Arbeitsgruppe 5

„Verantwortung und Schutzrechte in der vernetzten Welt“

11 Tipps für einen sicheren Umgang mit sozialen Netzwerken

Soziale Netzwerke gehören zu den meistgenutzten Online-Medien der Gegenwart. Sie sind eine neue Art der Kommunikation im öffentlichen und auch im privaten Raum. Dabei bieten soziale Netzwerke zahlreiche Chancen und Vorteile im Hinblick auf Vernetzung, Information und Präsentation der Nutzer. Aufgrund der zunehmenden Verbreitung sogenannter Smartphones sind die Nutzer sozialer Netzwerke ständig mit dem Medium verbunden und können es unabhängig von Zeit und Ort nutzen.

Obwohl es sich bei sozialen Medien um ein vergleichsweise junges Phänomen handelt, haben sie sich bereits in wenigen Jahren auf höchst rasante Weise verbreiten können. „Halb Deutschland ist Mitglied in sozialen Netzwerken“ betitelt der Branchenverband BITKOM eine Pressemitteilung vom 13. April 2011. Rund 70 Prozent der deutschen Unternehmen nutzen soziale Netzwerke. Sowohl für Unternehmen als auch für Privatpersonen gilt: Tendenz weiter steigend. Denn die Möglichkeiten, die soziale Netze bieten, sind vielfältig und lohnenswert.

Allerdings stellt diese Entwicklung private Nutzer, professionelle Nutzer, Unternehmen, aber auch den Gesetzgeber vor Herausforderungen. Worauf müssen gerade junge Erstnutzer achten? Wie stelle ich sicher, dass ich eine gute berufliche Reputation behalte? Wie stellen Unternehmen sicher, dass ihre Mitarbeiter sich adäquat in sozialen Netzen verhalten? Wo müssen Rechtsrahmen neu definiert oder geschaffen werden?

Hierzu geben die nachfolgenden 11 grundlegenden Tipps Auskunft.

1. Ob privat oder beruflich: Setzen Sie sich mit einem sozialen Netzwerk auseinander und nutzen Sie es bewusst!

Die Anmeldung bei einem sozialen Netzwerk ist mit wenigen Klicks geschehen, ebenso das Einstellen von Bildern oder das schnelle Absetzen von öffentlichen Kommentaren. Aber: Machen Sie sich vorher Gedanken, wie Sie öffentlich erscheinen wollen. Überlegen Sie, welche Äußerungen und Bilder Sie der Welt zeigen möchten und was Ihre Vorgesetzten, Kollegen, Nachbarn oder selbst die Lehrer Ihrer Kinder darüber denken könnten. Treffen Sie dann entsprechende Einstellungen zur Sichtbarkeit Ihrer Profile, Äußerungen und zu den einzelnen Datenfreigaben. Stellen Sie sicher, dass Sie das Geschäftsmodell des Anbieters verstehen; beispielsweise finanzieren sich viele kostenlose Services dadurch, dass Ihnen Werbung eingeblendet wird, die unter Umständen auf der Grundlage Ihrer Daten auf Sie zugeschnitten ist. Sich bewusst mit sozialen Netzwerken auseinanderzusetzen, heißt keineswegs, auf Spaß am Umgang miteinander zu verzichten – sondern nur, die Risiken zu minimieren.

Rechtliche Vertiefungshinweise:

In sozialen Netzwerken werden Einzelangaben über persönliche oder sachliche Verhältnisse verarbeitet. Diese Daten werden zunehmend zur Währung im Web 2.0. Die Zulässigkeit der Verarbeitung personenbezogener Daten hat zunächst einmal unter Berücksichtigung der verfassungsrechtlichen Vorgaben zu erfolgen, wonach jeder selbst entscheiden können sollte, wer was wann und bei welcher Gelegenheit über ihn weiß. Wer diese Entscheidungsfähigkeit verliert, kann die Konsequenzen seines Handelns und die Reaktionen seiner Kommunikationspartner nicht mehr effizient einschätzen und läuft damit Gefahr, individuelle Entfaltungs- und Entwicklungschancen aufgeben zu müssen. Zur Sicherung des informationellen Selbstbestimmungsrechts ordnet § 4 Abs. 1 BDSG an, dass der Umgang mit personenbezogenen Daten der Einwilligung des Betroffenen oder einer gesetzlichen Erlaubnis bedarf.

2. Beachten Sie bei der beruflichen Nutzung eines Netzwerks die Richtlinien Ihres Arbeitgebers und veröffentlichen Sie keine Interna!

Die berufliche Nutzung von sozialen Netzwerken ist mittlerweile in vielen Branchen zum alltäglichen Standard geworden. Als Arbeitnehmer können Sie sich mit Ihren Kollegen, mit Geschäftspartnern oder auch potenziellen Kunden und Arbeitgebern verbinden. Achten Sie bei der beruflichen Nutzung – besonders während der Arbeitszeiten – darauf, dass Sie die entsprechenden Vorgaben Ihres Arbeitgebers zur Nutzung sozialer Netzwerke kennen und berücksichtigen. Viele Firmen verfügen bereits über solche Richtlinien, so genannte „Social

Media Guidelines“.

Arbeitnehmer sind gut beraten, bei Ihrer Personal- oder Kommunikationsabteilung entsprechende Erkundigungen einzuholen. In jedem Fall sollten Sie sich – als Faustregel – so verhalten, wie Sie es auch bei einem normalen Gespräch etwa auf einer Messe tun würden. Reden Sie nicht schlecht über Ihre Firma oder über Kollegen, geben Sie keine Firmen- oder Kundeninterna heraus und leiten Sie relevante Themen wie etwa Beschwerden an die zuständigen Abteilungen weiter.

Als Arbeitgeber und Unternehmen sollten Sie hingegen nicht versuchen, die Nutzung sozialer Netzwerke vollständig aus dem Arbeitsalltag zu verbannen. Ihre Mitarbeiter würden sich bevormundet fühlen. Dies wird durch eine einschlägige Studie von Cisco Systems (Oktober 2010) belegt, wonach bspw. mehr als die Hälfte der Studenten Wert auf Social-Media-Richtlinien in ihren künftigen Unternehmen legen. Fast jeder Dritte würde grundsätzlich nicht in einem „unsozialen“ Unternehmen arbeiten wollen.

Rechtliche Vertiefungshinweise:

Mitarbeiter müssen sich im Rahmen der Nutzung sozialer Netzwerke ihrer ständig steigenden Informationsverantwortung bewusst werden. Sehr viel häufiger als früher tritt der Einzelne im Marktgespräch als unmittelbarer Repräsentant des Unternehmens auf. Dabei gilt es, die Verschwiegenheits- und Loyalitätserwartungen des Unternehmens mit den Erwartungen der Mitarbeiter und deren Kommunikationspartner auf eine transparente, authentische und direkte Gesprächskultur auszutarieren. Das bedeutet, dass auch im Social Web die berechtigte Wahrung von Betriebs- und Geschäftsgeheimnissen nicht mit Intransparenz verwechselt werden sollte. Die strafrechtliche Sanktionierung der Mitteilung von Geschäfts- und Betriebsgeheimnissen unter den Voraussetzungen des § 17 UWG stellt eine zumutbare Schranke dar. Die dahingegen weiter reichende – sich aus der arbeitsvertraglichen Pflicht zur Rücksichtnahme (§§ 241 Abs. 2, 242 BGB) – ergebende Verschwiegenheitsverpflichtung muss neben der Meinungsäußerungsfreiheit des Arbeitnehmers (Art. 5 Abs. 1 Satz 1 GG) gerade auch die durch einen offenen Austausch entstehenden positiven Effekte zielführend berücksichtigen.

Unternehmen sollten beachten, dass sie im Rahmen der privaten Internetnutzung durch Mitarbeiter während der Arbeitszeit zu Telekommunikationsanbietern werden können und dann zur Wahrung des Fernmeldegeheimnisses verpflichtet sind.

3. Nationaler Datenschutz vs. globales Internet: Berücksichtigen Sie das je nach Sitz des Anbieters gewährte unterschiedliche Datenschutzniveau!

Soziale Netzwerke verarbeiten die personenbezogenen Daten der Nutzer. Dies sollte nur im Auftrag und im Sinne der Nutzer geschehen. Daher sollten Nutzer vor dem Beitritt zu einem

sozialen Netzwerk besonders darauf achten, welches Datenschutzniveau vom Betreiber des sozialen Netzwerks gewährleistet wird. Denn weltweit gibt es ganz unterschiedliche Herangehensweisen an die Themen „Datenschutz“ und „Privatsphäre“, während das Internet und soziale Netzwerke globale und grenzüberschreitende Medien sind. Daher halten sich viele ausländische Anbieter nicht an deutsches Datenschutzrecht, obschon sie deutsche Nutzer durch deutschsprachige Websites, deutschsprachige AGB und Verwendung einer .de-Domain gezielt ansprechen.

Das deutsche Datenschutzrecht bietet ein im internationalen Vergleich hohes Schutzniveau und stellt konsequent die Kontrolle des Nutzers über seine Daten in den Vordergrund: Jede Erhebung, Verarbeitung und Nutzung seiner Daten setzt das Vorliegen seiner Einwilligung oder einer gesetzlichen Erlaubnis voraus. Ganz anders beispielsweise das US-amerikanische Datenschutzverständnis: Hier genügt häufig, dass sich der Nutzer darüber informieren kann, was mit seinen Daten passiert. Daher legen ausländische Anbieter von sozialen Netzwerken häufig Persönlichkeitsprofile von Nutzern an und geben diese Daten an Dritte weiter, ohne dass die Nutzer sich damit einverstanden erklärt haben.

Daher gilt: Informieren Sie sich darüber, welches Datenschutzniveau gewährt wird. Fragen Sie sich: Sind die Voreinstellungen der Privatsphäre restriktiv eingestellt (sog. privacy by default)? Kann ich stets und einfach die Privatsphäreeinstellungen überblicken und ändern? Prüfen Sie die Datenschutzerklärung!

Rechtliche Vertiefungshinweise:

Für nicht in den Mitgliedstaaten der Europäischen Union ansässige Betreiber sozialer Netzwerke, die nicht über eine Niederlassung in Deutschland verfügen, richtet sich die Anwendbarkeit des deutschen Datenschutzrechts gem. § 1 Abs. 5 Satz 2 BDSG nach dem Ort der Erhebung, Verarbeitung oder Nutzung der Daten (sog. Territorialitätsprinzip). Findet der Umgang mit personenbezogenen Daten in Deutschland statt, kommt deutsches Datenschutzrecht zur Anwendung, sofern die personenbezogene Daten enthaltenden Datenträger nicht lediglich gem. § 1 Abs. 5 Satz 4 BDSG zum Zweck des Transits durch Deutschland eingesetzt werden. Das deutsche Datenschutzrecht kann folglich grundsätzlich auch für jeden ausländischen Anbieter sozialer Netzwerke zur Anwendung kommen. Unter welchen genauen Umständen dies der Fall ist, ist umstritten und kann den einschlägigen Regelwerken nicht ohne weiteres entnommen werden.

Ein effizienter Datenschutz setzt voraus, dass datenschutzrechtliche Grundkonzepte bereits bei der Entwicklung neuer Technologien berücksichtigt und in deren Gesamtkonzeption einbezogen werden (sog. privacy by design). Die Grundeinstellungen von Produkten und Diensten sind zudem so zu gestalten, dass so wenig personenbezogene Daten wie möglich erhoben oder verarbeitet werden und für Dritte einsehbar sind (sog. privacy by default), ohne dass der Nutzer vor die Aufgabe der Bewältigung eines „undurchdringlichen

Optionsdickichts“ gestellt wird.

Gleichwohl darf ein effizienter Datenschutz nicht bei den Datenschutzforderungen nach „privacy by design bzw. default“ stehen bleiben. Zur Wahrung der informationellen Selbstbestimmung ist vielmehr auch erforderlich, dass die Prozesse offengelegt werden (Transparency), dass dem Nutzer auch (nachhaltig) geholfen wird (Assistance), dass der Nutzer vor diesem Hintergrund feinjustieren kann (Adjustment) und dass schließlich alles durch vertrauensbildende Maßnahmen begleitet wird (Trust). Ein wirksames Instrument kann in diesem Sinne ein Smart Privacy Management sein, wie es anlässlich des 5. Nationalen IT-Gipfels seitens der AG 5 als Konzept für einen effizienten Daten- und Jugendschutz in sozialen Netzwerken erarbeitet wurde.

4. Ihr Vertrauen verdient Transparenz: Prüfen Sie die Datenschutzerklärungen der Anbieter!

In der Datenschutzerklärung muss der Anbieter den Nutzer genau, vollständig, verständlich und transparent darüber informieren, wie, in welchem Umfang und zu welchem Zweck er die Daten des Nutzers verarbeitet und wer Kenntnis von ihnen nehmen kann. Im Gegensatz dazu entspräche eine allgemeine Aussage wie „Wir verwenden Deine Daten für Werbezwecke“ nicht den deutschen Anforderungen an eine Datenschutzerklärung.

Soziale Netzwerke für Kinder und Jugendliche sollten diese Informationen zudem spezifisch für junge Nutzer aufbereiten und zum Beispiel mit Kurzfilmen optisch aufwerten, wie dies z.B. im sozialen Netzwerk schülerVZ der Fall ist.[1] Bei Verständnisproblemen sollten sich gerade erwachsene Erstnutzer und junge Nutzer an den Betreiber wenden oder das Internet, ihre Eltern, ältere Geschwister oder Lehrer zu Rate ziehen.

Im Rahmen der Datenschutzerklärung muss der Anbieter gegebenenfalls auch Einwilligungserklärungen des Nutzers einholen. Dabei ist zu berücksichtigen, dass nach deutschem Recht minderjährige Nutzer nur in begrenztem Umfang solche Erklärungen abgeben können, da sie nicht vollständig die Bedeutung und die Konsequenzen einer solchen Einwilligung überblicken können.

Vor allem aber bedarf es immer dann solcher Einwilligungserklärungen, wenn die Daten an andere Unternehmen weitergegeben werden sollen.

Rechtliche Vertiefungshinweise:

Datenschutzerklärungen sind auch im Kontext sozialer Netzwerke Allgemeine Geschäftsbedingungen, die häufig Einwilligungserklärungen der Nutzer in den – oftmals sehr

[1] Vgl. http://www.schuelervz.net/l/rules, abgerufen am 22.09.2011.

umfassenden – Umgang mit deren personenbezogenen Daten enthalten. Derartige Vertragsklauseln müssen sich u.a. an den Vorgaben von § 4a BDSG und §§ 12, 13 TMG messen lassen. Der Nutzer sozialer Netzwerke muss folglich über Art, Umfang und Zwecke der Erhebung und Verwendung seiner Daten in allgemein verständlicher Form unterrichtet werden. Er muss die Möglichkeit erhalten, all diese Informationen vollzählig abzurufen und ohne Weiteres zur Kenntnis zu nehmen.

In der Praxis werden Bedeutung und Inhalt von Datenschutzerklärungen häufig unterschätzt. Der Nutzer sollten in diesem Zusammenhang bedenken, dass ungeachtet der Bezeichnung als „Datenschutzerklärung“ eine Einwilligung in Vorgänge erteilt wird, die gerade nicht seinem Schutz dienen, sondern eine Vermarktung personenbezogener Daten ermöglichen sollen. Eine genaue Durchsicht der Erklärungsinhalte ist folglich notwendig.

Auch die Weitergabe personenbezogener Daten zu Werbezwecken ist von der Einwilligung des Nutzers abhängig. Diese muss insbesondere ohne Zwang zustande kommen und ist jederzeit frei widerruflich.

5. Prüfen Sie, welche Rechte der Anbieter an Ihren Inhalten verlangt!

Die Rahmenbedingungen für die Rechte und Pflichten von Betreibern und Nutzern eines sozialen Netzwerks werden in den **Allgemeinen Geschäftsbedingungen** (AGB) geregelt. Dies gilt insbesondere für den sogenannten **„user generated content“**, also die **„von Nutzern generierten Inhalte“**. Darunter sind alle Beiträge zu verstehen, die die Nutzer selbst in das Netzwerk schreiben oder hochladen (Nachrichten, Posts aller Art, Fotos, Videos etc.). Viele Anbieter lassen sich mit der Vereinbarung ihrer AGB umfassende Nutzungsrechte an diesen Inhalten einräumen. Das kann bei einzelnen Typen sozialer Netzwerke gerechtfertigt sein. Häufig aber geht die Rechteeinräumung weit über das erforderliche Maß hinaus und offenbart Geschäftsmodelle, die den Nutzern nicht transparent gemacht werden. Sie sollten daher prüfen, welche Nutzungsrechte sich der Anbieter durch die AGB an Ihren Inhalten einräumen lässt. Vorbildlich sind beispielsweise soziale Netzwerke, die sich überhaupt keine Rechte an den Inhalten der Nutzer einräumen lassen.

Rechtliche Vertiefungshinweise:

In zunehmendem Maße besteht im Rahmen der Nutzung sozialer Netzwerke die Möglichkeit, selbst erstellte Inhalte in die Website der Diensteanbieter einzubinden und Dritten zugänglich

zu machen. Sind die vom Nutzer erstellten Inhalte urheberrechtlich geschützt, entscheidet er allein, wie sein Werk genutzt werden darf. Daher darf der Diensteanbieter die Inhalte nicht nutzen, wenn dies zwischen Nutzer und Diensteanbieter nicht ausdrücklich vereinbart wurde. Soll der Diensteanbieter zur Nutzung berechtigt sein, kann der Nutzer ihm Nutzungsrechte einräumen. Das Urheberrecht als ganzes ist dagegen nicht übertragbar (§ 29 Absatz 1 des UrhG). Inhalt und Umfang der Einräumung von Nutzungsrechten ist wie stets Frage der Vertragsgestaltung. Für die Vertragsauslegung gilt der Zweckübertragungsgrundsatz gemäß § 31 Absatz 5 UrhG, wonach die Nutzungsrechte tendenziell beim Urheber verbleiben.

Um eine zulässige Nutzung der von Nutzern generierten Inhalte zu ermöglichen, greifen viele Diensteanbieter auf Vertrags- und Nutzungsbedingungen zurück, die sich nicht nur an den oben genannten Bestimmungen des Urheberrechtsgesetzes über die Einräumung von Nutzungsrechten, sondern auch an den AGB-rechtlichen Vorschriften der §§ 305 ff. BGB messen lassen müssen. Ob diese Regelungen rechtlichen Bestand haben, ist im Einzelfall meist ohne die Einbindung juristischen Sachverstands nicht zu klären. Zudem besteht die Problematik, dass auch unwirksame Nutzungsvereinbarungen seitens der Betreiber sozialer Netzwerke zunächst wie wirksame Vereinbarungen behandelt werden.

Nutzern sozialer Netzwerke empfiehlt es sich daher, solche Vereinbarungen auf deren mögliche Folgen zu prüfen und ggf. von der Teilnahme an einem mit „kritischen“ Vertragsklauseln belasteten sozialen Netzwerk Abstand zu nehmen.

6. Überlegen Sie genau, welche Informationen und Bilder Sie für wen freigeben!

Der einfache Test: Was würden Sie einem wildfremden Menschen im Bus erzählen? Ihre Anschrift, Ihre politische Einstellung zu aktuellen kontroversen Themen – und vielleicht noch die Partybilder von letzter Nacht? Womöglich, aber wahrscheinlich nicht. Dementsprechend sollten Sie auch bei der Nutzung von sozialen Netzwerken genau abwägen, wem Sie welche Informationen bereitstellen. Enge Freunde oder jahrelange Geschäftspartner können natürlich Ihre Privat- oder Firmen-Adresse kennen, lose Bekannte Ihre Wanderfotos und vielleicht auch eine E-Mail-Adresse, komplett Fremde hingegen nur Ihren Namen und vielleicht Ihre Hobbies und Ihren Beruf. Viele soziale Netzwerker bieten die Möglichkeit, Sichtbarkeitseinstellungen sehr genau für bestimmte Personen oder Personengruppen einzustellen – nutzen Sie das!

Und noch ein Tipp zu Bildern: Denken Sie hier nicht nur an sich! Netzwerke bieten mitunter die Möglichkeit, Menschen direkt in Bildern zu kennzeichnen – machen Sie davon nur Gebrauch, wenn Sie wissen, dass der- oder diejenige auch wirklich damit einverstanden ist. Sonst kann es im schlimmsten Fall passieren, dass jemand, ohne es zu wissen, über Freunde in peinlichen Fotos öffentlich markiert wird.

Rechtliche Vertiefungshinweise:

Das allgemeine Persönlichkeitsrecht ist seit BGHZ 13, 334 (Leserbriefe) als ein durch Art. 1 in Verbindung mit Art. 2 GG verfassungsmäßig garantiertes Grundrecht und zugleich als ein nach § 823 Abs. 1 BGB geschütztes „sonstiges Recht“ anerkannt. Bei dem Recht am eigenen Bild handelt es sich um eine besondere Erscheinungsform des allgemeinen Persönlichkeitsrechts. Einfachgesetzlich wird das Recht am eigenen Bild durch das KUG geschützt. Gemäß §§ 22, 23 KUG ist die Verbreitung und öffentliche Zurschaustellung des Bildnisses einer Person ohne deren Einwilligung vorbehaltlich der dort näher geregelten Ausnahmen verboten. Ausnahmen liegen unter anderem dann vor, wenn Personen lediglich als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen.

Verstöße sind gemäß § 33 Abs. 1 KUG strafbar: Danach wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wer entgegen den §§ 22, 23 KUG ein Bildnis verbreitet oder öffentlich zur Schau stellt. Zudem können Verstöße gegen das KUG sowie Verletzungen des allgemeinen Persönlichkeitsrechts Unterlassungs- und Schadensersatzforderungen nach sich ziehen.

7. Nicht jeder ist der, der er vorgibt, zu sein: Prüfen Sie, mit welcher virtuellen Identität Sie sich einlassen!

Häufig sollen die Profile in sozialen Netzwerken ein realistisches Bild der Person wiedergeben, die das Profil angelegt hat. Aber nicht immer, und das ist – meistens – auch gut so! So gibt es viele Situationen, in denen Sie Wert auf die zutreffende Angabe ihrer Daten und somit die echte Darstellung ihrer Person legen sollten. Viele soziale Netzwerke sind ja gerade deswegen so attraktiv, weil sich die Nutzer gegenseitig erkennen können. Es kann aber auch Situationen geben, in denen Sie lieber anonym erscheinen wollen. In solchen Fällen sollten Sie nicht Ihren richtigen Namen als Profilnamen wählen; in der Regel akzeptieren die Betreiber von sozialen Netzwerken dies auch.

Als Konsequenz daraus ist bei der Kontaktaufnahme mit anderen virtuellen Identitäten zu beachten, dass nicht jeder im sozialen Netzwerk derjenige sein muss, der er vorgibt zu sein. So gibt es neben Profilen mit anonymen Phantasienamen auch sogenannte *Fake-Profile*, die vortäuschen, das Profil einer – tatsächlich unbeteiligten – dritten Person zu sein. Prüfen Sie daher immer, mit wem sie sich einlassen: Erscheinen das gesamte Profil und auch die Kontakte des Profils plausibel? Können andere Nutzer die Identität des Nutzers bestätigen? Besonders Kinder und Jugendliche sollten sich diese Fragen stellen, wenn sie in Kontakt mit anderen virtuellen Identitäten treten und diesen Kontakt eventuell im realen Leben ausbauen möchten, da ihre Erfahrungswerte im Umgang mit anderen Menschen oftmals noch nicht so ausgeprägt sind wie die von Erwachsenen.

Rechtliche Vertiefungshinweise:

§ 13 Abs. 6 TMG sieht vor, dass Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym ermöglichen müssen, soweit dies technisch mach- und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren. Ob die gegenwärtige Praxis einiger Betreiber sozialer Netzwerke, die eine anonyme oder pseudonyme Nutzung ihrer Dienste ausschließen oder nur sehr eingeschränkt zulassen, im Einklang mit den rechtlichen Vorgaben steht, ist bislang nicht abschließend geklärt. Fest steht aber, dass die Verwendung anonymer oder pseudonymer Profile im Rahmen sozialer Netzwerke einen wertvollen Beitrag zum Selbstdatenschutz leisten kann.

Das Erstellen sog. Fake-Profile, also von Profilen, die vorgeben, das Profil einer Dritten und unbeteiligten Person zu sein, ist in rechtlicher Hinsicht äußerst problematisch und sollte unterbleiben. Neben möglichen Verstößen gegen das KUG („fremde“ Profilbilder) besteht die Gefahr, dass die Eröffnung eines Mitgliedskontos unter falschem oder fremdem Namen auch den Tatbestand des § 269 StGB (Fälschung beweiserheblicher Daten) erfüllen könnte. Dies hat zum Beispiel das Kammergericht Berlin angenommen, als es über die Strafbarkeit der Einrichtung eines eBay-Accounts unter Verwendung der Namens- und Adressdaten einer fremden, bereits verstorbenen Person zu entscheiden hatte.

8. Soziale Netzwerke leben von der Gemeinschaft und vom Mitmachen: Melden Sie inakzeptables Verhalten!

Die Rahmenbedingungen für die Rechte und Pflichten von Betreibern und Nutzern eines sozialen Netzwerks werden in den AGB und häufig auch in einem ergänzenden Verhaltenskodex geregelt. Nicht zuletzt für junge Nutzer sollten diese Regeln verständlich formuliert sein. Bei Verständnisfragen sollten Kinder und Jugendliche Hilfe bei ihren Eltern suchen oder den Betreiber des Netzwerks kontaktieren.

In diesen Regelwerken finden sich die Verhaltens- und Spielregeln des Netzwerks, an die sich alle Beteiligten halten müssen. Solche Regelungen sind notwendig, damit die Nutzer respektvoll miteinander umgehen und sich nicht in ihren Rechten verletzen. Beispielsweise sollte ein Nutzer Fotos von anderen Nutzern nur dann in das soziale Netzwerk hochladen und/oder andere Nutzer auf dem Foto nur dann identifizieren, wenn der abgebildete Nutzer dem zustimmt. Andernfalls kann eine Verletzung der Rechte des abgebildeten Nutzers vorliegen, etwa des Rechts am eigenen Bild gemäß § 22 des KUG, die auch gegen die AGB und den Verhaltenskodex des sozialen Netzwerks verstößt.

Es besteht keine Verpflichtung der Anbieter von sozialen Netzwerken, von den Nutzern erstellte Inhalte „proaktiv“ zu überprüfen und z. B. festzustellen, ob Respektlosigkeiten oder gar Rechtsverletzungen vorliegen. Wichtig ist das Prinzip der Selbstkontrolle der Nutzer: Sie sind aufgefordert, den Betreiber darüber zu informieren, wenn Verstöße gegen die Regeln

des sozialen Netzwerks oder eine Verletzung von Rechten Dritter vorliegen. Für diese Mitteilungen der Nutzer sollten „Melde“-Funktionen vorhanden sein. Gute Betreiber von sozialen Netzwerken legen besonderen Wert darauf, dass diese Funktionen einfach zu finden und einfach zu handhaben sind. Auf diese Weise üben die Nutzer sozialer Netzwerke gegenseitig eine gewisse soziale Kontrolle aus. Gerade für junge Nutzer ist es wertvoll, sich mit den Regeln des Netzwerks auseinanderzusetzen, Verantwortung für deren Einhaltung zu übernehmen und so für sich und andere Nutzer eine positive Umgebung im Netzwerk zu erhalten.

Rechtliche Vertiefungshinweise:

Technologische Lösungen können in vielen Bereichen Instrumente eines wirksamen Interessenschutzes im Internet bilden. Gerade auf dem Gebiet des Schutzes des allgemeinen Persönlichkeitsrechts bieten sich oftmals sogenannte "Button-Lösungen" an, um Nutzer vor digitalen Verletzungshandlungen zu schützen. So gibt es beispielsweise die Möglichkeit, einen Einwilligungs-Button für die Vernetzung mit Bildern anderer Accounts einzuführen, wie es manche soziale Netzwerke schon getan haben.

Genauso kann mit der Möglichkeit von "Melde-Buttons" einiges an digitalem Unrecht unter Umständen recht schnell und unkompliziert beseitigt werden. Gegen Einträge auf Pinnwänden sollte man sich durch sogenannte "Notice-Buttons" zur Wehr setzen können.

In diesem Zusammenhang gilt, dass die Beweislast im Zweifel auf Seiten des vermeintlichen Verletzers liegt, der sich mit einem "Counter-Notice-Button" oder Ähnlichem gegen die Vorwürfe verteidigen können sollte.

9. Prüfen Sie, wie Ihr Profil aus der Perspektive anderer aussieht und welche Daten dabei verfügbar sind.

Viele Nutzer sowohl beruflicher als auch privater Netzwerke schätzen es, dass ihre Profile auch bei der Google-Suche nach ihrem Namen – in aller Regel ganz oben – erscheinen. So können Sie sicherstellen, dass Sie so gesehen werden, wie Sie es wollen. Um das sicherzustellen, beschäftigen Sie sich mit der Frage: Wie sieht Ihr Profil für andere Nutzer eigentlich aus? Was für Daten und Bilder können zum Beispiel Ihr Chef oder Ihre Nachbarn sehen? Das können Sie auf zweierlei Weise prüfen. Um zu sehen, wie gänzlich fremde Personen – auch Nicht-Mitglieder des jeweiligen sozialen Netzwerks – Ihr Profil sehen, loggen Sie sich kurz aus dem Netzwerk aus und suchen Sie dann nach Ihrem Profil. Um die Sicht anderer Netzwerk-Mitglieder nachzuvollziehen, rufen Sie die jeweiligen Vorschau-Funktionen auf. Diese heißen je nach Netzwerk etwas anders, zum Beispiel „Zur Ansicht für Profilbesucher“ oder „Anzeigen als…“. Überprüfen Sie, ob Sie mit dem Ergebnis einverstanden sind und passen Sie gegebenenfalls Ihre eingegebenen Daten und die

Sichtbarkeitseinstellungen an. Stellen Sie sicher, dass man Sie so sieht, wie Sie gesehen werden wollen.

Rechtliche Vertiefungshinweise:

Die Masse mittels sozialer Netzwerke zugänglicher Profildaten kann manche Arbeitgeber dazu veranlassen, auf diese Weise zusätzliche Informationen über bereits eingestellte oder zukünftige Arbeitnehmer zu gewinnen. Insoweit sieht § 32 Abs. 1 Satz 1 BDSG vor, dass personenbezogene Daten eines (zukünftigen) Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach dessen Begründung für die Durchführung oder Beendigung erforderlich ist. Ob ein sog. Bewerbercheck erforderlich ist, ist umstritten. Zudem ist fraglich, ob über die Regelungen des § 32 BDSG hinaus in der vorliegenden Konstellation die Vorschrift des § 28 Abs. 1 Satz 1 Nr. 3 BDSG, der die Erhebung von allgemein zugänglichen Daten gestattet, zur Anwendung kommen kann.

Klarheit könnte insoweit die geplante Regelung des Beschäftigtendatenschutzes im Entwurf eines Beschäftigtendatenschutzgesetzes schaffen: Nach dem eines dort vorgesehenen neuen § 32 Abs. 6 BDSG dürften Bewerberdaten grundsätzlich nur beim betroffenen Bewerber erhoben werden (§ 32 Abs. 6 Satz 1 BDSG). Eine Erhebung allgemein zugänglicher Daten wäre aber gestattet, sofern das schutzwürdige Interesse des Bewerbers am Ausschluss der Erhebung nicht überwiegt (§ 32 Abs. 6 Satz 2 BDSG). Letzteres soll insbesondere dann der Fall sein, wenn es sich um Daten aus privat genutzten sozialen Netzwerken handelt. Netzwerke, die zur Darstellung der beruflichen Qualifikation bestimmt sind, dürften dagegen vom Arbeitgeber eingesehen werden. Jedoch bestehen ernstliche Zweifel, wie in der Praxis eine sachgerechte trennscharfe Abgrenzung beruflich und privat genutzter Netzwerke erfolgen soll.

Sind Profile und Einträge in sozialen Netzwerken (wie Facebook oder Google+) und (Micro)-Blogging-Dienste (wie Twitter) den Suchmechanismen von Suchmaschinen zugänglich, können unter demselben Namen geführte Profile und Einträge verschiedener Plattformen dort leicht zu einer Art „Gesamtprofil“ verschmelzen. Speziell dafür vorgesehene Personensuchmaschinen bündeln die über eine Person im Netz vorhandenen Informationen sogar gezielt. Nutzer, die ihre Informationen in verschiedenen Plattformen verteilen, sind sich zwar möglicherweise der öffentlichen Preisgabe ihrer Daten für den Einzelfall bewusst, nicht jedoch der Reichweite der Auffindbarkeit und Verfügbarkeit in ihrer Gesamtheit. Wenn die auf diese Weise kombinierbaren Daten die Erstellung umfassender Persönlichkeits- und Bewegungsprofile ermöglichen, so ist dies mit dem verfassungsrechtlich gewährleisteten Grundrecht auf informationelle Selbstbestimmung nur schwer zu vereinbaren.

10. Verwenden Sie sichere, für jeden Dienst unterschiedliche Passwörter!

Wer Ihre Kennwörter kennt, kann sich damit für Sie in soziale Netzwerke einloggen, Ihre persönlichen Nachrichten lesen und in Ihrem Namen Kommentare veröffentlichen – mit enormen Gefahren für Ihr Privat- und Geschäftsleben.

Schützen Sie daher Ihre Online-Passwörter, indem Sie komplexe Systeme aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen verwenden und insbesondere für Dienste mit sensiblen Daten verschiedene Kennwörter verwenden! Dies können Sie erreichen, indem Sie kleine Änderungen einfügen, zum Beispiel eine unterschiedliche Zahl am Ende. Weitere Tipps finden Sie hier: http://redir.ec/passwort-tipps

Seien Sie besonders vorsichtig, wenn Sie an einem öffentlichen Computer (zum Beispiel in einem Internet-Café) im Internet sind – stellen Sie sicher, dass niemand Sie bei der Eingabe der Passwörter beobachtet, dass der Browser Ihr Passwort bei der Eingabe nicht speichert und dass Sie sich am Ende von allen Diensten abmelden.

Rechtliche Vertiefungshinweise:

§ 9 BDSG ordnet an, dass Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen haben, die erforderlich sind, um ein gesetzeskonformes Datenschutzniveau zu gewährleisten. Obgleich sich die Vorschrift nicht an private Nutzer richtet, kann die freiwillige Beachtung der aus dieser Datensicherheitsvorschrift folgenden Anforderungen ein Instrument eines effizienten Selbstdatenschutzes sein.

Ein unbefugter Zugriff auf personenbezogene Daten wird beispielsweise durch die Verwendung von Passwörtern oder spezieller Sicherheitssoftware verhindert. Im Internet kann zudem die Verwendung von Firewalls, digitalen Signaturen und Verschlüsselungsverfahren das persönliche Schutzniveau erhöhen.

11. Die Technik und die Funktionen bleiben komplex: Erweitern Sie Ihre Medienkompetenz und die Ihrer Kinder

Soziale Netzwerke sind vielfältige und komplexe Kommunikationsmedien. Es ist daher gerade für junge Nutzer, aber auch für erwachsene Erstnutzer wichtig, die vielfältigen Möglichkeiten dieser **Medien kompetent, selbstbestimmt und kritisch zu nutzen.** Daher sollten die Nutzer die erforderliche **Medienkompetenz** erwerben. Hierzu bieten einige soziale Netzwerke eine Vielzahl von „Hilfeforen“ und vor allem **Informationsmaterialien** an, die auf das jeweilige soziale Netzwerk zugeschnitten sind und sich in anschaulicher Form an die Nutzer, aber auch an Eltern, Lehrer und sonstige interessierte Kreise richten. Gerade

junge Nutzer und deren Eltern sollten sich mit diesen Materialien auseinander setzen.

Rechtliche Vertiefungshinweise:

Deutschland verfügt über einen Jugendschutzstandard auf sehr hohem Niveau, der auch im Internet Beachtung findet und Geltungskraft erfährt. Die Effizienz des Jugendschutzes wird allerdings dadurch eingeschränkt, dass die technologischen Möglichkeiten des Jugendschutzes beschränkt sind. So steckt bspw. die Entwicklung effizienter Altersverifikationsverfahren noch in den Anfängen und wirft die Frage auf, ob derartige Zugangsbeschränkungen nicht die Attraktivität und Konkurrenzfähigkeit sozialer Netze behindern. Im Interesse eines effektiven Jugendschutzes ist es erforderlich, dass vor allem junge Nutzer durch transparente und altersangemessen formulierte Datenschutzerklärungen sowie weitreichende Informationsangebote und Sicherheitshinweise gezielt zum Selbstdatenschutz animiert werden.

Gleichwohl bleibt der Jugendschutz in sozialen Netzwerken eine juristische Herausforderung. Dies gilt insbesondere für die Frage, ob und ggf. ab wann ein Minderjähriger über die Preisgabe und Verwendung seiner personenbezogenen Daten sachgerecht entscheiden kann. Insoweit kommt es primär darauf an, dass der Betroffene in der Lage ist, die Konsequenzen der Verwendung seiner Daten zu übersehen und sich deshalb verbindlich dazu zu äußern.

Abkürzungsverzeichnis

AGB	Allgemeine Geschäftsbedingungen
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
GG	Grundgesetz für die Bundesrepublik Deutschland
KUG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
StGB	Strafgesetzbuch
TMG	Telemediengesetz
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte
UWG	Gesetz gegen den unlauteren Wettbewerb