSCHÖN

ist gelernte Radio- und Fernsehtechnikerin. Nach dem Besuch der Technikerschule hat sie sich mit der Entwicklung von Systemelektrik für Hubschrauber bei eurocopter befasst.
Ihr politischer Werdegang beginnt 1983 mit dem Eintritt in die Junge Union. Seit 1985 ist sie Mitglied der CSU und engagiert sich in der Kommunalpolitik. 1994 wird sie Mitglied des Bayerischen Landtags und zieht 1998 in den Deutschen Bundestag ein. Als Mitglied des Haushaltsausschusses übernimmt sie von 2002 bis 2005 die Berichterstattung für den Einzelplan des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft und für den Bereich Raumfahrt des Bundesministeriums für Bildung und Forschung.
Gleichzeitig ist sie stellvertretende Vorsitzende der CSU-Landesgruppe und gehört seit 2005 auch dem Fraktionsvorstand an.
In der 16. Legislaturperiode übernimmt sie den Vorsitz der Arbeitsgruppe Bildung und Forschung und ist sowohl Sprecherin der CDU/CSU-Fraktion im Ausschuss für Bildung, Forschung und Technikfolgenabschätzung als auch stellvertretendes Mitglied im Haushaltsausschuss. Seit dem 31. Oktober 2008 ist sie Bundesministerin für Ernährung, Landwirtschaft und Verbraucherschutz und am 28. Oktober 2009 erfolgte die erneute Ernennung zur Bundesministerin.

steht, bleibt auch dort. Das Internet vergisst nichts. Meines Erachtens sollte jeder die selbst ins Netz gestellten Inhalte auch wieder löschen können, um dieses Risiko zu verringern.

Die Kampagne „Watch your Web“, die mein Haus fördert, soll Jugendliche für einen vorsichtigen Umgang mit persönlichen Informationen sensibilisieren. Genauso wichtig ist ein respektvoller Umgang miteinander im Internet, denn Mobbing ist längst auch dort ein Thema. Auch hier wollen wir Jugendliche, Lehrer und Eltern noch stärker sensibilisieren.

Im Rahmen der geplanten Bildungsinitiative meines Hauses zur Verbraucherkompetenz sollen für Schulen gezielte Angebote erarbeitet werden, um den selbstbestimmten und sicheren Umgang mit der digitalen Welt besser vermitteln zu können.

Information allein reicht aber nicht aus. Erforderlich sind auch gute rechtliche Rahmenbedingungen, damit das Internet Ausdruck der Freiheit bleibt. Die Selbstbestimmung der Verbraucherinnen und Verbraucher steht oben an und muss gewährleistet bleiben: Wer die ganze Menschheit an seinen persönlichen Erlebnissen teilhaben lassen möchte, soll dies dürfen – es muss aber auch möglich bleiben, nichts über sich preiszugeben oder Dinge nur bestimmten Personen oder zu bestimmten Zwecken mitzuteilen.

Die Bundesregierung prüft dazu, wie wir den Datenschutz im Internet weiter verbessern können. So wie sich das Internet und seine Möglichkeiten stets verändern, so muss auch die rechtliche Situation dynamisch angepasst werden. Hier stehen wir am Anfang einer grundlegenden Überprüfung.

Wie etwa geht man damit um, dass durch Anwendungen wie Google Streetview das eigene Lebensumfeld oder gar man selbst fotografiert wird und dies anschließend systematisch ins Internet eingestellt wird. Dies ist eine neue Qualität von Datensammlungen, auf die wir neue Antworten finden müssen.

Es ist äußerst problematisch, wenn hiervon nur diejenigen verschont bleiben, die ausdrücklich widersprechen. Ein virtueller Stadtrundgang mag interessant sein. Hier entsteht aber auch ein mögliches Einfallstor für kriminelle Handlungen. Einbrecher etwa könnten dankbar sein für diese Datenbank.

Datenschutz heißt aber auch, dass man sich nicht ständig Gedanken machen muss, wie man Einspruch gegen die subjektiv empfundene Verletzung der Privatsphäre erheben kann und gegenüber wem. Verbraucherinnen und Verbraucher darf nicht allein der Schutz für ihre persönlichen Daten übergestülpt werden. Die Regelungen zum Datenschutz müssen einen effektiven Schutz gewährleisten. Hier ist auch die europäische Ebene gefordert.

Datenschutz erfordert auch Datensicherheit. Hier sind in erster Linie die Unternehmen in der Pflicht. Browser sollten von Anfang an datenschutz- und sicherheitsfreundliche Voreinstellungen haben. Soziale Netzwerke sollten so eingestellt sein, dass die Nutzer ihre Profile aktiv freischalten und diese insbesondere für Suchmaschinen nur bei aktiver Freischaltung auffindbar sind. Inhalte, die mit Passwortschutz im Netz abgelegt werden, z.B. in E-Mail-Diensten, auf Speicherplätzen für Dateien und Fotos oder in sozialen Netzwerken, müssen effektiv vor Angriffen und Datenklau geschützt sein.

Insofern sind alle gesellschaftlichen Gruppen gefragt, dazu beizutragen, dass das Internet das freiheitlichste Medium der Welt bleibt, an dem sich jeder beteiligen kann, ohne seine Selbstbestimmung aufzugeben.

Zum Stand der Datenschutzdiskussion Stand 01/2010

Beitrag für das Projekt klicksafe

Gerhart Baum, Bundesminister a.D., Rechtsanwalt

Die Datenschutzdiskussion ist nach langen Jahren der Gleichgültigkeit wieder in Gang gekommen. Auslöser war ein jeden Rahmen sprengender Datenhandel, der im letzten Jahr bekannt und zum Skandalthema wurde und sogar einen sogenannten Datenschutzgipfel – einberufen durch die Regierung – auslöste. Der Datenschutz stand nicht auf der tatpolitischen Tagesordnung der letzten Jahre. Ein umfassendes politisches Reformkonzept zu diesem Freiheitsthema ist jetzt von der neuen Regierung angekündigt worden – auch zum Arbeitnehmerdatenschutz, der nach den Spitzelaffären bei Bahn und Telekom die Öffentlichkeit beschäftigt hat.

Nach dem legendären Volkszählungsurteil des Bundesverfassungsgerichts, das ein Grundrecht auf Datenschutz, die sogenannte informationelle Selbstbestimmung im Jahre 1983 festgelegt hatte, wurde Datenschutz in den letzten Jahrzehnten eher abgebaut, nicht aufgebaut. Schon das Nichtstun führte angesichts der explosionsartigen Entwicklung der Kommunikationstechnologie zu einem Abbau. Auch ist der Staat mit schlechtem Beispiel vorangegangen durch zahlreiche Sicherheitsgesetze und Sicherheitsmaßnahmen, die in 14 Fällen vom Bundesverfassungsgericht aufgehoben oder eingeschränkt wurden. Fakt ist: Die Sicherheitsbehörden sammeln immer mehr Daten, Daten unverdächtiger Bürger. Sie beschränken sich nicht auf eigene Datensammlungen, sondern greifen auf die großen Datendepots der Privaten zu. Jede neue große Datenbank wie z. B. die im letzten Jahr eingeführte Arbeitnehmerdatenbank ELENA trägt die Dynamik eines Abbaus des Datenschutzes in sich, weil sie Zugriffsbegehrlichkeiten weckt. Jede neue technische Maßnahme, wie z. B. der Körperscanner, wird ohne große Überlegung als Sicherheitsgewinn in Betracht gezogen, obwohl gar nicht abzusehen ist, wie die offenen Fragen beantwortet werden können. Aber es ist vorauszusehen: Wir werden hier erneut über den Tisch gezogen.

Gerhart Baum

Geboren 1931 in Dresden. Studium der Rechtswissenschaften in Köln; 1961: 2. juristisches Staatsexamen; Arbeit als Rechtsanwalt; ab 1962: 10 Jahre Mitglied der Geschäftsführung der Bundesvereinigung der Deutschen Arbeitgeberverbände; seit 1954: Mitglied der FDP, dort 30 Jahre im Vorstand und 9 Jahre Stellvertretender FDP-Bundesvorsitzender; 1972-1994: Mitglied des Deutschen Bundestages; 1972-1978: Parlamentarischer Staatssekretär im Bundesministerium des Innern; 1972-1976: Bundesminister des Inneren; ab 1992: für die UNO tätig, zuerst als Chef der deutschen Delegation in der UNO-Menschenrechtskommission in Genf und später als UN-Sonderbeauftragter für die Menschenrechte im Sudan. Einreichen vieler Verfassungsbeschwerden vor dem Bundesverfassungsgericht in puncto Menschenwürde mit Erfolg und in jüngerer Zeit auch gegen das nordrhein-westfälische Gesetz zur heimlichen Online-Durchsuchung privater Computer und zurzeit einer der Beschwerdeführer gegen das Vorratsdatenspeicherungsgesetz. Autor von zahlreichen Veröffentlichungen; Vorsitzender des Kuratoriums von „Musik der Jahrhunderte" in Stuttgart; Mitglied in verschiedenen kulturellen Gremien und Vorsitzender des Kulturrats NRW. Zurzeit tätig als Anwalt in Düsseldorf.

Blickt man auf das gesamte Problemfeld, also das der staatlichen wie der privaten Datenverarbeitung, ist die Lage so brisant wie nie zuvor. In seiner Rede zur Theodor-Heuss-Preisverleihung im April 2008 fasste Spiros Simitis, einer der Datenschutzpioniere in unserem Land, die Situation wie folgt zusammen:

„Nahezu jede personenbezogene Angabe wird heute gesammelt und gespeichert. Früher für selbstverständlich gehaltene Speicherungsgrenzen sind endgültig entfallen. Die Verarbeitungstechnologie schafft alle Voraussetzungen für multifunktionale Verwendung und systematische Vernetzung der Datenbestände. Auch die Trennung öffentlicher und privater

Datenbanken schwindet dahin.

Frank Rieger, Sprecher des Computerchaosclubs, spricht in seinem Gutachten zur Vorratsdatenspeicherung von der Gefahr, dass wir zu „digitalen Schattenrissen" werden, also umfassende „digitale Menschprofile" die Zukunft sein werden – der Mensch also nur noch „als Bündel von Merkmalen und Kategorien". Er ist aber mehr als die Summe seiner Daten. Dass man dies betonen muss, zeigt, wohin wir bereits geraten sind.

Es reicht eben nicht mehr, den einzelnen auf seine Datenherrschaft zu verweisen, also auf sein Selbstbestimmungsrecht. Er hat es in vielen Fällen überhaupt nicht, denn er weiß nicht welche Spuren er hinterlässt und was mit diesen geschieht.

Hüter der Verfassung waren in den letzten Jahren in vielen Fällen die Datenschutzbeauftragten deren Ansehen und Bedeutung immer weiter gewachsen ist, vor allem aber hat das Bundesverfassungsgericht, auch und vor allem mit dem wegweisenden Urteil zur Computerdurchsuchung und Computerüberwachung im Jahr 2008, Maßstäbe gesetzt. Ein neues Grundrecht wurde formuliert. Das Gericht ist sozusagen im Computerzeitalter angekommen.

Alles in Allem ist es ein Armutszeugnis für die Politik, dass neue Schutzstrategien, wie sie seit Jahren in zahlreichen Expertisen und in den Berichten der Datenschutzbeauftragten vorliegen, nicht zu gesetzlichen Rahmenbedingungen geführt haben. Inzwischen gibt es nicht nur im staatlichen sondern auch im privaten Bereich perfekte Überwachungsinfrastrukturen, die ineinander greifen. Die Reformvorschläge liegen also auf dem Tisch. Es geht um die Gewährleistung des Datenschutzes durch technische Gestaltungs- und Verarbeitungsregeln, durch neue Kontrollverfahren, durch Stärkung der Datenschutzbeauftragten, um nur einiges zu nennen. Hoffentlich gelingt es, kurzsichtigen Interessen von Wirtschaftsgruppen zu widerstehen, die an Datenverarbeitung interessiert sind. Die Gesetzesnovellen von 2009 sind dadurch leider entschärft worden.

Datenschutz, so haben wir es schon in den 70er Jahren gesehen, als ich im Bundesinnenministerium für das erste Bundesdatenschutzgesetz verantwortlich war, ist ein Freiheitsthema. Es bleibt dahingestellt, ob dieses durch die Aufnahme des Datenschutzes in das Grundgesetz gestärkt werden könnte. Besser als in den Urteilen von Karlsruhe zum Datenschutz, meine ich, kann Datenschutz nicht definiert werden. Gefragt ist vor allem verantwortliches Handeln der Politiker in der täglichen politischen Arbeit.

Die unkontrollierte Verwendung personenbezogener Daten tangiert und gefährdet letztendlich den demokratischen Charakter unserer Gesellschaft. Aus diesem Grunde darf nicht länger gezögert werden eine umfassende Reform des Datenschutzrechts in die Wege zu leiten. Sehr schwierig wird es sein, Datenschutz international zu koordinieren. Wir leben in den Zeiten der Globalisierung nicht auf einer Insel. Der Ausverkauf von europäischen Finanzdaten an die USA (Swift) zeigt, welchem Druck wir ausgesetzt sind — aber auch, dass wir ihm nicht widerstehen, obwohl eigene Sicherheitsbehörden diese Daten als irrelevant bezeichnet haben. In der Europäischen Gemeinschaft gibt es erhebliche Datenschutzdefizite und gefährliche Pläne, den Datenschutz aufzuweichen. Aus allem gibt es für uns nur eine Schlussfolgerung: Wir sollten für unsere Grundrechte, die einen strikten Bezug zum Prinzip der Menschenwürde haben, international kämpfen.

Ein weiteres wichtiges Feld ist die Bewahrung der Grundrechte im Internet. Der Rechtsstaat muss sich auch im Netz behaupten. Ein Spannungsverhältnis besteht durch die Gefahr der faktischen Endeignung von Kreativen im Internet. Dem kann nur mit einem modernen Urheberrecht begegnet werden. Auf der anderen Seite darf das Netz nicht zur Zensur durch staatliche Behörden missbraucht werden, wie das mit dem Gesetz gegen Kinderpornografie begonnen wurde, das der Bundespräsident zu Recht im Moment nicht unterzeichnet. Bemerkenswert ist immerhin, dass der Bundestag eine Enquete-Kommission zur Internetproblematik einzusetzen beabsichtigt. Auch die Bundesregierung hat ein laufendes Programm zur Untersuchung offener Fragen begonnen.

Wir müssen zur Selbstverteidigung übergehen – auch durch Datensparsamkeit und Datenaskese.

Alles in Allem: Ich plädiere seit langem für eine Bürgerbewegung zum Schutze der durch Art. 1 des Grundgesetzes geschützten Privatheit. Ich plädiere für eine Datenschutzbewegung nach dem Vorbild der erfolgreichen Umweltbewegung. In der letzten Zeit hat sich gezeigt, dass doch zahlreiche, vor allem auch jüngere Menschen, sich gegen Elemente des Überwachungsstaates und der Überwachungsgesellschaft wenden. Diese Chance sollte jetzt genutzt werden.

Datenschutz und Persönlichkeitsrechte in sozialen Netzwerken

Markus Berger-de León, CEO VZ-Netzwerke

Soziale Netzwerke im Internet haben sich in den letzten Jahren zu einem weltweiten neuen Massenmedium entwickelt. Über 700 Millionen Nutzer auf der ganzen Welt bewegen sich hier mehrmals täglich, um sich mit Freunden, Kollegen, alten und neuen Bekannten auszutauschen. Alleine die VZ-Netzwerke zählen heute bereits über 16 Millionen Nutzer, und es werden täglich mehr. Kaum ein anderes Medium wird von so vielen Menschen in Deutschland genutzt – und das bei einer enormen Aktivität der Mitglieder. Es gibt über neun Millionen unterschiedliche Gruppen zu jedem erdenklichen Thema. Jeden Tag werden 13 Millionen Nachrichten an Freunde geschrieben und über zwei Millionen Fotos hochgeladen. Diejenigen, die mit dem Internet aufgewachsen sind – die „Digital Natives" – organisieren inzwischen einen Großteil ihres Lebens über ihr Netzwerk: Von der nächsten Verabredung auf dem Sportplatz über die abendliche Partylocation bis hin zum gemeinsamen Lernen für die kommende Klassenarbeit. Ganz zu schweigen von Geburtstagsgrüßen, die kostenlos auf der Pinnwand hinterlassen werden.

Soziale Netzwerke haben mit ihrem enormen Erfolg die Kommunikation nicht nur im Internet, sondern in der Gesellschaft grundlegend verändert. Millionen Menschen kommunizieren hier schnell, einfach und vor allem kostenlos über alles, was die Welt bewegt, und nutzen ihr Profil nebenbei als eigene Präsentationsplattform. Parallel zu dieser rasanten Entwicklung entstehen aber auch viele Fragen – nicht nur für die Nutzer, sondern auch für die Betreiber, die Gesellschaft und die Politik: Wer ist für die Inhalte in sozialen Netzwerken verantwortlich? Sind die Daten der Mitglieder wirklich sicher? Können die Nutzer ihre Privatsphäre überhaupt noch schützen – und wenn ja wie? Wer klärt die Nutzer, vor allem Jugendliche, über die Chancen und Gefahren auf?

Markus Berger-de León

Jahrgang 1973, ist seit März 2009 CEO der VZnet Netzwerke Ltd. Sein Studium der Betriebswirtschaftslehre absolvierte er an der Wissenschaftlichen Hochschule für Unternehmensführung (WHU) – Otto Beisheim Graduate School of Management in Koblenz – und schloss mit dem Diplom in Betriebswirtschaftslehre ab. Weitere Studienerfahrungen sammelte er an der Columbia Business School und an der Plekhanov Russian Academy for Economics in Moskau. Seine berufliche Laufbahn begann er als Mitbegründer, Technischer Direktor und leitender Geschäftsführer eines eigenen Software-Unternehmens, das neue E-Procurement Services für Firmenkunden in ganz Europa aufbaute. Von 2002 bis 2007 war Markus Berger-de León bei der Jamba! GmbH tätig, die letzten zwei Jahre als Geschäftsführer mit der Gesamtverantwortung für das Unternehmen. Danach wurde er zum Vorstandsvorsitzenden der MY-HAMMER AG berufen. Neben seiner Tätigkeit als CEO der VZnet Netzwerke Ltd. ist Markus Berger-de León Vorstandsvorsitzender der Abacho AG und Mitglied des Aufsichtsrats der MY-HAMMER AG.

VZ-Netzwerke setzen konsequent auf Datenschutz, Privatsphäre und Aufklärung

Als Deutschlands größtes soziales Netzwerk nehmen die VZ-Netzwerke eine Vorreiterrolle bei der Beantwortung dieser wichtigen Fragen ein. Wir setzen uns konsequent für den Schutz der Privatsphäre, hundertprozentigen Daten- und Jugendschutz und insbesondere auch für die Aufklärung unserer Mitglieder ein. Das gleiche fordern und fördern wir von anderen Betreibern sozialer Netzwerke in Deutschland. Bereits Mitte 2009 haben wir daher ein Manifest auf den Weg gebracht, das unter dem Motto „Netzwerke mit Verantwortung" den Schutz und die

Sicherheit der Mitglieder sozialer Netzwerke gewährleisten soll. Neben der höchstmöglichen Datensicherheit – die uns erst kürzlich der TÜV SÜD nach einer intensiven Überprüfung bestätigt hat – spielt die Kontrolle über die eigenen Daten durch das Bereitstellen detaillierte Privatsphäre-Einstellungen und Transparenz eine zentrale Rolle. Jeder VZ-Nutzer wird daher gleich bei seiner ersten Registrierung automatisch auf die höchste Stufe gesetzt und auf die dringende Nutzung dieser Einstellungen hingewiesen. Wir verzichten zudem bewusst darauf, dass VZ-Profile über Suchmaschinen wie Google auffindbar sind, d.h.: Alle Informationen sind innerhalb unserer Netzwerke bestmöglich geschützt. Persönliche Daten werden nie ohne die klare, transparente Einwilligung der Mitglieder verwendet und können jederzeit vollständig vom Profilinhaber gelöscht werden. „Das Internet vergisst nicht" gilt also in diesem Fall nicht für die VZ-Netzwerke. Gleichermaßen wichtig ist außerdem ein professioneller Support, der sich um Fragen der Nutzer kümmert und rechtzeitig reagiert, wenn gegen die AGB oder den Verhaltenskodex verstoßen wird. Nur wenn die richtigen Voraussetzungen gegeben sind, funktioniert die Selbstregulierung in sozialen Netzwerken.

Lösungsansätze und Antworten auf zentrale Fragen rund um das Phänomen „soziale Netzwerke" zu finden, ist jedoch nicht nur die Aufgabe der Betreiber. Politiker, Eltern und Lehrer sind ebenfalls gefragt, wenn es darum geht, den richtigen und sicheren Umgang zu gewährleisten. Dabei spielt Aufklärung – genau wie bei der Nutzung jedes anderen Mediums – eine zentrale Rolle. Als Marktführer in Deutschland fördern wir mit unterschiedlichen Projekten gezielt Medienkompetenz: In unserem Netzwerk, aber auch zu Hause, an Schulen und ab sofort sogar „offline" – direkt vor Ort.

Mehr Sicherheit durch Aufklärung: „Wir bringen Medienkompetenz an deine Schule"

Zum Safer Internet Day 2010 starten wir als erstes soziales Netzwerk eine bundesweite „Aufklärungs-Tour". Unter dem Motto „Wir bringen Medienkompetenz an deine Schule" besucht unser schülerVZ-Kompetenzteam Schüler, Lehrer und Eltern direkt vor Ort. Unser Ziel ist es, den bewussten und richtigen Umgang in sozialen Netzwerken zu fördern und dabei zentrale Hinweise zu geben: Von der Wahl des Passwortes über die Privatsphäre-Einstellungen, den Fotos und Informationen im eigenen Profil bis hin zum richtigen Umgang mit Freunden und „unbekannten" Nutzern. Eine spezielle Sicherheitsseite im schülerVZ gibt zusätzlich Antworten auf Schwerpunktthemen wie „Passwort und Datensicherheit", „Selbstdarstellung und Privatsphäre" sowie „Melden und Ignorieren". Lehrer und Eltern bieten wir als Hilfestellung außerdem Lehrmaterialien und Arbeitsmappen zum Download an.

Gleiches Recht für alle Betreiber in Deutschland

Bei allen Sicherheits- und Aufklärungsmaßnahmen ist die Zusammenarbeit zwischen Betreibern, Politik und Gesellschaft heute und vor allem zukünftig entscheidend, um soziale Netzwerke für die Nutzer so sicher wie möglich zu gestalten. Noch stärker als bisher müssen klare Regeln für *alle* Betreiber in Deutschland gelten, denn: Soziale Netzwerke wachsen – jeden Tag – und entwickeln sich mit ausgewählten Funktionalitäten immer weiter. Regeln für soziale Netzwerke dürfen nicht davon abhängen, in welchem Land die Server eines Anbieters stehen. Mit jeder Innovation ergeben sich neue Fragen, die gemeinsam beantwortet werden müssen. Das hohe gesetzliche Schutzniveau in Deutschland beim Jugend-, Daten- und Verbraucherschutz sowie die Maßnahmen der aktiven Aufsichtsbehörden und Verbände müssen dringend auch für ausländische Anbieter in Deutschland greifen. Schließlich stehen wir heute erst am Anfang und nutzen nur einen Bruchteil der unendlichen Möglichkeiten, die das Internet und soziale Netzwerke noch bieten können.

Safety first:
Persönlichkeitsrechte wahren, Datenschutz sicher stellen

Maria Brosch, Geschäftsführender Vorstand Schulen ans Netz e.V.

Sicherheit im Netz wird bei Schulen ans Netz ganz groß geschrieben. Denn der Verein hat sich als bundesweit agierendes Kompetenzzentrum das verständige Lernen und Lehren mit digitalen Medien auf die Fahnen geschrieben. Schulen ans Netz unterstützt auch in diesem Jahr die Aktivitäten zum „Safer Internet Day" von „klicksafe". Ziel des Aktionstages ist es, die Aufmerksamkeit aller auf das Thema „Sicheres Internet" zu lenken.

Ein Leben ohne Medien ist in unserer Gesellschaft nicht mehr vorstellbar. Ob in Freizeit, Schule oder Beruf – die Informations- und Kommunikationstechniken haben in allen Bereichen unseres Alltags Einzug gehalten. Die Computerwelten faszinieren Kinder und Jugendliche in besonderer Weise, wobei Internet und Co. in ihrer Freizeitnutzung hohe Priorität genießen. Wichtig für die Jugendlichen ist die Fähigkeit, Informationen auszuwählen, zu bewerten und zu verarbeiten. Zudem ist ein versierter Umgang mit Web 2.0-Techniken notwendig, um selbstbestimmt und verantwortungsvoll medial basiert zu kommunizieren. Weniger berücksichtigt wird von den Jugendlichen dabei häufig der gewissenhafte Umgang mit eigenen persönlichen Daten sowie der Schutz der Persönlichkeitsrechte anderer. Jugendliche geben im Internet gerne viel von sich preis. Gleichzeitig hat sich das Internet verändert und stellt mit Web 2.0 neue Kommunikationsmöglichkeiten zur Verfügung. Soziale Netzwerke im Internet sind nicht mehr begrenzt und selbst von den Initiatoren nicht mehr zu überschauen bzw. zu kontrollieren. Daher warnen Datenschützer die Nutzerinnen und Nutzer vor einem unreflektierten Umgang mit den eigenen personenbezogenen Daten und verteidigen Datenschutz als Bürger- und Menschenrecht.

Aus dieser Situationsbeschreibung ergibt sich ein klarer Auftrag an die Pädagoginnen und Pädagogen.

Maria Brosch
ist seit Ende August 2009 Geschäftsführender Vorstand des Vereins Schulen ans Netz. Sie war vorher jahrelang im Bundesministerium für Bildung und Forschung tätig, zuletzt als stellvertretende Referatsleiterin für Grundsatzfragen der beruflichen Bildung. Die für die Sekundarstufe I und II ausgebildete Lehrerin ist als Bildungsexpertin mit umfangreichen und vielseitigen Erfahrungen in Theorie und Praxis ausgewiesen.

Jugendliche sensibilisieren

Kinder und Jugendliche werden sich weder durch Verbote noch aus Vernunftgründen vom Surfen im Internet und von der Kommunikation im Web 2.0 abhalten lassen. Sie müssen daher lernen, die Gefahren zu erkennen, und sie müssen lernen, sich und andere vor ihnen zu schützen.

Worum geht es konkret?

Wichtig für Jugendliche ist es zu lernen, reflektiert mit den eigenen Daten umzugehen. Sie müssen sich fragen, was sie über sich in sozialen Netzwerken veröffentlichen wollen, die Preisgabe welcher Daten ihnen – sofort oder auch erst in Zukunft – schaden könnte und welche Informationen ihnen in zehn oder 20 Jahren peinlich wären. Auch sollten sie erkennen, dass passwortgeschützte Netzwerke – wie beispielsweise „schülerVZ" – letztlich öffentlicher Raum sind. Den Jugendlichen sollte bewusst gemacht werden, dass personenbezogene Daten ein wertvolles Gut sind. Denn es ist kein Kavaliersdelikt, wenn Informationen über Menschen ohne deren Zustimmung oder sogar gegen deren Willen veröffentlicht werden. Das gilt beispielsweise für Videos aus dem Unterricht oder Fotos von der letzten Party. Die Allgemeinen

Persönlichkeitsrechte müssen eingehalten werden, denn diese nicht zu beachten, ist ein Verstoß gegen ein Grundrecht.

Lernräume schaffen

Web 2.0 ist für jedermann frei zugänglich. Schule braucht aber geschützte Räume, in denen auch jüngere oder Internet unerfahrene Schülerinnen und Schüler erste Schritte in die Welt der Datennetze machen können. In diesen geschützten Räumen können sie online kommunizieren, fachlich kooperieren und ihre Fertigkeiten im Umgang mit Internet und PC erproben. Die Schülerinnen und Schüler brauchen Bildungsplattformen, die ihnen einen umfassenden technischen Schutz (IT-Sicherheit) und zugleich Schutz ihrer Persönlichkeitsrechte (Datenschutz) bieten. Dies kann erreicht werden mit einem kontrollierten, auf Bildungseinrichtungen beschränkten Zugang oder mit der medienpädagogischen Begleitung durch die Plattformbetreiber.

Die Plattformen von Schulen ans Netz erfüllen diese Kriterien in hervorragender Weise. Ausgewählte Beispiele sind „qualiboXX“, das virtuelle Lernzentrum für die Berufsvorbereitung, „Beroobi“, das interaktive Jugendportal zur Berufswahl, und „Mixopolis“, das interkulturelle Jugend-Online-Portal zur Berufsbildung.

Lehrende qualifizieren

Pädagoginnen und Pädagogen, Lehrerinnen und Lehrer müssen dazu befähigt werden, ihre Arbeit auch nach datenschutzrechtlichen Kriterien zu bewerten. Sie sollten wissen, welche Einschränkungen sich daraus für ihre medienpädagogische Arbeit ergeben. So sind sie beispielsweise verpflichtet, für die Publikation von Fotos und Videos, die Schülerinnen und Schüler abbilden, deren bzw. die Einwilligung der Erziehungsberechtigten einzuholen. Dies gilt auch für die Registrierung der Schülerinnen und Schüler bei Lernplattformen oder bei Web 2.0-Diensten. Doch damit nicht genug: auch die Kenntnis der aktuellen gesellschaftlichen, politischen und kulturellen Diskussionen zum und um den Datenschutz gehört zu ihrem Handwerk.

Nur dann, wenn all diese Voraussetzungen berücksichtigt werden, bleibt „safety first“ keine hohle Phrase, sondern kann sich als grundlegende Voraussetzung zur Wahrung der Persönlichkeitsrechte im World Wide Web etablieren.

Von Schützern und Beschützten

Jutta Croll,
Geschäftsführerin Stiftung Digitale Chancen

Mit dem Begriff des Datenschutzes kann man in Deutschland seit den 70er-Jahren auch in der Öffentlichkeit etwas anfangen – damals wurden Datenschutzbeauftragte in den Ländern und auf Bundesebene, später auch bei Unternehmen und Konzernen mit entsprechenden Aufgaben betraut. Was sie dort tun, und wen oder was sie vor wem schützen sollen, ist dem Großteil der Bevölkerung aber auch heute noch weitgehend unklar. So genannte Datenpannen, über die zunehmend in den Medien berichtet wird, betreffen häufig die Weitergabe von Adressen oder Kundendaten durch Unternehmen, aber auch Privatpersonen sind – Stichwort Phishing – dem Risiko der ungewollten Preisgabe von Daten ausgesetzt.

Mit der weiten Verbreitung von Computern auch in den privaten Haushalten hat sich neben dem Datenschutz auch der Begriff der Datensicherheit etabliert. Sicher sollen die Daten sein und geschützt müssen sie werden. Was sind diese Daten, die es zu schützen gilt, die gesichert werden müssen – auch hier herrscht weitgehend Unwissenheit vor. Datenschutz und Datensicherheit sind ein Wortpaar, das vielfach synonym verwendet wird, im Grunde aber haben beide Worte eine völlig unterschiedliche Bedeutung. Datensicherheit meint, dass von mir produzierte Daten, z. B. die Dateien auf meinem Rechner, gesichert sein müssen gegen etwaige Beschädigung, Löschung oder Veränderungen durch meine eigenen Aktivitäten oder die Eingriffe anderer. Mit Datenschutz hingegen bezeichnet man den Schutz der auf meine Person bezogenen Daten vor der Erfassung, Kenntnisnahme und Verarbeitung durch Unbefugte. Mit Blick auf das Internet geht es dabei vor allem um Daten, die bei der Nutzung vom Serviceprovider und von Anbietern von Applikationen gespeichert werden.

Jutta Croll

ist seit April 2003 Geschäftsführerin der Stiftung Digitale Chancen, einer gemeinnützigen Organisation unter der Schirmherrschaft des Bundesministeriums für Wirtschaft und Technologie und des Bundesministeriums für Familie, Senioren, Frauen und Jugend.
Die Stiftung arbeitet an dem Ziel der Digitalen Integration von Bevölkerungsgruppen, die bei der Internetnutzung bisher unterrepräsentiert sind. Sie entwickelt Projekte und innovative Strategien zur Förderung der Medienkompetenz.
Jutta Croll ist als Wissenschaftlerin in verschiedenen Projekten zur Nutzung von Medien und Förderung der Medienkompetenz tätig. Sie hat von 1985 – 1990 an der Universität Göttingen Deutsche Literaturwissenschaft, Politikwissenschaften und Publizistik studiert und als Magistra Artium abgeschlossen. Freiberuflich ist sie u. a. für die UNESCO und den Brockhaus Verlag mit der Erstellung von Studien, Curricula und wissenschaftlichen Beiträgen befasst.
Sie ist Mitglied verschiedener Projektbeiräte und Steuerungsgruppen auf deutscher und europäischer Ebene, zurzeit u. a. Advisory Board des deutschen Safer Internet Centre, Mitglied der Arbeitsgruppe Medien und Integration bei der Beauftragten der Bundesregierung für Integration und Migration, Mitglied im Projektbeirat 'Barrierefrei informieren und kommunizieren' sowie in der Arbeitsgruppe 'Barrierefreies E-Government' des BMAS.

Ein wesentlicher Unterschied besteht darin, dass Daten- oder IT-Sicherheit sich auf gespeicherte Daten bezieht, Datenschutz im Sinne des Persönlichkeitsschutzes aber schon bei der Frage der Zulässigkeit der Erhebung von personenbezogenen Daten anfängt. So regelt der Datenschutzparagraph im Telemediengesetz, welche Daten der Anbieter einer Webseite beim Besuch eines Nutzers erfassen und wie lange er diese Daten speichern darf, während Datensicherheit die technischen Maßnahmen meint, die getroffene werden müssen, um zulässig gespeicherte Daten vor unberechtigten Zugriffen zu schützen (z. B. durch Passwortschutz etc.).

Im Rahmen einer bundesweiten Trainingskampagne qualifiziert die Stiftung Digitale Chancen in einem

Zeitraum von drei Jahren bis Ende 2011 im Auftrag des Bundeswirtschaftsministeriums mehr als eintausend Mitarbeitende der sozialen Arbeit und informellen Bildung für einen sicheren und kompetenten Umgang mit dem Internet. Ziel ist es, über diese Multiplikatorinnen und Multiplikatoren in weiten Teilen der Bevölkerung ein Bewusstsein für die Chancen, aber auch für die Risiken der Internetnutzung zu schaffen. Aus den ersten Schulungen wissen wir, dass ganz unterschiedliche Auffassungen davon, was schützenswerte Daten seien, verbreitet sind. Datensicherheit ist "ein wichtiges Thema", das im Training behandelt werden soll, so die einhellige Meinung. In der Diskussion geht es dann sehr schnell eher um den Datenschutz, die – unfreiwillige – Preisgabe persönlicher Daten steht im Mittelpunkt des Interesses.

Im angelsächsischen Sprachraum ist die Differenzierung genauer, hier spricht man von 'safety' und 'security', beide Begriffe werden im Deutschen mit dem Wort Sicherheit übersetzt. Daneben steht 'dataprotection' oft auch nur kurz 'privacy', im Deutschen als Schutz der Privatsphäre bezeichnet. Privatsphäre ist das Zauberwort, mit dem man auch diejenigen für das Thema interessieren kann, die bei Datensicherheit an Technikfreaks und bei Datenschutz an notorisch Ängstliche denken und sich selbst dabei ganz sicher fühlen. Privatsphäre ist etwas, das man nicht preisgeben, sondern bewahren möchte, etwas wofür man sich größtmöglichen Schutz wünscht.

Mit Blick auf das Internet heute und die vielfältigen Möglichkeiten, die es den Nutzerinnen und Nutzern bietet, muss man allerdings über den Begriff der Privatsphäre neu nachdenken. In sozialen Netzwerken geben die Menschen – junge und ältere – Informationen über sich selbst preis. Dies ist den Mitgliedern der Community durchaus bewusst, vielfach treffen sie in Kenntnis der Verbreitungsmöglichkeiten ihre Entscheidung, was andere über sie wissen sollen. Denn nur wer bereit ist, sich selbst darzustellen, erzielt den gewünschten Effekt – mit möglichst vielen Gleichgesinnten in Kontakt zu kommen. Jüngere Nutzerinnen und Nutzer können vielfach die Konsequenzen dieser Bereitschaft zur öffentlichen Darstellung nicht in vollem Umfang abschätzen. Doch bei der Abwägung von Risiko und Nutzen fällt die Entscheidung im Zweifel zu Gunsten des Vorteils, den man sich von der Offenheit erhofft. Kontakte sind die Währung des Internetzeitalters, deshalb scheint der Preis, den man dafür zahlt, die Sache wert.

Die Sphärentheorie unterscheidet mit Bezug auf das allgemeine Persönlichkeitsrecht zwischen der Intimsphäre, der Privatsphäre und der Individualsphäre eines Menschen. Die Intimsphäre ist der Bereich, den wir selten anderen offenbaren, die Privatsphäre öffnen wir gezielt ausgewählten Personen, die Individualsphäre teilen wir mit anderen, um uns selbst zu präsentieren. Diese drei Sphären repräsentieren unser persönliches Lebensumfeld, welches sich durch das Netz zunehmend verändert. Das Internet ist für viele Menschen fester Bestandteil des alltäglichen Lebens geworden, es gehört zu unserem Lebensumfeld. Deshalb ist es nur naheliegend, dass sich auch das Verständnis, was der jeweiligen Sphäre angehört, heute wandelt. Wenn diese Sphären sich in konzentrischen Kreisen um die eigene Person legen, dann sind diese Kreise heute enger gezogen. Das, was wirklich drin bleiben muss, was es zu schützen gilt, befindet sich in den innersten Kreisen. Alles das, was ein wenig weiter draußen angesiedelt ist, wird öffentlich. Die äußeren Kreise unserer Sphären überlappen sich bereits heute mit den Kreisen anderer Menschen – so entstehen Kontakte. Das ist es, was die meisten Menschen heute wollen und deshalb sind sie bereit, große Teile dessen, was früher als Intim- und Privatsphäre galt, mit anderen zu teilen: Familienfotos, persönliche Erfahrungen, sexuelle Vorlieben, eigene Bewertung von Produkten und Dienstleistungen, individuelle Meinungen über andere Personen.

Mit diesem Wandel geht ein verändertes Verständnis von Datenschutz einher. Datenschutz kann nur wirksam praktiziert werden, wo auch die Eigentümer der Daten selbst ein Schutzbedürfnis haben. Dieses angemessen zu entwickeln ist eine vorrangige Aufgabe des heutigen Datenschutzes und der Vermittlung von Medienkompetenz. Aber die durchaus zulässige Speicherung all dieser bereitwillig preisgegebenen Information birgt auch das Risiko, dass aus der Verknüpfung von an der einen Stelle veröffentlichten Infor-

mationen mit den an einer anderen Stelle gespeicherten Daten ein Profil gebildet werden kann, das der Nutzer selbst so niemals zusammengestellt hätte. Gegen diese Profilbildung ist auch Medienkompetenz kein gewachsenes Kraut.

Datenschutz und Persönlichkeitsrechte im Web 2.0

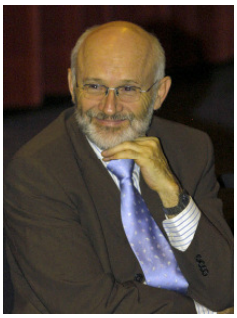
Siegfried Czernohorsky,
Referatsleiter im Ministerium für Bildung, Wissenschaft, Jugend und Kultur

Der Umgang mit virtuellen Welten ist heute ein Teil der Lebenswirklichkeit in einer digital geprägten Kultur. Vor allem für die junge Generation – die „digital natives" – spielen diese Welten eine wesentliche Rolle bei ihrer Sozialisation, Identitätsbildung und Beziehung zur Welt. Sie sind Teil ihrer Alltagskultur.

Das Web 2.0 bietet heute Standardplattformen für den Wissens- und Informationsaustausch und die Kommunikation nicht nur unter Jugendlichen. Vor allem soziale Netzwerke haben dabei eine wichtige Funktion bei der Erweiterung und Bereicherung sozialer Interaktion und bieten einen erkennbaren Mehrwert. Dies gilt vor in einer zunehmend globaleren Welt. Nicht dabei zu sein, wird als Makel wahrgenommen. Befürchtungen, die neuen Medien führten zu Vereinsamung und Isolation haben sich so nicht bestätigt. Vielmehr werden die neuen Kommunikationsmöglichkeiten zunehmend auch als Mittel der gesamtgesellschaftlichen Kommunikation, des politischen Diskurses und der politischen Willensbildung genutzt. Niedere technische Hürden und eine nahezu unbegrenzte Verfügbarkeit sind hierfür die entscheidenden Voraussetzungen.

Trotz aller Vorteile sollten die Risiken nicht unterschätzt werden: die leichtfertige Weitergabe persönlicher Daten für oft geringe Vorteile, mangelnde Kenntnisse – z. B. über technische Möglichkeiten des Selbstdatenschutzes – und ein unzureichendes Problembewusstsein, dass es sich bei sozialen Netzwerken eben nicht um vertrauliche Kommunikation in Privaträumen handelt. Hinzu kommen Erscheinungen wie der Missbrauch persönlicher Daten zu Mobbing im Internet, das Sammeln von Daten zu kommerziellen Zwecken, ihre nicht zu kontrollierende Weitergabe sowie potenzielle negative Auswirkungen der Spuren im Internet auf zukünftige beruf-

Siegfried Czernohorsy



Geboren 1950; Schulzeit und Abitur in Trier; 1972: Studium an der Universität Trier (Lehramt für Gymnasien); 1977/78: 1. und 2. Staatsexamen; 1979: Tätigkeit am Thomas-Morus-Gymnasium, Daun; ab 1990: Leiter des Medienzentrums Kreis Daun, hier Mitwirkung bei Modellversuchen im Bereich Medien und Medienerziehung sowie zahlreichen Hörfunk- und Filmprojekten zur Medienerziehung; ab 1995: Mitglied der Schulleitung des Thomas-Morus-Gymnasiums, Daun; 2001: Abordnung als Referent an das Ministerium für Bildung, Frauen und Jugend Rheinland-Pfalz; seit 2004: Leiter Referat 943 A: Medien und neue Informations- und Kommunikationstechnologien in der Schule, Abt. 4 A, Ministerium für Bildung, Wissenschaft, Jugend und Kultur, Rheinland-Pfalz; seit 2007: Projektkoordination: 10-Punkte-Programm der Landesregierung „Medienkompetenz macht Schule".

liche Karrieren. Das Internet ist zwar ein flüchtiges und schnelles Medium, es vergisst jedoch nichts.

Die informationelle Selbstbestimmung und der Schutz der Persönlichkeitsrechte haben in der Bundesrepublik Verfassungsrang. Sie sind Grundpfeiler der Bürgergesellschaft und eines demokratischen Staates. Angesichts des schnellen Wandels der Kommunikationsformen und seiner Mittel bedürfen diese Anliegen einer nachhaltigen Vergewisserung im gesamtgesellschaftlichen Diskurs. Dies gilt auch für die Bildungs- und Erziehungsprozesse in Schule, Jugendarbeit und Elternhaus.

Ein effektiver und zeitgemäßer Datenschutz bewegt sich im Spannungsfeld zwischen der Wahrung der Rechte auf freie Meinungsäußerung und der freien Entfaltung der Persönlichkeit einerseits und dem Sicherheitsbedürfnis der Bürgergesellschaft und des Staates andererseits. Er hat auch den Schutz des Einzelnen vor ökonomischer Übermacht und Datenmissbrauch sicherzustellen. Hierzu muss der Gesetzgeber einen Handlungsrahmen – auch im suprana-

tionalen Kontext – definieren. Weiterhin muss auch die Wirtschaft mit selbstregulierenden Maßnahmen einen Beitrag leisten.

In dem Prozess des schnellen Wandels der Kommunikationswege ist es weiterhin wichtig, für das Thema Datenschutz zu sensibilisieren und das Problembewusstsein aller, vor allem der an Bildung und Erziehung Beteiligten zu schärfen und den kompetenten Umgang mit den neuen Kommunikationsformen zu fördern. Diese Aufgabe ist ein „Bildungs- und Erziehungsauftrag" in neuer Form und ein unverzichtbarer Beitrag zur Förderung der Medienkompetenz als Schlüsselqualifikation in der Informations- und Wissensgesellschaft.

Schule, Jugendarbeit und Elternhaus benötigen für diese Aufgabe kompetente Unterstützung, wie z. B. aktuelle, alltagstaugliche, objektive und nachhaltige Informations-, Beratungs- und Qualifizierungsangebote. Hier sind staatliche Institutionen, pädagogische Einrichtungen, Verbraucherberatungsstellen, die Landesbeauftragten für den Datenschutz und auch die Verantwortung der Diensteanbieter der Internetwirtschaft gefordert.

Die Initiative „klicksafe" als europäischer Knotenpunkt ist ein kompetenter Partner, der aktuelle Entwicklungen frühzeitig aufgreift, Maßnahmen anstößt und Erfahrungen aus einem europäischen Netzwerk mit in den Prozess der Bewusstseinsbildung auf nationaler Ebene einbringt.

Die Bildungsministerien in den Ländern haben sich den Herausforderungen in vielfältiger Form angenommen. So wurden beispielsweise in Abstimmung mit dem Schulausschuss der KMK ein Informationsreader („Im Netz der neuen Medien") in hoher Auflage erstellt und Experten in den Ländern ausgebildet. In Rheinland-Pfalz wurden u. a. bereits 800 Lehrkräfte zu Jugendmedienschutzberaterinnen und -beratern in den Schulen ausgebildet.

Der Safer Internet Day hat sich inzwischen zu einem festen Datum nicht nur in den Köpfen der Medienpädagogen, sondern im Gedächtnis vieler, die mit den neuen Medien zu tun haben, entwickelt. Ca. 500 Schülerinnen und Schüler kommen am Safer Internet Day 2010 in einer zentralen Veranstaltung im ZDF in Mainz zusammen. Sie geben ihr Expertenwissen als „Medienscouts" an ihre Mitschülerinnen und Mitschüler weiter, um sie dabei zu unterstützen, das Internet bewusst und kompetent zu nutzen.

Datenschutz und Persönlichkeitsrechte im Web 2.0

Valentina Daiber, Telefónica O_2

Die Welt hat sich verändert und doch ist vieles gleich geblieben. Kinder und Jugendliche spielen ähnliche Dinge wie die Generation vor ihnen und gehen den gleichen sozialen Aktivitäten nach – sie tauschen sich über Schule und Alltag aus und besprechen ihre Probleme.

Im Vergleich zu früher geschieht dies jedoch mit gänzlich anderen Medien. Jedes zweite Kind hat heute bereits ein Mobiltelefon. Die Zahl steigt bei älteren Jugendlichen auf nahezu 100% und gleichzeitig steigt auch die technische Ausstattung der jungen Handynutzer weiter an. Dies hat viele Vorteile: Eltern schätzen es beispielsweise, wenn sie ihr Kind jederzeit erreichen können. Doch je mehr Funktionen das Gerät hat, desto schwieriger wird es oft für Eltern, nachvollziehen zu können, womit sich das Kind beschäftigt. So tauschen Jugendliche sich beispielsweise per Instant Messaging oder in Social Communities aus. Für Eltern und Pädagogen ist diese Lebenswelt im Web 2.0 kaum nachvollziehbar.

Um eine ausgewogene und sinnvolle Nutzung der neuen Medien durch Kinder und Jugendliche sicherzustellen, müssen alle Betroffenen Hand in Hand gehen: jugendliche Nutzer, Eltern, Pädagogen, Politik und Wirtschaft.

Telefónica O_2 nimmt das sehr ernst: Technische Schutzvorkehrungen, medienpädagogische Aufklärung und Preistransparenz sind wichtige Bestandteile unseres Jugendschutzprogramms. Als integriertem Telekommunikationsanbieter liegt es uns besonders am Herzen, Kinder und Eltern dabei zu unterstützen, die Services und Produkte im Internet und Mobilfunkbereich sicher und sinnvoll zu nutzen.

Der Aufbau von Medienkompetenz durch Aufklärung und Schulung im verantwortungsvollen Umgang mit der Technologie ist hierbei der richtige Weg. Nur so können Eltern und Erzieher ebenso wie Kinder und Jugendliche im Umgang auch mit möglichen Gefahren und Risiken sensibilisiert werden. Daher hat Telefónica O_2 gemeinsam mit klicksafe einen Elternratgeber sowie Check-Listen entwickelt. Diese sind auf unserem Kundenportal zum Download bereitgelegt.

Valentina Daiber
ist Leiterin der Abteilung Regulierungsrecht sowie Jugendschutzbeauftragte beim Telekommunikationsunternehmen Telefónica O_2 in München.

Nach dem Studium der Rechtswissenschaften war Frau Daiber zunächst wissenschaftliche Mitarbeiterin beim Institut für Europäisches Medienrecht (EMR) in Saarbrücken. 1998 wechselte sie als Rechtsreferentin zur damaligen Landeszentrale für private Rundfunkveranstalter (LPR) in Ludwigshafen, der heutigen LMK. Seit 1999 ist Frau Daiber in unterschiedlichen Funktionen bei Telefónica O_2 beschäftigt, wo sie seit 2003 auch die Funktion der betrieblichen Jugendschutzbeauftragten innehat. Seit 2006 ist Valentina Daiber Mitglied des Vorstandes der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM), seit 2009 Mitglied des Advisory Board des deutschen Safer Internet Centre.

Im Hinblick auf das Thema „Datenschutz im Jugendschutz" sind uns insbesondere folgende Punkte wichtig:

- Kinder und Schüler sollten zu mündigen Bürgern der Informationsgesellschaft erzogen werden. Hierzu ist es wichtig, dass ihnen bereits in jungen Jahren die Bedeutung der Privatsphäre und des Datenschutzes bewusst gemacht wird. Dieses Wissen ermöglicht es ihnen später, sachkundige Entscheidungen darüber zu treffen, welche Informationen sie gegenüber welchen Personen und unter welchen Bedingungen offen legen möchten.

- Telefónica O_2 ist mit der Europäischen Kommission einer Meinung, dass Web 2.0 und Social Networking Services mittlerweile eine große Bedeutung haben. Diese Entwicklung und die damit verbundenen Möglichkeiten sollten für alle Menschen in der Gesellschaft verfügbar sein. Im Kontext der unterschiedlichen Möglichkeiten für die gewinnbringende Nutzung von Social Networking Services erachtet Telefónica O_2 die Bildung und Sensibilisierung von Kindern, Eltern und Pädagogen als essentielle Komponente in der Strategie zum Schutz von minderjährigen Nutzern.

- Ebenso wie andere Netzbetreiber darf auch Telefónica O_2 nicht in die private Kommunikation zwischen zwei Personen eingreifen. Unsere Verantwortung besteht vielmehr darin sicherzustellen, dass unsere Services zuverlässig, kosteneffizient und vertrauenswürdig sind. Rechtliche Sicherheit im Kontext aller Online-Services ist für Telefónica O_2 und die gesamte Industrie zwingend notwendig, um innovative und nützliche Services für den Kunden anbieten und damit die Nachfrage des Marktes nach einer Weiterentwicklung der Kommunikationsprodukte erfüllen zu können.

- Bei der Gestaltung von Social Networking Services sind die datenschutzrechtlichen und jugendschutzrechtlichen Vorschriften des geltenden Rechtsrahmens anzuwenden, wobei auf die besonderen Interessen von Kindern und Jugendlichen Rücksicht zu nehmen ist. Der geltende Rechtsrahmen enthält ausreichend Instrumente für die verantwortungsvolle Ausgestaltung von Social Networking Services.

Datenschutz ist ein zentraler und wichtiger Punkt bei der Gestaltung von Social Networking Services. Andere Interessen müssen hierbei allerdings Berücksichtigung finden, wie z.B. Nutzerfreundlichkeit. Es bedarf einer Abwägung, die immer auch die besonderen Belange von Kindern und Jugendlichen beachten muss. Dies kann u.a. durch besondere Maßnahmen für Kinder und Jugendliche geschehen, z.B. strengere Standardeinstellungen, Einschränkung von Suchfunktionen sowie besondere Information über Meldewege bei Problemen und Beschwerden.

Ist Datenschutz uncool?

Dr. Alexander Dix,
Berliner Beauftragter für Datenschutz und Informationsfreiheit

Der Chef von Facebook, Mark Zuckerberg, hat gerade in einem Interview erklärt, die weltweit größte Online Community passe sich den geänderten sozialen Normen nur an. Als er mit Facebook in Harvard begonnen habe, hätten sich die Leute gefragt, warum man überhaupt Daten über sich ins Web stellen sollte. Mittlerweile würden die Menschen immer mehr Informationen über sich preisgeben und mit anderen teilen. Dem entsprächen die neuen Facebook-Grundeinstellungen. Zuckerberg ist offenbar der Meinung, Datenschutz sei nicht mehr so richtig zeitgemäß. Er hat übrigens auch 300 eigene Privatfotos öffentlich zugänglich gemacht, unter denen sich versehentlich auch private Aufnahmen seiner Freundin befanden.

Tatsache ist aber, dass Facebook mit diesen Grundeinstellungen seinen Nutzern praktisch vorschreibt, was sie wem zu offenbaren haben. Wer nicht aufgepasst hat, dessen Daten waren seit Dezember 2009 von heute auf morgen für alle Facebook-Mitglieder sichtbar und nicht nur für die „Freunde" des jeweiligen Users. Um das zu ändern, mussten die User Einstellungen ändern. Wem das zu umständlich war oder wer die geänderten Voreinstellungen überhaupt nicht mitbekommen hatte, der musste damit leben, dass das hochgeladene Profil einschließlich Foto und anderen Informationen wie Hobbys, Musik-Vorlieben etc. Leuten offenbart wurden, für die sie ursprünglich nicht gedacht waren. Offenbar hatte auch der Gründer von Facebook nicht mitbekommen, was die geänderten Voreinstellungen bedeuteten, denn er sperrte wenig später einige private Bilder seiner Freundin in seinem Profil, die durch die Umstellung für alle Facebook-Nutzer zugänglich geworden waren.

Das führt zu der Grundfrage, worum es beim Datenschutz überhaupt geht. „Datenschutz" ist ein veralteter Begriff, der so klingt, als gehe es um den Schutz von Daten um ihrer selbst willen. Worum es wirklich geht, hat der Chef von Google, Eric Schmidt, in schöner Offenheit so formuliert: „Wenn es etwas gibt, dass Sie andere nicht wissen lassen wollen, hätten Sie es vielleicht gar nicht erst tun sollen." Mit anderen Worten: wenn es nach Google geht, sollte kein Mensch mehr irgendwelche Geheimnisse vor irgendwem haben. Er sollte sich so verhalten, dass alle es wissen können (denn mithilfe von Google werden alle es wissen).

In einer solchen Gesellschaft will aber niemand leben. Letztlich brauchen wir den Datenschutz auch und gerade im Web 2.0, um uns frei bewegen zu können. Datenschutz schützt keine Daten, sondern das Grundrecht jedes einzelnen Menschen auf Verhaltensfreiheit. Verhaltensfreiheit gibt es nur, wenn jeder selbst entscheidet, was mit seinen Daten geschieht. Was hat Google mit Facebook zu tun ? Die

Dr. Alexander Dix

wurde am 2. Juni 2005 vom Abgeordnetenhaus zum Berliner Beauftragten für Datenschutz und Informationsfreiheit gewählt. Dr. Alexander Dix, LL.M., geb.1951, ist seit Juni 2005 Berliner Beauftragter für Datenschutz und Informationsfreiheit. Zuvor war er sieben Jahre Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg. Er ist Vorsitzender der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (international auch bekannt als "Berlin Group") und Mitglied der Artikel 29-Gruppe der Europäischen Datenschutzbeauftragten. Das Studium der Rechtswissenschaften in Bochum, Hamburg und London schloss er mit dem Grad eines Master of Laws an der London School of Economics and Political Science ab und promovierte 1984 zum Dr. jur. an der Universität Hamburg. Er begann seine Tätigkeit beim Berliner Datenschutzbeauftragten 1985 und war von 1990 bis 1998 dessen Stellvertreter.

Suchmaschine von Google durchsucht auch Online Communities, wenn diese es nicht verhindern (was möglich ist). Von niemandem kann aber verhindert werden, dass „Freunde“ oder andere Mitglieder der Community ein Suchprogramm („crawler“) im Inneren der Community starten, um dann massenhaft Daten von der Plattform abzusaugen und ins offene Internet zu stellen. Das widerspricht zwar den Nutzungsbedingungen der meisten communities, ist aber weder strafbar noch technisch mit Sicherheit auszuschließen. Das ist in den vergangenen Monaten mehrfach passiert und hat zu erheblicher Unruhe unter Usern geführt, weil sie dieses Risiko nicht gesehen haben (sie wurden von den Betreibern auch nicht darauf hingewiesen).

Die Behauptung, Datenschutz werde gerade von jungen Menschen als uncool empfunden, ist falsch. Meine eigenen Erfahrungen mit Jugendlichen, die sich mit dem Thema beschäftigen, belegen etwas anderes. Es mag sein, dass Jugendliche heute etwas anderes unter Datenschutz und Schutz der Privatsphäre oder der Persönlichkeitsrechte verstehen. Aber sie erwarten gerade, wenn sie sich in einem sozialen Netzwerk tummeln, ein bestimmtes Maß an Intimität und Schutz vor allgemeiner Beobachtung. Mit dieser Erwartung werben Plattformen wie Facebook und StudiVZ geradezu. Allerdings wird diese Erwartung immer wieder enttäuscht, weil die Betreiber (vor allem Facebook) den Nutzern vorschreiben, was mit ihren Daten passiert. Das ist alles andere als datenschutzgerecht. Es kommt auch vor, dass User sich nicht um die vorhandenen Einstellmöglichkeiten kümmern, die bestimmte soziale Netzwerke durchaus anbieten, um den Schutz der eigenen Profildaten zu verbessern.

Worauf sollte man achten, wenn man soziale Netze nutzt ?

1. **Sich genau ansehen, welche Einstellmöglichkeiten ein soziales Netz bietet, welche Informationen in punkto Datenschutz gegeben werden.** Je weniger Einstellmöglichkeiten eine Plattform hat und je spärlicher oder unverständlicher die Informationen zum Umgang mit Nutzerdaten sind, desto weniger vertrauenswürdig ist der jeweilige Anbieter. Man sollte sich auf anderen Plattformen umsehen, ob sie besser sind.

2. **Die vorhandenen Einstellmöglichkeiten sollte man gleich zu Beginn nutzen, um die eigenen Profildaten möglichst nur den „Freunden“ zu zeigen, die man sich ausgesucht hat.** Auch wenn man dies tut, muss man damit rechnen, dass Daten aus dem eigenen Profil – evtl. unter Einsatz von „crawler“-Programmen oder im Einzelfall – kopiert und ins offene Internet exportiert werden, wo sie auch für künftige Arbeitgeber oder andere sichtbar sind. Wer das cool findet, muss sich nicht darum kümmern, die anderen sollten genauer überlegen, was für Daten und Bilder sie hochladen. Auch für sog. „Apps“, das sind kleine Online-Programme von Dritten, sollte man die hoffentlich vorhandenen Datenschutzeinstellungen genau prüfen. Denn in der Regel kann auch der Anbieter eines solchen Fremdprogramms auf die zugänglichen Daten zugreifen. Oft werden aber Daten – möglicherweise verdeckt – zugänglich gemacht, die z.B. für ein einfaches Online-Spiel gar nicht notwendig sind.

3. **Möglichst unter Pseudonym im sozialen Netz auftreten.** Man muss sich zwar bei der Registrierung gegenüber dem Betreiber online identifizieren, kann sich aber dennoch anschließend einen passenden Spitznamen aussuchen. Jeder hat das Recht, einen Spitznamen in der community zu verwenden. Betreiber, die das untersagen, verstoßen gegen das Gesetz.

4. **Wenn man sich überhaupt in sozialen Netzen anmelden will, sollte man mehr als nur ein Netz nutzen.** Wie in der realen Welt hat man dann die Möglichkeit, verschiedenen „Freundeskreisen“ verschiedene Teile des eigenen Lebens mitzuteilen. **Es müssen und sollten gerade nicht alle alles über mich wissen.** Außerdem kann man in verschiedenen Netzen noch mehr interessante Leute kennenlernen.

Der Dr. Tafel in dir

Oder: Was Lehrerinnen und Lehrer über Datenschutz wissen sollten

Marco Fileccia, Elsa-Brändström-Gymnasium Oberhausen

Nehmen wir ein nicht ganz ernstgemeintes Fallbeispiel. Oberstudienrat Dr. Tafel ist ein typischer Digital Hippie: Außen cool, offensichtlich durchdigitalisiert, aber tief innen sehnt er sich nach Preußens Gloria und alten Oberlehrerzeiten ohne diesen ganzen Medienkram. Mit seinem üppigen Gehalt (A 14 Beamtentarif) investiert er regelmäßig in neue Technik, schleppt ein Netbook in den Unterricht, spricht über den Flur laufend Memos demonstrativ und lautstark in das digitale Aufnahmegerät, als sei es taub, und prahlt mit einem iPhone, das selbstverständlich die App „TeacherTool“ zur Notenverwaltung enthält (die Funktion „Sprachmemos“ im iPhone kennt er hingegen nicht). Schülerarbeiten nimmt er nur in digitaler Form online entgegen und macht sie auf dem USB-Stick in Größe seines Daumennagels mobil. Auf der Schulhomepage prangt sein Bild mit dem Link zum öffentlichen Facebook-Profil und einige Schüler haben ihn letztens erwischt, wie er im Unterricht twitterte „Bin im Unterricht. Langeweile“.

Zugegebenermaßen ist unser Fallbeispiel nicht ganz typisch… Trotzdem: Was hat so ein Mensch, was haben Lehrerinnen und Lehrer mit Datenschutz zu tun? Was haben wir in der Schule mit Datenschutz am Hut?

Lehrerinnen und Lehrer hantieren ständig mit persönlichen Daten von Schülerinnen und Schülern, so bspw. in Form von Notenlisten. Ohne auf die rechtlichen Fragen einzugehen, so hat jeder die Pflicht, diese sehr sorgfältig zu behandeln und vor Missbrauch zu schützen. Stellen Sie sich vor, unser Digital-Tafel lässt einen USB-Stick voller Schülerdaten in einem Café liegen, wo er eben noch mit seinem Netbook und Latte Macchiato saß. USB-Sticks und Dateien auf einem Laptop kann man verschlüsseln und per Passwort vor fremden Zugriff schützen.

Marco Fileccia

Jahrgang 1963. Unterrichtet am Elsa-Brändström-Gymnasium in Oberhausen die Fächer Biologie, Informatik, Politik und Sozialwissenschaften. Marco Fileccia war zuvor am Bert-Brecht Gymnasium Dortmund und einige Jahre pädagogischer Mitarbeiter im Bereich "Neue Medien in der Lehrerbildung" am NRW-Landesinstitut für Schule in Soest. Er ist Moderator in der Lehrerfortbildung im Bereich kooperatives Lernen und digitale Medien und arbeitet im Projekt "Schule der Zukunft" der NUA und des Schulministeriums NRW. Er ist Autor des klicksafe-Lehrerhandbuchs „Know-How für junge User – Materialien für den Unterricht“ sowie Mitautor der Zusatzmodule zu den Themen Cyber-Mobbing, Social Communites und Datenschutz. Seit Jahren veranstaltet Fileccia Elternabende und Informationsveranstaltungen für Lehrer über digitale Medien und Handys in der Initiative „Eltern+Medien“ der Landesanstalt für Medien Nordrhein-Westfalen (LfM) und des Grimme-Instituts. Er ist Beratungs-Spezialist für Medienliteratur auf „Lehrer-online“ und als Jurymitglied im Schülerwettbewerb der Bundeszentrale für Politische Bildung tätig.

Dr. Tafel macht es sich einfach und besitzt privat nur ein einziges Passwort (den Vornamen seiner Frau Andrea, den er aber nicht verrät). Außerdem hat er das Passwort des Schulrechners letztens dem Willi aus der 10. gegeben, weil er keine Zeit hatte, sich darum zu kümmern… Ist ein Kommentar notwendig? Passwörter sollten mehr als acht Zeichen haben, um es den bösen Buben schwerer zu machen, und sie sollten Sonderzeichen / Ziffern enthalten. Und man sollte sie nie weitergeben, und diese Informationen sollten wir an unsere Kinder weitergeben!

Was Dr. Tafel ahnt, aber nicht weiß (er ist schließlich kein Digital Native): Die Löschfunktion von Windows ist alles andere als sicher. Auch wenn er glaubt, die alte Notenliste von seiner Festplatte oder einem USB-Stick entfernt zu haben, so ist sie doch schnell wieder hervorzuzaubern. Es gibt spezielle Löschprogramme, die Daten sicher löschen können. Und

trotzdem sollte man unserem Paradelehrer Tafel raten, auch alte Festplatten nie weiterzugeben, sondern sicher zu zerstören.

Aber es geht nicht nur um technische Kompetenz… Lehrer und Lehrerinnen sollen Kinder auch erziehen (auch wenn Dr. Tafel davon träumt, sich selbst durch Medien überflüssig zu machen und die Erziehung komplett Dieter Bohlen zu überlassen). Ohne auf die formalen Beschreibungen von Bildungs- und Erziehungsauftrag einzugehen, so ist es doch überlegens- und vielleicht wünschenswert, Kinder und Jugendliche „fit" zu machen für diese digitale Welt. Medienkompetent könnte man das nennen. Und dazu gehören in einer vernetzten Internetwelt der Datenschutz und die Frage: Welche Daten von mir gebe ich im SchülerVZ preis? Wie schütze ich meine persönlichen Daten? Wie gehe ich mit den Daten anderer um? Sollte ich das Party-Foto wirklich veröffentlichen?

Doch unser Hr. Tafel ist so sehr Fachlehrer wie viele seiner Kolleginnen und Kollegen – da sieht er sich leider nicht in der Pflicht. Und das ist das Dilemma dieses wichtigen Themas: Es passt nirgendwo so richtig hinein, und ein Fach Medienlehre (wahlweise Medienkunde, Medienbildung) gibt es nicht überall und flächendeckend in unserem 16-Schulsysteme-Land. Wer das Thema trotzdem im Unterricht behandeln möchte: Die Broschüre „Ich bin öffentlich ganz privat. Datenschutz und Persönlichkeitsrechte im Web" von klicksafe bietet fix und fertig Unterrichtsmaterial dazu an.

Und auch die Schule als Institution hat eine (sogar gesetzlich fixierte) Pflicht zum Datenschutz. Oder haben Sie schon einmal eine Schulsekretärin erlebt, die am Telefon Adressen herausgibt? So selbstverständlich sollte es für alle Schulangehörigen sein (und damit ist ausdrücklich auch der Administrator der Schulhomepage gemeint), keine persönlichen Daten ohne Einverständnis ins Netz zu stellen. Das gilt für Schülerinnen und Schüler ebenso wie für Kolleginnen und Kollegen. Und das gilt für Fotos wie für Namen oder die Preisgabe von Hobbys.

Zum Schluss ein paar praktische Tipps für Lehrerinnen und Lehrer – mit schönem Gruß von Dr. Tafels Alter Ego:

- USB-Sticks sichern! Spezielle Software verschlüsselt den Inhalt von Datenspeichern, der danach nur noch per Passwort zugänglich ist.
- Starke Passwörter wählen und regelmäßig ändern. Und! Auch wenn es manchmal unbequem ist: Nie Passwörter weitergeben.
- Löschen Sie auch auf Schulrechnern alle temporären Dateien (Browserverlauf, Cookies etc.).
- Löschen Sie Schülerdaten auf Schulrechnern und auch auf dem heimischen Rechner nicht über den Windows-Papierkorb. Benutzen Sie sichere Löschprogramme!
- Heimische Festplatten … sollten Ihr Haus nie mehr verlassen und sicher zerstört werden, auch wenn der Computer verkauft oder entsorgt wird. Sie wissen, dass Spezialisten die Daten wieder herzaubern können.
- Sie dürfen NICHT in Schüler-Handys schauen, auch wenn ein Verdacht auf Missbrauch besteht. Das darf nur die Polizei.
- Holen Sie sich das generelle Einverständnis bspw. für Fotos in der Klassenliste, dem Sitzplan oder Klassenfotos von den Schülerinnen und Schülern und von den Erziehungsberechtigten. Am besten zu Beginn des Schuljahres.

Datenschutz und Persönlichkeitsrechte im Web 2.0 –
Kontrollverluste, „Einstellungssachen“ und Entwicklungsherausforderungen

Lars Gräßer, ecmc GmbH, Projekt mekonet

Für die einen ist „Web 2.0“ eine neue Technik (Stichwort „Ajax“), für andere eine neue Haltung gegenüber Medien oder aber nichts als „bloßer Jargon“. Das ist aber fast schon eine Minderheitenperspektive, denn für den Großteil der Bevölkerung ist der Begriff „Web 2.0“ schlichtweg ein unbekannter Begriff (Gapski/Gräßer 2007).

Der Nutzung tut das aber keinen Abbruch – Web 2.0-Angebote werden immer populärer. Die Nutzung geschieht interaktiv, indem Töne, Texte und (bewegte) Bilder veröffentlicht, oder passiv, indem die nutzergenerierten Inhalte zur Unterhaltung, Information o.ä. konsumiert werden, was immer noch die Mehrheit tut. Davon ausgenommen scheinen lediglich die boomenden sozialen Online-Netzwerke. Das gilt für die aktive Nutzung des „Mitmach-Netzes“ unter Jugendlichen, und zunehmend auch für Erwachsene.

Mit Web 2.0 ergeben sich neue Vernetzungs- und Lernpotenziale, neue Möglichkeiten der medialen Identitätsentwicklung. Gleichzeitig steigt aber die Gefahr, dass persönliche Daten durch andere verändert, weitergegeben und missbraucht werden (können). Die „schöne neue Welt“ im Web 2.0 ist ambivalent und wirft hinsichtlich der Datenschutz- und Persönlichkeitsrechte ganz unterschiedliche Fragen auf, entsprechend der gewählten Perspektive – eine Herausforderung für die Medienkompetenzförderung.

Aber der Reihe nach.

Kontrollverlust

Das „Mitmach-Netz“ vereinfacht nicht nur die aktive Mediennutzung. Einmal ins Internet gestellte Daten sind weltweit abrufbar und recherchierbar, wenn sie nicht entsprechend geschützt werden. Und selbst wenn: Sie werden kopiert, gespeichert und weiter gegeben, wenn sich etwa Dritte – dann häufig illegal – ihrer bemächtigen. Zunehmend geht die Kontrolle über die eigenen Daten verloren, da immer schwerer nachvollzogen werden kann, wo was gespeichert wurde, ob eine Einwilligung vorlag oder nicht und Daten zudem nur schwer rückstandslos gelöscht werden (können). Das gilt insbesondere, wenn eine einmal gegebene Einwilligung zur Veröffentlichung wieder rückgängig gemacht werden soll.

Lars Gräßer

Kommunikationswissenschaftler (M.A.), Jg. 1969, Schule und Abitur in Bielefeld, Ausbildung als Gastronom in Köln, dann Studium der Kommunikationswissenschaft, Politologie und Philosophie an der Universität Essen Duisburg. Tätigkeiten im Eventbereich sowie in der Unternehmenskommunikation. Seit 2001 als Projektmanager bei der ecmc GmbH in verschiedenen Projekten engagiert, wie z.B. mekonet — Medienkompetenz-Netzwerk NRW. Diverse Veröffentlichungen zu Social Media und Medienkompetenzförderung.

Abseits dieser (teils illegalen) Praktiken kommt hinzu: Die steigende Onlinenutzung erhöht die Verfügbarkeit von Datenspuren im Netz. Und selbst wenn die Veröffentlichung von Inhalten, wie Audiofiles, Texten und (bewegten) Bildern jeweils auf datenschutzgerechten Webangeboten erfolgt, erlaubt das Zusammenführen personenbezogener Informationen aus unterschiedlichsten Quellen plötzlich das Erstellen von umfassenden Persönlichkeitsprofilen – Unproblematisches wird problematisch. Rückschlüsse auf Gewohnheiten und Vorlieben werden möglich, etwa auf bevorzugte Freizeitaktivitäten. Oder Online-Wunschzettel werden zum Allgemeingut, wenn sie Profile in speziellen Personensuchmaschinen ergänzen. „Sinnenfreudige“ Wunschtitel mutieren dann schnell mal zur Peinlichkeit. Haben wir diese

(legalen) Möglichkeiten schon in vollem Umfang realisiert?

„Einstellungssachen"

Ein „Gegenwicht" bieten hier die immer feiner justierbaren Einstellungsmöglichkeiten der Online-Profile in den populären Online-Communitys, auch wenn die Anbieter hier gerne mal mit verwirrenden Optionen aufwarten und plötzliche „Optimierungen" empfehlen. Immerhin konnten sich die drei reichweitenstärksten deutschen Online-Community-Betreiber zu einer Selbstverpflichtung, dem „Kodex Jugendschutz und Datenschutz in Social Communities" zusammenfinden, die zumindest das Schutzniveau für Minderjährige hebt.

Personalberatungsgesellschaften können sich die Spuren im Netz für ihre Zwecke zunutze machen, etwa bei der Bewerber(innen)auswahl. Aber wer hier besonders vorsichtig ist, besonders sparsam und vorbildlich mit seinen Daten umgeht, ist auch nicht unbedingt bevorteilt, unabhängig vom Alter: Die ergebnislose Suche nach einer Netzidentität kann für medienaffine Berufsgruppen – und das werden in Anbetracht der medialen Durchdringung unseres Alltags immer mehr – ebenfalls zum Problem werden. Wird z. B. ein Medienpädagoge in fünf Jahren noch einen Job bekommen, wenn er kein sichtbares Mitglied in mindestens einer sozialen Online-Community ist und/oder sich in einem Blog offenherzig präsentiert?

Aufschlussreich (und nicht nur eitel) ist es, einmal den eigenen Namen in eine Suchmaschine einzugeben, um nach den eigenen Spuren im Netz zu suchen. Im angelsächsischen Sprachraum kursiert hierfür der Begriff „Ego-Diving"; das „Eintauchen ins Selbst". Das leitet über zur Identitätsentwicklung im Netz.

Entwicklung als Herausforderung

Immer ist die individuelle Mediennutzung vor dem Hintergrund biografischer Entwicklungsherausforderungen zu beurteilen. Hier steht die Erwachsenenwelt – siehe die persönliche (Berufs)Perspektive – vor ganz anderen Herausforderungen als etwa Heranwachsende, die an der Entfaltung der eigenen Identität noch arbeiten, häufig durch medial vermittelte Kommunikationen. Als die Telefone noch Kabel und eine Wählscheibe hatten, war niemand überrascht, wenn in Haushalten mit heranwachsenden Haushaltsmitgliedern stundenlang die Leitungen besetzt waren. Das hat sich aber radikal geändert, seit Chatprogramme und soziale Online-Communitys diese Funktion schrittweise übernommen haben und Web 2.0-Angebote dem Internet ein ‚persönlicheres Gesicht' geben. Geändert haben sich damit aber weniger „die Jugendlichen" in ihren Bedürfnissen nach Kommunikation und Selbstentfaltung, sondern vielmehr die medialen Wege der Bedürfnisbefriedigung. Geändert haben sich zudem die Medien – also hier das Web als Kommunikationsmedium – in ihrer/seiner scheinbar grenzenlosen Speicherkapazität und Distributionskraft.

Ob aber z. B. verfügbare Schutzmöglichkeiten in der medialen Kommunikation auch genutzt werden, ist eine Frage der aktuellen Bedürfnisse – und da geht es entwicklungsbedingt auseinander. Jugendlichen muss attestiert werden, dass sie sich in ihrem Sinne durchaus konsequent in Online-Communitys verhalten, wenn sie diese zum Beziehungsaufbau und -pflege nutzen (siehe Meister/Meise 2009) und deshalb auf Schutz teils verzichten. Sind sie aber auch kompetent? Jein! Problematisch bleiben die „Schnittstellen" zur Erwachsenenwelt. Man denke nur an prekäre Fotos von Saufgelagen oder markige Gruppentiteln auf Online-Profilen oder die Problematik des Cyberbullying (unter Jugendlichen), die hier außen vor bleiben soll.

Oder ist es eine Frage der biografisch vorliegenden Lebenserfahrung, was Privatheit bedeutet? Diesen Aspekt betont etwa Danah Boyd (in einem Interview mit dem Guardian von Anfang Dez. 2009): "As adults, by and large, we think of the home as a very private space – it's private because we have control over it. The thing is, for young people it's not a private space – they have no control. They have no control over who comes in and out of their room, or who comes in and out of their house. As a result the

online world feels more private because it feels like it has more control."

Zukunftsperspektiven

Wird sich das „Schnittstellenproblem" von selbst lösen, wenn die persönlichen Spuren im Netz für jeden zur Alltäglichkeit geworden sind (und der Kontrollverlust total)? Bedarf es strengerer Gesetze, etwa einer Ausdifferenzierung des Rechts auf informationelle Selbstbestimmung, oder muss dieses stärker als Bildungsaufgabe verstanden werden? Informationelle Selbstbestimmung ist ja kein Selbstzweck, sondern Grundlage einer freien, gerechten und demokratischen Gesellschaft. Und was ist dann kompetentes Verhalten? Kann die Erwachsenenwelt hier mit schlüssigen Konzepten aufwarten? Die Formulierung von Antworten ist die „Entwicklungsaufgabe" der Medienbildung, damit Kontrollverluste steuerbar bleiben und gleichzeitig altersangemessene Formen der Medienkompetenzförderungen gefunden werden.

Links und Quellen:

Harald Gapski, Lars Gräßer (2007): Medienkompetenz im Web 2.0 ? Lebensqualität als Zielperspektive. In: Praxis Web 2.0. Potenziale für die Entwicklung von Medienkompetenz. Hrsg. v. Lars Gräßer, Monika Pohlschmidt. Schriftenreihe Medienkompetenz des Landes Nordrhein-Westfalen, Band 7, Düsseldorf / München, S. 11-34. Online verfügbar unter: http://www.ecmc.de/teedrei/Publikationen-Detail.111.0.html?&tx_ttnews[tt_news]=251&tx_ttnews[backPid]=96&cHash=919f6be2cc

Danah Boyd (9. Dez. 2009): "People looked at me like I was an alien" , online verfügbar unter: http://www.guardian.co.uk/technology/2009/dec/09/interview-microsoft-researcher-danah-boyd

„Neuer Verhaltenskodex für Betreiber von Social Communities bei der FSM", online verfügbar unter: http://www.fsm.de/de/Web_2_0

Dorothee M. Meister, Bianca Meise (2009): Sozial und medienkompetent – Jugendliche in virtuellen sozialen Netzwerken. In: Medienkompetent in Communitys. Sensibilisierungs-, Beratungs- und Lernangebote. Hrsg. v. Harald Gapski, Lars Gräßer. Schriftenreihe Medienkompetenz des Landes Nordrhein-Westfalen, Band 8, Düsseldorf / München. S. 21-32.

mekonet kompakt: Datenschutz auf einen Blick, online verfügbar unter: http://www.mekonet.de/t3/index.php?id=160&no_cache=1&tx_ttnews[tt_news]=337&tx_ttnews[backPid]=158&cHash=08aa2d816d

mekonet kompakt: Rechtsfragen in der digitalen Welt auf einen Blick, online verfügbar unter: http://www.mekonet.de/t3/index.php?id=160&no_cache=1&tx_ttnews[tt_news]=336&tx_ttnews[backPid]=158&cHash=fbeabda236

Medienkompetenz ist auch die Kompetenz im Umgang mit Daten

Dr. Arnd Haller, Leitung Rechtsabteilung, Google Germany GmbH

Das Internet ist ein weltweites Netzwerk von miteinander verbundenen Rechnern, durch das Daten ausgetauscht werden. Jeder Internetnutzer, also jeder, der Informationen oder Leistungen im Internet anbietet oder nachfragt, ist selbst Sender oder Empfänger von Daten. Dies ist zwar eine digitale Binsenweisheit, allerdings ist sie keineswegs jedem Internetnutzer allzeit gegenwärtig. Zwar ist eine fundierte Kenntnis über den Austausch von Daten keine Notwendigkeit für die Internetnutzung, aber ein generelles Verständnis hierüber ist eine Grundvoraussetzung für einen verantwortungsvollen Umgang mit Internet-Angeboten. Dies gilt gleichermaßen für Kinder, Jugendliche und Erwachsene.

Die Intention dieser klicksafe-Broschüre liegt darin, das Verständnis vom Umgang mit Daten zu intensivieren und zu einer öffentlichen Diskussion über Fragen des Datenschutzes anzuregen, vor allem bei einer Nutzung von Diensten durch Kinder und Jugendliche. Dieses Ziel ist sehr zu begrüßen.

Die Welt im digitalen Wandel

Kaum jemand bestreitet, dass sich die Medienlandschaft durch das Internet und damit die Mediennutzung fundamental geändert hat. In der pre-digitalen Zeit der "klassischen Medien" gab es eine begrenzte Zahl an Redakteuren und Journalisten, die uns über die aus ihrer Sicht relevanten Ereignisse informiert haben und damit unsere Filter für Informationen waren. Selbst im "Steinzeitalter des Internet" (also den 70er und 80er Jahren) war dies nicht anders. Erst später traten gravierende Änderungen ein: Durch die Einführung des usenet, von newsgroups und durch das massenhafte Aufkommen der elektronischen Post via E-Mail wurde es erstmals einer Vielzahl von Personen ermöglicht, Informationen nicht nur zu konsumieren, sondern diese Informationen auch zu kommentieren, sie mit anderen zu diskutieren oder selbst Informationen zu verfassen und weltweit zu veröffentlichen. Dieser Prozess der Demokratisierung von Wissen und Informationen hält bis heute an und gipfelt darin, dass im Zeitalter von Facebook und YouTube jeder Netznutzer kostenlos und ohne technische Vorkenntnisse jede Art von Inhalt produzieren und verbreiten kann — in Text, Bild oder audiovisueller Form. Auch wenn es gilt, Auswüchse zu vermeiden und Rahmen zu definieren, so stellt dies vor allem auch aus Sicht von Kindern und Jugendlichen eine großartige Entwicklung dar. Warum?

Dr. Arnd Haller

ist seit 2005 Leiter der Rechtsabteilung der Google Germany GmbH. Er ist zuständig für die rechtlichen Belange von Google in Deutschland, Österreich und der Schweiz sowie seit 2007 auch für die skandinavischen Länder. Er ist Mitglied der Geschäftsleitung von Google in Deutschland. Zu seinen Haupttätigkeitsfeldern gehören der Gewerbliche Rechtsschutz, Urheberrecht und Wettbewerbsrecht, haftungsrechtliche Fragen und Datenschutz. Herr Haller ist Jugendschutzbeauftragter der Google Germany GmbH und Vorstandsmitglied der Freiwilligen Selbstkontrolle Multimediaanbieter (FSM) und von fragFINN e.V.

Kinder und Jugendliche reden (endlich) mit!

Der heutige Entwicklungsstand des Internet ermöglicht erstmals eine breite Partizipation aller Bevölkerungsgruppen und Altersklassen. Kinder und Jugendliche haben erstmals die Möglichkeit, sich selbst — ohne den "Filter" der Erwachsenenwelt — über Themen zu informieren, die sie interessieren; ihre

Meinungen und Ansichten einer potentiell unbegrenzten Vielzahl von Personen mitzuteilen; etwas über sich zu berichten und selbst „im Mittelpunkt“ zu stehen. Während "die alte Welt der klassischen Medien" eine reine Erwachsenenwelt war, bietet das Internet gerade für Minderjährige einen Bereich großer und neu hinzugewonnener Freiheit. Diese Freiheit bietet faszinierende Möglichkeiten und Vorteile, aber die Ausübung von Freiheit will auch gelernt sein.

Wahrnehmung von Freiheit erfordert Verantwortung

Einerseits bieten E-Mails, Chats, Blogs, Social Communities usw. einen hervorragenden Raum, um die neu gewonnene Freiheit sinnvoll zu gestalten. Andererseits erschwert das Internet das Austesten von Freiheit im privaten, eng umgrenzten Bereich, da eingestellte Inhalte häufig für viele sichtbar sind. Die Möglichkeit, dass man mit seinen Informationen eine potentielle Vielzahl von Personen weltweit zur gleichen Zeit erreichen kann, erfordert daher ein erhöhtes Maß an Verantwortung und Übung, die vor allem bei Kindern in der Regel noch nicht ausgebildet ist. Es ist nicht von der Hand zu weisen, dass es heute im Netz eine Vielzahl von privaten Äußerungen und intimen Bildern von Kindern und Jugendlichen gibt, über die man als Erwachsener die Nase rümpfen oder den Kopf schütteln kann. Die Vorstellung dessen, was derlei Mitteilungen später einmal auf dem Schulhof, der Universität, im Bewerbungsgespräch auslösen mögen, verleitet einige Erwachsene zu einer — häufig überzogenen — Fundamentalkritik an neuartigen Kommunikationsformen. Man mag den einzelnen Jugendlichen für sein Verhalten kritisieren, Eltern und Lehrern vorwerfen, sie hätten ihren Erziehungsauftrag nicht wahrgenommen oder von Internetanbietern inhaltliche Prüfungen eingestellter Inhalte verlangen. Am Ende erfordert die gewonnene Freiheit eine größere Verantwortung für seine eigenen Daten und für die Daten anderer — dazu gehört ein Lernprozess von Kindern und Jugendlichen, bei dem wir sie unterstützen müssen. So engagiert sich Google z.B. mit mehreren anderen Unternehmen bei der Kindersuchmaschine www.fragfinn.de, die Kindern das Auffinden von kindgerechten Inhalten erleichtern und damit einen spielerischen Umgang mit dem Internet unterstützen will.

Was können Unternehmen wie Google beitragen?

Eine Verantwortung tragen jedoch nicht nur die Internetnutzer und Erziehungsberechtigten selbst, sondern auch die Online-Unternehmen — insbesondere auch für den Datenschutz. Google ist sich dieser Verantwortung sehr bewusst. Hierzu gehört zunächst die Gewährleistung eines Höchstmaßes an Datensicherheit gegen Verlust, Diebstahl etc. Es geht aber auch darum, Internetnutzer dabei zu unterstützen, die Kontrolle über ihre eigenen Daten zu behalten. Dies betrifft Kinder und Jugendliche gleichermaßen wie Erwachsene. Notwendig ist etwa eine ausführliche und möglichst auch Kindern verständliche Information darüber, welche Daten von einem Unternehmen gespeichert sind und eine Erläuterung, wie damit verfahren wird. Unternehmen können dem Nutzer selbst Kontrolle über seine Daten geben und ihm ermöglichen, Daten zu löschen oder gar nicht erst erheben zu lassen. Und schließlich können sie einen Beitrag zur Entwicklung eines kompetenten Umgangs mit Daten leisten.

Google hat hier gerade im letzten Jahr entscheidende Beiträge geleistet, von denen ich nur einige wenige nennen möchte:

- Verständliche Informationen und hohe Transparenz
  Nur derjenige, der darüber informiert ist, über welche Daten ein Unternehmen verfügt und was mit den Daten passiert, kann bewusste Entscheidungen treffen. Google hat in seinem Datenschutz-Center (www.google.de/privacy) eine Vielzahl von Informationen zusammengestellt, die den Nutzer genau darüber aufklären, welche Daten Google erhebt und wie damit verfahren wird. So wird dem Nutzer mit dem "Google Dashboard" in einer branchenweit einzigartigen Initiative die volle Transparenz

über die bei Google hinterlegten Daten verschiedener Produkte angezeigt. Alle Dienste, bei denen eine Anmeldung über ein Google-Konto erforderlich ist, werden so für den einzelnen Nutzer auf einer einzigen Webseite übersichtlich angezeigt — und können darüber in Bezug auf ihre Datenschutzeinstellungen eingesehen und geändert werden (www.google.com/dashboard). Ich kann wirklich nur empfehlen: Ausprobieren!

- Wahlmöglichkeiten zum Schutz von Daten und für den einfachen Datenexport
  Google stellt eine Vielzahl von Instrumenten zur Verfügung, die es dem Nutzer selbst ermöglichen, darüber zu entscheiden, ob Google Daten speichert oder nicht. So lassen sich etwa Konversationen über Google Talk als „vertraulich" einstellen, so dass die ausgetauschten Texte nicht gespeichert werden; in Chrome, dem Browser von Google, lässt sich „inkognito" surfen. Google hat es sich ferner zur Aufgabe gemacht, den Wechsel von Google Produkten zu anderen Anbietern zu erleichtern — und gleichzeitig die eigenen Daten auf komfortable und einfache Weise mitnehmen zu können (was leider nicht die Regel ist). So lassen sich Daten von Google problemlos in andere Dienste exportieren, etwa gehostete Daten von Bloggern in einen anderen Blogdienst übertragen oder Kontakte und Bookmarks in andere Adressbücher mitnehmen (www.dataliberation.org).

Medienkompetenz ist eine gemeinsame Aufgabe

Datenschutz ist auch für Kinder und Jugendliche ein wichtiges Thema. Die Herausforderung des Jugendschutzes besteht allerdings weniger im Bereich des Schutzes von Daten, denn der sollte sich für alle Nutzer auf einem gleich hohen Niveau bewegen. Der graduelle Unterschied zwischen Minderjährigen und Erwachsenen besteht im Bereich des Datenschutzes eher in der Wahrnehmung und der verantwortungsvollen Ausübung des informationellen Selbstbestimmungsrechts. Hier müssen wir alle an einem Strang ziehen, um erfolgreich zu sein: Weder der Staat noch private Unternehmen werden die gewaltige Aufgabe allein lösen können, um aus den „digital natives" Internetnutzer heranwachsen zu lassen, die verantwortungsvoll mit den eigenen und fremden Daten umgehen. Eltern und Lehrern kommt hier eine wichtige Rolle zu. Institutionen wie klicksafe, aber auch Initiativen aus der Privatwirtschaft, allen voran die Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, können bei diesen Aufgaben unterstützen.

Wir bei Google freuen uns darauf, auch in den kommenden Jahren unseren Teil zu einer Verbesserung eines effektiven Schutzes von Kindern und Jugendlichen zu leisten. In diesem Sinne: Surf safe!

Datenschutz und Persönlichkeitsrechte im Web 2.0 –
Schutz vor falschen Freunden

Michael Hange, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Cyber-Kriminelle nehmen zunehmend auch soziale Netzwerke ins Visier. Mit gestohlenen Daten können sie dort Betrugsdelikte begehen und haben eine regelrechte Schattenwirtschaft für elektronische Identitäten geschaffen. Nutzer sind daher verstärkt aufgefordert, ihre Daten zu schützen – zum eigenen Nutzen und im Interesse der Internet-Community.

Heute ist das World Wide Web für viele Menschen ein Raum, in dem ganz selbstverständlich persönliche Kontakte geknüpft und Freundschaften gepflegt werden. Soziale Netzwerke bilden dafür eine beliebte Plattform, auf der die Nutzer oft sehr private Informationen veröffentlichen. Vor allem junge Menschen nutzen diese Angebote in großer Zahl: Die größten sozialen Netzwerke haben mehrere hundert Millionen Mitglieder, Tendenz weiterhin steigend.

Doch wie im „echten Leben" sollten Nutzer auch im Web 2.0 ein gesundes Misstrauen an den Tag legen. Die bedenkenlose Preisgabe von Daten macht es Cyberkriminellen einfach, in sozialen Netzwerken potenzielle Opfer auszuspionieren und gezielt anzugreifen. Durch Phishing mithilfe gefälschter E-Mails verschaffen sich die Täter beispielsweise Zugang zu einem Nutzerprofil und können danach unter falschem Namen andere Nutzer täuschen. So nutzen sie das gegenseitige Vertrauen, das in den sozialen Netzwerken herrscht, für betrügerische Zwecke aus.

Soziale Netzwerke sind attraktiv für Online-Kriminelle

Da die Profile in sozialen Netzwerken oft detaillierte Angaben zu persönlichen Interessen enthalten, sind sie auch für den gezielten Versand von Werbung attraktiv. Gefährdungspotential geht zudem von den Kontaktlisten der Nutzer von sozialen Netzwerken aus, die oft hunderte Adressen umfassen, an die Kriminelle Schadsoftware verschicken können – so verbreitete sich zum Beispiel der Wurm „Koobface" 2009 dramatisch in Facebook und MySpace. Vor diesem Hintergrund hat sich der Handel mit gestohlenen Identitäten und persönlichen Informationen inzwischen zu einem Millionengeschäft für IT-Kriminelle entwickelt, die die Daten auf Online-Plattformen handeln. So wurde der „Identitätsdiebstahl" zu einer der am schnellsten wachsenden Bedrohungen im Internet, wie der Lagebericht zur IT-Sicherheit 2009 des Bundesamts für Sicherheit in der Informationstechnik zeigt.

Michael Hange
Diplom-Mathematiker, ist seit 1977 in der Bundesverwaltung auf dem Gebiet der IT-Sicherheit tätig. Von 1994 bis Anfang 2009 war er Vizepräsident des BSI, bis Oktober 2009 ständiger Vertreter des IT-Direktors im BMI. Seit dem 16. Oktober 2009 ist Michael Hange Präsident des Bundesamtes für Sicherheit in der Informationstechnik.

Der Bedarf an unabhängiger Aufklärung ist groß

Wir verstehen es vor diesem Hintergrund als wichtigen Auftrag, dem Thema Web 2.0 künftig eine bedeutende Rolle bei der Aufklärung und Sensibilisierung der IT-Nutzer einzuräumen. Denn in der Öffentlichkeit stellen wir einen zunehmenden Bedarf an Informationen über Gefährdungen und Schutzmöglichkeiten von kompetenter und unabhängiger Stelle fest. Bereits heute leistet das BSI beispielsweise durch die Beratung von Behörden, Bürgern und Unternehmen und mit Dienstleistungen wie dem Bürger-CERT und der Webseite www.bsi-fuer-buerger.de einen Beitrag. Mit dem geplanten

Ausbau des BSI als zentrale Cyber-Sicherheitsbehörde wird unser Engagement im Bereich Aufklärung und Sensibilisierung in Zukunft noch zunehmen – auch in Kooperation mit Partnern und Initiativen. Ziel ist es, die IT-Sicherheit kontinuierlich zu erhöhen und so den Schutz sensibler Daten – ob privater oder geschäftlicher Natur – zu gewährleisten.

Neben dem sensiblen Umgang mit den eigenen Daten bedarf es dabei auch ganz handfester technischer Schutzmaßnahmen. Die Bedrohungsszenarien der Informationstechnik haben sich in den letzten Jahren erheblich verändert und entwickeln sich zunehmend aggressiver mit technisch ausgefeilter Finesse und krimineller Energie. IT-Sicherheit ist in dieser Hinsicht Grundvoraussetzung für Datensicherheit.

Für den Bürger heißt das: Grundlegenden Schutz bietet eine aktuelle Schutzsoftware mit Virenscanner und Firewall. Aber auch hier ist mittlerweile Vorsicht geboten: Kriminelle bieten online gefälschte Virenscanner, so genannte Scareware an, die nicht nur wirkungslos sind, sondern einen Computer ganz im Gegenteil sogar mit Schadsoftware infizieren können. Neben einem aktuellen Antivirenschutz bleibt es auch in sozialen Netzwerken unverzichtbar, ein sicheres Passwort zu wählen – Geburtstagsdaten haben dort nichts zu suchen. Zum Schutz vor Schadsoftware sollten Internetnutzer darüber hinaus niemals auf Links klicken, die in E-Mails von unbekannten Absendern angeboten werden. Bei dubiosen E-Mails von Freunden, in denen man zum Beispiel um Geld gebeten wird, sollte man nachfragen – vielleicht verbirgt sich dahinter eine falsche Identität.

Schutz des Einzelnen bedeutet auch Schutz der Gemeinschaft

Diese individuellen Sicherheitsmaßnahmen schützen nicht nur den einzelnen Nutzer – von ihnen profitieren alle Bürger im Internet. Denn jeder schlecht geschützte Computer ist ein potenzielles Einfallstor für die Täter, die aus gekaperten PCs riesige „Botnetze“ mit zum Teil mehreren tausend PCs bilden. Deren große Rechenkapazität dient dann zum massenhaften Versand von Spam-Mails oder für Angriffe auf Webseiten („Distributed Denial-of-Service-Attacken“). Hier kann jeder IT-Nutzer durch Aufmerksamkeit und grundlegende Sicherheitsvorkehrungen dazu beitragen, den Tätern ihr Geschäft so schwer wie möglich zu machen. Dann bleibt das Internet auch in Zukunft ein gerne besuchter Raum für geschäftliche und private Aktivitäten.

Datenschutz 2.0 –
Voraussetzungen für eine kinder- und jugendgerechte Informationsgesellschaft

Kai Hanke, Referent für Medien, Deutsches Kinderhilfswerk e.V.

„Datenschutz kann […] nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss."[1]

Das Internet und die Nutzung von Web 2.0-Angeboten sind heute nicht nur für Kinder und Jugendliche selbstverständlich. Wir alle nutzen das Internet und sind aufgrund der zunehmenden kommunikations- und informationstechnischen Durchdringung unserer Gesellschaft in unserem Alltag in ein komplexes Geflecht digitaler Daten eingebunden. Und wir alle hinterlassen dort auch Spuren, geben mehr oder weniger bewusst personenbezogene Daten von uns oder anderen Preis. Dies ist die Ausgangslage.

Will man sich an der Diskussion um Datenschutz und Persönlichkeitsrechte beteiligen, ergeben sich zwei maßgebliche Problemdimensionen: Einerseits ist Datenschutz eine Frage der Regulierung von Datensicherheit und -verwaltung in technischen Systemen. Andererseits ist Datenschutz und die Wahrung von Persönlichkeitsrechten eine sozialkulturelle Frage, eine Frage des Verhaltens verschiedener gesellschaftlicher Akteure, die entweder Daten sammeln, verwalten, weitergeben oder von sich preisgeben.

Das Deutsche Kinderhilfswerk nähert sich diesen Fragen als Interessenvertreter von Kindern und Jugendlichen vor allem unter Berücksichtigung ihrer eigenen Interessen und Bedürfnisse. Aus dieser Perspektive heraus ist es zunächst nötig zu klären, wie und warum Kinder und Jugendliche das Internet nutzen und welche Haltung sie zum Schutz persönlicher Daten haben. Erst daraus lassen sich sinnvoll Forderungen ableiten, mit denen Datenschutz im Interesse von Kindern und Jugendlichen diskutiert und letztlich verbessert werden kann.

Kai Hanke
Geboren 1978, Studium der Kommunikations- und Medienwissenschaft, Psychologie und Erziehungswissenschaft an der Universität Leipzig und der Binghamton University, New York. Seit Februar 2009 Referent für Medien im Deutschen Kinderhilfswerk e.V. (Berlin).

Medienhandeln von Kindern und Jugendlichen – kein Bewusstsein für Datenschutz?

Kinder und Jugendliche nutzen das Internet heute wie selbstverständlich. Dabei surfen Kinder zwar noch nicht im selben Maße wie ihre jugendlichen Zeitgenossen. Aber wie aktuelle Studien zeigen, nimmt auch die kindliche Internetnutzung stetig zu[2]. Kinder neigen dazu, das Netz explorativ und spielerisch zu nutzen. Damit verbunden ist oftmals, dass sie bestimmte Risiken nicht als Konsequenzen ihres Medienhandelns absehen können. Besonders schwer werden Risiken von ihnen meist dann wahrgenommen, wenn Konsequenzen nicht direkt erfahrbar sind, sondern erst mittelbar oder zeitverzögert drohen. Gerade im Bereich des Datenschutzes mangelt es auch Kindern an einem Risikobewusstsein.

Während Kinder aber oftmals noch in Begleitung von Eltern surfen, nutzen Jugendliche das Netz schon weitgehend selbstständig und jenseits pädagogischer Kontrolle. Ihr Medienverhalten zeichnet sich dabei zwar durch technische bzw. Handhabungskompetenzen aus. Ihre Fähigkeit bzw. Motivation, das eigene Medienhandeln und Medieninhalte kritisch zu hinterfragen, ist hingegen oftmals weniger stark ausgeprägt. Bezüglich der Internetnutzung machen bei

Jugendlichen besonders kommunikative Onlineaktivitäten einen Großteil des Medienverhaltens aus. Denn der Austausch und Abgleich mit Gleichaltrigen, der schon immer ein wichtiger Teil jugendlicher Identitätsarbeit war, spielt sich heute in vielfältiger Weise online ab: In Chatrooms und über Instant Messaging Programme, per E-Mail und vor allem in Sozialen Online-Netzwerken. Dort werden eigene Profile gepflegt und kreativ ausgestaltet, Informationen über sich selbst (und andere) als inszenierte Selbstdarstellungen preisgegeben. Diese Formen der Selbstdarstellungen vollziehen sich zum Teil ohne ein Bewusstsein dafür, wem die preisgegebenen Informationen wirklich zugänglich sind und welche Risiken sich damit verbinden, entsprechende Daten ggf. sogar Unbekannten zur Verfügung zu stellen[3].

Diese Unbekümmertheit im Umgang mit eigenen und fremden Daten ist keine neue Eigenschaft heutiger Kinder und Jugendlicher. Allerdings ist mit dem Internet als neuem Medium für jugendliche Identitätsarbeit eines nicht mehr selbstverständlich: Fehlverhalten oder Dinge, die einem später vielleicht peinlich sein könnten, gerieten mit der Zeit in Vergessenheit. Heute ist das etwas anders. Kaum eine Information, die einmal digital und anderen zugänglich gespeichert war, kann einfach so vergessen gemacht werden. Das Internet vergisst nichts so leicht! Die vielfältigen Formen des Datenmissbrauchs, die dadurch möglich werden, sind bekannt und sollen hier nicht erneut und in Gänze aufgezählt werden. Als Beispiel sei nur an die letzten Fälle von Datenphishing in Sozialen Netzwerken oder an Internetkriminalität im Zusammenhang mit Onlinbanking oder Kreditkartenbetrug erinnert. Trotzdem spielt dieses theoretische Risikobewusstsein bei vielen Internetnutzern kaum eine Rolle in der Nutzungspraxis. Jugendlichen beispielsweise ist die Gefahr, Opfer von Cyberbullying und einer massiven Verletzung ihrer Persönlichkeitsrechte zu werden, fast noch die gegenwärtigste und relevanteste Bedrohung. Für die Gefahren, die mit anderen Formen des Datenmissbrauchs verbunden sind, sind sie wenig sensibel.

Doch auch in Anbetracht dieser Umstände und Risiken ist es nicht sinnvoll, Kindheit und Jugend heute – einem allzu kulturpessimistischen und generalisierenden Impuls folgend – als bedroht anzusehen. Vielmehr ist es wichtig, die Potenziale der medial vernetzten Informationsgesellschaft für die Identitätsarbeit von Kindern und Jugendlichen sowie für ihre gesellschaftliche Partizipation nutzbar zu halten und gleichzeitig dafür zu sorgen, dass alle Akteure innerhalb dieser Gesellschaft einen verantwortungsvollen Umgang mit den neuen medialen Gegebenheiten entwickeln. Dies gilt es, pädagogisch und durch gesellschaftliche (und gesetzliche) Rahmenbedingungen aufzugreifen. Darauf aufbauend müssen wir Kindern wie Jugendlichen die Unterstützung zukommen zu lassen, die sie in diesen neuen Lebenswelten für eine erfolgreiche Identitätsarbeit benötigen.

Handlungsbedarf und Verantwortlichkeiten

Unter der Maßgabe des Vorrangs des Kinderwohls, die das Deutsche Kinderhilfswerk heute mehr als je zuvor für notwendig und möglich hält, lassen sich verschiedene Forderungen aufstellen, die den Datenschutz in all seinen Facetten betreffen und die – jeweils mit verschiedenen Verantwortungsträgern – eine Optimierung des Datenschutzes und der Datenschutzkultur zum Ziel haben.

Es muss insgesamt zu einer Bewusstseinsänderung sowie zu einer Anpassung der Praxis bei der Erhebung und Speicherung von Daten kommen. Dies gilt nicht nur, aber insbesondere für kommerzielle Anbieter. Sofern diese Anpassungen nicht auf anderen Wegen durchsetzbar sind, wären hier auch Veränderungen der gesetzlichen Rahmenbedingungen nötig:

1. Dabei sollte viel weitgehender ein sensibler Umgang mit der Erhebung personenbezogener Daten und die Sicherung dieser Daten vor Zugriffen Dritter gewährleistet werden. Vor allem Angebote für Kinder und Jugendliche sollten die Erhebung persönlicher Daten auf das für die jeweilige Dienstleistung notwendige Mindestmaß beschränken.

2. In diesem Kontext sind auch Prinzipien informationeller Selbstbestimmung wieder stärker in den Blick *aller* Anbieter zu rücken. Ziel muss es sein, Kunden und Nutzern eine möglichst einfache und

komplette Löschung persönlicher Daten zu ermöglichen, wenn sie dies wünschen. Dies würde es beispielsweise Jugendlichen in Online Netzwerken ermöglichen, persönliche Daten zu löschen, die sie nicht (mehr) online preisgeben wollen.

3. Anbieter von Internetangeboten oder sonstiger Dienste, die von Kindern und Jugendlichen genutzt werden, müssten stärker dazu beitragen, Hinweise zum Datenschutz verständlich zu machen. Dies könnte beispielsweise bedeuten, AGBs oder Datenschutzerklärungen neben den juristisch verbindlichen Textversionen in leicht verständlichen Versionen anzubieten. Erst dies würde die nötige Transparenz schaffen, die viele Nutzer benötigen, um die Konsequenzen von Datenweitergabe angemessen einschätzen zu können.

In diesem Kontext wäre auch ein – beispielsweise vom Bundesbeauftragten für Datenschutz und Informationsfreiheit gefordertes – Datenschutz-Gütesiegel hilfreich, das Usern allgemein und insbesondere Kindern und Jugendlichen eine Orientierung bieten würde, welche Anbieter verantwortungsvoll mit persönlichen Daten ihrer Nutzer umgehen.

Allerdings kann Datenschutz nicht einfach nur eine Aufgabe von Anbietern sein. Für den kompetenten Umgang mit Medien müssen auch Nutzer heute ein Bewusstsein für den Schutz eigener und fremder Daten entwickeln. In diesem Sinne gilt es, Kinder und Jugendliche bei der Entwicklung spezifischer Medienkompetenzen beispielsweise im Web 2.0-Bereich gezielt zu unterstützen. Dies erfordert eine nachhaltige, medienpädagogisch fundierte Förderungsstruktur. Zudem ist es dringend notwendig eine kinder- und jugendgerechte Landschaft mit sicheren Internetangeboten für Kinder bereitstellen zu können, die auch Usern mit geringeren Kompetenzen erste Surf- und Lernerfahrungen in sicheren Online-Umgebungen ermöglicht. Das Deutsche Kinderhilfswerk beispielsweise erarbeitet derzeit in Bezug auf ebendieses Ziel ein pädagogisch betreutes Online-Video-Portal, auf dem Kinder den verantwortungsvollen Umgang mit Web 2.0-Angeboten spielerisch erlernen können.

Schlussbemerkung

Bei der Diskussion um die Optimierung von Datenschutz und der Wahrung von Persönlichkeitsrechten geht es um zwei Handlungsbereiche. In Bezug auf gesellschaftliche Akteure, die persönliche Daten sammeln, stellt sich das Ziel, dass Daten nicht unnötigerweise gesammelt werden dürfen und ggf. gesammelte Daten sicher vor dem Zugriff Dritter verwaltet werden. Solange beides nicht gewährleistet ist, ist Datenschutz als defizitär zu bezeichnen. Zum anderen muss eine Optimierung aber auch auf diejenigen abzielen, die Daten von sich preisgeben. Hier sind Maßnahmen zur Bewusstmachung der Risiken und Konsequenzen bei der Preisgabe sowohl eigener als auch fremder persönlicher Daten sowie bei einem Verlust der Kontrolle über eigene Daten nötig. Nur so können insbesondere Kinder und Jugendliche einen bewussten Umgang mit Medien im Allgemeinen und speziell dem Internet kultivieren und sich auch in der heutigen Informationsgesellschaft ein Leben – nicht nur informationeller – Selbstbestimmung aufbauen. Insgesamt ist dabei – auch für Erwachsene – das Verständnis einer neuen Kultur digitaler Öffentlichkeit notwendig. Nutzer müssen sich heute bewusst machen, welche Daten und Informationen an welcher Stelle wirklich privat sind, wo sie nur beschränkt öffentlich sind und schließlich, wo sie allgemein zugänglich sind.

Bei allen möglichen Risiken sollten wir jedoch die Chancen und Potenziale der Internetkommunikation nicht aus den Augen verlieren. Es ist die Aufgabe einer Gesellschaft, Kindern und Jugendlichen durch eine sinnvolle Verzahnung von Datenschutz, Jugendmedienschutz und zuvorderst der Förderung von Medienkompetenz diese Potenziale nutzbar zu machen. Denn Kinder und Jugendliche haben ein Recht darauf, sich auch mittels des Internet ihnen verständliche und angemessene Informationen zu beschaffen, sich entsprechende Unterhaltungsangebote zu erschließen und natürlich auch, sich aktiv und kreativ an gesellschaftlichen Debatten und Entscheidungen zu beteiligen. Dafür ist ein sicheres und zielgruppenadäquates Internet eine zentrale Voraussetzung.

[1] Quelle: Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Aktueller Handlungsbedarf beim Datenschutz - Förderung der Datenschutzkultur (http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/78DSK_AktuellerHandlungsbedarf.html?nn=409240, Zugriff: 14.01.2010)

[2] vgl. hierzu z.B.: Medienpädagogischer Forschungsverbund Südwest, KIM-Studie 2008. Kinder und Medien, Computer und Internet. Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger. Stuttgart, S. 38

[3] vgl. hierzu: Medienpädagogischer Forschungsverbund Südwest, JIM-Studie 2009. Jugend, Information, (Multi-)Media. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger. Stuttgart, S. 47

StudiVZ, Yasni & Co. –
Plädoyer für eine Neuordnung des Datenschutzrechts

Prof. Dr. Thomas Hoeren, Westfälische Wilhelms-Universität Münster

Vor kurzem machte ich in der Vorlesung BGB-AT einen ungewöhnlichen Test. Ich war erschrocken über die unglaubliche Offenheit meiner Studierenden, was deren StudiVZ-Profil angeht. Hobbys, Saufgewohnheiten, Partyfotos – ich war beim Surfen wie vor den Kopf gestoßen. Also loggte ich mich unter falschem Namen in StudiVZ ein (ich weiß, ein AGB-Verstoß) und sammelte alle dort befindlichen Daten einer meiner Studentinnen, die ich mir zuvor wegen eines Fotos mit Bierflasche am Hals ausgesucht hatte. Ich glich diese Daten mit weiteren Daten aus Yasni, 123people und anderen Personensuchmaschinen ab und erstellte einen Steckbrief mit Foto, den ich in 500er Kopie in der Vorlesung verteilte. Überschrift: „Würden Sie dieser Studentin einen Job geben?“ Der Schock saß – die „Studis“ gingen massiv dazu über, ihre Datenschutzeinstellungen bei StudiVZ zu überdenken.

Datenschutz ist wichtiger denn je. Ging es früher „nur“ um den Schutz des Bürgers gegen einen übermächtigen Staat und dessen Datensammelwut und später um eine Absicherung von Kunden gegen das Data Mining von Unternehmen, geht es nunmehr um eine globale Frage: Wie kann man den Betroffenen in einer Welt schützen, in der jedes Datum von Jedermann auf der Welt einsehbar, nutzbar und missbrauchbar ist? In einer solchen Informationsgesellschaft hat sich der Datenschutz vom Persönlichkeitsrecht hin zu einem allgemeinen Recht der medialen und informationellen Selbstbestimmung entwickelt. Gleichzeitig müssen die Datenschutz-Veteranen sehen, dass User selbst komplette Persönlichkeitsprofile ins Netz stellen – ohne mit der datenschutzrechtlichen Wimper zu zucken: „Ich habe doch nichts zu verbergen, wieso sollte ich dann nicht von mir im Netz erzählen? Ich will doch neue Freunde – dann muss ich von mir auch etwas preisgeben.“ So denken viele, gerade junge Menschen. Wie soll der Staat hier reagieren? Kann, darf und soll er den Bürger vor sich selbst schützen? Und wie schützt man den Bürger, wenn sich das Web sich immer an alles erinnert? Der im Web allgegenwärtige Trash-Datenpool führt zu persönlichkeitsrechtlichen Verwerfungen und konterkariert auch das Vertrauen in Internet-Informationen selbst.

Prof. Dr. Thomas Hoeren
ist Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster und Richter am Oberlandesgericht Düsseldorf.

Meines Erachtens bedarf es hierzu einer Grundsatzdiskussion, die alle bisherigen Dogmen des Datenschutzes auf den Prüfstand stellt. Die Orientierung des Datenschutzrechts an der Einwilligung des Betroffenen ist dabei ebenso fragwürdig wie die allgemeinen Ermächtigungsgrundlagen des Datenschutzrechts im Hinblick auf berechtigte Interessen der verarbeitenden Stelle. Die kaum verständliche Regelungsstruktur des BDSG etwa zum Direktmarketing (§ 28 Abs. 3) ist dabei ebenso zu hinterfragen wie die unrealistischen Wertungen hinter den Scoringregeln des § 28 b BDSG. Auch sollte sich der Datenschutz von der engen Bindung an Persönlichkeitsrechte frei machen und zu einem allgemeinen Informationsverwendungsrecht fortentwickelt werden. Es geht um die Frage eines allgemeinen Datenrechts und der Frage, wer „Eigentümer“ an Daten ist. Dahinter steckt die allgemeine Frage eines Leitbildes der Informationsgerechtigkeit, die bislang kaum Gegenstand von rechtswissenschaftlicher und informationswissenschaftlicher Forschung gewesen ist. Wie kann man gerecht Herrschaftsrechte an Infor-

mationen zuweisen, ohne die Belange der Allgemeinheit und der Betroffenen außer Acht zu lassen?

Kompliziert wird die Lage dadurch, dass wir uns hier in einer globalen Fragestellung bewegen, die wir nicht nur nationalstaatlich im Schnellgang lösen können. Hier ist Geduld erforderlich und selbstkritischer Dialog mit fremden Kulturen und deren Wertungen. Ein solcher Diskurs kann nur bei Beachtung der Gebote der Verfahrensgerechtigkeit gelingen. An einer Diskussion über die Konturen des Informationsrechts müssen alle Betroffenen fair und gleichrangig beteiligt werden. Insofern ist viel wichtiger als das materielle Datenschutzrecht mehr ein transparentes Entscheidungsverfahren in der Politik, das allen Interessenverbänden und Betroffenen gleiche Chancen auf Gehör gewährleistet.

Internet in Kinderhand erfordert Medienkompetenz

Fritz-Uwe Hofmann,
Deutsche Telekom AG

Das Internet und neue Medien sind als wichtige Kommunikationsinstrumente und Unterhaltungsmedien aus dem Alltag von Kindern und Jugendlichen nicht mehr wegzudenken. Rund 70 Prozent der Kinder nutzen einen Computer zu Hause und sogar die Hälfte der Kinder nutzt das Internet regelmäßig. Bereits heute haben Internetanwendungen die klassischen elektronischen Medien als primäre Informationsquelle bei Jugendlichen abgelöst. Doch welcher gesellschaftliche Handlungsbedarf ergibt sich hieraus?

Gerade Web 2.0-Angebote und Social Communities üben einen sehr großen Reiz für Kinder und Jugendliche aus. Die Möglichkeiten, z.B. selbstgemachte Fotos und Videos mit Freunden zu teilen, sind für Kinder sehr verlockend. Gleichwohl gehen mit sozialer Vernetzung über das Internet auch Risiken einher. In der Vergangenheit wurde immer wieder über unterschiedliche Phänomene diskutiert: Wie geht man mit sog. Gewaltvideos um, die körperliche Übergriffe auf Kinder dokumentieren, oder wie kann man verhindern, dass Kinder zu viel über sich oder Andere preisgeben? Immer wieder kam die Forderung auf, dass die Wirtschaft hier handeln muss. Doch sind die Eingriffsmöglichkeiten für die Wirtschaft nicht immer gegeben - letztlich entscheidet der Nutzer selbst, wie er mit den unterschiedlichen Inhalten umgeht und diese verantwortungsbewusst nutzt. Dies wiederum setzt aber eine hohe Kompetenz im Umgang mit den neuen Medien voraus.

Internet in Kinderhand – erfordert eine Stärkung der Medienkompetenz

Für die Deutsche Telekom ist der Schutz von Kindern und Jugendlichen ein wichtiger Beitrag bei der Nutzung neuer Medien durch Kinder. Gerade deshalb bietet die Deutsche Telekom unterschiedliche Lösungen an, die Kinder vor nicht altersgerechten Inhalten schützen können.

Fritz-Uwe Hofmann *leitet seit 2007 den Bereich Politische Interessenvertretung Deutschland der Deutschen Telekom AG. Damit verantwortet er u.a. zahlreiche Aktivitäten der Deutschen Telekom im Bereich des Jugendschutzes sowie der Medienkompetenz-Förderung. Fritz-Uwe Hofmann ist Mitglied des Kuratoriums der Initiative „Ein Netz für Kinder" und Mitglied des Vorstands des Vereins FragFinn e.V.*

Der wichtigste Hebel für den individuellen Schutz von Kindern ist die Stärkung der Kompetenz von Kindern und Jugendlichen für einen kritischen Umgang mit neuen Medien. Die Deutsche Telekom engagiert sich deshalb in unterschiedlichen Initiativen, die Kindern und Jugendlichen Tipps und Tricks für einen kritischen und verantwortungsvollen Umgang mit neuen Medien an die Hand geben. Durch die aktive Mitarbeit in dem unter der Schirmherrschaft des Bundesinnenministeriums stehenden Vereins „Deutschland sicher im Netz" oder durch die Kooperation mit der Polizeilichen Kriminalprävention von Bund und Ländern sowie einer Kooperation mit dem Informationszentrum für den Mobilfunk, wollen wir Kinder und Jugendliche für das „Erlebnis Internet" und den Umgang mit den neuen Medien fit machen.

Einzelpersonen, Initiativen und die Wirtschaft selbst sind hier in den letzten Jahren sehr aktiv geworden. Primäre Aufgabe muss es nun sein, Kinder und Jugendliche auch in der Schule für Fragen des adäquaten Umgangs mit den eigenen Daten zu sensibilisieren. Nur so können Kinder und Jugendliche den

entsprechenden Umgang mit solchen Daten im Alltag erlernen.

Die Deutsche Telekom begrüßt die vielfältigen Initiativen von Schulen und Lehrern, die diese Fragen im Unterricht gemeinsam mit den Schülern aufarbeiten. Gleichwohl müssen diese Aktivitäten auf eine breitere Basis gestellt werden, z.B. durch eine Integration der Medienkompetenz-Förderung in die Rahmenlehrpläne der Schulen.

Eine stärkere Integration dieser Inhalte in den Schulunterricht wird zwangsläufig auch dazu führen, dass die zahlreichen Angebote, die von regionalen Lehrerfortbildungseinrichtungen angeboten werden, noch stärker nachgefragt werden. Denn eine wichtige Voraussetzung für die Vermittlung von Medienkompetenz in der Schule ist auch die Integration neuer Medien in die Aus- und Weiterbildung der Lehrkräfte. Schon heute gibt es eine Fülle von fundierten Materialien, die Lehrer bei der Ausgestaltung von Unterrichtseinheiten unterstützen. Nicht zuletzt das Handbuch von klicksafe sowie die Initiative Teachtoday.eu geben den Lehrern praktische Hilfsmittel an die Hand.

Attraktive Kinderangebote bereitstellen

Eine weitere wichtige Voraussetzung für eine hohe Akzeptanz und eine sichere Nutzung neuer Medien durch Kinder und Jugendliche ist die Schaffung eines attraktiven und altersgerechten Angebots für Kinder. Dieses Angebot muss gleichzeitig dem hohen Schutzniveau der persönlichen Daten insbesondere von Kindern Rechnung tragen.

Sowohl im gesellschaftlichen Umfeld (z.B. Blinde-Kuh, Seitenstark-, fragFINN-Angebote) als auch im kommerziellen Bereich entstehen hochwertige und anspruchsvolle Angebote für Kinder und Jugendliche. Auch die Deutsche Telekom bietet mit einem eigenen Kids-Portal (http://kids.t-online.de) hochwertige Inhalteangebote für Kinder und Jugendliche an und arbeitet dabei mit unterschiedlichen Partnern aus dem gesellschaftlichen Raum zusammen.

Einen weiteren Schub erhält die Kinder-Internet-Landschaft durch die gemeinsam von Politik und Wirtschaft initiierte und getragene Initiative „Ein Netz für Kinder". Diese Initiative hat zum Ziel, kindgerechte Angebote im Internet zu fördern und einen sicheren Surfraum für Kinder unter dem Namen „fragFINN" zu schaffen. Getragen wird diese Initiative von der Bundesregierung, den Ländern sowie Unternehmen und Verbänden aus der Medien- und Telekommunikationsbranche. Auch die Deutsche Telekom unterstützt die Initiative „Ein Netz für Kinder" und ist Gründungsmitglied des fragFINN e.V.

Nur mit gemeinsamen Aktivitäten kann es gelingen, Kinder und Jugendliche nachhaltig für einen sensiblen Umgang mit den eigenen persönlichen Daten im Internet zu sensibilisieren. Die Deutsche Telekom setzt hierzu auch weiterhin auf die intensive Zusammenarbeit mit unterschiedlichen Akteuren. klicksafe ist in diesem Zusammenhang ein sehr wichtiger Partner für uns.

Datenschutz 2.0 –
Eine Herausforderung nicht nur für User

Katja Knierim, jugendschutz.net

Im Netz zu Hause: Willkommen in der jugendlichen Medienwelt

Die modernen Medien sind heute selbstverständlicher Bestandteil jugendlichen Alltags: Das Handy ist ständiger Begleiter, Youtube ersetzt das Fernsehen, statt mit Freunden zu telefonieren wird via Instant Messenger gechattet. Kommunikation ist das wichtigste Nutzungsinteresse. Deshalb stellt das Web 2.0 mit seinen vielfältigen Kontakt- und Mitmachmöglichkeiten inzwischen die „virtuelle Heimat" vieler Jugendlicher dar.

Die Internet-Nutzung wird immer vielfältiger: auch Handys haben Zugang, Spielkonsolen bieten Zugriff, unterschiedliche Angebotstypen vernetzen und vermischen sich. Social Communities besitzen eigene Channel auf Videoplattformen, Handyclips werden im Netz präsentiert, Mobilfunkbetreiber stellen „Community-Flatrates" zur Verfügung. Der Jugend- und Datenschutz wird bei dieser Vielfalt zu einer wachsenden Herausforderung, der Jugendliche und deren Eltern allein nicht mehr gewachsen sind. Hier sind vor allem Anbieter und auch die Politik gefordert.

Datenpool Web 2.0: Kontrollverlust vorprogrammiert

In Social Communities vernetzen sich Jugendliche mit Freunden und Bekannten, lernen neue Leute kennen und tauschen sich mit ihnen aus. Voraussetzung, um überhaupt gefunden oder als Partner akzeptiert zu werden, ist die Preisgabe persönlicher Informationen. Junge User stellen deshalb eine Fülle privater Daten ein, um sich für andere interessant zu machen und sich selbst darzustellen. Sie präsentieren, wer sie sind (oder gerne wären), was sie gerade machen und was sie bewegt. Was ist schon dabei, denken sie, wähnen sie sich doch unter Gleichgesinnten und in geschützten Räumen.

Katja Knierim

geboren 1978, studierte in Frankfurt am Main Germanistik und Theater-, Film- und Medienwissenschaften und kam 2006 zu jugendschutz.net in Mainz, wo sie als Leiterin des Referats Chats, Messenger und Communitys tätig ist. Ihr Team und sie recherchieren und bewerten die Jugendschutzrisiken von kinder- und jugendaffinen Kommunikationsdiensten, entwickeln Materialien für Pädagoginnen und Pädagogen, Eltern, Kinder und Jugendliche und fordern Betreiber zur Etablierung effektiver Schutzmaßnahmen auf.
jugendschutz.net wurde 1997 von den Jugendministerien aller Bundesländer gegründet, drängt auf die Einhaltung des Jugendschutzes im Internet und sorgt dafür, dass Anbieter problematische Inhalte rasch verändern, löschen oder für Kinder und Jugendliche sperren.
Das Referat Chats, Messenger und Communitys von jugendschutz.net startete 2004 als Projekt, wird seit 2006 von der Landesanstalt für Kommunikation (LFK) gefördert und ist seit dem vergangenen Jahr fester Bestandteil der Arbeit von jugendschutz.net.
Mehr Infos unter: www.jugendschutz.net und www.chatten-ohne-risiko.net.

Doch der Schein trügt: Die Recherchen von jugendschutz.net belegen, dass es im Web 2.0 häufig zu problematischen oder sogar gefährlichen Situationen für Kinder und Jugendliche kommen kann. Dieses Risiko steigt, wenn Jugendliche viele persönliche Daten preisgeben: Sie machen sich dann auch für Fremde – seien es nun Belästiger, Beleidiger oder Werbefirmen – identifizierbar, einschätzbar und angreifbar. Schnell verlieren sie die Kontrolle, weil persönliche Informationen, die einmal eingestellt wurden, sich schnell verbreiten oder verschiedene Quellen kombiniert werden können.

Die Datenschutzproblematik darf nicht jugendlichen Usern und ihren Eltern allein aufgebürdet werden, da sie die Risiken meist gar nicht abschätzen können.

Schon bei der Anmeldung erfragen viele Anbieter Daten, die – teils ohne Warnung – ins Profil übernommen werden. Privatsphäre-Einstellungen sind selten richtig vorkonfiguriert oder nur umständlich sicher zu gestalten. Es fällt nicht leicht, die Kontrolle zu behalten – zumal die Informationen über die eigene Person auch von anderen kommen können. Mal postet ein Freund ein Foto, mal wandert ein selbst gedrehtes Video von Handy zu Handy. Wie können und sollen Jugendliche ihr Recht auf informationelle Selbstbestimmung wahrnehmen, wenn sich nicht mehr nachvollziehen lässt, wer was wann über wen weiß bzw. veröffentlicht hat?

Gemeinsam für mehr Sicherheit: Anbieter tragen Verantwortung für Datensparsamkeit

Der Jugendschutz im Web 2.0 lässt sich nur verbessern, wenn alle ihren Teil der Verantwortung übernehmen. Natürlich müssen Jugendliche und ihre Eltern Risiken über den pfleglichen Umgang mit eigenen und fremden Daten aufgeklärt werden. Dabei haben sich Peer-Education-Konzepte (Jugendliche lehren Jugendliche) wie die Medienscouts als erfolgreiche Methode erwiesen. Sie nutzen das technische Verständnis der Jugendlichen, regen zur Reflexion der eigenen Mediennutzung an und machen sie zu Multiplikatoren für Internet-Sicherheit. Eltern und pädagogischen Fachkräften stehen umfangreiche Info-Materialien zur Verfügung, z.B. die Broschüren „Ein Netz für Kinder“ (Datenschutz für Kinder) oder „Chatten ohne Risiko?“ (Datenschutz für Jugendliche) unter http://jugendschutz.net/chatten.

Die größte Verantwortung für die Sicherheit jugendlicher User tragen aber die Anbieter kommunikativer Dienste. Ihrer Verantwortung für den Schutz persönlicher Daten kommen sie noch nicht ausreichend nach. Richten sich Angebote gezielt an ein minderjähriges Publikum oder werden von diesem regelmäßig besucht, so sind die Betreiber aufgefordert, für ein Höchstmaß an Datensparsamkeit zu sorgen. Zudem müssen sie durch sichere Voreinstellungen in den Bereichen Privatsphäre und Fremdkontakte verhindern, dass persönliche Daten unabsichtlich veröffentlicht werden. Hilfen und die Kommunikation wichtiger Schutzstrategien müssen dem Alter der Zielgruppe entsprechend und gut platziert in die Angebote integriert werden.

Aufgabe von Politik sowie Jugend- und Datenschutzinstitutionen wird es sein, dies von den Anbietern verstärkt einzufordern, sichere Angebote für Kinder zu fördern und die Entwicklung eines kompetenten Umgangs von Jugendlichen mit Datenschutzrisiken zu unterstützen.

Datenschutz und Persönlichkeitsrechte im Web 2.0 –

Treffpunkt Internet - Mit Sicherheit gut!

Dr. Kristina Köhler, Bundesministerin für Familie, Senioren, Frauen und Jugend

Von Generation zu Generation wird das Internet selbstverständlicher im Leben von Kindern und Jugendlichen. Bereits Vorschulkinder beschäftigen sich mit Internetangeboten, rund 60 Prozent aller 6- bis 13-Jährigen gehen bereits ins Internet. Gerade die neuen Dienste wie Schüler-Communitys und Videoportale bieten ihnen Interaktions- und Kommunikationsmöglichkeiten, die ihnen als Plattform für ihre Selbstdarstellung und Kontaktmöglichkeit mit Gleichaltrigen dienen und deshalb besonders attraktiv und reizvoll für sie sind. Web 2.0 - das Kommunikations- und Mitmachnetz wird immer beliebter bei Kindern und Jugendlichen, 71 % aller 12- bis 13-Jährigen sind in irgendeiner Form im Web 2.0 aktiv. Dabei dürfen wir nicht vergessen, dass die Nutzung des Internets, insbesondere des Web 2.0, oftmals die Preisgabe persönlicher Daten voraussetzt und immer wieder neue Anforderungen an den Jugend- und Datenschutz stellt.

Dr. Kristina Köhler

Geboren am 3. August 1977 in Wiesbaden.
Persönlich: 1997 - 2002: Studium der Soziologie, Mittlerer und Neuerer Geschichte und Philosophie an der Johannes-Gutenberg-Universität Mainz; 1998 - 2002: Studium der Politikwissenschaft; Februar 2002: Abschluss als Diplom-Soziologin, Wahlpflichtfächer Politikwissenschaft und Philosophie; Februar 2009: Promotion zum Dr. phil. am Institut für Politikwissenschaft, Universität Mainz, bei Prof. Dr. Jürgen W. Falter.
Politisch: 1994: Eintritt in die CDU; 2000 - 2001: Stadtverordnete der Landeshauptstadt Wiesbaden; seit 2002: Mitglied des Landesvorstands der CDU Hessen; seit 2002: Mitglied des Deutschen Bundestages; seit 30. Nov. 2009: Bundesministerin für Familie, Senioren, Frauen und Jugend.

Leider machen viele Kinder und Jugendliche belastende Erfahrungen. Die Vielfalt der Nutzungsmöglichkeiten und der schnellen technischen Entwicklungen bergen zahlreiche Gefährdungsmöglichkeiten und Risiken. Rücksichtslose Anbieter nutzen die Leichtgläubigkeit von Kindern aus und fragen zu viele Daten ab. Kinder und Jugendliche nutzen die Mitmachmöglichkeiten oft leichtfertig oder in Unkenntnis und geben zu viel Persönliches preis. Teilweise sind sie Cyber-Mobbing und sogar kriminellen Angriffen wie sexuellen Belästigungen und Datenraub ausgeliefert.

Gemeinsam müssen wir Risiken reduzieren! In einer Kultur gemeinsamer Verantwortung müssen wir unsere Kräfte bündeln, um Kinder und Jugendliche einerseits zu schützen und sie andererseits altersangemessen am Internet teilhaben zu lassen. Dabei sehe ich vor allem Politik, Anbieter, pädagogische Fachkräfte und Eltern in der Pflicht.

Kinder brauchen besonderen Schutz - Schutzräume für Kinder entwickeln. Gesetze sollen den Schutz unserer Kinder vor problematischen Inhalten und Gefahren gewährleisten und müssen über Ländergrenzen hinweg durchgesetzt werden. Anbieter stehen in der Verantwortung, ihre Internetseiten so zu gestalten, dass Kinder nicht gefährdet sind. Ich wünsche mir sichere Varianten großer Internetangebote für Kinder. Mehr Bedarf gibt es auch im Bereich attraktiver eigenständiger Kinder- und Jugendplattformen, bei denen Sicherheit und Datenschutz oberstes Gebot ist. Mit unserer gemeinsamen Initiative "Ein Netz für Kinder" fördern wir solche Angebote und wollen einen sicheren Surfraum aufbauen, der gewährleistet, dass Kinder nur auf geprüften Seiten surfen können.

Mehr Sensibilität von Anbietern gefordert. Wichtig ist, dass der Datenschutz und der Schutz der Persönlichkeitsrechte vor allem bei Kindern und Jugendlichen in hohem Maß gewährleistet werden, ohne dass Angebote unattraktiv werden. Angebote, die sich an Kinder richten, sollten überhaupt keine Daten abfragen oder aber sicherstellen, dass nur Eltern diese angeben können. Bei Angeboten für Jugendliche sollte eine möglichst sparsame Datenerhebung ausreichend sein und es muss sichergestellt werden, dass Jugendliche den Umgang mit ihren persönlichen Daten verstehen lernen. Dazu gehört auch, dass höchste Sicherheitseinstellungen die Regel sein sollten, von der der Jugendliche nur bewusst abweichen kann.

Erziehende Fachkräfte und Eltern brauchen Unterstützung, um ihre Kinder und Jugendlichen im Netz zu begleiten, damit sie lernen, die Chancen der neuen Medien zu nutzen und den Risiken wirksam begegnen können. Die Vermittlung und Stärkung der Medienkompetenz und Elternverantwortung für Eltern, Erziehende, aber auch für pädagogische Fachkräfte sowie für Kinder oder Jugendliche ist ein Schwerpunkt der Arbeit des Bundesministeriums für Familie, Senioren, Frauen und Jugend. Hierzu gibt es vielschichtige Informationen, Kampagnen, Broschüren und Websites.

Auch Kinder und Jugendliche müssen wir fragen und einbeziehen, denn sie sind ohnehin bereits zu eigenen Programmchefs ihrer Internetnutzung geworden. Das Bundesministerium für Familie, Senioren, Frauen und Jugend unterstützt Projekte wie Peer Education und engagiert sich in der Diskussion um Medienführerscheine. Kinder und Jugendliche sollen so intensiv wie möglich bei der Entwicklung eines kompetenten Umgangs mit den neuen Medien unterstützt werden.

Die Dialogplattform Forum Internet, die ich bis Mitte des Jahres installieren möchte, soll dabei helfen, einen gesamtgesellschaftlichen Konsens über Freiheit im Internet und über die Weiterentwicklung des Kinder- und Jugendschutzes im Internet zu finden. Alle Verantwortlichen und Interessengruppen müssen hier eingebunden werden.

Safer Internet Day 2010: Langer Atem und neue Ideen

Ich hoffe, dass mit Initiativen wie dem Safer Internet Day 2010 einmal mehr unser aller Bewusstsein geschärft wird, welchen hohen Wert der Schutz unserer Kinder und Jugendlichen im Netz hat.

Für *Kinder* wünsche ich mir, dass Sicherheit und Schutz ihrer Daten und Persönlichkeitsrechte im Internet die höchste Priorität gewinnt. Sie brauchen eigene Chats und Communitys, die keinerlei Risiko bergen. Hier können sie andere Kinder treffen, sich austauschen und gleichzeitig lernen, die Dienste des Internets kompetent zu nutzen. Aber auch Videoplattformen und Soziale Netzwerke, die von Kindern genutzt werden, müssen den Datenschutz und die Persönlichkeitsrechte von Kindern beachten und dürfen medienpädagogische Bemühungen nicht unterlaufen.

Für *Jugendliche* wünsche ich mir, dass Sicherheit und Schutz ihrer Daten und Persönlichkeitsrechte im Kontext zu ihrer zunehmenden Selbständigkeit und Selbstbestimmtheit stehen. Sie müssen lernen können, welche Daten sie von sich preisgeben möchten, wie sie sich gegen Datenmissbrauch wehren können und dass sie sparsame Datenerhebungen erwarten und fordern können. Entsprechend ihrem Alter müssen auf Internetseiten die Risiken für sie kalkulierbar und zu handhaben sein.

Dies wird uns gelingen, wenn alle, die an dieser Stelle Verantwortung für Kinder und Jugendliche tragen, mit Fachkenntnis, Ideenreichtum und sozialer, ethischer Verantwortung die anstehenden Aufgaben angehen.

Für Datenschutz kann jeder selbst etwas tun und Google ist der falsche Feind

Ulrike Langer, Medien- und Marketingjournalistin, medialdigital.de

Wer sich im Netz bewegt, produziert zwangsläufig Daten — da hilft kein Lamentieren, das ist Fakt. Aber für den Schutz unser persönlichen Daten und unserer Reputation im Netz können wir selbst eine Menge tun. Dafür müssen wir gar nicht nach immer neuen Gesetzen rufen. Wer ein Profil bei einem Netzwerk wie Facebook, StudiVZ und Co. hat, sollte sich unbedingt die Zeit nehmen, die Datenschutzeinstellungen seiner Seiten zu überprüfen. Bei Facebook sind beispielsweise inzwischen viele Daten per se einsehbar, wenn man als Nutzer nicht aktiv per Filter diese Freigaben abschaltet. Außerdem lohnt es sich, bei Freundschaftsanfragen lieber auch mal "nein" zu sagen. Ein Netzwerk mit echten Freunden und richtigen Kontakten aufzubauen sollte wichtiger sein, als möglichst viele "Fans", "Friends" oder "Follower" als reines Statussymbol vorweisen zu können. Denn jemanden bei Facebook und Co. Eintritt zu gewähren, den man überhaupt nicht kennt, birgt Risiken. Einem völlig Fremden würde man schließlich auch nicht in der U-Bahn seine Urlaubsfotos zeigen oder erzählen, ob man "Fan" der SPD ist oder morgens gerne die erste Schulstunde schwänzt.

In den Kommentarspalten von Foren, Blogs oder Nachrichtenportalen kann man ebenfalls viel für den Schutz seiner Online-Reputation tun. Eine simple Maßnahme, die dabei helfen kann: Meinung auf Blogs, in Foren oder in den Kommentarspalten von Nachrichtenportalen wenn möglich unter dem eigenen Namen äußern. Das hat für beide Seiten Vorteile. Erstens für den Adressaten eventueller Kritik. Man wägt auf diese Weise genauer ab, was man eigentlich sagen möchte, ob das Gesagte missverständlich sein könnte und ob es nicht auch einen freundlicheren Ausdruck dafür gibt. Zweitens: Wer nächste Woche oder nächstes Jahr noch zu seinen Äußerungen stehen kann, braucht sich auch keine Sorgen zu machen, ob nicht doch jemand den Schutzmantel der Anonymität wegreissen könnte. Denn worüber sich viele Kommentar-Rüpel und Schmähkritiker keine Gedanken machen: Webseitenbetreiber können über E-Mail- und IP-Adressen eine Menge über den Absender herausfinden.

Ulrike Langer
ist freie Medien- und Marketingjournalistin in Köln. Sie beschäftigt sich vor allem mit den Chancen, Bedingungen und Auswirkungen des digitalen Medienwandels für Medien, Marketing und den Journalismus. Zu ihren Auftraggebern gehören u.a. die Fachmagazine medium, W&V Media und Horizont. Ulrike Langer betreibt das Fachblog medialdigital.de. Sie ist Fellow (ehemalige Stipendiatin) des deutsch-amerikanischen Journalisten-Austauschprogramms Arthur-F.-Burns.

Für überzogen halte ich die europäische Angst vor der "Datenkrake" Google. Es passt einfach nicht zusammen, wenn immer mehr Webnutzer wie selbstverständlich immer mehr kostenfreie Google-Dienste nutzen wollen (Googlemail, Google-Suche, Google-Maps etc.), sich gleichzeitig aber darüber beschweren, dass Google dadurch immer mehr Daten sammelt, um sie seinen Werbekunden zum Einblenden möglichst individuell passender Werbung zur Verfügung zu stellen. Das ist Googles Geschäftsmodell. Und noch hat niemand Google einen Missbrauch der gesammelten Daten nachgewiesen. Wem bei soviel Daten in der Hand eines einzigen Anbieters unbehaglich ist, der sollte öfters mal auf Alternativen ausweichen. Es gibt zu jedem Dienst von Google Alternativen. Die Google-Suche hat pikanterweise hierzulande einen Marktanteil von 90 Prozent, mehr als in fast jedem anderem Land der Welt. Dabei ist die Microsoft-Suche Bing Google in Teilen überlegen, freie Webmaildienste gibt es auch von

GMX oder Hotmail und OpenStreetmap ist eine frei editierbare Landkarte der gesamten Welt.

Mehr Sorge als von Google ausgespielte personalisierte Werbung bereiten mir die Datenskandale der jüngsten Zeit (z.B. vertrauliche Kundendaten der Telekom im Besitz von Adresshändlern, Datendiebstahl bei Kreditkartendienstleistern) oder das Gebaren der Bundesregierung in puncto Datenschutz im Netz. Das Gesetz zur Vorratsdatenspeicherung (totale Überwachung des elektronischen Datenverkehrs) ist schon seit zwei Jahren in Kraft. Das Blockieren von Webseiten mit Stoppschildern — ein Vorschlag der Ex-Familienministerin zur Eindämmung der Kinderpornografie im Netz — ist zumindest auf Eis gelegt. Doch schon kommt der nächste zweifelhafte Vorschlag: Der aktuelle Entwurf zum Jugendmedienschutz-Staatsvertrag. Darin wird allen Ernstes von allen "Anbietern" (Access-Provider, Webhoster und Inhalteanbieter werden hier in einen Topf geworfen) eine Klassifizierung ihrer Inhalte nach Altersstufen gefordert. Und außerdem eine Abschaltung von Seiten, welche als nicht "jugendfrei" klassifiziert werden, zu Zeiten, in denen sich Jugendliche im Netz bewegen. Also eigentlich immer, außer vielleicht zwischen 2 Uhr nachts und 6 Uhr morgens. Doch wer kontrolliert die Kontrolleure? Wer soll entscheiden, ob eine Seite mit einem Stoppschild versehen oder zeitlich beschränkt werden muss? Und nach welchen juristisch standhaltenden Kriterien? Es gibt Daten, welche der Staat legitimerweise sammeln darf und muss, um seinen hoheitlichen Aufgaben nachzukommen — zum Beispiel Steuerdaten. Doch wo beginnt die vorsorgliche Datensammelwut, wo beginnt ein totalitärer Überwachungsstaat? Mehr Bewusstsein für solche Fragen zu wecken, halte ich für ebenso wichtig wie Anleitungen zum persönlichen Datenschutz.

Datenschutz in der Informationsgesellschaft

Dr. Severin Löffler,
Leiter Recht & Politik, Mitglied der Geschäftsleitung Microsoft Deutschland GmbH

1 | Verlässlicher Umgang mit Daten hat Priorität

Je mehr Menschen Computer und Internet nutzen, desto mehr Informationen werden übertragen. Dabei wollen die Nutzer darauf vertrauen können, dass ihre persönlichen Daten in guten Händen sind. Gleichzeitig wollen sie genau wissen, was mit ihren Daten geschieht. Als Anbieter von Technologien und Services hat Microsoft sich deshalb zum Ziel gesetzt, verlässliche Lösungen zu schaffen und für die nötige Transparenz zu sorgen. Denn Vertrauen ist eine der wichtigsten Voraussetzungen für die Akzeptanz und Nutzung von Informationstechnologien. Nur Anwender, die sich uneingeschränkt sicher fühlen, schöpfen die Möglichkeiten des Internets aus. Beispielsweise möchten sie, wenn sie die Vorteile individueller Dienste nutzen, die Kontrolle über ihre persönlichen Daten behalten. Vor allem bei Anwendungen wie Suchmaschinen, personalisierten Online-Services und Online-Werbung ist Datenschutz wichtig.

Für Unternehmen hat der sorgfältige Umgang mit Kundendaten ebenfalls große Bedeutung und stellt ein Qualitätsmerkmal dar, von dem auch der Geschäftserfolg abhängen kann. Allein der Verdacht auf mögliche Unsicherheiten im Umgang mit sensiblen Daten kann die Wettbewerbsfähigkeit eines Unternehmens ernsthaft gefährden und dessen Ruf beschädigen. Zudem müssen Unternehmen sicherstellen, dass sie gesetzliche Richtlinien einhalten (Compliance). Unter anderem gilt es, bestimmte Informationspflichten zu erfüllen, wobei der sichere Umgang mit Daten eine wichtige Rolle spielt.

1.1 | Datenschutz gewinnt an Brisanz

Das Verständnis von Sicherheit hat sich in den vergangenen Jahren stark verändert. Es geht nicht mehr nur um den Schutz von Computern und der Netz-

Dr. Severin Löffler
ist seit Oktober 2008 als Senior Director Legal and Corporate Affairs bei der Microsoft Deutschland GmbH tätig. In dieser Funktion leitet er die Bereiche Legal und Corporate Affairs. Severin Löffler berichtet an Dorothee Belz, Associate General Counsel EMEA, und ist Mitglied der Geschäftsleitung der Microsoft Deutschland GmbH.
Er startete seine Laufbahn als Rechtsanwalt bei der Kanzlei Friederich, Ernst, Engelhard & Partner in München. Vor seinem Start bei Microsoft arbeitete er sieben Jahre bei der internationalen Großkanzlei Clifford Chance. Der Volljurist promovierte im internationalen Medienrecht.

Infrastruktur vor Hackern und Schadprogrammen. Sondern auch darum, den Zugriff auf gespeicherte Daten zu kontrollieren. Das betrifft Informationen für Online-Banking auf dem Privat-PC genauso wie vertrauliche Kunden- und Finanzdaten auf Servern von Unternehmen und Behörden.

Außerdem hat Datenschutz für die Anwender eine größere Bedeutung bekommen. Das ergab die Microsoft-Sonderbefragung „Sicher Surfen 2008: Wie schützen sich Onliner im Internet?“ im Rahmen des (N)Onliner Atlas 2008 von der Initiative D21 und TNS Infratest. Im Mittelpunkt des Interesses der Befragten stehen nicht mehr wie in den Jahren zuvor Viren und Trojaner. Vielmehr gewinnt das Thema Datenschutz an Brisanz. 22 Prozent der Befragten möchten mehr über die Sicherheit ihrer Daten erfahren – das sind 15 Prozentpunkte mehr im Vergleich zum Vorjahr und damit ein Anstieg um das Dreifache.

1.2 | Welche Daten geschützt werden müssen

Daten entstehen bei fast allen Anwendungen – beim Einkaufen und Surfen im Internet oder bei der Text-

erstellung mit Office-Programmen. Überall hinterlässt der Nutzer seine Spuren. Zum Teil direkt, beispielsweise wenn er im Internet Formulare ausfüllt; zum Teil auch indirekt durch Metadaten in Dokumenten, der IP-Adresse oder Cookies.

Informationen, die Rückschlüsse auf den Nutzer zulassen, bedürfen eines besonderen Schutzes. Dies sind zum einen pseudonyme Daten, die zwar den Nutzer nicht eindeutig identifizieren, aber mit ihm assoziiert werden könnten. Beispielsweise Informationen und Profile von Nutzern, die nicht an ein Individuum gebunden sind. Zum anderen gibt es persönliche Informationen. Sie lassen sich einer Person genau zuordnen, dazu gehören Name, E-Mail-Adresse, Kreditkartennummer und biometrische Daten. Einige dieser Angaben, wie Passwörter oder PIN, sind so sensibel, dass sie speziell geschützt werden müssen.

2 | Datenschutz in der Praxis

2.1 | Unternehmen: Datenschutz schafft Vorteile

Unternehmen erheben Kundendaten aus unterschiedlichen Gründen. Beispielsweise können sie damit einen persönlicheren Service bieten. Kennen sie Verhalten und Vorlieben ihrer Kunden, können sie außerdem innovative Geschäftsfelder entwickeln. Wenn sie sorgfältig mit diesen Informationen umgehen, verschafft ihnen das einen Wettbewerbsvorteil. Damit die Daten von Kunden und auch Mitarbeitern gut geschützt sind, sollten Unternehmen über den gesamten Lebenszyklus einer Information für deren Sicherheit sorgen (Data Governance Lifecycle). Das beginnt schon beim Erheben und Sammeln der Daten. Beispielsweise sollten Kunden die Wahl und Kontrolle haben, welche Informationen sie preisgeben möchten. Bei der Speicherung und Nutzung gelten ebenfalls Sicherheitsanforderungen. Unter anderem muss das Unternehmen den Zugang regeln und die Daten vor Missbrauch schützen. Schließlich sollte die sichere Archivierung oder Vernichtung sensibler Informationen gewährleistet sein.

Regeln einhalten

Verantwortliches Handeln heißt auch, sich an Regeln zu halten. In diesem Zusammenhang spielt das Thema Compliance eine große Rolle. Das bedeutet, Unternehmen müssen gesetzliche Regeln erfüllen und sollten zusätzlich freiwillige Vorschriften einhalten. Beispielsweise schreibt der Gesetzgeber vor, dass Informationen eine bestimmte Zeit aufbewahrt werden müssen. Dabei sind Datensicherheit und -schutz entscheidend. Compliance geht jedoch über Datenspeicherung hinaus, sie umfasst auch das Datenmanagement. So müssen Unternehmen Archivierungsregeln aufstellen und für die Sicherheit, Integrität und Auffindbarkeit der Informationen sorgen. Wichtig dabei ist eine Strategie, die Menschen, Prozesse und Technologien einbezieht.

Welche Folgen es haben kann, wenn die betroffenen Abteilungen in Bezug auf Datenschutz nicht zusammen arbeiten, verdeutlicht eine entsprechende Studie („Microsoft Study on Data Protection and Role Collaboration Within Organizations“), die das Ponemon Institute LLC im Oktober 2007 in den USA, Großbritannien und Deutschland durchgeführt hat. Kernergebnis: Drei Viertel der befragten Unternehmen, bei denen kaum eine Kooperation stattfand, verzeichneten in den vergangenen 24 Monaten einen oder mehrere Datenmissbräuche. Vor allem muss die Kommunikation zwischen denjenigen, die Daten sammeln und den Sicherheits- und Datenschutz-Experten stimmen. Das ist jedoch in Unternehmen nur selten der Fall. Lediglich ein Drittel der Marketing-Mitarbeiter tauscht sich mit den Sicherheitsexperten über die Datensammlung und -nutzung aus.

2.2 | Microsoft: Datenschutz als Unternehmensgrundsatz

Datenschutz ist für Microsoft seit Langem ein wichtiges Thema. Neben Sicherheit, unternehmerischer Integrität und der Zuverlässigkeit von Software, Diensten und Produkten bildet es die vierte Säule der Trustworthy Computing Strategie, die 2002 von Bill Gates als oberster Unternehmensleitsatz formuliert wurde. Im Bereich des Datenschutzes gilt dabei

der Grundsatz: Sicherheit geht vor Funktionalität – und zwar bei der Entwicklung aller Microsoft-Produkte und -Services. Die so geschaffenen Lösungen sollen den Anwendern helfen, vertrauensvoll mit den digitalen Medien umzugehen und sich vor Datenmissbrauch zu schützen.

Klare Richtlinien für die Produktentwicklung

Microsoft hat in den vergangenen Jahren seine internen Datenschutzrichtlinien für die Bereiche Vertrieb und Marketing sowie Entwicklung stetig verbessert. So gilt beispielsweise bereits seit 2005 im Unternehmen das Prinzip des Security Development Lifecycle (SDL), in das Datenschutzstandards für die Softwareentwicklung integriert wurden. So achten alle Microsoft-Entwickler von Anfang an darauf, dass neue Software und Services datenschutzkonform sind – und zwar über den gesamten Produktlebenszyklus hinweg.

Ein Ziel dabei ist es, den Verbrauchern die Kontrolle über ihre persönlichen Informationen zu geben. Sie sollen genau wissen, welche Daten gesammelt, an wen diese verteilt und wie sie verwendet werden. Ohne ihr Einverständnis werden beispielsweise keine persönlichen Informationen von ihrem Computer übertragen. Auch haben die Anwender jederzeit Zugriff auf ihre Daten und können diese bearbeiten. Die Microsoft Datenschutzstandards sind zudem öffentlich zugänglich. So können auch freie Entwickler ihre Anwendungen entsprechend anpassen.

Seine Datenschutzrichtlinien entwickelte Microsoft auf Basis der Datenschutz-Leitlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) sowie der Datenschutzrichtlinie der Europäischen Union. Darüber hinaus setzt sich Microsoft für weltweit gültige Datenschutzrichtlinien bei der Software- und Serviceentwicklung ein. Politik, Unternehmen und Wissenschaft sollten diese gemeinsam erarbeiten. Ein Beispiel: Microsoft engagiert sich in der International Association of Privacy Professionals (IAPP). Mehr als 4.000 Datenschutzexperten aus 32 Ländern haben sich in diesem Verband zusammengeschlossen. Ihr Ziel ist es, den Austausch und die Weiterbildung im Bereich Datenschutz zu fördern.

Außerdem ist Microsoft Mitglied des TRUSTe Privacy Seal Program und der Network Advertising Initiative (NAI).

Gütesiegel bescheinigen Qualität

Dass Microsoft die Datenschutzanforderungen erfüllt, belegen auch Datenschutz-Siegel für Microsoft-Produkte. Diese Qualitätszeichen werden von unabhängigen Prüfstellen, wie dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), verliehen. Beispielsweise hat die Anwendung Windows Genuine Advantage (WGA) Version 1.7 für Windows XP ein Gütesiegel vom ULD erhalten. Diese Anwendung überprüft, ob auf Computern autorisierte Software-Lizenzen laufen. So weiß der Nutzer, ob sein Windows XP legal ist und damit den Sicherheitsanforderungen von Microsoft entspricht. Die Einhaltung des Datenschutzes beim Windows Update Service wurde ebenfalls vom ULD mit einem Gütesiegel bescheinigt.

Eine Weiterführung des Gütezeichens auf europäischer Ebene ist das European Privacy Seal (EuroPriSe): Es prüft die Einhaltung europäischer Datenschutzrichtlinien. Neun Partner aus acht EU-Mitgliedsstaaten wollen unter der Leitung des ULD mit EuroPriSe einen europäischen Standard für die Bewertung von IT-Produkten und IT-basierten Services schaffen. Wer das Siegel erhalten möchte, muss einen zweistufigen Evaluationsprozess durch unabhängige Experten durchlaufen. Das Pilotprojekt läuft bis November 2008.

2.3 | Suchmaschinen und Online-Werbung: anonym surfen

Gemeinsam mit qualifizierten Partnern entwickelt Microsoft auch den Datenschutz bei Suchmaschinen und Online-Werbung weiter. Ziel ist es, einen offenen Dialog mit anderen Unternehmen, Wissenschaftlern und Verbraucherschützern anzustoßen – und international gültige Rahmenbedingungen zu schaffen.

Den Datenschutz bei Bing hat Microsoft bereits deutlich verbessert. Vor allem bei der Personalisierung der Suchdienste: Die Nutzer haben mehr Kontrollmöglichkeiten darüber, welche Informationen verwendet werden, damit die Online-Services auf ihre Bedürfnisse zugeschnitten sind. Für die Weiterentwicklung und Verbesserung von Bing erhebt Microsoft auch Daten über die Anwender und ihr Verhalten. Diese Informationen können jedoch anonym bleiben. Das bedeutet, es gibt keinerlei Verbindung oder Verlinkung, die Rückschlüsse auf den einzelnen Nutzer zulässt. Microsoft hat folgende Regeln für den Schutz der Privatsphäre bei der Online-Suche und -werbung aufgestellt:

- Datenschutzrichtlinien müssen transparent und leicht verständlich sein. Nur so können die Nutzer bewusste Entscheidungen treffen. Die Microsoft Online-Datenschutzerklärung wird regelmäßig aktualisiert und ist von den meisten Webseiten zugänglich.

- Die Nutzer sollen die Kontrolle behalten. Beispielsweise können sie genau bestimmen, welche Informationen sie von Microsoft erhalten möchten. Dazu gehören unter anderem Opt-out-Möglichkeiten bei Werbeangeboten.

- Suchanfragen sind getrennt abgelegt von Informationen, die den Nutzer eindeutig identifizieren würden. So wird verhindert, dass diese Daten ohne Zustimmung der Nutzer miteinander verbunden werden können.

- Daten aus der Suche mit Bing werden nach 6 Monaten vollständig gelöscht. Dies umfasst das endgültige Entfernen von Cookies, der gesamten IP-Adresse und anderer Identifizierungsmerkmale. Bei der Datenspeicherung für personalisierte Suchanwendungen müssen die Nutzer den Bedingungen zustimmen.

2.4 | Privatanwender: Sicheres Verhalten fördern

Mit Windows Vista hat Microsoft den Schutz der Anwender weiter erhöht. Es ist das erste Betriebssystem, das von Anfang an nach dem Prinzip des Security Development Lifecycle (SDL) entwickelt wurde. Sicherheit hat demnach oberste Priorität. So aktiviert Windows Vista unter anderem automatisch die Firewall und ruft Updates auf. Der PC ist damit immer gut geschützt. Eltern haben außerdem die Möglichkeit, spezielle Jugendschutzeinstellungen vorzunehmen. Ihr Nachwuchs kann dann beispielsweise auf keine Seiten mit pornografischen Inhalten oder Glücksspielangeboten klicken und nur vorher festgelegte Spiele aufrufen.

Digitale Identitäten verwalten

Eine weitere Funktion von Vista ist Windows CardSpace. Diese Anwendung vereinfacht und verbessert die Identitätskontrolle im Internet. Der Anwender erstellt eine oder mehrere virtuelle Karten mit persönlichen Informationen oder lässt sich diese beispielsweise von seiner Bank oder einem Online-Shop ausstellen. Windows CardSpace verwaltet die digitalen Identitäten – ähnlich wie eine Brieftasche, in der mehrere physische Karten stecken. Der Nutzer verwendet dann die Karte mit den für eine Anwendung relevanten Informationen. Beispielsweise Name, Adresse und Zahlungsinformationen, wenn er online einkauft. Windows CardSpace basiert auf offenen Kommunikationsstandards und unterstützt unterschiedliche Software auf allen Plattformen.

Privatsphäre wahren

Mehr Sicherheit und Datenschutz im World Wide Web bietet der Internet Explorer 8. Er unterstützt das sichere und anonyme Navigieren auf Internetseiten. Mit der optionalen Funktion „InPrivate-Browsen“ bleibt der Nutzer unerkannt. Der Browserverlauf, temporäre Internetdateien, Formulardaten, Cookies, Benutzernamen und Kennwörter werden nicht gespeichert. So gibt es auf dem genutzten PC keinerlei Spuren und Hinweise auf Suchverlauf und Surfverhalten. Weitere Sicherheitskomponenten des Internet Explorer 8 sind der SmartScreen-Filter, mit dem Microsoft das Erkennen von Phishingseiten verbessert sowie eine Funktion, die auf manipulierte Webseiten hinweist.

Medienkompetenz trainieren und Jugend schützen

Innovative Technologien sind eine Möglichkeit, die Privatsphäre der Anwender zu wahren. Doch auch die Nutzer sollten ein stärkeres Bewusstsein für den Schutz ihrer Daten entwickeln. Gerade im Internet handeln viele sorglos. In sozialen Netzwerken wie StudiVZ, Facebook oder Xing geben sie oft sehr persönliche Daten preis. Den Anwendern fehlt häufig das Wissen darüber, was mit diesen Daten geschieht und wer Zugang dazu hat. Ihnen ist meist nicht bewusst, dass sie die Datenschutzeinstellungen in ihrem System oder ihrem Browser in der Regel selbst vornehmen müssen.

Microsoft unterstützt deshalb Initiativen, die den Nutzern sicheres Verhalten im Internet vermitteln. Denn wie im realen Leben auch, müssen die Nutzer lernen, möglicherweise gefährliche Situationen auch online zu erkennen und angemessen zu reagieren. Mit dem Internet Risk Behaviour Index, kurz IRBI, hat Microsoft gemeinsam mit Wissenschaftlern der Münchner Ludwig-Maximilians-Universität (LMU) erstmals eine realitätsnahe Simulation riskanter Online-Situationen, darunter Datenschutz-Szenarien, entwickelt. Seit Juni 2008 können Nutzer ihr sicherheitsrelevantes Verhalten auf www.irbi.de trainieren und verbessern. Sie spielen typische Gefahrensituationen – etwa den Software-Download aus einer nicht vertrauenswürdigen Quelle – am Bildschirm durch. Für die Bewältigung der Aufgaben erhalten die Nutzer Punkte, die sich zum Internet Risk Behaviour Index addieren. Je nachdem, wie die Nutzer abschneiden, bietet Microsoft ihnen online Hilfestellungen an.

Um schon bei jungen Nutzern ein stärkeres Bewusstsein für Sicherheit und Schutz der Privatsphäre im Web herzustellen, hat Microsoft die Initiative „Sicherheit macht Schule“ (www.sicherheit-machtschule.de) gegründet. Sie dient als Forum für Unterrichtsideen, in dem Lehrer, Eltern und andere Verantwortliche Anregungen erhalten, wie sie Kinder und Jugendliche zu umsichtigem Verhalten anleiten können. Beispielsweise üben sie mit den Schülern, welche Passwörter sicher sind und wie sie selbst ein starkes Passwort auswählen. Weitere Initiativen wie die Internauten (www.internauten.de) und klicksafe (www.klicksafe.de) vermitteln den Kindern und Jugendlichen, wie sie sich im Internet richtig verhalten und Risiken vermeiden können.

Datenschutz –
unüberhörbares Thema am Kinder- und Jugendtelefon

Rebecca Maier, Helpline „Nummer gegen Kummer“, Saferinternet.de

Seit November 2008 ist das Kinder- und Jugendtelefon von Nummer gegen Kummer e.V. unter den kostenlosen, anonymen Rufnummern 0800 – 111 0 333 und 116 111 als deutsche Helpline Anlaufstelle auch bei Problemen im Internet. Die Beraterinnen und Berater hören zu, entlasten emotional und leisten konkrete Hilfe, wenn es um Cyber-Mobbing, sexuelle Belästigung im Chat, Abzocke, Pornografie, Computer-Spielsucht oder um jugendgefährdende Inhalte geht. Detaillierte Daten zu den Anrufen wird Nummer gegen Kummer e.V. erst Anfang 2011 vorlegen können. Doch eines lässt sich schon jetzt mit Gewissheit sagen: Kinder und Jugendliche sind emotional tief betroffen, wenn ihre persönlichen Daten missbraucht werden. Dies bestätigen zum einen Fallbeispiele aus der Internetberatung, die Kindern und Jugendlichen neben dem telefonischen Beratungsangebot unter www.kijumail.de zur Verfügung steht. Zum anderen belegen dies die Erfahrungsberichte der 50 MultiplikatorInnen, die bislang an der bundesweiten Zusatzqualifizierung „Safer Internet“ teilgenommen haben, die gemeinsam mit klicksafe konzipiert wurde.

Die Verzweiflung ist groß, wenn das eigene Netzwerk-Profil „gehackt“ wurde und im Namen des Kindes beleidigende E-Mails an gute Freunde, womöglich auch Lehrer verschickt wurden oder wenn plötzlich Hobbys wie „ficken, bumsen und mobben“ auf der Profilseite präsentiert werden. Häufig wissen die Anrufenden nicht, dass sie das Profil löschen oder den „Bully“ sperren können. Doch auch wenn sie Funktionen, wie das Melden oder das Löschen des Profils, kennen, bleibt die Verunsicherung, dass nun alle mit dem Finger auf sie zeigen und sagen „Du bist echt so dumm!?“, weil sie selbst nicht bemerkt haben, dass ihnen ein übler Streich gespielt wurde. In den Beratungsgesprächen zu solchen oder ähnlichen Fällen geht es einerseits um die Sensibilisierung von Kindern und Jugendlichen, wie sie ihre persönlichen Daten in Zukunft besser schützen können. Viel dringender sehen wir hier jedoch unsere Aufgabe, emotional zu entlasten, gemeinsam das verlorene Selbstbewusstsein wiederzufinden, damit das Kind die Scham überwinden und die betroffenen Freunde ansprechen kann, um Missverständnisse aufzudecken. Die rund 3.000 ehrenamtlichen BeraterInnen am Kinder- und Jugendtelefon sind intensiv dafür ausgebildet worden, gemeinsam mit dem Betroffenen Schritte aus dem Gefühlschaos anzugehen, z. B. eigene Fähigkeiten zu entdecken oder vertraute, wohlgesinnte Personen auszumachen, mit deren Hilfe das Kind oder der Jugendliche sein Problem bewältigen kann.

Es ist unerlässlich, Kinder und Jugendliche über die Vorsichtsmaßnahmen im Netz und den richtigen (technischen) Schutz aufzuklären. Dies sollte in der Familie oder Schule ebenso geschehen wie in Frei-

Rebecca Maier (M.A.)

studierte Erziehungs- und Kommunikationswissenschaften an der Freien Universität Berlin mit den Schwerpunkten mediale Ausbildung, Film und Fernsehen für Kinder. Freiberufliche Arbeit für Kinder-Filmfestivals in Berlin und Gera. Assistent bei der Freiwilligen Selbstkontrolle Fernsehen e.V., Co-Autor der Dokumentation über Medienausbildung in Kindergarten und Grundschule; Projektmanagement bei ecmc GmbH, redaktionelle Arbeit und Handouterstellung, Öffentlichkeitsarbeit für Medienerziehungsprojekte; Referentin bei der Initiative “Eltern+Medien” der Landesanstalt für Medien Nordrhein-Westfalen. Seit November 2008 arbeitet sie für Nummer gegen Kummer e.V. und das Projekt „Safer Internet“ , dessen Koordinierung sowie das Erstellen und die Durchführung von Schulungen für Multiplikatoren in Kooperation mit klicksafe stattfindet.

zeiteinrichtungen und Internet-Cafés. Aber das allein reicht nicht aus. Die Anfragen an der Helpline zeigen deutlich, dass Jugendliche darüber reden wollen und darüber reden können müssen, wie es sich anfühlt, wenn intime, persönliche, „geheime" Daten in die falschen Hände gelangen. Nur so lässt sich die Fähigkeit zur Empathie fördern. Es gilt gemeinsam ein Bewusstsein dafür zu schärfen, dass jeder vorsichtig und verantwortungsvoll mit den Daten anderer umgehen muss und Persönlichkeitsrechte nicht verletzen darf. Dafür sollten Erwachsene mit gutem Vorbild vorangehen. Leider erleben Kinder und Jugendliche täglich in ihrem Umfeld, wie Erwachsene und Medienanbieter zu schlechten Beispielen werden, indem sie Daten kopieren, missbrauchen, unüberlegt weitergeben u.v.m.

Gerade in der Pubertät sind verlässliche Personen für Jugendliche wichtig. Hier ist die „Nummer gegen Kummer" ein vertrauenswürdiger Gesprächspartner, denn die Helpline ist anonym. Die Nummer der Anrufer taucht weder auf einem Display noch auf der Telefonrechnung auf. Auch in der Internetberatung bleibt die Anonymität des Absenders gewahrt. Gleichermaßen werde die Daten der Beraterinnen und Berater von „Nummer gegen Kummer" geschützt. Dafür hat der Dachverband für seine Mitglieder verbindliche Richtlinien erarbeitet, die für alle 93 Träger des Kinder- und Jugendtelefons und der 47 Standorte des Elterntelefons verpflichtend sind. Seit 1991 unterstützt die Deutsche Telekom AG Nummer gegen Kummer e.V. dabei, die strengen Auflagen technisch umzusetzen.

Die Zahlen sprechen für sich – über 800.000 Anrufe sind 2008 beim Kinder- und Jugendtelefon zu allen Themen, die für junge Menschen wichtig sind, eingegangen. Insbesondere dann, wenn überall die „Vorsicht im Umgang mit persönlichen Daten" thematisiert wird, muss es einen geschützten Raum geben, der schnell erreichbar ist. Kinder und Jugendliche sollten unbedingt über Persönliches reden können, um ihren Sorgen und Nöten, ihrer Scham und Verletzbarkeit Ausdruck zu verleihen. Vertrauen und sich auf seine eigenen Gefühle verlassen zu können, ist ein wichtiger Baustein bei der Unterstützung zur Alltagsbewältigung und der Förderung auch von Medienkompetenz – eine wichtige Aufgabe am Kinder- und Jugendtelefon.

Gibt es eine „Datenschutzmoral“ für Anbieter von sozialen Netzwerken?

Dr. Johannes Mainusch, Vice President Operations, XING AG

Ein Buchstabe macht den Unterschied: Das ‚s‘. Wann immer ein Nutzer auf XING unterwegs ist, zeigt das „https://“ in der Adresszeile des Browsers an, dass die Verbindung verschlüsselt ist – wie bei guten E-Mail-Anbietern oder beim Online-Banking. Als einziges soziales Netzwerk liefert XING die komplette Plattform für eingeloggte Mitglieder verschlüsselt aus. Das ist technisch ein erheblicher Aufwand, wenn es etwa um die Einbindung von Werbung oder von Services wie Google Maps geht; aber er lohnt sich, denn er schafft Vertrauen, das höchste Gut eines Netzwerks.

Bei den meisten anderen Sicherheitsaspekten steht nüchtern betrachtet das oft propagierte Gebot der Datensparsamkeit im Gegensatz zu dem, was Networking ausmacht: Persönlichkeit. Wer in einem sozialen Netzwerk nur ein Pseudonym hinterlegt hat, eine Wegwerf-Email benutzt und keine persönlichen Fotos einstellt, dessen Daten sind natürlich im Burggraben des Web-2.0-Nihilismus geschützt. Was im Freizeitbereich unter Umständen funktioniert, würde beruflichem Networking mit Mehrwert radikal entgegenstehen; eine vertrauens- und respektvolle professionelle Atmosphäre ließe sich damit nicht herstellen. Wir wollen, dass bei XING authentische Nutzer miteinander kommunizieren.

Ergo gibt es bei XING Minimalangaben, die erforderlich sind: der komplette bürgerliche Name und die Firmenzugehörigkeit. Ein Foto ist nicht vorgeschrieben, wer sich allerdings wie die überwältigende Mehrheit unserer Mitglieder für ein Bild im Profil entscheidet, muss ein echtes und einigermaßen aktuelles verwenden. Damit haben wir gute Erfahrungen gemacht, denn die Mitglieder finden sich so in einer deutlich persönlicheren Community wieder.

Diese persönliche, nicht von Pseudonymen übersäte Umgebung schafft Vertrauen und zeigt: Viele Sicherheitskomponenten des Netzwerkens lassen sich nicht so leicht in eine Schublade stecken wie die eingangs erwähnte Verschlüsselung, sind nicht pauschal sicher oder unsicher. Möchte man bei Google gefunden werden oder nicht? Dahinter steckt nicht nur der Aspekt „Sicherheit/Privatsphäre“, sondern, viel komplexer, das Management des eigenen Online-Rufs.

Dr. Johannes Mainusch

Als Vice President Operations betreut Dr. Johannes Mainusch den Betrieb und die technische Entwicklung der XING-Plattform, einer High-Traffic-Site mit über 8,3 Millionen Mitgliedern weltweit. Er verfügt über langjährige Erfahrung im Bereich iterativer und agiler Projektmethoden, die er sowohl bei Lufthansa Systems als Projektleiter als auch als freier Berater für zahlreiche Unternehmen der Industrie- und Logistikbranche einsetzte. Mit seinem umfangreichen technischen Hintergrund quer über alle Programmiersprachen, Datenbanken und Infrastrukturkomponenten hinweg analysiert und optimiert er komplexe IT-Systeme, etwa für bessere Performance oder effizientere Entwicklung.

Unsere Philosophie bei XING fußt auf zweierlei Säulen: Geboten und Angeboten. Für uns als Plattform gebietet es sich, maximalen Schutz bereitzustellen (etwa die eingangs erwähnte Verschlüsselung), also die Voraussetzung für maximales Vertrauen. Gleichzeitig essenziell ist es, die richtigen Werkzeuge und Einstellungen anzubieten, damit die über 8.3 Millionen Mitglieder auf unserer Plattform das Management ihrer eigenen Online-Reputation selbst in die Hand nehmen können, damit diese sich verbinden können und gleichzeitig adäquat vor unbefugtem Zugriff geschützt sind.

Unsere ethische Verpflichtung ist, das Vertrauen, das Menschen in uns setzen, zu respektieren und entsprechend zu handeln. Unsere Arbeit besteht darin,

sicherzustellen, dass die Einstellungen und Daten der Mitglieder nur dort sichtbar sind, wo sie auch sichtbar sein dürfen. Dementsprechend gilt: Wer nicht außerhalb der Plattform gefunden werden möchte, der stellt die entsprechende Option einfach ab. Wer nicht möchte, dass seine Beiträge oder auch nur der eigene Name in Gruppen außerhalb des Netzwerks lesbar sind, trifft die entsprechenden Optionen, Gruppenmoderatoren und unser Community Management wachen darüber, dass diese Wünsche eingehalten werden. Kontaktdaten wie auch sensible Informationen werden grundsätzlich nicht offen angezeigt, sondern lassen sich individuell für jeden bestätigten Kontakt freigeben und deaktivieren. Unser Team von Community Management und Customer Care ist direkter Ansprechpartner für die Mitglieder bei Verstößen oder Konflikten; auch die Moderatoren der über 30.000 Gruppen überprüfen, dass die Netiquette eingehalten wird. Zudem begrüßen wir alle Initiativen und Vorschläge von außen, die sich mit Sicherheitseinstellungen in sozialen Netzwerken allgemein und bei XING im Besonderen auseinandersetzen – so wie im Sommer 2009 die Initiative des Verbraucherschutzes.

Haben Anbieter von sozialen Netzwerken eine moralische Verpflichtung? Durchaus – aber vielmehr gilt, insbesondere bei einem Business-Netzwerk wie XING: Sie haben ein Interesse daran, Vertrauen aufzubauen, eine aktive Community aufzubauen, Mitglieder für die Plattform zu gewinnen. Das kann nur geschehen, wenn sich der Einzelne beim Netzwerken sicher vorkommt. Es ist für erwachsene Business Professionals nicht nötig, permanent behütet und voreinander beschützt zu werden; wohl aber erwarten Sie zurecht, dass die eigenen Einstellungen respektiert werden. Das ist unser Gebot – moralisch, gesetzlich, wirtschaftlich; somit ist bei XING das ganze Jahr über „safer internet day".

Datenschutz und Persönlichkeitsrechte im Web 2.0

Ekkehard Mutschler,
Jugendmedienschutzbeauftragter des Deutschen Kinderschutzbundes e.V.

Ein medienkompetenter Umgang mit den bestehenden Angeboten der elektronischen Medien eröffnet Kindern und Jugendlichen die Chance zu sozialer und politischer Partizipation – wie es in der UN-Konvention über die Rechte des Kindes festgeschrieben ist. Der Deutsche Kinderschutzbund (DKSB) setzt sich für die Beteiligung von Kindern bei allen Entscheidungen, Planungen und Maßnahmen, die sie betreffen, ein. Er befürwortet ausdrücklich eine Teilhabe der Kinder und Jugendlichen an der medialen Welt und unterstützt dabei die Umsetzung der UN-Konvention über die Rechte des Kindes, zu deren Forderungen unter anderem der „Zugang zu den Medien…" (Artikel 17), aber auch der „Schutz der Privatsphäre und Ehre" (Artikel 16) gehören.

Jedem Kind stehen ab Geburt gewisse Grundrechte zu. Dazu zählt auch das Recht auf informationelle Selbstbestimmung. Es besagt, dass grundsätzlich jede Person selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann. Da Kinder und Jugendlich allerdings häufig noch nicht in der Lage sind, den Sinn und Zweck und vor allem auch die Konsequenzen der Preisgabe ihrer Daten zu durchschauen, sind die gesetzlichen Vertreter – meist die Eltern – dazu verpflichtet, die datenschutzrechtlichen Interessen der Heranwachsenden zu wahren. Je älter ein Kind wird, desto mehr sollte ihm die Möglichkeit gegeben werden, seine Meinung zu äußern und es sollte von den Eltern zunehmend in die Entscheidungsprozesse eingebunden werden. Dieser Übergang des Einwilligungsrechtes ist ein wichtiger Schritt für die Entwicklung des Kindes, birgt jedoch – gerade in Zeiten von Web 2.0 – auch Gefahren.

Das Web 2.0 lebt zu einem großen Teil davon, dass sehr viele persönliche Daten, Bilder und Videos ins Netz gestellt werden. Die Konsequenzen und Risiken, die daraus entstehen können, sind vielen Jugendlichen – und selbst vielen Erwachsenen – nicht bewusst oder sie werden unterschätzt. So ist für Jugendliche nicht ohne weiteres abzusehen, dass ihre in einem Sozialen Netzwerk veröffentlichten Daten und Bilder eben nicht nur Freunde, sondern meist jeder sehen kann – und dass die unbekümmerte Weitergabe persönlicher Daten beispielsweise auch einmal zum Stolperstein für die berufliche Karriere werden könnte. Sie müssen zudem bedenken, dass alle ins Netz gestellten Informationen und Dateien jederzeit von Dritten missbraucht werden können.

Auch beim Veröffentlichen von Daten und Bildern anderer Personen muss einiges beachtet werden – das Netz ist kein rechtsfreier Raum. Nicht alles, was im Internet – und in Sozialen Netzwerken im Speziellen – möglich ist, ist auch erlaubt. Persönlichkeitsrechte, wie zum Beispiel das Recht am eigenen Bild und das Urheberrecht, gelten auch im World Wide Web! Gerade bei Kindern und Jugendlichen herrscht Unwissenheit und mangelndes Unrechtsbewusstsein darüber, dass im Internet veröffentlichte Texte, Videos, Lieder und Bilder grundsätzlich urheberrechtlich geschützt sind und daher nicht ohne weiteres

Ekkehard Mutschler

Ist Bauleiter in Rente; Ehrenamtliche Tätigkeiten: Jugendmedienschutzbeauftragter und Schriftführer beim Deutschen Kinderschutzbund Bundesverband e.V. und Landesvorsitzender des Deutschen Kinderschutzbund Landesverband Bayern e.V. Zudem ist er Stellv. Vorsitzender der Nummer gegen Kummer e.V. Herr Mutschler ist Prüfer für die öffentliche Hand bei der FSK sowie Mitglied im Fachbeirat der Stiftung Digitale Chancen und im Advisory Board des deutschen Safer Internet Centre.

anderweitig verwendet werden dürfen. Ein Verstoß gegen dieses Urheberrecht kann mit hohen Geldstrafen geahndet werden. Auch das Bloßstellen und Belästigen anderer Menschen (Klassenkameraden, Lehrer etc.) – ob in Wort oder Bild – mit Hilfe elektronischer Kommunikationsmittel (das sogenannte Cyber-Mobbing) ist nicht nur verwerflich, sondern auch strafbar, da es massiv gegen die Persönlichkeitsrechte dieser Personen verstößt.

Sobald Kinder und Jugendliche die Angebote des Web 2.0 nutzen, müssen sie für die Konsequenzen und Gefahren vom Umgang mit persönlichen Daten im Netz sensibilisiert werden und Unterstützung erfahren. Wie wichtig diese neue Form der Jugendkultur geworden ist, zeigt eine Studie der Medienforschung: Bereits 68% aller Deutschen zwischen 14 und 19 Jahren nutzen Soziale Netzwerke. Diese Netzgemeinschaften werden aus medienpädagogischer Sicht durchaus begrüßt, denn sie bieten den Kindern und Jugendlichen neuartige Chancen der Präsentation, Kontaktaufnahme und des Experimentieren mit der eigenen Identität. Sie finden dort einen außerschulischen, „intimen" Raum für ihre Kommunikation mit Gleichaltrigen, in dem sie ihre emotionale Unabhängigkeit von den Eltern entwickeln können. Durch ihre Selbstdarstellung im Netz definieren sie Fragen wie „Wer bin ich?", „Wer will ich sein?" oder „Welche Facetten von mir sind interessant?" und testen gleichzeitig ihren eigenen „Marktwert".

Die Verantwortung für den Medienumgang und die Medienerziehung von Kindern und Jugendlichen können Eltern oder Erzieher nicht alleine tragen. Sie brauche Hilfe durch die Plattform-Betreiber, die nutzerfreundliche „Räume" schaffen müssen, die die Daten- und Persönlichkeits-Rechte der Anwender achten, wahren und schützen. Hier herrscht in jedem Fall Nachholbedarf. Ferner steht der Gesetzgeber in der Pflicht, das geltende Recht an die neuen Gegebenheiten anzupassen. Schließlich gilt es, die Eltern und Pädagogen in ihrer Medienkompetenz zu stärken. Der Deutsche Kinderschutzbund bietet dazu Medienkurse „Wege durch den Mediendschungel. Kinder und Jugendliche sicher in der Medienwelt begleiten®" an.

Gefühlte Privatheit im offenen Netz

Prof. Dr. Klaus Neumann-Braun,
Lehrstuhl für Medienwissenschaft, Universität Basel

Wie schnell ist ein unbedarfter Klick im Netz gemacht und schon zeitigt dieser unangenehme Folgen: Man hat sich wider Willen ein Dienstleistungsabonnement beschert und soll nun kräftig zahlen. Oder man surft unschuldig auf einer Website umher und erhält im Anschluss daran eine SMS mit Wuchergebühr geschickt. Wie viel an Aufwand bedarf es dann, sich aus solchen — im Alltagsverständnis — betrügerischen Fallstricken zu befreien! Oder man zeigt Vertrauten auf Freundschaftsportalen persönliche Bilder, die in der Folge im Netz an ganz unerwarteter Stelle wieder auftauchen mit möglicherweise negativen Folgen — das Netz als neues Archiv unserer privaten Alltagskultur.

Es muss also gute Gründe geben, sich trotz dieser Risiken und Ärgernisse im Netz zu bewegen und zu kommunizieren. Allgemein betrachtet ist die Darstellung von Privatem in der öffentlichen Kommunikation mehr denn je überaus attraktiv. Auch in den klassischen Medien wie bspw. dem Fernsehen ist über die Jahre hinweg der Anteil an Programmen, die mit den Begriffen Realitätsfernsehen, Real-People-Formate, Doku-Soaps usf. gefasst werden, stetig gestiegen. Der Austausch und Vergleich mit den anderen Menschen „wie du und ich" via Medien fasziniert jung und alt ganz offensichtlich sehr.

SNS treffen die Bedürfnisse ihrer jugendlichen User: Für das Medium Netz gilt Gleiches. In den Freundschaftsportalen (Social Network Sites/SNS) wie Facebook, Schüler-/Studi-VZ u.a. finden junge Menschen neue Möglichkeiten der Gestaltung ihrer Kommunikation. SNS stellen ein Instrument zum dynamischen Kommunikations- und Beziehungsmanagement mit Gleichaltrigen dar. SNS können als ein vergleichsweise Erwachsenen-freier Raum begriffen werden, in der die Kontrolle durch Autoritäten (Eltern/ Lehrer) minimiert zu sein scheint. Als Folge entsteht eine ‚gefühlte Privatsphäre', in der man sich dem mitunter turbulenten Peer-Review meint überlassen zu können. Und SNS stellen weiterhin ein besonderes Experimentierfeld für mannigfaltige Möglichkeiten der Selbstdarstellung, -Inszenierung und Identitätsarbeit dar.

Prof. Dr. Klaus Neumann-Braun

Nach Lehr- und Forschungstätigkeiten an den Universitäten Freiburg, Trier, Frankfurt, Koblenz-Landau und Wien (Gastprofessur) ist Prof. Dr. Klaus Neumann-Braun seit 2005 Ordinarius für Medienwissenschaft am Institut für Medienwissenschaft (ifm) der Universität Basel und Autor zahlreicher Publikationen insbesondere zu den Themenschwerpunkten Medien- und Kommunikationssoziologie, Populärkulturanalysen, Publikumsforschung, Jugendmedienkulturforschung, Interpretative Methoden (Ethnographie, Visuelle Soziologie); zuletzt u.a. „Coolhunters – Jugendkulturen zwischen Medien und Mark", Frankfurt am Main: Suhrkamp 2005 (zus. m. B. Richard), "Die Bedeutung populärer Musik in audiovisuellen Formaten", Baden-Baden: Nomos 2009 (zus. mit Ch. Jost, D. Klug, A. Schmidt), "Doku-Glamour im Web 2.0: Party-Portale und ihre Bilderwelten", Baden-Baden: Nomos 2010 (zus. mit J. Astheimer).

Aufmerksamkeitsspirale und Zugzwänge des Mediums: Diese Optionen sind jedoch mit spezifischen Befürchtungen verknüpft: Wer nicht online ist und nichts von sich preis gibt, verpasst – so die Sorge vieler jungen Menschen - den Anschluss. Nur wer Inhalte einstellt, erhält auch Aufmerksamkeit und seinen Platz innerhalb der Community. Dem Wunsch, Teil einer Gruppe sein wollen und bei anderen Interesse an der eigenen Person wecken zu wollen, steht der Wunsch möglichst wenig von sich preiszugeben gegenüber. Ein ständiger — kräftemäßig sicherlich nicht unaufwändiger — Aushandlungsprozess was ‚gerade

noch geht' oder was schon zu viel ist scheint vonnöten.

Unterschiedliches/mangelndes Problembewusstsein und fehlender Weitblick: Was als Privat eingestuft wird bzw. mit wem man wann welche Inhalte teilen möchte variiert von Person zu Person beträchtlich und ändert sich in der Regel auch mit der Zeit. Was heute bzw. als Jugendlicher ‚witzig' erscheint, wird einige Zeit später möglicherweise als peinlich und unangemessen betrachtet. Fotos, die der eine akzeptabel findet und (selbst ohne böse Absicht) online stellt, stellen für den anderen einen Eingriff in dessen Privatsphäre dar. In diesem Feld unterschiedlicher Wertmaßstäbe und Kontrollvorstellungen seinen Weg zu finden ist eine schwierige Aufgabe, für die die jungen Menschen auf keine ‚klassischen' Vorbilder zurückgreifen können. SNS wurden bisher hauptsächlich von Jugendlichen und jungen Erwachsenen genutzt. Eltern bzw. LehrerInnen haben teilweise selbst kaum entsprechende Erfahrungen, Kenntnisse und Kompetenzen um zu einem sinnvollen Umgang mit den Angeboten anleiten zu können (s.u.). So gesehen sind die heutigen jungen Menschen in tragender Weise auf sich selbst gestellt.

Privacy Paradox: Durch die vorrangig Peer-Group-intern praktizierte Kommunikation entsteht teilweise das trügerische Gefühl, die Inhalte auf SNS wären privat und würden von Außenstehenden kaum wahrgenommen—- die (unsichtbare) Anwesenheit Unbefugter wird gerne ausgeblendet. Oft werden erst im konkreten Konfliktfall die Risiken der Verbreitung von Inhalten im Netz realisiert. Der Anschein einer gefühlten Privatheit steht im Widerspruch zur tatsächlichen Offenheit des Mediums.

Die Definition der **beiden zentralen Begriffe „privat" und „öffentlich**" hat sich offensichtlich in den vergangenen Jahren stark verändert. In der gegenwärtig sich stark wandelnden Gesellschaft haben sie weniger denn je für alle dieselbe Bedeutung. Gerade Jugendliche experimentieren damit, sich selbst zu ‚veröffentlichen' – nicht nur im Internet! – beispielsweise um Feedback zu erhalten, welches wiederum wie bereits erwähnt zu ihrer Identitätsbildung beiträgt.

Gegenläufige Interessen der Marktteilnehmer (SNS Anbieter und UserInnen): Die Interessen der Seitenbetreiber stehen zum Teil in starkem Widerspruch zu jenen der UserInnen. Während die Betreiber eine möglichst offene und reichhaltige Datenfreigabe präferieren, um profitabel wirtschaften zu können (Problem der Finanzierung von Open Source Softwareanwendungen), liegt es im Interesse der UserInnen, eher wenig von sich preiszugeben. Teilweise gehen die Anbieter hier mit fragwürdigen Methoden vor, aktuell bspw. zu sehen am Fall der neuen Sicherheitseinstellungen und Default Settings von Facebook. Man kann sich des Eindrucks nicht erwehren, dass generell eine (gezielte) technische und inhaltliche Überforderung von Jugendlichen etabliert wird. Die durchaus vorhandenen technischen Möglichkeiten, Inhalte vor den Augen Unbefugter verbergen zu können, sind zum Teil deutlich versteckt und unübersichtlich in den Einstellungen-Menüs positioniert. Generell sind die Unterschiede in Bezug auf die angebotenen Sicherheitseinstellungen zwischen den verschiedenen Sites sehr groß (Problem der Wahrnehmung dieser durch die User bei gleichzeitigem Gebrauch verschiedener SNS) und die Default Settings (Voreinstellungen der Profilfreigaben) nicht unbedingt im Interesse der UserInnen. Insbesondere die auf den SNS einsehbaren AGBs sind wenig User-freundlich und werden aufgrund ihres Umfangs und ihrer Komplexität nur von wenigen wirklich zur Kenntnis genommen.

Risikobedingungen und Gefahren im Internet – am Beispiel der SNS: Im Rahmen der Arbeit unserer Basler Forschungsgruppe „Jugendbilder im Netz" (s. den Forschungsblog www.netzbilder.wordpress.com) haben Nina Hobi und Ulla P. Autenrieth zahlreiche Gespräche mit Jugendlichen und jungen Erwachsenen über ihren Gebrauch von SNS durchgeführt und ausgewertet. In Einzelinterviews wie auch in Grup-

pendiskussionen wurden immer wieder die folgenden Chancen und Risiken genannt:

@ Fehlende Kontrollinstanz(en): Jugendliche können Inhalte ohne Gatekeeper (Redakteure/Eltern/Lehrer etc.) einem breiten Publikum zugänglich machen - jedoch:

@ Inhalte sind ohne wenn und aber öffentlich bzw. der Zugang zu diesen de facto nur schwer zu beschränken bzw. eingerichtete Beschränkungen sind teils einfach zu umgehen; die ‚gefühlte Privatheit' verhindert jedoch eine hinreichende Realisierung dieses Strukturprinzips

@ Inhalte sind leicht kopierbar und Verbreitung der Inhalte deshalb unkontrollierbar

@ Inhalte sind speicherbar, noch Jahre später können Daten wieder auftauchen, das Netz vergisst nichts

@ ‚Unfälle' sind nur schwer zu beheben (damit zusammenhängend der im Entstehen begriffene Markt für sog. Reputation Defender).

@ Peer Group *intern*: Cyberbullying/Mobbing/ verschiedene mitunter kontroverse Ansichten zu privaten Inhalten (Dissen)

@ Peer Group *extern*: Kontrollverlust über Daten und eingestellte Inhalte: Datenmissbrauch/Einblick Unbefugter (Marktforschung/Stalker/Chef/beruflicher Werdegang usf.).

Datenschutz und Persönlichkeitsrechte im Internet – was tun?

Herausforderung Medienkompetenz oder die mangelnde Internet-Kompetenz der über 35-Jährigen: Die über 35-Jährigen üben in ihren Rollen als Eltern, Lehrer und Politiker zentrale Erziehungs- und Vorbildfunktionen aus. Auch sind sie es, die Gesetze zum Umgang mit neuen Medien zu erlassen. Dass sie jedoch zu wenig über das Internet wissen, führt dazu, dass sie den Entwicklungen nicht selten recht unbedarft bis hilflos gegenüberstehen und Eltern oder Lehrer ihre Vorbild- und Anleitungsfunktion eben nicht hinreichend gekonnt wahrnehmen können. Die Medienkompetenz der Kinder und Jugendlichen beruht deshalb stärker auf den eigenen Erfahrungen im Netz als auf einer fundierten Aufklärung durch Eltern und Lehrer. Unter diesen Umständen muss es auch als kontraproduktiv angesehen werden, wenn ‚ahnungslose' Eltern und Lehrer trotzdem kontrollieren wollen, was Jugendliche online unternehmen und über sog. Fake-Profile in die SNS-Portale und die Profile ihrer Kinder resp. Schüler gelangen. Solche Aktionen werden von den Betroffenen als ein **fehlender Respekt für die Privatsphäre und persönlichen Belange von Jugendlichen** gewertet. Datenschutz – so die SNS-User - heißt auch, dass Eltern oder Lehrer die Profile ihrer Kinder und Schüler nicht ohne deren Einwilligung anschauen sondern den Schutz der Privatsphäre achten.

Wenn Elternhaus und Schule nur bedingt bei der Förderung der Internet-Kompetenz mitwirken, welchen Beitrag können dann öffentlich geförderte medienpädagogische Initiativen leisten? Die Quintessenz der Interviews mit Jugendlichen: **Tipps zum Umgang mit dem Internet gibt es zuhauf – das Problem ist nur, dass die Tipps (Broschüren) manches Mal an der Realität vorbei gehen.** Ein Beispiel: Dass in SNS die richtigen Namen angegeben werden, weil sie dazu dienen, dass man von Bekannten gefunden werden kann, ist eine Tatsache. Trotzdem empfehlen fast alle Tipp-Sammlungen, man sollte dies nicht tun. Wenn jeder unter (s)einem Pseudonym in SNS kommunizieren würde, käme jedoch keine Vernetzung zustande, da niemand mehr gefunden werden könnte, außer man gibt im offline-Leben den Nickname bekannt. Will man also das Prinzip der SNS nicht ad absurdum führen, sind Klarnamen in Profilen beinahe unumgänglich. Sinnvoller wäre der Ratschlag: in Communities, wo dies dem Normalfall entspricht, den eigenen Namen verwenden, aber mit allen anderen Daten sehr, sehr bewusst umgehen und sich eingehend mit den Privatsphäre-Einstellungen des Portals befassen.

Weiter wird von jungen Usern kritisiert, die **Tipps für Kinder und Jugendliche** seien oft in gekünstelter Jugendsprache gehalten. Dies führe ganz bestimmt nicht dazu, dass die Jugendlichen die Tipps besonders ernst nehmen würden, vor allem dann nicht,

wenn die Hinweise zusätzlich ihrer Realität (Fotos auf SNS sind gefährlich, nie mit Klarnamen anmelden, nie mit unbekannten Personen chatten usf.) widersprechen würden. Die plumpe sprachliche Anbiederung eines Broschüren-Satzes wie „Du findest, das Internet ist ´ne verdammt großartige Sache …" löst bei jedem normalen Kid und Teen in der Regel eine hohe „Anbiederungs-Alarmstufe" (O-Ton) aus. Naheliegende Frage: Wieso wird bei der Erarbeitung der Tipp-Sammlungen nicht mit den zukünftigen Rezipienten, den Kindern und Jugendlichen, eng zusammengearbeitet?

Notwendige Diskussionsfelder:

Interesse der Älteren und (offene) Kontrolle: Eltern und Lehrer sollten sich ohne Vorurteile und Abwertungen den Internetaktivitäten junger Menschen zuwenden, sich mit diesen über deren Internet-Surfen und Chatten usf. austauschen (was voraussetzt, dass sie sich auch selbst damit beschäftigen) und sich zeigen lassen, was die Jugendlichen selbst zeigen möchten! Grenzen sollten gemeinsam verhandelt und in der Folge dann auch akzeptiert werden. Kontraproduktiv sind Verbote und Kontrollversuche hinter dem Rücken der Jugendlichen. Kontrolle und Begleitung ist jedoch dann angezeigt, wenn Jugendliche im Netz gleichsam mit Haut und Haaren verloren gehen. Und hierbei zeigt sich, dass sich der Austausch ebenfalls unter Eltern und Lehrern sehr hilfreich auswirken würde: neue Kommunikationsprobleme lassen sich am besten kommunikativ lösen.

Das Thema Internetsicherheit sollte als Pflicht-Thema in der Lehrer-Ausbildung aller Schultypen und später auch in den Lehrplänen der Schulen Eingang finden. Wie wir Sprachen und Naturwissenschaften lehren und lernen sollte auch alles Entscheidende über die Medien der Kommunikation vermittelt und angeeignet werden.

Schließlich die Aufgabe der Marktteilnehmer - Schaffung von User-freundlichen AGBs: Wie bei der seinerzeitigen Klingelton-Streitfrage auch: Kinder und Jugendliche sollten nicht direkt zu unsinnigem Konsum gereizt werden und sie sollten auch nicht durch kleingedruckte, seitenlange, schwer verständliche Texte in Anhängen hinters Licht geführt werden. Ähnlich wie schon lange im Bereich der Fernsehwerbung praktiziert müssen Verbraucherschutz und Anbieter verantwortungsbewusst zusammenwirken, den Heranwachsenden einen Handlungsrahmen zu garantieren, der nicht einer versteckten Entmündigung und Vernutzung in die Hände arbeitet. Damit ist keinem gedient. Technisch gesehen ist unsere Gesellschaft sicherlich bereits umfassend im digitalen Zeitalter angekommen – kulturell gesehen jedoch nur in Maßen. Es gibt noch viel zu tun!

Datenschutz und Persönlichkeitsrechte im Web 2.0 –

An welchen Stellen muss angesetzt werden, um Datenschutz zu verbessern? Brauchen wir neue, strengere gesetzliche Regeln?

Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

„Web 2.0“, „Cloud Computing“, „Mobile Internet“, „Internet of Things“: Diese Begriffe stehen für dramatische Änderungen. Netbanking ist heute alltäglich, Schüler bewerten ihre Lehrer, ein wachsender Teil des Lebens spielt sich in sozialen Netzwerken ab und Handy-Nutzer können per Internet geortet werden. Die virtuelle Welt wird zunehmend real. Wird damit die Privatsphäre zum Auslaufmodell? Verschwinden unsere Persönlichkeitsrechte in einer virtuellen Wolke?

Wir dürfen die mit der rasanten technologischen Entwicklung, neuen Diensten und elektronischen Geschäftsmodellen einhergehenden Gefahren nicht ignorieren. Es gibt aber auch in diesem neuen Umfeld Stellschrauben zum Schutz persönlicher Daten: Rechtliche, technische und kulturelle.

Erneute, schon vielfach wiederholte Ratschläge an die Internet-Nutzer sind sicherlich sinnvoll, verhallen aber oft ungehört – aus Gleichgültigkeit, aus Unkenntnis oder Naivität. Als alleinige Erklärung für den virtuellen Daten-Striptease taugt dies jedoch nicht. Denn man darf nicht vergessen, dass ein soziales Netzwerk gerade dazu dient, sich selbst und seine Interessen zu präsentieren und neue Kontakte zu knüpfen oder alte zu pflegen. Und warum schreibt ein Blogger, wenn nicht, damit seine Berichte und seine Meinungen gelesen werden? Dies alles bedeutet zwangsläufig, dass man – wie auch immer wieder punktuell in der realen Welt - ein Stück seiner Privatsphäre preisgibt. Trotzdem ist der Umkehrschluss falsch, dass die Nutzer damit generell auf den Schutz ihrer Daten verzichten und sie jeglicher Verwendung durch Dritte überlassen.

Auch gut gemeinte Appelle an Anbieter sind nur begrenzt wirksam. Nach wie vor können viele soziale Netzwerke nur genutzt werden, wenn die Mitglieder bei der Anmeldung diverse persönliche Daten preisgeben, etliche davon obligatorisch. Dabei muss oft bezweifelt werden, dass alle diese Daten für die Teilnahme tatsächlich erforderlich sind. Noch immer sind die technischen Voreinstellungen vieler Netzwerke so konfiguriert, dass kein ausreichender Datenschutz gewährleistet ist. Schnell haben Nutzer jedoch vergessen, die Einstellungen den eigenen Wünschen entsprechend zu ändern. Datenschutzhinweise und sonstige Erklärungen sind mal spärlich, mal langatmig, teils schlecht verständlich und rechtlich zumindest zweifelhaft. Weder so noch so erreichen sie den eigentlichen Adressaten, den Nutzer. Und immer mal wieder versuchen Anbieter, den Mitgliedern ihres Netzwerks eine Einwilligung in die Nutzung ihrer Profildaten für Werbezwecke abzuringen, bisher jedoch ohne Erfolg. Denn spätestens bei solchen überfallartigen Aktionen haben nicht nur die Betroffenen überdeutlich ihren Unmut kundgetan.

Verbesserte Regeln zum Umgang mit persönlichen Daten könnten hier nachhelfen. Das Datenschutzrecht stammt ganz wesentlich aus der Offline-Welt

Peter Schaar

Diplom-Volkswirt, geb. 1954 in Berlin. Von 1980 bis 1986 in verschiedenen Funktionen in der Verwaltung der der Freien und Hansestadt Hamburg tätig, 1986 bis 2002 beim Hamburgischen Datenschutzbeauftragten. 2002 bis 2003 Geschäftsführer eines Datenschutzberatungsunternehmens, seit 2007 Lehrbeauftragter an der Universität Hamburg. Seit Dezember 2003 ist Schaar Bundesbeauftragter für den Datenschutz, seit 2006 auch Bundesbeauftragter für die Informationsfreiheit. Im November 2008 wurde er vom Deutschen Bundestag für weitere fünf Jahre im Amt bestätigt. Auszeichnungen: Preis der Friedrich-Ebert-Stiftung „Das politische Buch 2008“ für das Buch Das Ende der Privatsphäre; „eco Internet AWARD 2008“, Sonderpreis der deutschen Internetwirtschaft.

oder der Frühphase des Internet und muss dringend modernisiert werden. „Datenschutz 2.0" ist angesichts der vielfältigen Verknüpfungen von realen und virtuellen Aktivitäten aber mehr als die Forderung nach einem eigenen Internet-Datenschutzgesetz. Denn die allgemeinen Datenschutzbestimmungen gelten schon heute auch für das Netz. Und das eigens für Online-Dienste geschaffene Telemediengesetz enthält Vorgaben für die Anbieter darüber, wie sie mit den Daten der Nutzer umgehen sollen. Diese Regelungen müssen aber auf den aktuellen Stand gebracht werden. Allein auf nationaler Ebene lassen sich Datenschutzbestimmungen heute nicht mehr durchsetzen. Damit sie wirksam werden, brauchen wir auch einen verbesserten internationalen Rahmen für den Umgang mit personenbezogenen Daten.

Gesetzliche Regelungen müssen nachhaltig sicherstellen, dass bei verschiedenen technologisch möglichen Alternativen die datenschutzfreundlichste auszuwählen ist, vor allem indem man so wenig persönliche Daten verarbeitet wie möglich. Am Anfang stehen daher allgemeine Regeln und Prinzipien, die sich auch bei fortschreitender technischer Entwicklung und neuen Diensten konkretisieren und anwenden lassen. Auch die Idee eines technischen Verfallsdatums für elektronisch gespeicherte Daten entbehrt nicht eines gewissen Charmes. Bei näherem Hinsehen stellt sich aber heraus, dass sie sich nur schwer umsetzen lässt. Ein Verfallsdatum kann nur dann wirksam werden, wenn alle Beteiligten sich daran halten.

Die Anbieter müssen zu datenschutzfreundlichen Voreinstellungen ihrer Dienste verpflichtet werden. So sollten die in soziale Netzwerke eingestellten Daten nur dann öffentlich zugänglich werden, wenn der Nutzer sie freigeschaltet hat.

Der Staat sollte sich beim Umgang mit persönlichen Daten vorbildlich verhalten. Die in den vergangenen Jahren eingeführten Befugnisse der Sicherheitsbehörden gehören deshalb auf den Prüfstand. Die Vorratsdatenspeicherung von Telekommunikationsdaten erhöht die Datenhalden statt sie abzubauen. Deshalb sollte auf sie verzichtet werden.

Die Verwertung persönlicher Daten muss strikt begrenzt werden, d.h. außerhalb des von den Betroffenen bestimmten Kontextes dürfen sie nicht verwendet werden, auch dann nicht, wenn der Betroffene sie über das Internet zugänglich gemacht hat. Die Bildung von Persönlichkeitsprofilen durch Zusammenführung von Daten hinter dem Rücken der Betroffenen ist zu unterbinden.

Klarere Transparenzregelungen und geeignete technische Mittel müssen es dem Nutzer erleichtern, seine Datenschutzrechte wahrzunehmen. Etwa indem die Anbieter verpflichtet werden, Kerninformationen über den Umgang mit persönlichen Daten an prominenter Stelle ihres Web-Auftritts zu platzieren und mit passenden Beratungsangeboten den Nutzer zu unterstützen. Die Betroffenen sollten auch ein Recht auf elektronische Einsichtnahme in die über sie gespeicherten Daten erhalten.

Schließlich führt kein Weg daran vorbei, dass auch die Nutzer sich verantwortlich verhalten, denn schließlich sind sie im Web 2.0 nicht bloß Konsumenten sondern auch Anbieter von Informationen – über sich selbst und über andere. Wer die Vorteile interaktiver Dienste in Anspruch nimmt, muss auch die Rechte und die Privatsphäre Dritter respektieren. Deshalb sollten die Regelungen zum Schutz der Privatsphäre – insbesondere das Datenschutzrecht - auch dann gelten, wenn Privatnutzer Informationen über Dritte veröffentlichen. Auch die Schulen und Hochschulen müssen sich verstärkt diesem Thema zuwenden.

Internetsicherheit

Klaus Staeck,
Präsident der Akademie der Künste, Berlin

Wir reden von „Internetsicherheit“ und sind doch eigentlich ahnungslos. Ahnungslos, was mit unseren persönlichen Daten geschieht, die wir freiwillig oder unfreiwillig Tag für Tag mit beinahe jedem Mausklick preisgeben. Ahnungslos aber auch, was sich an pornographischen, rassistischen, Hass predigenden, die Geschichte verfälschenden und betrügerischen Inhalten ohne Einschränkung abrufen lässt.
Wir freuen uns an schnellen Google- oder ebay-Ergebnissen und unser Misstrauen wird nicht einmal geweckt, wenn nach drei Einkäufen per Internet das Angebot auf dem Bildschirm erscheint: „Das könnte Sie auch noch interessieren!“. Die Suchmaschine, die meine Interessen kennt. Nur noch ein Schritt und aus Argwohn wird Vertrauen.

Aber es geht um mehr, manchmal auch um Schlimmeres.

Für eine Recherche über Neonazi-Seiten im Netz und über die Wachsamkeit, mit der YouTube angeblich „bedenkliche Inhalte“ löscht, sobald die Plattform davon erfährt, erhalte ich statt dessen von YouTube immer neue Empfehlungen in Sachen Nazipropaganda. Nach „Waffen-SS in Feindesland“, ein schon 36.000 mal von Nazi- und Militaria-Freaks aufgerufener Marsch mit Filmeinspiel, hatte ich gar nicht gefragt. Er wird mir ohne Zugangssperre offeriert und ich bekomme nur ein paar Klicks weiter als Zugabe noch perfidere Kostproben, diesmal zum Beispiel aus der italienischen Neonazi-Szene, wo auch antisemitische Karikaturen erscheinen – das Portal gibt immer neue Ratschläge bis irgendwann einer meiner Klicks vor einer Schranke endet: „Dieses Video ist in Deinem Land nicht verfügbar.“ Doch was stattdessen empfohlen wird, steht dem Gesperrten kaum nach, es marschieren Hitlerjungen unter Hakenkreuzfahnen und Gesängen nach Nürnberg. Einen Link zu diesem Video erhält man auch über „Metapedia, die alternative Enzyklopädie“. Hier, beim tiefbraunen Pendant zu Wikipedia, gibt es Naziungeist pur. Im Impressum wird „NFSE media AB, Sweden“ als Urheber genannt. Offenbar eine sichere Adresse um weltweit in 11 Sprachen mit ungebrochener, aufgefrischter Naziideologie zu wirken. Horst Wessel bekommt eine Heldenbiographie wie einige hundert andere sogenannte „Blutopfer“. Rassenideologie wird hemmungslos verbreitet als hätte es den Holocaust nie gegeben. Dieser wird statt dessen als „Schuldindustrie“ und „Shoah-Business“ diffamiert, für die Relativierung des Massenmords verweist ein Link auf den Leugner Garaudy. Mit mehr als 7000 deutschen Artikeln, von teilweise erheblichem Umfang und eifrig aktualisiert, folgen wir nach 83.000 (!) ungarischen vor 5.000 englischsprachigen auf dem zweiten Platz.

Wenn wir über Sicherheitskonzepte für das Internet reden, dann sollten wir nicht nur an leichtfertig ins Netz gelangte Familienfotos und Kontonummern denken. Sicherheit heißt auch, für eine weltweite

Klaus Staeck

wurde am 28. Februar 1938 in Pulsnitz/Sachsen geboren, aufgewachsen in Bitterfeld. Nach dem Abitur 1956 Übersiedlung nach Heidelberg. Jurastudium in Heidelberg, Hamburg und Berlin. Daneben Beginn der Arbeit als politischer Grafiker. Seit 1969 Zulassung als Rechtsanwalt. Mehrfach Teilnahme an der documenta. Seit 1982 Mitglied im P.E.N.-Zentrum, seit 1986 Gastprofessor an der Kunstakademie Düsseldorf. Mehr als 3000 Einzelausstellungen. Preise u.a.: 1979 Kritikerpreis, 1996 Gustav-Heinemann-Bürgerpreis. Seit 1990 Mitglied der Akademie der Künste, Berlin. 2006 Wahl (2009 Wiederwahl) zum Akademie-Präsidenten. (Ausführliche Biografie unter www.staeck.de)

Ächtung von Hass-Propaganda und Nazi-Inhalten im Internet einzutreten. Wer als Betreiber und Autor solcher Portale ausfindig gemacht wird, muss einer weltweiten Verfolgung sicher sein. Hier endet die „Freiheit der Andersdenkenden“, wenn diese eine freie Gesellschaft insgesamt bedroht.

Datenschutz als Bildungs- und Erziehungsaufgabe

Edgar Wagner,
Landesbeauftragter für den Datenschutz Rheinland-Pfalz

I. Weshalb ist Datenschutz nicht nur eine Gesetzgebungs- und Kontrollaufgabe sondern auch eine Bildungs- und Erziehungsaufgabe?

Analysiert man die Datenschutzsituation der letzten Jahre, ist auf der Seite der Bürgerinnen und Bürger ein mangelndes bzw. **mangelhaftes Datenschutzbewusstsein** festzustellen und auf der Seite des Staates und der Wirtschaft eine ausgeprägte **Datengier**.

1. Das mangelhafte Datenschutzbewusstsein der Menschen kommt zum einen im **Datenexhibitionismus** zum Ausdruck, der für das Internet kennzeichnend ist, vor allem für die dortigen sozialen Netzwerke, die wiederum der vorläufige Höhepunkt einer jahrzehntelangen Entwicklung sind. Diese hatte ihren ersten Anschub von den 68ern erhalten und deren Zuwendung zu Werten wie Autonomie und Selbstverwirklichung. Es folgten öffentliche Bekundungen privatester Angelegenheiten wie etwa das öffentliche Bekenntnis von einigen Hundert Frauen, abgetrieben zu haben. Dem schlossen sich Fernsehformate an wie Big Brother mit der Dauerbeachtung des Privatlebens einer Handvoll Frauen und Männer über mehr als 100 Tage. Zu Massenphänomen und zu Datenexhibitionismus wurde diese Entwicklung – wie gesagt – mit dem Internet und vor allem mit den darin angebotenen sozialen Netzwerken.

Dieser Datenexhibitionismus wird auf Bürgerseite außerdem ergänzt durch eine Haltung, die man mit **„Daten-Verramschen"** umschreiben könnte. Für geringe Versprechungen sind viele bereit, persönliche Daten zwar nicht der Öffentlichkeit, aber der Wirtschaft zur Verfügung zu stellen: Für zwei Prozent Rabatt den Betreibern von Kundenkarten und für eine kleine Gewinnchance den Veranstaltern von Gewinnspielen. Persönlichen Daten wird nicht der Wert zuerkannt, der ihnen zusteht. Eher werden sie als wertlose oder minderwertige Ware angesehen, die man zu Schleuderpreisen verhökert.

Dass der Datenexhibitionismus und das Daten-Verramschen kein Datenschutzbewusstsein entstehen lassen, liegt auf der Hand. Dies wird auch bestätigt durch einschlägige Untersuchungen. Eine Studie der Europäischen Kommission aus dem Jahre 2008 zeigt, dass das Datenschutzbewusstsein der Bundesbürger im Vergleich zu den Einwohnern der Nachbarstaaten mit am schlechtesten ausgeprägt ist. Nur 20 % der Deutschen haben danach eine vage Ahnung davon, welche Datenschutzrechte ihnen die Gesetze einräumen. Noch schlechter sind eigentlich nur noch die Werte der Österreicher. Dem entspricht es, dass nach einer Studie von Microsoft

Edgar Wagner

Am 27. Mai 1950 in Mainz geboren, begann er 1970 sein Jurastudium in Mainz und Göttingen, legte er 1976 das erste Staatsexamen ab und begann sein Referendariat beim Oberlandesgericht Koblenz. Nach dem zweiten Staatsexamen im Jahr 1978 wurde er Richter am Verwaltungsgericht Mainz. 1980 wechselte er in den Wissenschaftlichen Dienst des rheinland-pfälzischen Landtags und wurde dort im Jahr 1994 dessen Leiter. In dieser Funktion war Wagner zugleich stellvertretender Direktor beim Landtag. Im Jahr 2001 wurde Wagner Leiter der Abteilung Informationsdienste, Presse- und Öffentlichkeitsarbeit. In der Plenarsitzung am 14. März 2007 wurde er mit Unterstützung aller im Landtag vertretenen Fraktionen zum Nachfolger von Prof. Dr. Walter Rudolf gewählt. Seine Amtszeit begann am 15. April 2007 und endet am 14. April 2015.

Deutschland aus dem Jahre 2008 nur jeder zweite Internetnutzer die Datenschutzbestimmungen von Internet-Dienstanbietern durchliest, wobei unsere Erfahrungen dahingehen, dass es in Wirklichkeit noch viel weniger sind. Auch das zeigt das Desinteresse vieler Internetnutzer am Datenschutz. Das sehen die Betroffenen selbst so. Nach der o.g. Studie der Europäischen Union meinten 77 % aller Befragten, dass das Bewusstsein für den Datenschutz nur sehr gering ausgeprägt sei.

Es ist also auch ein Mythos, dass die „Online-Generation besonders kompetent im Umgang mit dem Internet sei. Nach den einschlägigen Studien haben nur rund ein Drittel der 18 bis 24-Jährigen gute Anwendungsfertigkeiten. Der Rest ist mit komplexen Webanwendungen überfordert, bevorzugt einfache Applikationen oder lässt es ganz bleiben. Letzteres gilt vor allem für den Selbstdatenschutz.

2. Auf der Seite von Staat und Wirtschaft stellen wir dagegen eine ausgeprägte **Datengier** fest. Für die Wirtschaft sind die persönlichen Daten der Bürgerinnen und Bürger ein wichtiges Wirtschaftsgut, die Voraussetzung für Umsatz und Gewinn. Beim Staat sind die Daten Voraussetzung, um staatliche Zwecke erfüllen zu können. Der Staat benötigt als Sozialstaat Daten und er benötigt sie als Sicherheitsstaat auch. Als solcher holt er sich die Daten, wo immer er sie findet: Beim Bürger, notfalls aber auch – die Vorratsdatenspeicherung zeigt es – bei der Wirtschaft.

3. Mit der überkommenen Datenschutzsystematik ist dem mangelndem Datenschutzbewusstsein und der ausgeprägter Datengier nicht beizukommen, zumal sich beide gegenseitig noch verstärken, da mangelndes Datenschutzbewusstsein die Datengier von Staat und Wirtschaft nur noch erhöht. Außerdem kann Datenschutzbewusstsein den Bürgerinnen und Bürgern nicht verordnet werden und die Datengier der Wirtschaft nicht normativ gesättigt werden. Die Diskussion um die gesetzliche Verschärfung des Adresshandels hat dies gezeigt. Und was den Staat selbst anbelangt: Ein „informationelles self-restraint“ ist zwar in den Datenschutzgesetzen für die datenverarbeitenden Stellen als Programmsatz ausgestaltet, aber für die Gesetzgeber im Bund und in den Ländern eben kein Verfassungsgrundsatz.

Ein vernünftiger Umgang mit den persönlichen Daten muss den Bürgerinnen und Bürgern, der Wirtschaft und dem Staat deshalb auf andere Weise nahegebracht werden: Ein Weg ist eben die Bildung und Erziehung der Bürgerinnen und Bürger.

4. Diese Notwendigkeit ergibt sich auch noch aus einem anderen, einem dritten Grund. Er hängt mit der rasanten Entwicklung der Informations- und Kommunikationstechnologie zusammen. Das Internet als ein weltweit und zentral organisiertes Netz lässt steuernde Eingriffe und Reglementierungen der Staaten nur noch im beschränkten Umfange zu. Und selbst dort, wo nationale Gesetze noch Regelungsansätze bieten, lassen sie sich nur sehr eingeschränkt durchsetzen. Denn – so formulierte es Prof. Roßnagel schon Mitte der 90er Jahre – „die staatliche Hoheitsgewalt stößt im immateriellen Raum globaler Netzwerke an ihre Grenzen“.

Und selbst dort, wo diese Grenzen vielleicht noch nicht erreicht sind, wird die staatliche Hoheitsgewalt von vielen – vor allem von jugendlichen – Nutzern des Netzes rigide in Frage gestellt. Die Freiheit im Netz ist das Ziel der digitalen Revolutionäre. So ist der staatliche Schutzauftrag im Netz zum einen technologisch begrenzt und zum anderen gesellschaftlich in Frage gestellt. Wenn der Staat seine Bürger aber nicht mehr ausreichend schützen kann, wird es Zeit für ein ergänzendes Schutzkonzept.

Dies sind im Wesentlichen die Gedanken, die Prof. Roßnagel bereits Mitte/Ende der 90er Jahre formuliert und entwickelt hatte, um das Prinzip des Selbstdatenschutzes zu legitimieren und zu

begründen. Seine Gedanken treffen auch heute noch zu. Wahrscheinlich kann man sagen, dass sich seine Problembeschreibung sogar noch verschärft hat, wenn man an die rasante Entwicklung der Informationstechnologien denkt. Ich nenne nur das Stichwort „Internet der Dinge" und in diesem Zusammenhang die RFID-Technologie.

II. Was ist unter Datenschutz zu verstehen, wenn man ihn als Bildungsaufgabe begreift? Wie könnte ein Bildungsprogramm „Datenschutz" aussehen?

Sicherlich geht es bei einer entsprechenden Bildungsaufgabe nicht, jedenfalls nicht in erster Linie, um den Inhalt der zahllosen allgemeinen und bereichsspezifischen Datenschutzgesetze des Bundes und der Länder. Sie haben überwiegend nicht die Bürgerinnen und Bürger zum Adressaten, sondern die datenverarbeitenden Stellen und damit den Staat und die Wirtschaft. An sie wenden sich die Datenschutzgesetze. Sie haben deshalb auch den Vollzug dieser datenschutzrechtlichen Ordnung sicherzustellen.

Gleichwohl hat der Staat natürlich auch dafür zu sorgen, dass die Bürgerinnen und Bürger von diesen Regeln – wie von den sonstigen Gesetzen auch – erfahren. Dafür sind die Gesetzgeber im Rahmen ihrer Öffentlichkeitsfunktion unter Einbeziehung der Medien ebenso verpflichtet, wie die exekutiven Vollzugsorgane im Rahmen ihrer Informationsarbeit. Andere – auch nicht staatliche Stellen – beteiligen sich an dieser Aufklärungsarbeit, etwa die Verbraucherschutzorganisationen.

Aber das ist nicht mit Bildungsarbeit, nicht mit dem Datenschutz als Bildungsaufgabe, gemeint. Diese Aufgabe hat einen anderen Gegenstand. Bei ihr geht es um das Grundrecht bzw. die Grundrechte selbst, also um das informationelle Selbstbestimmungsrecht im Allgemeinen und in diesem Kontext auch um die vom Bundesverfassungsgericht in seiner Online-Entscheidung betonten informationstechnischen Systeme. Bildungsarbeit in dem hier zu behandelnden Sinne hat also die Aufgabe darauf hinzuwirken, dass jeder Einzelne verantwortungsvoll von diesen Rechten und von diesen Systemen Gebrauch machen kann. Im Mittelpunkt der Bildungsaufgabe „Datenschutz" steht also die **informationelle Selbstverantwortung**. Alles, was an Wissen und Einsicht notwendig ist, um diese Selbst- und Eigenverantwortung wahrnehmen zu können, gehört deshalb zu den datenschutzrechtlichen Bildungs- und Erziehungszielen. Das bedeutet im Wesentlichen ein Dreifaches:

- Erstens: Das informationelle Selbstbestimmungsrecht und das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme müssen vermittelt werden, ihr Inhalt, ihre Ableitung aus der Privatsphäre und ihre Bedeutung für den Einzelnen und die Gesellschaft.
- Zweitens: Über die Gefahren, die diesen Rechten drohen, muss ebenso aufgeklärt werden und zwar zuförderst über die Gefahren im Internet, aber natürlich auch über die Gefahren in der realen Welt. Es muss klar sein, wo Datenspuren hinterlassen werden, wer diese Datenspuren lesen kann und welche Konsequenzen dies für jeden Einzelnen zur Folge haben kann.
- Drittens und vor allem: Es muss vermittelt werden, welche Möglichkeiten die Bürgerinnen und Bürger haben, um diesen Gefahren selbst begegnen zu können. **Selbstdatenschutz** ist in diesem Zusammenhang das Stichwort, das von Prof. Roßnagel bereits Mitte der 90er Jahre in die datenschutzrechtliche Diskussion eingeführt worden war. Nur das schleswig-holsteinische Landesdatenschutzgesetz hat diesen Gedanken bisher ausdrücklich in den Gesetzestext aufgenommen. Von vielen Datenschutzbeauftragten wurden allerdings rechtliche, technische und organisatorische Maßnahmen zum Selbstdatenschutz entwickelt. Sie finden sich als Orientierungshilfen oder Handreichungen im Internet. Dort können sie heruntergeladen

werden. Man kann sie auch in Fachaufsätzen nachlesen. Aber wer tut dies? Notwendig ist es also, diese Konzepte – und die vielen Initiativen, die es auch von anderer Seite gibt – nicht nur zu entwickeln, sondern auch dort bekannt zu machen, wo sie bekannt sein müssen: bei den Bürgerinnen und Bürgern.

Mit dem Datenschutz als Bildungsaufgabe reagieren wir aber nicht nur auf Defizite. Diese Aufgabe ist auch ein Gebot unserer Zeit. Der Umgang mit virtuellen Welten ist Teil der Lebenswirklichkeit in einer digital geprägten Kultur. Vor allem für die junge Generation spielt sie eine wesentliche Rolle bei ihrer Sozialisation, ihrem Freizeitverhalten, ihrer Selbstfindung und ihrer Identität und ihren Beziehungen zur Welt. Die Vorstellung vor allem jugendlicher Mediennutzer von persönlicher Identität, von Privatheit und Intimität, von informationeller Selbstbestimmung und Persönlichkeitsrechten unterliegt einem steten Wandel – auch im Spannungsfeld mit berechtigten ökonomischen Interessen, der freien Meinungsäußerung und auch dem Sicherheitsbedürfnis der Bürgergesellschaft und des Staates. In diesem Prozess des Wandels ist es wichtig, für das Thema Datenschutz zu sensibilisieren, das Problembewusstsein bei den an Bildung und Erziehung Beteiligten zu schärfen und diese Fragestellung nachhaltig in formalen Bildungsprozessen zu verankern. Ein effektiver und zeitgemäßer Datenschutz ist eine der Grundlagen der Bürgergesellschaft und eines demokratischen Staates und bedarf der nachhaltigen Vergewisserung im Diskurs der Schule, des Elternhauses und der breiten Öffentlichkeit. Er ist eine Zukunftsaufgabe, die angesichts der stürmischen medialen Entwicklung einer permanenten Vergewisserung und Anpassung auf der sicheren Grundlage verbriefter Verfassungsgebote und -aufträge bedarf.

Der FSM-Verhaltenskodex

für Betreiber von Social Communities im Spannungsfeld zwischen Jugendschutz und Datenschutz

Sandra Walter, Justitiarin, Freiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM)

Im März 2009 verabschiedeten die reichweitenstärksten deutschen Social Community-Betreiber VZnet Netzwerke Ltd., Lokalisten Media GmbH und wer-kennt-wen.de GmbH unter dem Dach der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM) einen Verhaltenskodex[1], der den Jugendschutz, Datenschutz und Verbraucherschutz in den deutschen Angeboten der beteiligten Anbieter deutlich verbessert.

Dieser Verhaltenskodex ist das jüngste Beispiel einer Reihe von Branchenstandards, die von der FSM initiiert wurden. Die FSM arbeitet seit 12 Jahren aktiv an der positiven Gestaltung und zukunftsorientierten Weiterentwicklung des Jugendmedienschutzes und ist die einzige nach dem Jugendmedienschutzstaatsvertrag anerkannte Einrichtung der Freiwilligen Selbstkontrolle für Telemedien in Deutschland. In den vergangenen Jahren haben viele Mitgliedsunternehmen zusammen mit der FSM auf freiwilliger Basis Verhaltenskodizes entwickelt, um die Belange des Jugendschutzes bei Suchmaschinen, im Mobilfunk, in Chatdiensten, im Teletext und bei Social Communities noch intensiver zu verfolgen.

Von den vereinbarten Regelungen des Verhaltenskodex für Social Communities profitieren derzeit ca. 30 Millionen Nutzer von schuelerVZ.net, studiVZ.net, meinVZ.net, lokalisten.de und wer-kennt-wen.de. Der Unterzeichnung vorausgegangen waren mehrere Monate intensiver Beschäftigung mit dem Thema in einer FSM Arbeitsgruppe. Die Anbieter und die FSM entwickelten dabei, ungeachtet der wettbewerblichen Stellung der Unternehmen, Branchenstandards für Social Communities, die in vielen Regelungen über die gesetzlichen Verpflichtungen hinausgehen.

Das Ergebnis ist der **„Verhaltenssubkodex für Betreiber von Social Communities bei der FSM“**, ein 17-seitiges Dokument mit mehr als 50 fixierten Einzelmaßnahmen.

Sandra Walter
Rechtsanwältin und seit 2002 Justitiarin der Geschäftsstelle der FSM. Zu ihren Tätigkeiten gehörte u.a. die langjährige Arbeit als Beauftragte der FSM Beschwerdestelle. Seit 2008 verantwortet sie den Bereich Web2.0 und hat die Erarbeitung des Verhaltenskodex für Social Communities geleitet. Beisitzerin der BPjM ist Sandra Walter seit 2005.

Der Untertitel „Jugendschutz und Datenschutz in Social Communities“ weist schon deutlich daraufhin, dass neben den natürlich fokussierten Jugendschutzaspekten auch Datenschutzfragen involviert sind.

Innerhalb des Verhaltenskodex werden zunächst allgemeine Grundsätze für den Betrieb der Dienste festgelegt - hier sind beispielsweise umfangreiche Regelungen über Aufklärungsmaßnahmen zu erwähnen. Zudem werden auch konkrete Vorgaben zur Gestaltung der einzelnen Dienste gemacht, so zum Beispiel für die Erstellung von Profilen in der Community oder zum Upload von Daten. Im Folgenden wird beispielhaft erläutert, welche jugendschutzrechtlichen Grundsätze den Verhaltenskodex ausmachen. Darüber hinaus werden die Aspekte diskutiert, die auch den Belangen des Datenschutzes Rechnung tragen bzw. die sich in einem Spannungsverhältnis mit dem Datenschutz befinden.

Ein typischer Konfliktpunkt zwischen Datenschützern und Jugendschützern besteht in der Frage der Nutzung von Social Communities unter realem Namen oder anonym bzw. pseudonym. Während sich Datenschützer für die anonyme oder pseudonyme Nutzung aussprechen, sehen Jugendschützer in der Nutzung von Klarnamen Vorteile für den Schutz Minderjäh-

riger. Durch das Agieren unter dem realen Namen werden Hemmschwellen aufgebaut, sich in der Community sozial inadäquat zu verhalten. Ferner werden durch die Maßnahme die positive Atmosphäre und auch die soziale Selbstkontrolle innerhalb der Plattform gestärkt. Darüber hinaus wissen Minderjährige genauer, mit wem sie es in der Social Community kommunizieren und möglichen pädophil veranlagten Personen wird es in Folge der Authentizität eines Netzwerks erschwert, Kontakt zu Minderjährigen aufzunehmen. Grundsätzlich läuft eine strikte anonyme Nutzung auch dem generellen Konzept eines Netzwerkes – nämlich der Auffindbarkeit von und der Interaktion zwischen realen Personen – zuwider. Aus diesen Erwägungen entschieden sich die in der FSM vereinigten Anbieter in dem Verhaltenskodex für die stärkere Betonung des Jugendschutzes und damit für eine Förderung der Nutzung von Social Communities unter realem Namen. Eine anonyme Nutzung wird durch die Plattformen jedoch nicht sanktioniert, so dass auch den Vorgaben des Datenschutzes Rechnung getragen wird.

Eine ganz zentrale Regelung des Verhaltenskodex ist die Verpflichtung der Nichtauffindbarkeit von Profilen der unter 16-Jährigen durch externe Suchmaschinen. Diese Einstellung ist auch durch die Nutzer nicht veränderbar. Mit dieser Maßnahme werden Informationen, die jüngere Nutzer über sich in der Community preisgeben, sehr effektiv geschützt. Leider ist diese Maßnahme bei vielen sozialen Netzwerken kein Standard, die Mitglieder der FSM besetzen hier eine Vorreiterposition.

Weiterhin ist im Verhaltenskodex geregelt, dass der Auslesbarkeit von Profildaten über 16-Jähriger durch Suchmaschinen widersprochen werden kann. Jedoch gehen in der gelebten Praxis alle drei beteiligten Anbieter von Social Communities in diesen wichtigen Punkten bereits über den Verhaltenskodex hinaus und gestalten ihr Produkt noch abgeschlossener, als die Selbstverpflichtung fordert: Sie schließen eine Auffindbarkeit aller Nutzerprofile durch externe Suchmaschinen generell aus.

Zudem ist geregelt, dass bei Nutzern unter 14 Jahren standardmäßig strengere Privatsphäreeinstellungen vorliegen, so dass die Profildaten grundsätzlich nur für Freunde sichtbar sind und eine weitergehende Freischaltung nur aktiv durch den Nutzer selbst erfolgen kann. Aus Gesichtspunkten des Jugendschutzes sind die unter 14-Jährigen einerseits besonders schutzwürdig. Andererseits stellt eine generelle Nichtauffindbarkeit das Grundrecht auf informationelle Selbstbestimmung von Minderjährigen, aber auch das Entstehen und Bestehen von zwischenmenschlicher Vernetzung in Social Communities, in Frage.

Um die Nutzer zu befähigen selbst aktiv zu werden, verpflichten sich die Betreiber der Communities dazu, eine deutlich sichtbare Ignorierfunktion gegenüber anderen Nutzern und eine Meldefunktion für regelwidriges Verhalten vorzuhalten. Außerdem besteht die Verpflichtung, eine deutlich wahrnehmbare Möglichkeit zur Löschung des Nutzerprofils anzubieten und mit der Abmeldung dann automatisch Fotos, Videos und weitere vom Nutzer hochgeladene Dateien zu entfernen. Durch diese Maßnahme greift die Vermutung, dass das Internet nichts vergisst, für die beteiligten Communities nicht.

Die Maßnahmen zur konkreten Gestaltung der einzelnen Dienste innerhalb der Community werden durch Aufklärungsmaßnahmen zur besseren Sichtbarkeit der Regelungen flankiert und darüber hinaus wird die Aufklärung als zentrales Element zur Sensibilisierung der Nutzer begriffen.

Diese Beispiele zeigen deutlich, dass sich der Jugendmedienschutz und der Datenschutz nicht grundsätzlich ausschließen, sondern sich in einer fruchtbaren Zusammenarbeit gegenseitig ergänzen können. In Fällen, in denen die Rechtsgüter divergierende Maßnahmen von den Anbietern fordern, wird versucht eine praxistaugliche Lösung zum Wohle des Nutzers zu entwickeln, die beiden Rechtsgütern Rechnung trägt.

[1]Abrufbar unter www.fsm.de/de/Web_2_0

[2]Siehe Beschluss des Düsseldorfer Kreises der Datenschutzbeauftragten vom 17./18.April 2008 unter http://www.datenschutz-berlin.de/content/deutschland/duesseldorfer-kreis bzw. http://www.datenschutz- berlin.de/attachments/487D__sseldorfer_Kreis_April_2008_Datenschutzkonforme_Gestaltung_sozialer_Netzwerke.pdf?1212737975

Spuren im Netz –
Die Perspektive des Jugendmedienschutzes

Verena Weigand, Leiterin der Stabsstelle Kommission für Jugendmedienschutz (KJM)

Das Web 2.0 macht es kinderleicht, Informationen zu verbreiten und zu bearbeiten, Kontakte herzustellen und sich auszutauschen. Man stellt sich selbst dar – und hinterlässt Spuren. Diese viel genutzten Möglichkeiten des Mitmach-Netzes haben Auswirkungen auf die ganze Gesellschaft, aber auch auf jeden Einzelnen: So müssen die Grenzen von Öffentlichkeit und Privatheit neu definiert werden. Und das Individuum steht vor der Herausforderung, seine Identität im Netz managen zu müssen. Eine nicht ganz einfache Aufgabe, denn die Interaktivität des Netzes birgt neben vielen Chancen auch Risiken, vor denen vor allem Kinder und Jugendliche geschützt werden sollten. Für die Einhaltung der gesetzlichen Bestimmungen im Jugendmedienschutz-Staatsvertrag (JMStV), der erstmals privaten Rundfunk und Telemedien unter einem Aufsichtsdach zusammenfasst, ist seit 2004 die Kommission für Jugendmedienschutz (KJM) zuständig.

Neben den vielen unzulässigen und entwicklungsbeeinträchtigenden Internet-Inhalten (Pornografie, Volksverhetzung, problematische Foren) stehen dabei die vielfältigen kommunikativen Features des Web 2.0 immer mehr im Fokus der Aufsicht: Denn hier werden junge Nutzer häufig angepöbelt, gemobbt oder gar sexuell belästigt. Das ist nicht zuletzt deshalb möglich, weil sie ihre Daten, Fotos und Videos oft unbekümmert preisgeben, etwa in beliebten Social Communities (schülerVZ, Lokalisten, u.ä.). Oder die jugendliche Unbekümmertheit wird schlichtweg missbraucht, um Geld zu machen: So sind findige Anbieter von Online-Spielen jetzt auf die Idee gekommen, Jugendliche das Spielen mit ihren Daten statt mit Geld bezahlen zu lassen – um nur ein Beispiel zu nennen. Das Langzeitgedächtnis des Netzes und die Tatsache, dass über einmal ins Netz gestellte Daten problemlos fremd verfügt werden kann, lassen die jungen User dabei gerne außer Acht.

Verena Weigand

Referentin für Jugendschutz und Medienpädagogik der Bayerischen Landeszentrale für neue Medien (BLM) und stellvertretende Vorstandsvorsitzende der Stiftung Medienpädagogik Bayern. Daneben ist sie u.a. Vorstandsvorsitzende des Vereins Programmberatung für Eltern e.V., Vorstandsmitglied des Vereins Internet-ABC, Mitglied des Advisory Board des deutschen Safer Internet Centre, stellvertretendes Mitglied des Vergabeausschuss Games der Bayerischen Staatsregierung und Fachbeirätin der Stiftung Zuhören. Zuvor war sie als Autorin und Redakteurin bei Jugendzeitschriften und Fachverlagen tätig, arbeitete als wissenschaftliche Mitarbeiterin an der Ludwig-Maximilians-Universität München und leitete ein gymnasiales Tagesheim. Sie studierte Erziehungswissenschaften, Psychologie, Jura, Buchwissenschaft und Verlagswesen.

Die KJM kritisiert, dass viele Plattformen diesen Daten-Striptease fördern – etwa indem sie eine freie Verfügbarkeit für alle Zugreifenden als Profilvoreinstellung angeben. Weder thematisieren sie den Umgang mit persönlichen Daten hinreichend, noch gibt es Sicherheitsvoreinstellungen. Dazu kommt, dass die Datenschutzerklärungen oder AGBs in vielen Fällen sehr ausführlich und unverständlich formuliert sind. Bei internationalen Plattformen muss man sich gar in englischer Sprache mit diesen schwierigen Themen beschäftigen.

Außerdem thematisieren Anbieter die kommerzielle Nutzung und den Verkauf personenbezogener Daten häufig zu wenig. Die allermeisten Plattformen haben generell ein kommerzielles Interesse, machen das aber nicht transparent.

Die Situation des Jugendmedienschutzes ist – gerade beim Medium Internet und insbesondere in Bezug

auf Web 2.0-Anwendungen – hoch komplex. Zwar unterliegen auch Web 2.0-Inhalte den Regelungen des JMStV. Allerdings befinden sich Anbieter von interaktiven Plattformen, die ausschließlich oder überwiegend die technischen Voraussetzungen für die Einstellung von sogenanntem „user-generated content" oder Kommunikationsfeatures zur Verfügung stellen, in einer rechtlichen Sondersituation. Sie sind zunächst nur für die eigenen Inhalte verantwortlich. Host- oder Access-Provider können für Fremdinhalte – um die es in den allermeisten Fällen auf Plattformen geht – nach bisheriger Rechtslage nur zur Verantwortung gezogen werden, wenn sie von den problematischen Inhalten Kenntnis haben. Dann müssen sie die Inhalte entfernen. Technische Zugangskontrollen müssen sie erst umsetzen, wenn üblicherweise problematische Inhalte zugänglich gemacht werden und die Maßnahmen für den Anbieter zumutbar sind. Ein weiterer Punkt, der die Aufsicht erschwert, ist, dass viele der Anbieter von großen Portalen im Ausland sitzen und so die deutschen gesetzlichen Grundlagen nicht greifen. Aufgrund der Flüchtigkeit der Inhalte, die für die Aufsicht eine besondere Herausforderung darstellen, sind Präventivmaßnahmen durch die Anbieter grundsätzlich Erfolg versprechender.

Deshalb hat die KJM bereits im September 2004 zehn Netz-Regeln formuliert, die unter www.kjm-online.de abrufbar sind. Sie skizzieren Regelungen einer wünschenswerten Selbstregulierung, ergänzen die gesetzlichen Regelungen und Richtlinien und werden derzeit – gemeinsam mit der Freiwilligen Selbstkontrolle Multimedia (FSM) und den Internet-Anbietern – weiterentwickelt. In Bezug auf den Datenschutz fordern sie:

„Der Anbieter, der personenbezogene Daten erhebt, trägt dafür Sorge, dass den Interessen von Kindern und Jugendlichen nicht geschadet oder deren Unerfahrenheit ausgenutzt wird. Der Anbieter beachtet bei der Gestaltung seines Angebotes, dass Kinder und Jugendliche im Umgang mit personenbezogenen Daten noch unerfahren sind und trägt dazu bei, sie für einen sorgfältigen Umgang mit ihren Daten zu sensibilisieren. Der Anbieter unternimmt das ihm technisch und organisatorisch Mögliche, um personenbezogene Daten von Kindern erst dann zu erheben, wenn Eltern zugestimmt haben oder zumindest in Kenntnis gesetzt wurden. Der Anbieter erhebt persönliche Daten von Kindern (Daten, die Eigenschaften von Kindern beschreiben, ohne bereits personenbezogen zu sein) nur in begründeten Einzelfällen nach vorherigem Warnhinweis. Dieser Grundsatz soll auch nicht durch attraktive Gewinnspiele unterlaufen werden."

Normal

Dieter Willinger,
Web-Projektmanager und Konzeptionist, ausgestiegen.com

Ich wäre gern normal. Dann würde ich Apple super finden. Dann würde ich von Social Media predigen und es verkaufen. Dann würde ich Facebook nutzen. Dann wäre ich eben normal. So wie die Mehrheit der Menschen. Bin ich aber nicht. Ich finde Apple nicht toll, halte die aufgeblasenen Versprechen von Social Media Beratern nicht aus und Facebook nutze ich auch nicht. Stattdessen finde ich Linux gut, glaube an die Prinzipien von Open Source und habe ausgestiegen.com gemacht. Ich bin eben nicht normal. Und gehöre damit zur Minderheit. Und ich würde manchmal gerne nicht zum zehnten Mal erklären, warum Apple eigentlich nicht so toll ist, was es mit dem Thema Datenschutz bei Facebook auf sich hat und warum ausgestiegen.com als Scherz begonnen hat. Ein Scherz in einer "sozial medialisierten" Welt. Anachronistisch, nämlich eine Website ohne Login und Freundschaftsanfrage. Beinahe schon asozial, weil ich ohne "XYZ gefällt das"- Zustimmungen auskommen muss. Bestenfalls gibt es Gedanken zum Nachlesen. Und das war es schon. Keine Third-Party-Applikationen, denen ich mit dem Zustimmen der Nutzungsbedingungen meine Profilinformationen und Freundschaftsbeziehungen frei Haus liefere. Keine Instrumentalisierung meiner Freunde, die mich wieder zur Nutzung überreden sollen. Kein Zwang jemals wieder überhaupt die Seite aufzusuchen. Isoliert in einer vernetzten Welt, die der Information hinterher hechelt als wäre es der Treibstoff, der den Motor am Laufen hält. Und waren es früher Lokalblätter, die den Bedarf an Informationen aus der unmittelbaren physischen Umgebung bedient haben, ist die Einheit weiter runter gebrochen worden auf den Freund, den Kollegen, den unbekannten anderen User. Ich könnte nämlich etwas verpassen. Ich könnte nicht Teil haben an diesem oder jenen Ereignis. Ich könnte zurück bleiben. Ich könnte einen ökonomischen Vorteil durch Nicht-Teilnahme verlieren.

Dieter Willinger
1978 geboren, lebt und arbeitet in Niederösterreich und Wien als Web-Projektmanager und Konzeptionist. Er inszenierte seinen Ausstieg aus Facebook und XING mit der Website ausgestiegen.com, die innerhalb des letzten Jahres in Deutschland, Österreich und der Schweiz mediales Echo hervorgerufen und zur Diskussion über soziale Netzwerke beigetragen hat.

Bild: Christoph Haiderer - www.christophhaiderer.com

Ich könnte übrig bleiben. Ich könnte Angst haben, mit mir allein. Angst haben ist normal. Angst davor schlecht da zu stehen, eine Nachricht zu verpassen oder Ansprüchen meiner Freunde und Kollegen nicht gerecht zu werden. Es ist aber nicht normal, wenn diese Angst normal wird. Und das passiert. Öfter als man denkt. Und das ist der Punkt, wo ich dann doch manchmal ganz gern nicht normal bin.

Datenschutz – what else?

Christian Wirsig,
Communications Manager, Kaspersky Lab

Über 350 Millionen Nutzer haben ein Facebook-Konto, laden pro Monat rund 1 Milliarde Bilder und 10 Millionen Videos hoch und wissen meist nicht, was mit ihren Daten passiert. Doch Datenschutzprobleme tauchen nicht nur im "Mitmach-Web" auf, denn im Internet lassen sich verschiedenste Quellen einfach verknüpfen – das betrifft jeden Online-Nutzer.

George Clooney ist etwas Besonderes. Nein, diesmal ist nicht gemeint "besonders gutaussehend", sondern er ist besonders vorsichtig im Umgang mit Daten im Internet. Denn Clooney gehört zu den wenigen Stars, die mit sozialen Netzwerken auf Kriegsfuß stehen. So hat er sich kürzlich als Facebook-Hasser geoutet [1], während seine Kollegen Tod & Teufel in sozialen Netzen und Microblogging-Diensten wie Twitter veröffentlichen. Doch Datenschutz und Privatsphäre im Internet sind auch für Otto-Normal-Nutzer derzeit heiß diskutierte Themen. Der Grund: Vor allem soziale Netzwerke wie Facebook und StudiVZ boomen [2], was mit den eingestellten Daten passiert, ist aber allzu oft unklar. Kürzlich hat Facebook-Chef Mark Zuckerberg in einem Interview [3] die Privatsphäre im Internet als alte Konvention bezeichnet. Hintergrund: Facebook hatte kurz vorher die Datenschutzeinstellungen für seine Nutzer so verändert, dass private Informationen über die Facebook-Suche einfacher gefunden werden können. Diese laxere Haltung gegenüber privaten Daten sei nur eine Reaktion auf Veränderungen in der Gesellschaft, erklärte der Facebook-Chef. Fazit: Sie können sich als Internet-Nutzer nicht darauf verlassen, dass die Anbieter von Web-Diensten schon dafür sorgen werden, dass Ihre Daten geschützt bleiben. Sie müssen selbst aktiv werden.

Christian Wirsig
ist seit Januar 2006 bei der Kaspersky Labs GmbH tätig. Zunächst war er als Marketing-Redakteur für Broschüren und Artikel verantwortlich, seit Anfang 2008 betreut er als Communications Manager Central Europe die interne und externe Kommunikation des Unternehmens in Deutschland, Österreich und der Schweiz.

Die Welt entblößt sich

Neben Communities sind auch Homepages oder ein eigener Blog ein gefundenes Fressen für alle Neugierigen. Gefühle, Stimmungen, Ansichten, alles das kriegt man in den Online-Tagebüchern brühwarm und ungefiltert serviert. Dabei sollte dem Verfasser klar sein, dass auch Personalverantwortliche oder Arbeitskollegen auf den Blog stoßen können. Selbst Blogs, die bei einer Google-Recherche nicht gleich zu finden sind, können einfach aufgestöbert werden. Wer etwa eine Mail-Adresse mit eigener Domain nutzt, der kann sich sicher sein, dass www.die_angegebene_domain.de von Empfängern ausprobiert wird. Meist ist dann der Blog nicht weit entfernt.

Heiße Diskussionen

Aber die Diskussion um Datenschutz ist schon so alt wie das Web selbst. Schon lange vor den sozialen Netzwerken und Web 2.0 haben sich Communities mit klassischer Forenfunktion einen Namen gemacht, in denen Nutzer meist Hobbys diskutieren. Den gleichen Ansatz gibt es seit Jahrzehnten in Usenet. Im Hinterkopf sollte man auch dabei haben: Wer in Foren ohne Pseudonym und vielleicht noch mit Foto

allzu wild vom Leder zieht, der kann sich selbst schaden. Denn die Beiträge sind für die Web-Ewigkeit gespeichert. Selbst wenn man als Nutzer einen Beitrag per Foren-Software entfernen kann, taucht er meist immer noch im Cache von Suchmaschinen auf. Auch auf den Beruf können sich solche Netzaktivitäten auswirken, denn der Einsatz von Internet-Tools hat bei Personalern zugenommen. Gut ein Drittel nutzt schon seit Jahren regelmäßig Google & Co. im Rahmen eines Such- und Auswahlprozesses [4]. Um allgemeine Informationen über die Kandidaten zu gewinnen, setzen knapp 30 Prozent das weltweite Netz grundsätzlich immer ein, Tendenz steigend.

Internet gefühlsecht

Auch Partnersuche, Reiseplanung und Einkäufe verlagern sich ins Web. Daran ist zwar nichts Verwerfliches, aber die Angaben bei Flirt-Börsen sind so ziemlich das Persönlichste, was man im Web finden kann. Selbst wenn der Anbieter selbst seriös ist und Ihre Daten schützt, kann ein geklautes Passwort dazu führen, dass diese Daten in falsche Hände geraten. Ebenso verhält es sich bei Online-Reisebüros oder allgemein Online-Shops, in denen etwa schon Kreditkartendaten, Suchprofile oder Interessen hinterlegt sind. Das ist einerseits bequem, weil man mit einem Mausklick bezahlen kann, andererseits kann jeder, der den Zugang knackt auch auf Ihre Kosten einkaufen.

Finden Sie sich selbst

Doch wie kann man den Fluss der Informationen über sich selbst eingrenzen? Als erstes sollten Sie prüfen, wie es um Ihren Online-Ruf bestellt ist. Eine einfache Google-Suche nach sich selbst verrät viel. Welche Profile in sozialen Netzwerken tauchen auf? Wo ist der Link zur privaten Homepage? Vielleicht erscheinen auch Links auf Webseiten Ihres Arbeitgebers. Schnell kriegen Sie einen Eindruck, was man auf die Schnelle über Sie in Erfahrung bringen kann. Wichtig: Sehen Sie sich auch mögliche Verknüpfungspunkte an: So kann man die private Adresse aus dem Homepage-Impressum einfach bei Google Maps eingeben und sich kinderleicht einen Eindruck über Ihre Wohngegend verschaffen. Übrigens können Nutzer von Google-Diensten neuerdings schnell rausfinden, was Google über Sie weiß: Das Dashboard (https://www.google.com/dashboard) zeigt es im Überblick an. Neben Google kann auch ein Besuch bei www.yasni.de nicht schaden. Die Personensuchmaschine wird etwa gerne von Personalberatern genutzt. Sie listet Telefonbucheinträge, Amazon-Wunschzettel, Xing-Profile und weitere Quellen auf.

Daten nachträglich löschen

Unerwünschte Daten im Internet haben sogar schon für das Entstehen einer neuen Dienstleistung gesorgt, dem Online-Reputation-Management. Dabei ist man sich einig, dass es besser ist, erst gar keine unerwünschten Daten zu veröffentlichen. Ist das Kind aber in den Brunnen gefallen, gibt es mehrere Möglichkeiten. Bei Telefonbucheinträgen oder Nutzerprofilen auf sozialen Netzwerken können Sie selbst aktiv werden: Hier reicht meist eine Mail oder ein Fax an den Anbieter oder man kann die Veröffentlichungseinstellungen selbst bearbeiten. Nicht mehr genutzte Accounts bei Web-Diensten kann man meist beim Betreiber löschen lassen. Schwieriger wird es bei Suchmaschinen. Zwar müssen Google & Co. Löschanträge prüfen, nur weil man selbst einen Eintrag als unpassend empfindet, ist aber noch kein Grund dafür, dass dieser Eintrag verschwindet.

Richtiges Verhalten

Wichtiger ist es, in Zukunft das richtige Maß für persönliche Daten im Internet zu finden. Richtig ist der Mittelweg zwischen Hardcore-Gezwitscher und Berghütte ohne Internet-Verbindung: Wer mit Freunden über Facebook Kontakt halten will, der kann das auch guten Gewissens tun. Man sollte sich aber die Zeit nehmen und die Einstellungen zur Privatsphäre prüfen. Dort ist aufgelistet, wer welche Informationen sehen kann. Im Zweifelsfall sollten Sie bei der Angabe und Herausgabe von Infos erst einmal konservativ sein, Schweigen ist hier wirklich

Gold. Wichtig: Achten Sie auch darauf, dass Ihre Freunde genauso umsichtig mit Daten umgehen, denn schnell ist man bei Facebook auf Fotos markiert und taucht in Videos auf.

Bei den meisten Web-Shops ist zwar das Zahlen via Kreditkarte üblich, die Daten sollten Sie aber nicht beim Anbieter hinterlegen. Geben Sie sie nur über eine sichere Internet-Verbindung ein. Sicherer ist natürlich die Bezahlung per Nachnahme oder Rechnung. Auf den ersten Blick praktische Funktionen wie ein öffentlicher Wunschzettel bei Amazon sollten Sie auch immer kritisch sehen, denn so kriegt jeder mit, welchen Hobbys Sie nachgehen. Im Zweifel verzichten Sie einfach auf den Wunschzettel im Web und schreiben eine Mail mit Wünschen.

Passende Schutz-Software

Eine aktuelle Schutz-Software ist für alle Internet-Nutzer Pflicht, vor alle aber für die, die auch viel im Mitmach-Web unterwegs sind. Denn schnell nistet sich sonst ein Schädling ein, der Zugangsdaten zu sozialen Netzwerken und anderen Diensten abgreift. Neben einem Schutzpaket wie Kaspersky Internet Security gehört aber auch eine leistungsfähige Passwort-Verwaltung mit zum Pflichtprogramm. Denn wer kann sich sonst schon zufällig erzeugte Passwörter mit Sonderzeichen, Ziffern sowie Groß- und Kleinschreibung merken? Komfortabel funktioniert hier etwa der Kaspersky Password Manager.

[1] www.people.com/people/article/0,,20304800,00.html

[2] www.facebook.com/press.php#/press/releases.php?p=133917

[3] www.ustream.tv/recorded/3848950

[4] www.bdu.de/presse_321.html

Unternehmen verführen Kinder und Jugendliche mit Gewinnspielen zur Preisgabe ihrer Daten im Internet

Dr. Theo Wolsing, Verbraucherzentrale NRW

Viele Unternehmen unterlaufen gesellschaftliche Bemühungen, Kinder für einen sparsamen Umgang mit ihren personenbezogenen Daten im Internet zu sensibilisieren. Sie bieten zwar kindgerechte Online-Beiträge an, beim Datenschutz nutzen sie häufig die Unerfahrenheit der Mädchen und Jungen aus. Oftmals hat man sogar den Eindruck, als ob bereits Unter-Zehnjährige genauso wie Erwachsene mit Gewinnspielen geködert und zur Preisgabe ihrer Daten bewegt werden sollen.

Diesen Eindruck konnte man bei einer Sichtung von elektronischen Adventskalendern 2009 gewinnen. Diese seit über 100 Jahren bei Kindern beliebte vorweihnachtliche Beschäftigung, findet immer mehr Verbreitung auch im Internet. Hinter verschlossenen Türen verbargen sich nicht etwa gute Ratschläge oder Süßigkeiten. Hier winkten veritable Attraktionen wie Brett- und PC-Spiele, Play-Station, Beauty Cases und andere begehrte Artikel. Tagesgewinne im Wert von über 100 Euro waren keine Seltenheit.

Mädchen und Jungen verfügen über geringe geschäftliche Erfahrungen. Sie reagieren spontaner und emotionaler als Erwachsene. Deshalb sind an Angebote wie Adventskalender im Internet höhere Anforderungen zu stellen als an Attraktionen für geschäftsfähige Personen. Das gilt insbesondere in Bezug auf einen sparsamen Umgang mit personenbezogenen Daten. Bei einem Gewinnspiel reicht es völlig aus, nach der E-Mail-Adresse und ggf. einem Kennwort der Teilnehmer zu fragen. Für eine Gewinnbenachrichtigung sind keine weiteren Angaben erforderlich. Selbst wenn Veranstalter von Gewinnspielen die Daten der Teilnehmer anschließend vernichten, geht die Sammlung personenbezogener Daten, wie Anschrift oder Altersangabe zu weit. Die Gefahr ist nämlich groß, dass Kinder die Abfrage solcher Daten für normal halten und dies auch bei anderen Gelegenheiten so handhaben, wenn der Seitenbetreiber weniger seriös mit Kundendaten umgeht.

Dr. Theo Wolsing
Leiter der Stabsstelle Informationsmanagement in der Verbraucherzentrale NRW, 1987 – 1999 Mitglied der Rundfunkkommission der Landesanstalt für Rundfunk NRW, 1996 – 1998 Mitglied einer Arbeitsgruppe der Europäischen Kommission zur Vorbereitung des Programms „Safer Internet Action Plan", Mitglied der Expertenkommission „Klicksafe Preis für Sicherheit im Internet".

Dass man mit Minimalangaben an einem Gewinnspiel teilnehmen kann, haben leider nur zwei der untersuchten Kalender (pombaer.de und wendy.de) bestätigt. Bei allen anderen Kalendern mussten Kinder zusätzlich mindestens Vor- und Zuname sowie ihre Anschrift angeben. Fehlte eine der Angaben, war eine Teilnahme am Gewinnspiel nicht möglich.

Vier der 12 untersuchten Kalender (bruder.de, kinder.de, polly pocket.de und bravo.de) verlangten verpflichtend Geburtsdatum bzw. Alter, bei zwei weiteren war die Altersangabe freiwillig, bei dreien die der Telefonnummer. Dass die Datensammelwut der Betreiber von Kinderadventskalendern ähnlich groß ist wie die von den Anbieten herkömmlicher Gewinnspiele, zeigte auch die Tatsache, dass acht Veranstalter die Kinder dazu einluden, ihren Newsletter zu abonnieren.

Eine Information darüber, was mit ihren Daten geschieht, konnten kindliche Besucher häufig nicht oder nur mit unvertretbarem Aufwand feststellen. Lediglich vier der 12 Adventskalender klärten die Teilnehmer in transparenter Weise über die Daten-

nutzung auf (fruchttiger.de, pombaer.de, pferdeundponny.de sowie just4girls.de). Sie erklärten in kindgemäßer Sprache, dass sie die Angaben nur im Zusammenhang mit dem Gewinnspiel verwenden wollten. Vier weitere Seitenbetreiber (bravo.de, bruder.de, mickymaus.de und wendy.de) gaben im Umfeld des Anmeldeformulars keinerlei Hinweis darauf, wie sie die Daten der Kinder zu verwenden gedachten. Während man auf einer Internetseite (bravo.de) auf Umwegen erfahren konnte, dass im Zusammenhang mit Gewinnspielen gesammelte Daten nur für die Benachrichtigung genutzt würden, müssen Teilnehmer an den Gewinnspielen der drei anderen Adventskalender damit rechnen, nach Weihnachten mit Werbemüll zugeschüttet zu werden.

Bei vier weiteren Adventskalendern (hallohund.de, maedchen.de, pollypocket.de und kinder.de) fanden sich zwar ebenfalls Datenschutzhinweise, sie waren aber entweder so versteckt angebracht, dass Kinder sie in der Regel nicht finden. Oder aber sie waren in lupenreinem Juristendeutsch formuliert, sodass kein Junge oder Mädchen etwas damit anzufangen weiß. Formulierungen wie „Ich stimme den Gewinnspiel-AGB zu“ (hallohund.de) sind nicht kindgemäß, vor allem dann nicht, wenn sich dahinter zehn Seiten Text verbergen und sich die Datenschutzhinweise erst nach einem Klick auf einen weiteren Link öffnen.

Besonders dreist war das Vorgehen der als „Familienportal“ firmierenden Seite „kinder.de“. Sie hatte im Teilnahmeformular die Einverständniserklärung bereits voraktiviert und ganz am Ende der Seite tatsächlich doch darauf hingewiesen, dass „der Teilnehmer …. weiterführende Informationen zu den Produkten, Herstellern oder Vertreibern (erhält), sofern er die Einverständniserklärung angeklickt hat.“

Die Beispiele zeigen, dass die unternehmerische Verantwortung Kindern gegenüber nicht besonders ausgeprägt ist. Vielmehr bleibt festzuhalten, dass Kinderadventskalender die Teilnehmer zu einer unkritischen Weitergabe ihrer Daten ermuntern. Jungen und Mädchen werden frühzeitig „sozialisiert“, möglichst viel von sich preiszugeben. Kinder erleben, bevor sie die Tragweite überhaupt richtig erfassen können, vielfach das „volle Programm“ des Marketing, ohne dem etwas Adäquates entgegensetzen zu können. Attraktive Preise tun ein Übriges: Nicht nur Kinder geben angesichts enormer Gewinne schon aus (falsch verstandener) Dankbarkeit gern ihre Daten weiter.

Wer als Eltern Wert darauf legt, dass ihre Kinder ein sparsamen Umgang mit personenbezogener Daten lernen, sollte seine Sprösslinge selbst von so harmlos anmutenden Angeboten wie Kinderadventskalender eher fernhalten.

Interview mit dem Youth Panel

Mit Bastian (14), Peter (16), Brian (15), Niklas (15), Melissa (14), Karolina (15), Lilian (14)
Interview: Stefanie Rack und Eva Borries, klicksafe

Interviewer: In welchen Sozialen Netzwerken seid ihr, und seit wann?

Alle: SchülerVZ, Facebook, MySpace, Twitter, wkw, YouTube.
Lilian: SchülerVZ seit 2007. Facebook seit Ende Oktober.
Melissa: Facebook hab ich auch erst seit neuestem.
Karolina: Facebook seit Dezember 2009, bin gerade erst eingeladen worden.
Niklas: Ich bin auch noch bei schüler CC.

I: Wo seid ihr am Aktivsten und warum?

Melissa: Facebook, wegen den Spielen, die ich da spielen kann, wie z.B. Farmville.
Peter: Ich check schülerVZ regelmäßig um zu gucken, ob man neue Freunde oder Nachrichten hat, ob es neue Pinnwandeinträge gibt oder ob man gegruschelt worden ist.
Lilian: Facebook seit Kurzem, weil ich da die Leute treffen kann, die ich beim Youth Panel Meeting in Luxemburg kennen gelernt hab. Und auch wegen den Spielen.
Karolina: Ich mach viel auf MySpace. Ich hab da eine Supportpage. Und auf Twitter schreib ich mit meinen Leuten.

I: Was ist das, eine Supportpage?

Karolina: Ich stell halt Bilder von Stars hoch, rede mit anderen Leuten was die gut finden, mach da auch Singcontest oder so.

I: Weißt du, welche Bilder von den Stars du rechtlich nehmen kannst und welche nicht?

Karolina: Ich weiß das eigentlich schon. Ich schau immer auf Plattformen wo steht, dass man die verwenden kann. Ich bearbeite die Bilder auch meistens selbst nochmal, also mach einen Rahmen drum oder so. Welche Bilder man nicht hochladen darf, wie z.B. pornografische Bilder, das steht bei jedem Upload dabei.

Youth Panel
klicksafe *realisiert seit Januar 2009 an einem Gymnasium in Rheinland-Pfalz das* ***Youth Panel*** *des deutschen Safer Internet Centre, eine Internet-Arbeitsgruppe, die alle 14 Tage statt findet. Es geht in dieser AG darum, dass Jugendliche Auskunft über Internetthemen geben, die sie beschäftigen. Was machen sie beispielsweise in Sozialen Netzwerken, welche Gefährdungspotentiale erkennen sie im Netz? Welche Gefahren sehen sie z.B. auch für jüngere Schüler? Wie repräsentieren sie sich selbst im Web 2.0 (Selbstdarstellung in Social Communities)? Welche Anwendungen tätigen sie? Wie oft, wie lange? Welche „Trends" realisieren und nutzen sie? Was wünschen sie sich für das Web in Zukunft? etc. Die Jugendlichen sind hier Botschafter und Trendscouts ihrer eigenen Generation.*

I: Hat sich euer Verhalten, was den Schutz eurer Daten angeht, verändert im Lauf der Zeit?

Peter: Man wird mit der Zeit irgendwie vorsichtig, man hört ja auch eine ganze Menge was passieren kann. Das Interesse an den Plattformen lässt mit der Zeit automatisch nach.
Niklas: Ich hab von Anfang an mein Profil klein gehalten. Am besten man verwendet Spitznamen oder kürzt den Nachnamen ab.
Brian: Das Geburtsdatum wird noch angegeben damit andere zum Geburtstag gratulieren können.
Bastian: Mein Vater hat mit drauf geguckt, als ich meine Seiten in den Social Communities erstellt habe, deswegen habe ich von Anfang an nichts angegeben.
Melissa: Also am Anfang hatte ich bei schülerVZ alles mögliche, Bilder und alles. Aber mit der Zeit wurd alles irgendwie doof, da kamen dann auch dumme

Kommentare und so. Und dann war es ja auch mal so, dass irgend jemand schülerVZ gehackt hatte und sich die Bilder geklaut hat. Deshalb hab ich dann die Bilder alle wieder runter genommen und mein Profil bearbeitet.

I: Wie bearbeitet?

Melissa: Ich hab auf jeden Fall weniger von mir hingeschrieben, also MSN- und ICQ-Nummer rausgenommen und es so gemacht, dass nur meine Freunde alles sehen können.

I: Von wem kamen eigentlich die dummen Kommentare?

Melissa: Von Leuten, die mich geaddet hatten und die ich aber eigentlich gar nicht kannte. Jungs vor allem, so 17-Jährige. Die wollten sich dann auch treffen. Das war mir dann zu viel.

I: Und was genau hast du dann gemacht?

Melissa: Ich hab die wieder aus meiner Freundesliste rausgeschmissen.

I: Und wie ist das bei dir, Lilian?

Lilian: Eigentlich hat sich mein Profil nicht sehr verändert, außer, dass man jetzt meinen Nachnamen nicht sehen kann. Ich wusste vorher nicht, wie man das abkürzen konnte, also das mit dem Initial, aber dann haben mir das Freunde gezeigt. Jetzt steht da sogar gar nichts mehr, nur Lilian.

I: Warum wolltest du den Nachnamen nicht mehr haben?

Lilian: Eigentlich auch wegen dem Hackerskandal und es hilft eigentlich auch nicht viel bei der Suche.

I: Wenn dich jemand sucht, wie findet der dich dann? Über die Schule?

Lilian: Ja, auch, oder ich suche die Leute selbst. Oder meistens durch Freunde.

I: **Welche Einstellungen macht ihr für eure Sicherheit? Oder macht ihr überhaupt welche?**

Niklas: Ja, klar. Meine Seiten sind nur sichtbar für Freunde. *(Bastian und Peter stimmen zu.)*
Brian: Ich habe keine Ahnung, was ich eingestellt habe. Keinen Plan. Ich hab mich damit noch nie beschäftigt.
Lilian: Ich hab da eigentlich gar nichts von mir drin!

I: Warum nicht?

Lilian: Ich find's überhaupt insgesamt nicht so wichtig, dass man so viel über sich erzählt, wenn man sich zum Beispiel mal in einem Chat unterhält, dann erfährt man eigentlich viel mehr.

I: Und warum machen das dann die ganzen Leute?

Melissa: Na ja, die wollen halt auffallen.
Karolina: Ich hab jetzt auch weniger Bilder online. Ich find inzwischen, das geht niemanden an. Jetzt will ich das nicht mehr. Wenn ich mich mit jemandem gut versteh, dann schicken wir uns Bilder zu.

I: Bei welchen Handlungen im Netz denkt ihr an die Sicherheit eurer Daten oder: denkt ihr überhaupt an die Sicherheit eurer Daten?

Niklas: Man macht sich irgendwie immer Gedanken, man weiß ja wie das Internet ist…
Melissa: Früher hab ich nicht so drüber nachgedacht, da wusste ich auch noch nix darüber, dass man Sachen klauen kann usw. und da war mir das alles auch egaler. Aber inzwischen, was man so hört, was man so alles Mieses machen kann…

I: Was kann man denn so machen?

Melissa: Also Bilder klauen und so, dann kann es auch sein, dass sich jemand als dich ausgibt und Falsches über dich schreibt.
Lilian: Letztens hab ich mir eine neue E-Mailadresse gemacht und da wollten die wissen, was ich für eine Telefonnummer hab und auch meine Adresse, da hab ich dann was erfunden. Ich finde, das geht die

nix an. Nicht, dass die meine Sachen an Dritte weitergeben und wer weiß, was noch so alles passiert. Ich werd eh schon so zugespamt.

I: Wieso glaubst du, dass Daten an Dritte weitergegeben werden können?

Lilian: Also, da war kein Kasten oder kein Schild wo drauf stand, dass sie das nicht machen.

I: Habt ihr schon mal was von Datenschutzerklärung gehört? Die steht immer bei den AGB. Lest ihr sowas?

Lilian: *(seufzt)* Ja, ich les aber immer nur die erste Hälfte und dann lass ich das.
Melissa: Ich les immer die Überschriften und wenn mich die interessieren, dann les ich auch den Text dazu.

I: Wisst ihr darüber Bescheid, dass Drittanwender auch Informationen über euch sammeln können, selbst wenn ihr sie nicht selbst frei gegeben habt?

Melissa: Das wusste ich noch nicht.
Karolina: Ich wusste das schon; das geht mir dauernd so. Wenn ich jetzt z.B. auf eine Seite gehe, wo man z.B. voten kann, dann fragen die, ob du willst, dass die Seite auf deine Seite zugreifen kann… Die spammen halt immer meine Freunde zu, wenn ich eine Frage beantwortet hab, daran bin ich auch schon gewöhnt, ich krieg halt auch immer die ganzen Spam-Mails von meinen Freunden, die wollen, dass ich das Quiz mach.

I: Wo ist das?

Karolina: Bei Twitter mach ich das.

I: Habt ihr schon mal selbst negative Erfahrungen mit Abzocke, Datenklau oder Persönlichkeitsrechtsverletzungen gemacht?

Niklas: Ich hab mich mal blöderweise bei einer Internetseite angemeldet und dann eine Email bekommen und hatte so ein Abo für 99Euro für SMS an der Backe. Meine Mutter hat dann einen Brief mit einer Kopie meines Kinderausweises nach China (!) geschickt und die Sache war geklärt.
Melissa: Es gibt auch Leute auf unserer Schule, die gemobbt wurden im Internet. Da gab's Beleidigungen im Internet und bei MSN und dann ist das in der Schule weitergegangen und alle wussten das. Das ist von Klasse zu Klasse weitergegangen.

I: Was macht man dann?

Melissa: Wenn ich weiß, wer das ist, dann würd ich zu dem gehen und mit dem reden. Oder erstmal mit den Eltern.
Karolina: Von mir gab es auch einmal ein Fake-Profil, das hat ein Freund von mir gesehen, der hat mich gefragt, ob das stimmt was da drauf steht, dass ich in so einen Michael verliebt sein soll, den kannte ich gar nicht. Dann hat der Freund von mir das den Betreibern gemeldet, dass das Profil ein falsches Profil ist, und dann haben die das Profil runter genommen.

I: Und, hat dich das verletzt?

Karolina: Mich hat das schon verletzt und vor allem war ich verwundert. Ich hab mich gefragt, warum gerade ich.

I: Habt ihr sonst noch Fälle erlebt, wo das Recht am eigenen Bild verletzt wurde, also z.B. Bilder oder Videos unerlaubt verwendet wurden?

Bastian: Es hat mal jemand einen Link rumgeschickt von einer Internetseite von einem Typ, der hat eine Internetseite eingerichtet nachdem er mit seiner Ex Schluss hatte und hat Nacktbilder von der reingestellt… Voll übel.
Melissa: Bei einer Freundin von mir wurden Bilder geklaut und verunstaltet, im Endeffekt war das aber dann doch ein Freund, da hatten die zu der Zeit Stress. Das haben die dann unter sich geklärt und es wurde wieder runter gestellt.
Lilian: Bei mir war mal was, aber nicht so schlimm. Ich war mit einer Freundin schwimmen, dann haben wir Bilder gemacht und die Freundin von mir hat die Bilder online gestellt. Da hab ich sie gebeten, die wieder runter zu nehmen. Besser wäre schon gewe-

sen, wenn sie mich vorher gefragt hätte.
Lilian: Wir hatten da auch noch einen Fall mit unserer Klassenlehrerin. Wir hatten da ne Halloweenparty gefeiert, wir durften Filme drehen und da hat dann jemand einen Film auf YouTube gestellt und die Lehrerin war auch drauf.
Karolina: Die Lehrerin sieht man 2 Sekunden und sie hat gleich einen Anwalt eingeschaltet. Das war schon extrem.
Lilian: Zu dem Zeitpunkt wussten wir aber auch gar nicht, dass es dieses Recht am eigenen Bild überhaupt gibt. *(Die anderen nicken.)*

I: Meint ihr, dass eure Eltern anders mit persönlichen Daten im Internet umgehen als ihr?

Bastian: Ich glaub auch bei den Erwachsenen ist es wie bei den Jungen, die einen kennen sich aus oder machen nix, die anderen machen es genau wie die Schüler und nutzen alles und geben auch viel an.
Melissa: Also, meine Eltern benutzen wkw oder so wirklich nur um zu kommunizieren und die nehmen auch nicht irgendwelche Leute an, die sie gar nicht kennen.

I: Macht ihr das?

Melissa: Ab und zu, weil man dann grad Lust hat, die kennen zu lernen. Ich add eh niemanden, meist werd ich eh geaddet.

I: Bei welchen Plattformen?

Melissa: Facebook, schülerVZ und MSN.

I: Dann nimmst du auch Fremde an?

Melissa: Ja. Aber es gibt auch welche, die nur Mist gemacht haben, dann hab ich die gelöscht. Die wollten z.B. Bilder von mir und sich treffen, die hab ich dann rausgeschmissen. Ich wollte eigentlich nur so in Kontakt bleiben. Aber manchmal sind das Freunde von Freunden, und dann add ich die schon auch mal.

I: Glaubt ihr, dass Mädels anders mit ihren Daten umgehen als Jungs?

Alle Jungs: Ja, auf jeden Fall. Die sind viel leichtsinniger.
Alle Mädchen schütteln den Kopf…
Lilian: Ich denke, viele präsentieren sich anders im Netz, als sie wirklich sind. Oft sind die Personen ganz anders als z.B. im Chat.
Karolina: Ich kann im Internet manchmal besser mit den Leuten schreiben als im wirklichen Leben. Ohne Bild geht das auch manchmal einfacher. Und manchmal braucht man den persönlichen Kontakt.
Melissa: Es sind viele so, aber ja auch nicht alle.

Die Namen der Jugendlichen wurden von der Redaktion geändert.

Impressum

Titel:
Datenschutz und Persönlichkeitsrechte im Web
klicksafe Datenschutz-Dossier zum Safer Internet Day 2010

Die einzelnen Beiträge geben die Meinung der jeweiligen Autorin/ des jeweiligen Autors wieder.

Stand: Januar 2010

Herausgeber:
Die Initiative „klicksafe“ (www.klicksafe.de) ist ein Projekt im Rahmen des „Safer Internet Programms“ der Europäischen Union. Es wird von einem von der Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz koordinierten Konsortium getragen. Diesem gehören die LMK (www.lmk-online.de) und die Landesanstalt für Medien NRW (LfM) (www.lfm-nrw.de) an.
klicksafe ist Teil des Verbundes der deutschen Partner im Safer Internet Programm der Europäischen Union. Diesem gehören neben klicksafe die Internet-Hotlines internet-beschwerdestelle.de (durchgeführt von eco und FSM) und jugendschutz.net sowie das Kinder und Jugendtelefon von Nummer gegen Kummer (Helpline) an.

Koordinator klicksafe: Peter Behrens, LMK

The project is co-funded by the European Union, through the Safer Internet plus programme:
http://ec.europa.eu/saferinternet.

Kontakt:

klicksafe-Büros

c/o Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz
Turmstraße 10
67059 Ludwigshafen
Tel: 06 21 / 52 02–271
Fax: 06 21 / 52 02–279
E-Mail: info@klicksafe.de
URL: www.klicksafe.de

c/o Landesanstalt für Medien Nordrhein-Westfalen (LfM)
Zollhof 2
40221 Düsseldorf
E-Mail: klicksafe@lfm-nrw.de
URL: www.klicksafe.de