



# 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 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 Kundenschaft 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,

### 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.

und Xing, mit mehr als 7,5 Millionen Mitgliedern das größte deutsche Business-Network.

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 unkonventi-

onell 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 Synergieeffekte 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.