

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

05.06.2008

Seite 1

Der BITKOM vertritt mehr als 1.200 Unternehmen, davon 900 Direktmitglieder mit 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien.

Der BITKOM beteiligt sich maßgeblich an der Initiative „Deutschland sicher im Netz e.V.“ (DSiN), die über Risiken im Internet aufklärt und praktische Lösungen anbietet. Zugleich ist BITKOM Gründungsmitglied der Initiative „Ein Netz für Kinder“. Diese Initiative hat mit der Webseite „fragfinn.de“ einen sicheren Surfraum speziell für den Nachwuchs geschaffen. Anlässlich des Safer Internet Day hat BITKOM zusammen mit dem Bundesministerium für Verbraucherschutz in Berlin eine Konferenz zur „Sicherung der Identität in der Digitalen Welt“ veranstaltet.

Die BITKOM Position zur datenschutzkonformen Gestaltung von Social Networks ist die erste Bewertung einer sich in Entwicklung befindlichen Materie. BITKOM wird zukünftige relevante Änderungen der Technik und anderer Umstände in die Position aufnehmen und in der Bewertung berücksichtigen.

Zusammenfassung

- Datenschutz ist ein zentraler Punkt und wichtiger Punkt bei der Ausgestaltung eines Social Networks. Es gibt jedoch auch andere Interessen die hier mit berücksichtigt werden müssen, insbesondere der Schutz der Mitglieder vor Straftaten und die Effektivität der Strafverfolgung; unter anderem aber auch die technische Sicherheit des Netzwerks und die Nutzerfreundlichkeit. Es bedarf einer Gesamtabwägung.
- Anbieter eines Social Networks müssen ihre Nutzer zu Beginn des Nutzungsvorgangs über die Art, den Umfang und die Zwecke der Erhebung personenbezogener Daten informieren. Diese Informationspflichten dürfen aber nicht überspannt werden. Die Praxis zeigt, dass zu umfangreiche Informationen oder ein zu komplizierter Registrierungsprozess genau zum Gegenteil des gewünschten Ergebnisses führen, die Nutzer beschäftigen sich mit dem wichtigen Thema Datenschutz nicht mehr. Sie sind vielmehr von einer zu langen Datenschutzerklärung abgeschreckt und kehren im schlechtesten Fall dem Online-Dienst den Rücken zu.
- Eine Speicherung von Nutzungsdaten ist erlaubt, sofern die Nutzer darin wirksam eingewilligt haben. Die Speicherung von Nutzungsdaten dient der Sicherheit und dem Schutz des Social Networks wie auch der einzelnen Mitglieder und ermöglicht eine effektive Strafverfolgung.
- Eine Verwendung, Auswertung und Übermittlung personenbezogener Daten zu Werbezwecken ist nur erlaubt, sofern die Nutzer darin eingewilligt haben.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel. +49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner:

Dr. Kai Kuhlmann
Bereichsleiter Recht
Tel. +49. 30. 27576-131
Fax +49. 30. 27576-139
k.kuhlmann@bitkom.org

Präsident

Prof. Dr. Dr. h. c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer

Dr. Bernhard Rohleder

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 2

- Bei der konkreten Ausgestaltung des Netzwerks genießen die Anbieter eines Social Networks unternehmerische Freiheit. Soweit er die datenschutzrechtlichen Vorschriften und die Informationspflichten beachtet, kann der Anbieter entscheiden, welche Einstellmöglichkeiten (einschließlich Grundeinstellungen), Suchfunktionen usw. er dem Nutzer anbietet.
- Eine gesetzliche Verpflichtung, die Nutzung eines Social Networks auch anonym oder unter einem Pseudonym zuzulassen, besteht regelmäßig nicht. Eine solche Verpflichtung steht sowohl dem Zweck eines Social Networks als auch der Qualität und den Sicherheitsinteressen der Nutzer entgegen.

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 3

Inhalt	Seite
1 Nutzervertrauen in der digitalen Wirtschaft	4
2 Rechtliche Rahmenbedingungen	5
2.1 Information der Nutzer	5
2.2 Datensicherheit	6
2.3 Speicherung von Nutzungsdaten	6
2.4 Nutzung von Daten	7
2.5 Datenschutzrechtliches Koppelungsverbot?.....	7
3 Weitere Möglichkeiten und Maßnahmen zur individuellen Gestaltung der Privatheit	8
3.1 Individuelle Privacy-Einstellungen	8
3.2 Informationen über urheber- und persönlichkeitsrechtliche Vorgaben	9
3.3 Angemessene Transparenz	9
3.4 Individuelle Einstellungen für Werbung	9
3.5 Anonyme oder pseudonyme Nutzung des Netzwerks?.....	9
3.6 Verhaltenskodex für die Nutzer.....	10

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 4

1 Nutzervertrauen in der digitalen Wirtschaft

Fast jeder fünfte Deutsche (18 Prozent) hat bereits Informationen über sich im Internet veröffentlicht – in der Generation der 14- bis 29-Jährigen bereits jeder Zweite. Am beliebtesten sind Profile in sozialen Netzwerken.

Soziale Netzwerke im Internet dienen zur schnellen Vernetzung und Kommunikation mit anderen Nutzern, wie u. a. mit alten und neuen Freunden, Bekannten oder Kollegen. Die Mitglieder tauschen sich dabei in Form von Nachrichten und Fotos aus und diskutieren in selbst gegründeten Diskussionsgruppen über unterschiedliche Themen.

Dem Nutzervertrauen im Allgemeinen und dem Datenschutz im Speziellen kommt bei Social Networks eine zentrale Bedeutung zu, wie die Diskussion der letzten Monate gezeigt hat.

Bei dieser Diskussion um das Nutzervertrauen wird vielfach nicht beachtet, dass seit der Erfindung des World Wide Web eine neue Generation herangereift ist, die mit neuen Technologien und Kommunikationsformen groß geworden ist und die Möglichkeiten der virtuellen Welt des Internets als selbstverständlichen Teil ihres Alltags begreift, sog. „Digital Natives“ (im Gegensatz zu der älteren Generation der „Digital Immigrants“, die einen fundamentalen Wechsel bewältigen müssen)¹. Die Voraussetzungen für die Schaffung von Nutzervertrauen müssen sich nicht zuletzt auch an dieser neuen Nutzer- und Verbrauchergeneration orientieren und deren Verständnis von Privatheit berücksichtigen.

Zur Wahrung des verfassungsrechtlich geschützten informationellen Selbstbestimmungsrechts ist es daher vor allem sach- und interessensgerecht, den Nutzer durch die notwendigen Informationen in die Lage zu versetzen, bewusst und eigenverantwortlich tragfähige Entscheidungen zu treffen. Es sollte nicht die „schützende Bevormundung“, in den Vordergrund gestellt werden, sondern die Ermöglichung selbstbestimmten Handelns². Rechtliche Eingriffsmechanismen sind vor diesem Hintergrund erst dort notwendig, wo die Basis dieses selbstbestimmten Handelns, die notwendige Informationshoheit des Nutzers digitaler Angebote und die Durchsetzung seiner Entscheidungen über die Nutzung seiner personenbezogenen Daten konkret gefährdet sind.

Zu beachten ist darüber hinaus, dass Datenschutz und IT-Sicherheit exemplarisch für eine grundsätzliche Tendenz der digitalen Wirtschaft stehen: Verbraucher- und Unternehmensinteressen sind nicht automatisch Gegenpole, sondern decken sich weitgehend. Denn das Vertrauen der Nutzer in die Integrität der Dienste ist aus Anbietersicht

¹ So auch das sog. „Rome Memorandum“ der International Working Group on Data Protection in Telecommunication vom 4. März 2008 m. w. N.;

http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf?1208438491

² Ausführlich wird dieser Themenkreis in der Veröffentlichung „Standpunkte – Vertrauen in die digitale Wirtschaft“ behandelt: <http://www.bitkom.org/de/publikationen/38338.aspx>

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 5

eine der maßgeblichen Voraussetzungen für langfristige Nutzungsverhältnisse bzw. Kundenbeziehungen. Die Anbieter haben zudem häufig die erheblichen wirtschaftlichen Folgen von Problemen in den Bereichen Sicherheit und Datenschutz zu tragen.

Social Networks nutzen Datenschutz und IT-Sicherheit deshalb als Qualitätsmerkmal ihres Angebots und sichern diese Qualität aus eigenem Antrieb. Wie und in welcher Weise diese Qualität von den Anbietern gesichert wird, sollte daher, wenn gleichzeitig das gesetzlich vorgegebene Maß erfüllt wird, als Bereich unternehmerischer Entscheidungen respektiert werden. Die unternehmerische Entscheidungsfreiheit korrespondiert dabei mit der Entscheidungsfreiheit der Nutzer, eine bestimmte Plattform zu nutzen oder von ihrer Nutzung abzusehen. Zur unternehmerischen Entscheidung gehört auch der notwendige Freiraum, um eine Plattform mit ihren Funktionen und dem vorgeschalteten Registrierungsvorgang nutzerfreundlich und schlank zu gestalten.

Mehrere gesetzliche Vorschriften bilden den von allen Anbietern zu beachtenden Sockel. Diese Vorschriften sind im folgenden Teil 2 dargelegt. Über diese gesetzlichen Vorgaben hinaus kann der Anbieter eines Social Networks kundenorientierte und vom Kunden individuell konfigurierbare Mechanismen anbieten. Diese freiwilligen Maßnahmen zur flexiblen Gestaltung der Privatheit sind Gegenstand der Ausführungen in Teil 3.

Die Überwachung der Einhaltung datenschutzrechtlicher Vorgaben ist Aufgabe der Datenschutzaufsichtsbehörden. Die Ausgestaltung der nach dem Gesetz bestehenden Freiräume unterfällt hingegen wieder der unternehmerischen Entscheidungsfreiheit der Anbieter eines Social Networks. Dazu zählt auch die Frage, ob und welche Mechanismen zur individuellen Gestaltung der Privatsphäre den Nutzern angeboten werden. Den Datenschutzbehörden kommt insoweit eine beratende Funktion zu.

2 Rechtliche Rahmenbedingungen

Im Folgenden sollen kurz die Vorgaben des geltenden Rechts an die Anbieter von Social Networks dargelegt werden. Maßgeblich ist vor allem das Telemediengesetz (TMG), ergänzend kann das Bundesdatenschutzgesetz (BDSG) gelten.

Im Einzelnen:

2.1 Information der Nutzer

Wenn Anbieter von Social Networks personenbezogene Daten ihrer Nutzer erheben, sind sie verpflichtet, die Nutzer zu Beginn des Nutzungsvorgangs über die Art, den Umfang und die Zwecke der Erhebung zu informieren (§ 13 Abs. 1 TMG). Im Interesse der Rechtssicherheit ist eine klare Abgrenzung bezüglich Art und Inhalt der Informationspflicht erforderlich.

Es sind alle Zwecke anzugeben, die der Diensteanbieter im Zeitpunkt der Erhebung verfolgt. Die Information muss in allgemein verständlicher Form erfolgen. Sofern die Information dem Nutzer nicht schon vorher, zum Beispiel im Rahmen der Registrierung gegeben worden sind, muss der Nutzer zu Beginn des Nutzungsvorgangs unterrichtet werden.

Weitergehende Informationspflichten bestehen nicht. Der Sinn und Zweck des § 13 Abs. 1 TMG liegt darin, dem Nutzer die konkrete Art und Weise der Datenverarbeitung

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 6

möglichst transparent zu machen. Dieser Sinn und Zweck macht zugleich auch die Grenzen der Informationspflicht der Anbieter deutlich. Die Informationen, die dem Nutzer gegeben werden müssen, können nicht weiter reichen als der konkrete Vorgang der jeweiligen Datenverarbeitung. Insbesondere kann ein Anbieter von Social Networks daher nicht gesetzlich verpflichtet sein, dem volljährigen Nutzer Hinweise für sein eigenes Verhalten zu geben oder auf die möglichen Folgen eventueller Handlungen dritter, nicht mit dem Anbieter verbundener Personen hinzuweisen.

Eine andere Beurteilung kann aus Gründen des Jugendschutzes geboten sein. Anbieter von Social Networks, die sich ausschließlich oder doch überwiegend an Jugendliche richten, sollten daher die besondere Schutzbedürftigkeit berücksichtigen und jugendliche Nutzer auf die möglichen Folgen und Risiken ihres eigenen Verhaltens hinweisen.

2.2 Datensicherheit

Der Diensteanbieter hat nach § 13 Abs. 4 TMG durch technische und organisatorische Vorkehrungen den sog. „Systemdatenschutz“ sicherzustellen. Vorgesehen sind in § 13 Abs. 4 TMG die Möglichkeit des jederzeitigen Nutzungsabbruchs (Nr. 1), die Löschungspflicht von personenbezogenen Nutzungsdaten nach Nutzungsende (Nr. 2), der Schutz der Vertraulichkeit (Nr. 3), die Durchführung der informationellen Trennung (Nr. 4), die Beschränkung der Verarbeitung von Abrechnungsdaten (Nr. 5) und die Vermeidung des Zusammenführens von Nutzerprofilen (Nr. 6). Sinn der Vorschrift ist, dass die normierten Schutzziele, die Ausformungen des Rechts auf informationelle Selbstbestimmung sind, vom Anbieter erreicht werden. Die Vorgaben sind deshalb auch nur dort und nur dann verpflichtend, wo bzw. wenn personenbezogene Daten berührt sind.

Darüber, wie die Schutzziele vom Anbieter zu erfüllen sind, trifft das TMG keinerlei Aussage. Die Anbieter haben insoweit einen Gestaltungsspielraum. Es bleibt daher vollständig den Anbietern von Social Networks überlassen, welche organisatorischen und technischen Vorkehrungen sie treffen.

2.3 Speicherung von Nutzungsdaten

Anbieter von Social Networks dürfen Nutzungsdaten speichern, sofern eine informierte Einwilligung der Nutzer hierzu eingeholt worden ist. Für die Anbieter von Social Networks kann die Speicherung von Nutzungsdaten ein unumgängliches Instrument sein, um die Sicherheit der Plattform zu gewährleisten. Die Speicherung ermöglicht eine effektive Strafverfolgung bei strafrechtlich relevanten Verhaltensweisen von Nutzern (Volksverhetzung, Beleidigungen, kinderpornographische Inhalte, Stalking etc.) und dient damit der Sicherheit und dem Schutz der Community und des einzelnen Mitglieds. Die Möglichkeit der Einwilligung spiegelt das grundgesetzlich gewährleistete Recht des Nutzers auf informationelle Selbstbestimmung wieder. § 15 Abs. 4 TMG steht der Einwilligungsmöglichkeit nicht entgegen. § 15 Abs. 4 TMG erlaubt als spezielle gesetzliche Ausnahme zu dem in § 12 TMG festgelegten Grundsatz die Speicherung von Nutzungsdaten ohne Einwilligung des Nutzers in einer speziellen Konstellation (Abrechnungszweck). Diese Vorschrift ist nach Historie, Systematik, Sinn und Zweck jedoch kein abschließender Erlaubnistatbestand, der die Speicherung mit Einwilligung des Nutzers sperrt.

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 7

2.4 Nutzung von Daten

Will der Anbieter eines Social Networks personenbezogene Nutzungsdaten für Werbezwecke verwenden oder für Werbezwecke an Dritte übermitteln, muss er nach den Bestimmungen des TMG dafür zuvor die Einwilligung des Nutzers einholen.

Eine Einwilligung der Nutzer ist hingegen nicht erforderlich, falls keine personenbezogenen Daten für die Werbemaßnahme ausgewertet bzw. verwendet werden. Das Einblenden von Werbebannern ist daher auch ohne Einwilligung der Nutzer erlaubt.

Ein derzeit gängiges Verfahren zur Schaltung zielgruppenspezifischer Werbung ist der Einsatz sog. Targeting-Techniken. Bei zielgruppenspezifischer Werbung mit Hilfe von Targeting werden bei der Erhebung der Nutzerdaten diese Daten durch algorithmische Verschlüsselung zunächst in bestimmte Merkmale umgewandelt. Aufgrund dieser Merkmale können aus der gesamten Nutzergruppe unterschiedliche Cluster gebildet werden, die das verschlüsselte Merkmal aufweisen. Ein Vermarkter und andere Dienstleister (Adserver) bekommen lediglich eine Liste mit diesen codierten Merkmalen, die keinerlei Rückschlüsse auf einzelne Personen und deren persönliche Daten erlaubt. Der Einsatz einer Targeting-Technik durch den Anbieter eines Social Networks stellt sich als Auswertung personenbezogener Daten dar und bedarf daher einer Einwilligung der Nutzer. Eine Übermittlung personenbezogener Daten an Dritte findet dabei jedoch nicht statt.

Erstes Fazit

Die Ausgestaltung und die rechtliche Bewertung der einzelnen Punkte 2.1 bis 2.4 ist im Detail abhängig von der jeweiligen Gestaltung der technischen Prozesse (Beispiel: Datensicherheit) und der Benutzerführung (Beispiel: Registrierungsprozess) des Social Networks. Darüber hinaus können sich spezifische rechtliche Anforderungen dort ergeben, wo sich die Community aus Kindern oder Jugendlichen zusammensetzt. Grundsätzlich aber gilt: Social Networks, die die genannten gesetzlichen Anforderungen umsetzen, genügen den Vorgaben des Datenschutzrechts.

Um den Nutzer in die Lage zu versetzen, bewusst und eigenverantwortlich tragfähige Entscheidungen zu treffen, sollte die Nutzung des Internets und auch soziale Netzwerke zukünftig viel stärker als bisher von der Bildungspolitik aufgegriffen werden. Soziale Netzwerke sind neue Medien der Kommunikation und der Selbstdarstellung. Jugendliche müssen lernen, verantwortungsvoll damit umzugehen. BITKOM plädiert daher für eine stärkere Verankerung der Medienkompetenz in den Schulplänen.

2.5 Datenschutzrechtliches Koppelungsverbot?

Für Social Networks kann sich bei der Ausgestaltung der Registrierungsbedingungen die Frage stellen, ob es zulässig ist die Mitgliedschaft eines Nutzers davon abhängig zu machen, dass er in die Verwendung seiner Daten für Zwecke einwilligt, die über die Nutzung des Networks hinausgehen (z. B. für zielgruppenspezifische Werbung). Das TMG hat zu dieser Frage in § 12 Abs. 3 eine Regelung getroffen, die sich an dem Grundgedanken des verfassungsrechtlich geschützten Rechts auf informationelle Selbstbestimmung orientiert: Die Koppelung der Nutzung des Dienstes an die Einwilligung des Nutzers ist unbedenklich, wenn durch das Einwilligungsverlangen die Entscheidungsfreiheit des Betroffenen nicht unzulässig beschränkt wird. Eine Beeinträch-

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 8

tigung der Entscheidungsfreiheit liegt immer dann nicht vor, wenn andere Anbieter gleichwertige Dienste der fraglichen Gattung anbieten, die der Nutzer ohne unzumutbare Nachteile in Anspruch nehmen kann. Das Verbot einer Koppelung würde für Anbieter eines Social Network daher lediglich dann greifen, wenn nicht in ausreichender Form alternative Dienste existierten. Die Frage, ob alternative Dienste zur Verfügung stehen, ist anhand des Konzepts der funktionellen Austauschbarkeit vorzunehmen, wobei ein objektiver Maßstab anzulegen ist. Eine bestimmte Zielgruppenausrichtung des Angebots und bestimmte Vorlieben der Nachfrager sind insoweit irrelevant. Die derzeit angebotenen Community-Websites bilden daher zusammen den relevanten Markt. Die Nutzer haben also derzeit eine große Auswahl, so dass die Anbieter nicht dem datenschutzrechtlichen Koppelungsverbot unterliegen.

3 Weitere Möglichkeiten und Maßnahmen zur individuellen Gestaltung der Privatheit

Anbieter von Social Networks haben über den gesetzlichen Standard (2.1 - 2.4) hinaus vielfältige Möglichkeiten, ihre Plattform für den Nutzer durch Maßnahmen zur individuellen Gestaltung der Privatheit attraktiv zu machen.

Als Parameter und Orientierung für diese Maßnahmen sollten vor allem die Eigenverantwortlichkeit des Nutzers, seine individuelle, informationelle Selbstbestimmung und die Transparenz des Dienstes genutzt werden.

3.1 Individuelle Privacy-Einstellungen

Die gesetzlichen Vorgaben sollen nur den Standard beim Datenschutz sichern (dazu oben 2.1-2.4). Darüber hinaus muss Raum bleiben für eine vom Nutzer eigenständig bestimmte und kontrollierte Individualisierung seiner Privatheit im Social Network.

Im Interesse der Nutzer gewähren Anbieter von Social Networks ihren Nutzern die Möglichkeit, den Grad der gewünschten Privatheit durch eigenen Einstellungen (Privacy Settings) möglichst individuell, differenziert und flexibel vorzunehmen. Das betrifft zum Beispiel die Möglichkeit, die Einsehbarkeit der Profildaten individuell einzustellen. Das Anbieten einer solchen Möglichkeit ist jedoch lediglich Ausdruck einer gesteigerten Nutzerfreundlichkeit und ist gesetzlich nicht vorausgesetzt.

Ein Grundpfeiler des Nutzervertrauens im digitalen Kontext ist die notwendige Akzeptanz der Nutzer bezüglich der ihnen zgedachten Schutzmechanismen. Ein Höchstmaß an Akzeptanz wird aber am ehesten dann erreicht, wenn der Nutzer den gewünschten Schutz selbst festlegen kann. Letztlich ist das auch eine direkte Konsequenz des verfassungsrechtlich gesicherten Rechts auf informationelle Selbstbestimmung, denn der selbst gewählte Schutz ist in der Regel der individuell sachgerechte Schutz.

Nutzervertrauen steht insoweit auch in unmittelbarem Zusammenhang mit dem Grundsatz der Verhältnismäßigkeit und Subsidiarität staatlicher Regulierung. Ein Übermaß an Regulierung verhindert am Markt die Entwicklung flexibler, kundenorientierter und vom Kunden auch individuell konfigurierbarer Mechanismen, die für ein Social Network ein ganz wesentliches Qualitätsmerkmal darstellen.

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 9

3.2 Informationen über urheber- und persönlichkeitsrechtliche Vorgaben

Regelmäßig besteht in Social Networks für den Nutzer die Möglichkeit, Fotos online einzustellen (Profilfoto, Fotoalben etc.). Hierbei können fremde Urheberrechte, aber auch die persönlichkeitsrechte Dritter berührt werden. Die Betreiber von Social Networks sollten die Nutzer daher an einer geeigneten Stelle in kurzer Form über die rechtlichen Rahmenbedingungen informieren..

3.3 Angemessene Transparenz

Schon oben zu 2.1 ist dargelegt worden, dass die gesetzlichen Pflichten zur Information des Nutzers immanente Grenzen haben. Ob über das gesetzlich geforderte Maß hinausgehende Informationen durch den Anbieter nützlich und sinnvoll sind, kann nicht pauschal beantwortet werden, sondern muss in jedem konkreten Einzelfall sorgfältig abgewogen werden:

Ohne Zweifel ist Transparenz eine Grundvoraussetzung für ein eigenverantwortliches Handeln des Nutzers. Mehr Information führt aber nicht notwendig zu höherer Transparenz; im Gegenteil: Eine Informationsübersättigung wirkt häufig kontraproduktiv.

Die Entwicklung im TMG und TKG zeigt deutlich die Grenzen von Informationspflichten. Hinweise, Tipps und Informationen verlieren dort ihre Wirkung, wo sie dem Nutzer im Übermaß gegenüberstehen. Wird der Nutzer digitaler Dienste mit einem unsachgemäßen Maß an Informationen konfrontiert, wird er im besten Falle von deren Fülle verwirrt werden oder aber – das zeigt vielfach die Erfahrung– sie gänzlich ignorieren. Die an sich Verbraucherschützend ausgerichteten Instrumente verlieren dann ihre Wirkung, weil sie ein anderes Element der Verbraucherpolitik untergraben – die notwendige Akzeptanz des Nutzers.

Transparenz bedeutet vor diesem Hintergrund daher, auch das dem jeweiligen Dienst angemessene Maß an Nutzerinformation zu wahren.

3.4 Individuelle Einstellungen für Werbung

Wie die Einstellungen zur Privatheit bieten auch die Formen der zielgruppenspezifischen Werbeansprache Raum für individuelle Anpassungen und flexible Handhabung seitens des Nutzers. Sofern der Anbieter eines Social Networks Daten der Nutzer aufgrund einer Einwilligung auch für Zwecke der zielgruppenspezifischen Werbung nutzt, kann dem Nutzer die Möglichkeit gegeben werden, die ihn erreichende Werbung (differenziert nach den einzelnen Formen der Werbung und Informationen) individuell durch Widerruf seiner jeweiligen Zustimmung seinen Interessen anzupassen (Opt-out-Verfahren). Wie bei den Privacy-Einstellungen (vgl. oben 3.1) besteht auch hierzu keine gesetzliche Verpflichtung.

3.5 Anonyme oder pseudonyme Nutzung des Netzwerks?

Für die Anbieter von sozialen Netzwerken kann sich die Frage stellen, ob es sinnvoll ist, den Nutzern die anonyme oder pseudonyme Nutzung des Netzwerks zu ermöglichen. Eine gesetzliche Verpflichtung hierzu trifft Anbieter von Social Networks regelmäßig nicht:

§ 3a des Bundesdatenschutzgesetzes normiert das allgemeine Gebot der Datenvermeidung und Datensparsamkeit. Als Konkretisierung dieses Gebots muss der Diensteanbieter gemäß § 13 Abs. 6 des Telemediengesetzes (TMG) die anonyme oder pseudonyme Nutzung des Dienstes ermöglichen, allerdings nur dann, wenn ihm

Stellungnahme

Datenschutzkonforme Gestaltung von Social Networks

Seite 10

dies technisch möglich und zumutbar ist. Eine Unzumutbarkeit liegt dann vor, wenn der konkrete Dienst seinem Inhalt nach eine Identifizierbarkeit des Nutzers voraussetzt, was anhand der Verkehrsauffassung zu beurteilen ist. Bei Social Networks besteht sowohl aus der Sicht der Nutzer als auch aus der Sicht der Anbieter ein wichtiger Aspekt gerade in der eigenen Auffindbarkeit bzw. in der Auffindbarkeit von konkreten Personen, Freunden und Bekannten. Die pseudonyme Nutzung der Plattform steht dieser Funktion und der Qualität des Netzwerks diametral entgegen und ist daher unzumutbar.

Auch unter einem weiteren, wichtigen Aspekt ist eine anonyme oder pseudonyme Nutzung von Social Networks fragwürdig. Es liegt auf der Hand, dass die Bereitschaft zu gesetzeswidrigen Verhaltensweisen oder Verstößen gegen einen Verhaltenskodex (vgl. 3.6) steigt, wenn sich der Nutzer hinter einem Pseudonym verbergen kann. Social Networks wollen insoweit den Nutzern in der virtuellen Welt aber keine anderen Handlungsspielräume eröffnen, als sie in ihrer realen Alltagswelt haben.

Insbesondere ist in diesem Zusammenhang auf einen immanenten Zielkonflikt zwischen dem Schutz der Jugend und Datenschutz hinzuweisen. Das Prinzip der pseudonymen Nutzung wird in Web2.0-Plattformen durch Phänome wie „Grooming“ (Annäherungsversuche gegenüber jugendlichen Teilnehmern) oder das sog. „Cyberbullying“ (Mobbing unter Schülern unter Einsatz von Medien) auf die Probe gestellt. Es ist daher wichtig, die datenschutzrechtliche Diskussion nicht allein auf dem Boden vertrauter formaler Prinzipien zu führen, sondern den sich verändernden gesellschaftlichen wie technologischen Kontext zu berücksichtigen. Dieser Kontext spricht gerade aus der Nutzerperspektive gegen die Ermöglichung pseudonymer Nutzung.

Letztlich sprechen daher aus Anbieter- und aus Nutzersicht gewichtige Gründe gegen eine pseudonyme Nutzung des Social Networks.

3.6 Verhaltenskodex für die Nutzer

Anbieter eines Social Networks sollten ihre Nutzer auf einen verbindlichen Verhaltenskodex verpflichten. Ein derartiger Verhaltenskodex sollte sowohl die Einhaltung der gesetzlichen Vorschriften als auch die Verpflichtung auf soziale und ethische Mindeststandards beinhalten. Der Anbieter sollte darüber hinaus die Möglichkeit haben, Nutzer bei Verstößen gegen den Kodex von der weiteren Nutzung der Plattform auszuschließen.