

Soziale Netzwerke – Reize und Risiken der schönen neuen virtuellen Internetwelt

Wer-kennt-wen, SchülerVZ, StudiVZ, Lokalisten, MySpace, Facebook, Twitter oder das Business-Netz Xing – wer kennt nicht mindestens eines dieser sozialen Netzwerke. Sie wachsen ständig und sind vor allem bei jungen und internetbegeisterten Surfern zwischen 18 und 35 Jahren ein großes Thema. Wer über das Internet kommunizieren will, kommt an diesen Netzwerken kaum noch vorbei. Soziale Netzwerke sind wie der Dorfmarktplatz früherer Jahrhunderte. Man trifft alte Freunde, Bekannte oder Geschäftspartner. Man plaudert mit ihnen, lästert, tauscht Neuigkeiten aus, knüpft geschäftliche Kontakte oder will einfach nur Spaß haben.

Der Unterschied zum Dorfmarktplatz: Das Dorf ist jetzt global und es ist nicht mehr an Marktzeiten gebunden. Rund um die Uhr, rund um die Welt sind die virtuellen Treffpunkte verfügbar. Die Nutzer legen Profile und kleine Homepages an, die Name, Foto, Tätigkeit, Interessen und – je nach Netzwerk – viele weitere Informationen enthalten. Die Menschen erzählen und zeigen, was sie gerade beschäftigt. Der Reiz am virtuellen Marktplatz liegt in seiner vermeintlichen Anonymität. Doch bei der Freude am Austausch mit Online-Bekanntschäften bleibt oftmals der Schutz der eigenen Privatsphäre auf der Strecke.

Denn die User bewegen sich in der virtuellen Welt nicht in einem geschützten Raum. Wer beim Netzgeplauder oder beim Einstellen von Filmen und Fotos allzu freizügig persönliche Daten preisgibt, muss mit unkalkulierbaren Folgen rechnen. Sind erstmal Informationen ins Netz gestellt, bleiben sie dort meist für mehrere Jahre und können später einmal ungeahnte Folgen haben. Soziale Netzwerke sind Goldgruben für Werbeindustrie und Datenhändler. So werden die aus dem Netz gesammelten Daten häufig dazu benutzt, Surfer mit passgenauer und personenbezogener Werbung per Post oder E-Mail zu bombardieren. Die Gruppe „Fashion Angels“ wurde seinerzeit in einem Schülernetzwerk eigens kreiert, um Lieblingsmarken und Kaufgewohnheiten modebewusster Teenies zu erforschen.

Auch Personalabteilungen machen sich zunehmend ein eigenes Bild von ihren Bewerbern, indem sie gezielt per Suchmaschine nach Informationen stöbern. Peinliche Party- oder Urlaubsfotos oder unbedacht ins Netz gestellte Forenbeiträge haben dabei schon so manchem Anwärter die Chance auf einen Job gekostet.

Arbeitgeber verwenden soziale Netzwerke auch gerne einmal, um ihre Angestellten zu überwachen. So hat beispielsweise im November 2008 eine krankgeschriebene

Schweizer Bankangestellte die fristlose Kündigung erhalten, weil sie sich während ihrer Krankheit auf der Plattform Facebook getummelt und ihr Arbeitgeber ihre vielfältigen Aktivitäten verfolgen konnte.

Deine Spuren im Netz ...

Immer wenn es darum geht, dass der Staat oder öffentliche Einrichtungen personenbezogene Daten erheben, geht meist ein großer Aufschrei quer durch die Republik. Man denke nur an die Diskussion um die Volkszählung in den 80er-Jahren oder an die aktuelle, im Zuge der allgemeinen Terrorbekämpfung geführte Debatte über den biometrischen Fingerabdruck im Personalausweis. Ähnlich hitzige Diskussionen wurden Anfang 2008 anlässlich der damals in Kraft getretenen Neuregelung der Telekommunikationsüberwachung (Vorratsdatenspeicherung von Telefon- und Internetdaten) geführt.

Über die vielen vertrags- und datenschutzrechtlichen Probleme, die sich im Zusammenhang mit der Nutzung von Internetplattformen ergeben, machen sich hingegen die wenigsten Verbraucher Gedanken.

Schon bei der Anmeldung werden heutzutage im Internet allzu freizügig die persönlichen Daten – bis hin zur eigenen Bankverbindung oder Kreditkartennummer – angegeben.

In den meisten sozialen Netzwerken besteht die Möglichkeit, Gruppen beizutreten oder solche zu eröffnen. Dort werden Angaben zu Hobbys, gemeinsamen Interessen und persönlichen Vorlieben gemacht. Die Nutzer können hier mit anderen Interessierten in Foren diskutieren, bei vielen Anbietern auch Fotos und persönliche Videos einstellen, wobei die Beiträge häufig unabhängig von den Privatsphäreinstellungen sind und somit von allen Mitgliedern der jeweiligen Gruppe – bei einigen Anbietern sogar von allen Mitgliedern der Internetplattform – gelesen werden können. Der Nutzer verliert dann den Überblick darüber, wer seine Daten einsieht und gegebenenfalls weiterverwendet und wird so zum Objekt der Datenverarbeitung. Es entsteht rasch ein nicht mehr überschaubares Geflecht von Mitgliedern und Profilen und nicht selten gerät die eigene Identität im Netz außer Kontrolle.

Achtung:

Was einmal in sozialen Netzwerken und damit im weltweiten Netz steht, ist publiziert. Dieser Charakter einer Veröffentlichung muss jedem Nutzer klar sein. Was in erster Linie für den eigenen Freundes- oder Bekanntenkreis gedacht war, kann genau so gut von einem künftigen Arbeitgeber oder von weniger wohlwollenden Mitmenschen gelesen und genutzt werden. Vor jeder Angabe sollte man daher immer wieder die Frage an sich selbst stellen: Ist das wirklich eine Information, die ich mit der Öffentlichkeit teilen möchte?

Datenschutz wird oft kleingeschrieben

Bei vielen Anbietern gestaltet sich der Datenschutz alles andere als verbraucherfreundlich. So sind die Voreinstellungen meist sehr großzügig angelegt. Oftmals wird darauf verzichtet, die Verbindungen zu verschlüsseln, so dass theoretisch jeder, der sich im gleichen Netzwerk befindet, diese Daten mitlesen kann.

Immer wieder berichten Betroffene in den Beratungsstellen der Verbraucherzentrale Hessen, dass sie zwar ihre Anmeldung bei einem sozialen Netzwerk rückgängig gemacht und ihr eigenes Profil vollständig gelöscht haben, eigene Freunde und Bekannte aber gleichwohl durch Einladungsmails und sonstige Werbebotschaften weiterhin belästigt werden, weil der Anbieter bei der Anmeldung offensichtlich den gesamten Adressdatenbestand des ehemaligen Nutzers ausgelesen hat. Dies ist kein Einzelfall.

Häufig kommt es vor, dass die eigenen E-Mail-Kontaktdaten automatisch mit den beim jeweiligen Netzwerk gespeicherten E-Mail-Konten abgeglichen werden und Nutzer bereits bei der Installation der Anwendungen pauschal neben vielen eigenen auch Daten ihrer Kontakte freigeben. Das widerspricht dem Grundsatz, dass jeder Verbraucher selbst und aktiv entscheiden können muss, welche Daten er wem zur Verfügung stellt.

Die Benutzer sollten daher genau prüfen, was sie wem gestatten wollen:

- Wer soll etwa auf das eigene Benutzerprofil Zugriff haben?
- Wer auf die persönlichen Fotos und Videos?
- Wer darf mit mir Kontakt aufnehmen?
- Wer meiner Freunde soll vom Betreiber E-Mail-Benachrichtigungen erhalten?

- Müssen die anderen Nutzer um Erlaubnis fragen, bevor sie jemanden auf einem Foto verlinken?
- Sollen meine Daten und Inhalte auch für Suchmaschinen auffindbar sein?

Und der Datenhandel blüht weiter ...

Bereits im August 2008 hatte der Verbraucherzentrale Bundesverband eindrucksvoll unter Beweis gestellt, wie einfach es ist, an sensible Daten zu kommen. Mit Hilfe eines Mittelsmanns erwarb der Verband innerhalb kürzester Zeit sechs Millionen Datensätze. Vier Millionen davon waren sogar mit Kontoverbindungen versehen. Der illegale Handel mit Kundendaten wird weiter blühen. Daran werden auch die jüngsten Änderungen des Datenschutzrechts vermutlich nicht viel ändern.

Mit vielen Ausnahmen und Übergangsfristen sind am 1. September 2009 einige Änderungen des Bundesdatenschutzgesetzes (BDSG) in Kraft getreten, die die unbefugte Verwendung persönlicher Kundendaten zu Werbezwecken und den Adressenhandel erschweren sollen. So müssen beispielsweise Erklärungen in Verträgen, dass man mit der Nutzung seiner Daten für Werbezwecke einverstanden ist, seit dem 1. September 2009 deutlich hervorgehoben sein.

Darüber hinaus enthält auch das Telemediengesetz vielerlei Einschränkungen, was die Verwendung personenbezogener Daten angeht.

Dennoch wird es auch künftig leicht sein, den Kunden Einwilligungen in die Verwendung ihrer Daten zu Werbezwecken unterzuschieben. Ganz abgesehen davon, unterliegen manche Betreiber gar nicht dem deutschen Recht.

Die meisten sozialen Netzwerke sammeln in der Regel mehr Daten, als sie eigentlich brauchen. Insofern fragt man sich häufig, weshalb für die Anmeldung vollständige Geburtsdaten, Geschlecht und die Postleitzahl des Wohnortes angegeben und selbst Schule, Hochschule und Unternehmen abgefragt werden müssen. Auch die Angabe einer gültigen Email-Adresse ist meist ein Pflichtfeld. Die Erfassung umfangreicher Datensätze ist weder zwingend notwendig, um die Nutzung der Plattform technisch zu realisieren, noch um rechtliche Anforderungen abzudecken.

Auch das Thema "Verschlüsselung" erscheint bei einigen Plattformen problematisch. Ist die gesamte Sitzung im Netzwerk verschlüsselt? Wie sind die Möglichkeiten, die persönlichen Daten selbst zu verwalten und den Zugang zu ihnen zu kontrollieren? Sind zumindest Anmeldung und Konfigurationsseiten verschlüsselt und damit Nutzernamen und Passwörter geschützt?

Die Allgemeinen Geschäftsbedingungen (AGB) sollten eigentlich Aufschluss darüber geben, wie der jeweilige Anbieter mit dem Thema Datenschutz umgeht. Die

meisten Nutzer werden allerdings überfordert sein, sich mit den in Juristendeutsch abgefassten langen Klauselwerken inhaltlich auseinander zu setzen. Abgesehen davon sind vor allem die Regelungen der Betreiber zur umfassenden Datennutzung und -verarbeitung kritisch zu sehen.

Bei einem bekannten Netzwerk heißt es beispielsweise im Kleingedruckten:

„Wir können deine Anwendung, Inhalte und Daten zu jeglichem Zweck, einschließlich kommerziellen Zwecken (wie die Bereitstellung von Werbung für bestimmte Zielgruppen und die Indexierung von Inhalten für die Suche), analysieren“.

Mit dieser weitreichenden, in rechtlicher Hinsicht kaum tragbaren Regelung soll eine umfangreiche Datenanalyse – zu welchem Zweck auch immer – legitimiert werden, und zwar offenbar unabhängig davon, ob der Verbraucher eine entsprechende Einwilligung abgibt. Der Verbraucher kann anhand dieser intransparenten Klausel auch nicht erkennen, zu welchem Zweck seine Inhalte und Daten überhaupt analysiert werden sollen und muss darüber hinaus mit Werbemaßnahmen in jeglicher Form rechnen.

Ende September 2009 ging die Meldung durch die Medien, dass der Anbieter Facebook seine umstrittene "Beacon"-Technologie (zu deutsch "Blinklicht" oder "Leuchtfeuer") beendet. Das soziale Netzwerk hatte vor gut zwei Jahren über Nacht einen Rückkanal zwischen sich und dem Web geschaffen. Hatte der Kunde die Werbetechnik aktiviert, meldeten gut 44 Werbepartner wie zum Beispiel die Auktionsseite ebay automatisch an andere Nutzer zurück, was das Facebook-Mitglied so alles trieb. War man bei Facebook angemeldet, merkte das die Partnerseite und verschickte dann die Daten. Auf diesem Wege wurde der Freundeskreis von Facebook-Mitgliedern automatisch über deren Einkäufe bei den Werbepartnern informiert. Das zweifelhafte "Schnüffel-Leuchtfeuer" soll nun in Folge eines vor einem US-Gericht geschlossenen Vergleichs vollständig abgeschaltet werden. Nach US-Medienberichten wird das Unternehmen nun mit 9,5 Millionen Dollar (6,5 Millionen Euro) eine Stiftung zur Förderung des Datenschutzes im Internet gründen.

Tipp:

Um dem Datenmissbrauch vorzubeugen, sollte man darauf achten, private und geschäftliche Daten nicht öffentlich verfügbar zu machen. Egal wie verlockend das Angebot sozialer Netzwerke auch klingen mag: Verbraucher sollten auch stets den jeweiligen Anbieter sorgfältig unter die Lupe nehmen, einen Blick ins Kleingedruckte werfen, grundsätzlich misstrauisch sein und sich im Zweifel beraten lassen.

Der Verbraucherzentrale Bundesverband (vzbv) hat übrigens im Juli 2009 fünf soziale Netzwerke – darunter die Plattformen MySpace, Facebook, lokalisten.de, wer-kennt-wen.de und Xing – wegen verbraucherfeindlicher Geschäftsbedingungen und mangelhafter Datenschutzbestimmungen abgemahnt und zur Unterlassung aufgefordert.

Wenn das Urheberrecht verloren geht

Manche Betreiber lassen sich über ihre Allgemeinen Geschäftsbedingungen weitreichende Rechte an den Inhalten ihrer Nutzer einräumen. So könnte es unter Umständen passieren, dass das selbst geknipste und hochgeladene Foto schon morgen in der Zeitung erscheint oder sich das hochgeladene Video in der abendlichen Comedy-Sendung eines Privatsenders wiederfindet.

Tipp:

Auch hinsichtlich der Einräumung von Nutzungs- und Urheberrechten gilt es, die Allgemeinen Geschäftsbedingungen (AGB) immer ganz durchzulesen. Auf die Teilnahme bei einem Netzwerk, das Klauseln mit weitreichenden Rechteübertragungen vorsieht, sollte verzichtet werden.

Kinder und Jugendliche

Vor allem Kinder und Jugendliche befinden sich häufig im Wettstreit darüber, wer die meisten bestätigten Freundschaftskontakte in einer Internet-Community hat – frei nach dem Motto: je mehr Kontakte, desto angesehener bin ich in der Schule und in meinem Freundeskreis.

Dabei bedenken Kinder und Jugendliche in der Regel nicht, dass sie sich durch ihre Auftritte selbst gläsern machen, indem sie in ihren Profilen ihre Daten und Bilder einer breiten anonymen Öffentlichkeit bekannt machen. Auch potentielle Belästiger können auf den Internetplattformen viele Informationen über Kinder und Jugendliche sammeln (zum Beispiel Kontaktdaten oder Gewohnheiten). Jugendschutz ist in den meisten sozialen Netzwerken höchstens rudimentär umgesetzt – die Betreiber fragen nach dem Alter und prüfen es häufig nicht einmal. Gerade bei Schüler-Plattformen kommt oftmals auch der Trugschluss hinzu, die Schüler wären tatsächlich nur unter sich, da in der Regel zur aktiven Teilnahme eine Einladung nötig ist. Schüler wiegen sich daher gern in Sicherheit und meinen, die Plattform wäre eltern- und lehrerfrei.

Tatsächlich ist es aber ohne größeren Aufwand möglich, eine Einladung zu organisieren, sei es über den eigenen Bekanntenkreis oder über Internetforen.

Tipp:

Gerade bei Angeboten für Kinder und Jugendliche gilt es, die Angebote umso sorgfältiger zu prüfen und sich über die Sicherheitsoptionen und die Allgemeinen Geschäftsbedingungen zu informieren. Insbesondere sollten Sicherheitstipps, Hilfen und Ansprechpartner für die jugendlichen Nutzer aufgeführt sein.

Wie man seine Profil- und Privatsphäreinstellungen in einigen der sozialen Netzwerke sicherer macht, zeigt das vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz geförderte Jugendangebot Watch Your Web (<http://www.watchyourweb.de>).


Neben der Datensicherheit sollten auch die sozialen Risiken bedacht werden. Problematisch wird es vor allem dann, wenn die Kommunikation über das Online-Netzwerk den sozialen Kontakt im wirklichen Leben ersetzt.

Fazit

Die Bedeutung sozialer Netzwerke in der digitalen Welt nimmt stetig zu. Medienkompetenz ist heute eine Schlüsselqualifikation und sollte künftig bereits in der Grundschule auf dem Lehrplan stehen. Mediennutzer müssten frühzeitig in die Lage versetzt werden, Gefahren, die sich aus der Bekanntgabe von persönlichen Informationen und Daten ergeben, richtig einzuschätzen. Hier wird der Staat gefordert sein, vor allem aber auch die Wirtschaft selbst.

Weitere Informationen für Internetnutzer

www.surfer-haben-rechte.de

Welche Rechte habe ich in Sozialen Netzwerken? Welche Fallen drohen beim Download von Programmen? Internetnutzer erhalten auf der Seite  [Surfer haben Rechte](#) grundsätzliche Informationen zu den Rechtsthemen Urheberrecht, Datenschutz und allgemeines Vertragsrecht. Praxisnah informiert die Webseite, was bei konkreten Angeboten im Onlinealltag zu beachten ist.

Checklisten (z.B. http://www.surfer-haben-rechte.de/cps/rde/xbcr/ls_digitalrechte/Checkliste_Soziale_Netzwerke.pdf) helfen dabei, die wichtigsten Punkte im Blick zu behalten. Außerdem stellt der Verbraucherzentrale Bundesverband (vzbv) seine Aktivitäten im Bereich Internet vor.

Verantwortet wird das Angebot vom Projekt „Verbraucherrechte in der digitalen Welt“ im Verbraucherzentrale Bundesverband (vzbv), gefördert vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV). Die Internetseite, die Ende August 2009 auf einer gemeinsamen Pressekonferenz mit Verbraucherministerin Ilse Aigner der Öffentlichkeit präsentiert wurde, soll im Projektverlauf weiter wachsen und stets die neuesten Entwicklungen widerspiegeln.

Ratgeber

- Ratgeber: **“Meine Daten schützen“** (1. Auflage 2008, 160 Seiten) – Tipps zum Umgang mit persönlichen Daten und sicheren Surfen und Mailen im Web u. a., Preis: 12,80 Euro, erhältlich in allen Beratungsstellen der Verbraucherzentrale Hessen; bei Bestellung zuzüglich 2,50 Euro Versandkosten.

Bestellungen an:

Verbraucherzentrale Hessen e.V.,
Große Friedberger Straße 13-17, 60313 Frankfurt am Main
Bestell-Telefon: (069) 97 20 10 - 30 (AB)
Bestell-Fax: (069) 97 20 10 - 40
E-Mail: ratgeber@verbraucher.de
<http://www.verbraucher.de>

Beratungsangebot der Verbraucherzentrale Hessen

- Telefonische Beratung zu Verbraucherrechten in der digitalen Welt: **0900-1-972010** (1,75 € pro Minute aus dem Festnetz der Deutschen Telekom AG – andere Anbieter, insbesondere im Mobilfunk, können zusätzliche Entgelte berechnen).
- Auskunft- und Servicetelefon: Informationen über das Beratungsangebot und das Beratungsstellennetz der Verbraucherzentrale Hessen unter **0180 5 972010** (0,14 € pro Minute aus dem Festnetz der Deutschen Telekom AG – andere Anbieter, insbesondere im Mobilfunk, können zusätzliche Entgelte berechnen; ab dem 1.3.2010 Mobilfunkpreise maximal 0,42 € pro Minute).

Tel. 01805-972010
(0,14 €/ Min. a. d.
Festnetz der DTAG,
Mobilfunk ggf. abwei-
chend; ab 1.3.2010
Mobilfunkpreise
maximal 0,42 €)
vzh@verbraucher.de
www.verbraucher.de

Hinweis:

Diese Verbraucherinformation wurde im Rahmen des vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz geförderten Projektes wirtschaftlicher Verbraucherschutz erstellt.

Veröffentlichung/Stand: 6. Oktober 2009

Diese Verbraucherinformation gibt den Stand der Dinge zum Zeitpunkt ihrer Veröffentlichung wieder.