Web 2.0 Applikationen im Unternehmen und der Datenschutz – datenschutzrechtliche Anforderungen an das Web 2.0 Verhalten und seine Regelbarkeit

Dr. Eduard Wessel

Konzerndatenschutzbeauftragter
Evonik Industries AG
45128 Essen
eduard.wessel@evonik.com

Abstract: Wirtschaftsunternehmen erkennen zunehmend die Bedeutung und die Chancen von Web 2.0 Applikationen. Der Einsatz solcher Anwendungen bietet erhebliche Potentiale für eine effektive und effiziente Kommunikation, Koordination und Kooperation in den Geschäftsprozessen eines Unternehmens.

Andererseits bestehen Risiken darin, dass Mitarbeiter in Blogs oder Facebook-Beiträgen Tatsachen oder Meinungen verbreiten können, die für das Unternehmen schädlich sind. Dabei ist ein privates Web 2.0 Verhalten anders zu bewerten, als ein Beitrag über den vom Arbeitgeber zur Verfügung gestellten Internet-Anschluss.

Der Beitrag befasst sich mit den tatsächlichen und rechtlichen Möglichkeiten von Web 2.0 Anwendungen im Arbeitsverhältnis. Dabei werden insbesondere Internetrecherchen im Bewerbungsverfahren sowie die Nutzung von sozialen Netzwerken durch Mitarbeiter einer datenschutzrechtlichen Betrachtung unterzogen. Zudem wird beleuchtet, welche Pflichten dem Arbeitgeber zum Schutz seiner Mitarbeiter obliegen und wie die bestehende Rechtslage heute in Unternehmen umgesetzt wird.

1 Chancen

Wirtschaftsunternehmen erkennen zunehmend die Bedeutung und die Chancen von Web 2.0 Applikationen (Social Networks, Microblogging, Weblogs, Video-Sharing, Wikis, auch Social Media genannt). Der Einsatz von Web 2.0 Anwendungen scheint erhebliche Potentiale für eine effektive und effiziente Kommunikation, Koordination und Kooperation in den Geschäftsprozessen eines Unternehmens zu bieten.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

Bereits 2009 ergab eine Erhebung von Web2.0@Work unter weltweit 1300 IT-Managern, dass die Nutzung sozialer Netzwerke durch Mitarbeiter in Unternehmen bereits Realität ist. 95 % aller Unternehmen böten ihren Angestellten einen ungehinderten Zugang zu Web 2.0 Seiten. 66 % der IT-Verantwortlichen waren der Meinung, dass Web 2.0 einen wesentlichen Mehrwert biete und ihrem Geschäft zugutekomme [Ta11].

Besonders schnell wächst das Interesse daran, was nicht die Medien, sondern Millionen Onlinenutzer selbst über Unternehmen und Marken im Netz veröffentlichen. Die 5-Sterne-Bewertung eines bestimmten Produkts fördert die Kaufentscheidung eben stärker als die unternehmenseigene Werbung. Und der Blog über die fantastischen Arbeitsbedingungen spricht Bewerber mehr an als jede Hochglanzbroschüre.

Immer öfter bedienen sich Unternehmen maßgeschneiderter Personalplattformen für das E-Recruiting, um sich besser auf die Erwartungen der Stellenbewerber einzustellen und so ein gezieltes Personalmarketing oder gar Personalassessment zu etablieren.

Aber auch die von Mitarbeitern genutzten sozialen Netzwerkdienste können dem Unternehmen wirtschaftliche Vorteile bringen. So bestehen große Erwartungen vor allem in Hinblick auf die Optimierung von Geschäftsprozessen sowie die Generierung von Umsätzen. Wichtige Informationen und persönliche Kontakte aus allen Branchen lassen sich per Mausklick einfach miteinander austauschen und vernetzen.

Nach einer Studie von McKinsey im Jahre 2009 konnten bereits 2 von 3 Unternehmen nach eigenen Auskünften mittels Web 2.0 Instrumenten die Effizienz des eigenen Marketings erhöhen [vgl. BCM11].

Heute können soziale Netzwerke wie Facebook und Xing in Unternehmen von Beschäftigten privat, mit und ohne Erlaubnis des Arbeitgebers, zum Austausch mit Freunden, Bekannten oder Kollegen genutzt werden. Der Arbeitgeber kann jedoch auch seine Beschäftigten generell oder bestimmte Abteilungen, wie z.B. den Vertrieb oder die Unternehmenskommunikation, dazu anhalten, soziale Netzwerke zur Kontaktpflege sowie zum Auf- und Ausbau des Kundenstamms einzusetzen.

2. Risiken

Nach dem Bericht der International Working Group on Data Protection [Rom08] scheinen soziale Netzwerke die Grenzen dessen zu verändern, was gesellschaftlich als die Privatsphäre von Personen gesehen wird: Personenbezogene Daten über Einzelne – und insbesondere riesige Mengen digitaler Bilder und Videos - werden öffentlich (und global) in einer nie vorher da gewesenen Weise und Menge verfügbar.

Abgesehen von den technischen Risiken bringen die neuen Möglichkeiten der sozialen Netzwerke aber auch eine Reihe von rechtlichen und sozialen Gefahren und Herausforderungen mit sich. So können zum Beispiel die technischen Möglichkeiten zu einem ausgedehnten „Data Mining“ verführen. Die Kenntnis von z. B. Bewegungsprofilen oder Gesundheitsdaten der Mitarbeiter ermöglichen so eine erste Analyse zu produktiven und weniger produktiven Mitarbeitern.

Aber wie ist es zu bewerten, wenn Nutzer berufliche Informationen preisgeben? Welche Informationen sind „beruflich“, welche „privat“? Kann – auch unbewusst – dem eigenen Arbeitgeber Schaden entstehen? Welche Risiken bestehen darin, dass Mitarbeiter von E-Mail Accounts des Arbeitgebers Tatsachen oder Meinungen verbreiten können, die für das Unternehmen schädlich sind? Wenn zum Beispiel betriebliches Know-how oder firmeninterne Informationen an Dritte weitergegeben werden. Auch abfällige Kommentare über Kunden oder zur Konkurrenz können über die IP-Adresse des Computers leicht dem Arbeitgeber zugerechnet werden und ihn in ein schlechtes Licht rücken. Bekannte Beispiele sind die Stewardessen, die bei Facebook über Fluggäste meckern oder ein Angestellter, der seine Abneigung gegen Homosexuelle oder einen abfälligen Kommentar über die Arbeitsmoral eines Kollegen über das Twitter-Konto seines Arbeitgebers in die Welt hinaus posaunt.

Rechtliche Gefahren drohen aber auch den Mitarbeitern selbst. Wenn ihnen vom Arbeitgeber Zugang zu Web 2.0-Plattformen gewährt wird, dann ist zu berücksichtigen, dass die meisten der personenbezogenen Informationen, die in sozialen Netzwerkdiensten publiziert werden, auf Initiative der Nutzer selbst und mit ihrer Einwilligung veröffentlicht werden. Im Hinblick auf den Schutz der Privatsphäre könnte darin eine der grundlegendsten Herausforderungen gesehen werden. Denn während die „traditionelle“ Datenschutzgesetzgebung sich mit der Definition von Regeln zum Schutz der Bürger gegen unfaire oder unverhältnismäßige Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung (einschließlich Strafverfolgungsbehörden und Geheimdienste) und von Unternehmen beschäftigt, gibt es nur sehr wenige Regelungen zur Veröffentlichung personenbezogener Daten auf Initiative der Betroffenen selbst, weil dies vor der Entwicklung sozialer Netzwerkdienste weder in der „Offline-Welt“ noch im Internet ein großes Problem darstellte. Außerdem wird die Verarbeitung personenbezogener Daten aus öffentlichen Quellen traditionell in der Datenschutz-gesetzgebung privilegiert.

Gleichzeitig aber ist – worauf das „Rom Memorandum“ zu Recht hinweist – eine neue Generation von Nutzern entstanden: Die erste Generation, die aufgewachsen ist, während das Internet bereits existierte. Diese „digitalen Eingeborenen“ haben ihre eigene Art der Nutzung von Internet-Diensten entwickelt, und eigene Ansichten darüber, was sie als der privaten bzw. der öffentlichen Sphäre zugehörig empfinden. Darüber hinaus könnten sie – da die meisten von ihnen im Teenager-Alter sind – eher bereit sein, Datenschutzrisiken einzugehen, als die älteren „digitalen Einwanderer“. Generell scheint es, als seien jüngere Leute eher zur Veröffentlichung (manchmal intimer) Einzelheiten über ihr Leben im Internet bereit.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

Gesetzgeber, Datenschutzbehörden wie auch Anbieter sozialer Netzwerkdienste sind deshalb mit einer Situation konfrontiert, die kein vergleichbares Beispiel in der Vergangenheit hat. Während soziale Netzwerkdienste eine neue Bandbreite von Möglichkeiten für die Kommunikation und den Austausch von allen Arten von Informationen in Echtzeit bieten, kann die Nutzung solcher Dienste auch zu Gefährdungen der Privatsphäre der Nutzer (und Anderer, die nicht einmal Teilnehmer an sozialen Netzwerkdiensten sind) führen.

3. Regelungsbedarf und -möglichkeiten

Bei Datenerhebungen seitens des Arbeitgebers stehen regelmäßig zwei Sachverhalte im Mittelpunkt der rechtlichen Betrachtung:

- Die Internetrecherchen in Bewerbungsverfahren
- Die Regelbarkeit und Sanktionierbarkeit des Verhaltens von Mitarbeitern in sozialen Netzwerken

3.1 Internetrecherchen im Bewerbungsverfahren

Kaum mehr wegzudenken ist bei den Unternehmen eine Vorauswahl von Stellenbewerbern mit Hilfe des Internets. Ziel ist es dabei, im Rahmen einer Vorauswahl, den Kreis der Bewerber einzuengen. Dabei wird ein Abgleich zwischen Schriftform und der „Wirklichkeit“, wie sie sich im Internet darstellt, vorgenommen. Wer z. B. als Hobby Literatur, Marathon und Kunstreisen angibt, wird durch zahlreiche Partybilder am Strand aus dem Facebook Profil erklärungsbedürftig. Und wer sich als Pressesprecher bei einem Energieversorger bewirbt und mit der Plakette „Atomkraft? Ja bitte“ erscheint, wird durch eingestellte Photos bei der Castor-Demo unglaubwürdig. Vor dem Hintergrund arbeitsrechtlicher Frageverbote möchte der Arbeitgeber also gerne heikle Fragen vorab klären und sein Bild durch einen Hintergrund Check abrunden. Auf diesem Weg gelangen die „Recruiter“ oft zu sehr privaten Inhalten oder auch zu politischen Einstellungen der Bewerber.
Entsprechend der zunehmenden Bedeutung in der Praxis entsteht bereits ein neuer Geschäftszweig zur „Politur am virtuellen Image“ wie er z.B. unter [Dein11], [Myim11] angeboten wird.

Soweit der Arbeitgeber Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person erhebt und nutzt, die sich als Bewerber an ihn wendet, gelten die Bestimmungen des Beschäftigtendatenschutzes im Rahmen des BDSG. Daneben sind bei Bewerbungsverfahren, insbesondere vor dem Hintergrund des Allgemeinen Gleichbehandlungsgesetzes (AGG) und der dazu ergangenen Rechtsprechung, bestimmte Frageverbote z. B. nach Familienplanung, sexueller Neigung, Alter, Weltanschauung, Religion usw. zu beachten.

Nach dem BDSG sind personenbezogene Daten unmittelbar beim Betroffenen zu erheben. Außerdem bedürfen sie einer gesetzlichen Erlaubnis oder aber der Einwilligung des Betroffenen. Schon die Frage des Verbots der mittelbaren Datenerhebung (§ 4 Ab. 2 Satz 1 BDSG) ist rechtlich streitig. Bejahte man es uneingeschränkt [Dä09, § 32 Rn. 56], würde die Internetrecherche stets ausscheiden, weil keine unmittelbare Datenerhebung beim Betroffenen erfolgt. Jedoch greift nach der herrschenden Meinung [vgl. Fo10, S. 431 und Ob08, S. 1563] dieses Verbot des § 4 Abs. 2 Satz 1 BDSG nicht, wenn eine andere Rechtsgrundlage besteht. Als Erlaubnistatbestand in Betracht kommen die Einwilligung des Betroffenen, eine Betriebsvereinbarung oder die Zulässigkeitsnormen des BDSG, §32 oder § 28.

- Eine Betriebsvereinbarung als Rechtsgrundlage scheidet schon deshalb aus, da der Betriebsrat nur ein Mandat für Arbeitnehmer des Betriebes hat, nicht aber für Bewerber.

- Die rechtfertigende Einwilligung durch den Bewerber muss freiwillig sein. Das setzt voraus, dass der potentielle Arbeitgeber auf den Zweck der Erhebung, Verarbeitung oder Nutzung der Daten vorher hinweist. Bei einer Online-Bewerbung müsste ein solcher Hinweis vor dem Einstellen der Bewerbungsunterlagen erfolgen. In der Regel ist das praxisuntauglich, da ein solches Vorgehen einen Abschreckungseffekt hätte und den Zweck, die Papierform nachvollziehen zu können, vereiteln könnte.

- Bleibt § 32 Abs. 1 BDSG, wonach personenbezogene Daten eines Beschäftigten (=Bewerbers) für Zwecke des Beschäftigungsverhältnisses erhoben, genutzt oder verarbeitet werden dürfen, wenn dies für „die Begründung eines Beschäftigungsverhältnisses … erforderlich ist“. Problematisch ist das Merkmal der Erforderlichkeit, wenn dem Bewerber die Frage auch direkt gestellt werden kann. Jedenfalls ist es heute übereinstimmende Rechtsmeinung, dass jedenfalls die Internetrecherche zu „verbotenen Fragen“ im Sinne des AGG unzulässig ist und die Einstellung nicht von diesem Kriterium abhängig gemacht werden darf.

- Die rechtliche Diskussion konzentriert sich deshalb heute auf die Heranziehung des Auffangtatbestandes des § 28 Abs 1 Nr. 3 BDSG, der nach einhelliger Meinung auch bei (entstehenden) Arbeitsverhältnissen neben § 32 BDSG anwendbar ist. Danach ist die Erhebung und Nutzung allgemein zugänglicher Daten zulässig, soweit nicht schutzwürdige Interessen des Bewerbers an dem Ausschluss der Erhebung offensichtlich überwiegen. Die Abwägung findet vor dem Hintergrund der durch Art. 5 Grundgesetz geschützten Informationsfreiheit zwischen allgemein zugänglichen Daten und den schutzwürdigen Interessen des Bewerbers statt. Zweifellos überwiegen die Schutzinteressen des Bewerbers bei AGG-widrigen Recherchen, sowie bei eindeutigem Privatcharakter der Daten (z.B. die sich nur an einen privaten Adressatenkreis wenden). Auch Daten, die sein Persönlichkeitsrecht verletzen, weil sie ihn z.B. stigmatisieren, sozial ausgrenzen oder an den Pranger stellen, sind aus Schutzerwägungen tabu für den Arbeitgeber. Bei vom Bewerber selbst in Xing oder Monster eingestellten Daten, mit denen der Bewerber für sich wirbt, kann allerdings kein schutzwürdiges Interesse festgestellt werden.

ISBN 978-3-88579-286-4

Schwieriger ist die Abgrenzung bei archivierten Daten im Netz, die entweder durch vergangene Ereignisse eingestellt oder vom Bewerber selbst in soziale Netzwerke eingetragen wurden. Hier billigt die Rechtsprechung mittlerweile den Betroffenen nur einen deutlich gelockerten Privatsphärenschutz zu. Der Entwurf zur Neuregelung des Beschäftigtendatenschutzes berücksichtigt diese Interessenlage, indem er die Datenerhebung öffentlich zugänglicher Daten nur zulässt, soweit sie bei bestimmungsgemäßer Nutzung für jeden abrufbar sind und Art und Ausmaß der Datenerhebung im Hinblick auf ihren Zweck nicht unverhältnismäßig sind. Im Klartext heißt das: soweit eine Mitgliedschaft in einem sozialen Netzwerk von jedermann erlangt werden kann, sind solche dort eingestellten Daten auch für jedermann abrufbar. Sind die eingestellten Daten dagegen nur einem beschränkten Personenkreis zugänglich, liegt eine allgemeine Zugänglichkeit nicht vor, mit der Folge, dass solche Daten einer Recherche seitens des Arbeitgebers entzogen sind.

3.2 Die Regelbarkeit und Sanktionierbarkeit von Web 2.0 Aktivitäten im laufenden Arbeitsverhältnis

Im laufenden Arbeitsverhältnis stellt sich die Frage, ob der Arbeitgeber zum eigenen Schutz das Verhalten seiner Mitarbeiter in sozialen Netzwerken regeln und bei Erforderlichkeit sanktionieren darf. Also seine Kenntnisse über das Verhalten der Mitarbeiter arbeitsrechtlich überhaupt und in einem eventuellen Gerichtsverfahren verwerten darf.

Aktivitäten der Arbeitnehmer und die damit zusammenhängenden Fragen lassen sich im Allgemeinen – neben den eindeutigen Verbots- oder Verhaltensnormen (Verrat von Geschäfts- und Betriebsgeheimnissen, § 17 UWG, Recht am eigenen Bild, § 22 KunstUrhG) - mit „herkömmlichen“ arbeitsrechtlichen Werkzeugen bewältigen [vgl. RR11, S. 256]. Die aus dem Arbeitsrecht erwachsenden Anforderungen an das Verhalten gegenüber Geschäftspartnern, Kunden, Kollegen oder der Öffentlichkeit sind lediglich in das Social Media Zeitalter zu übertragen. Da das Web 2.0 Verhalten eines Mitarbeiters allerdings auch außerhalb der Arbeitszeit im privaten Bereich stattfindet, ist zunächst zu klären, unter welchen Umständen der Arbeitgeber das Verhalten überhaupt regeln und sanktionieren darf.

Die Problematik der Rechtmäßigkeit der privaten E-Mail- und Internetnutzung am Arbeitsplatz und die Regelungs- und Sanktionsmöglichkeiten des Arbeitgebers hängen entscheidend davon ab, ob der Arbeitgeber eine solche Nutzung zulässt oder nicht [RR11, S. 257].

Der Arbeitgeber kann Aktivitäten im Internet für private Zwecke während der Arbeitszeit gänzlich untersagen. Das gilt auch für die Nutzung der Betriebs-IT, die der Arbeitgeber auf dienstliche Zwecke beschränken darf. Wenn der Arbeitgeber die private Nutzung während der Arbeitszeit verbieten kann, darf er sie grundsätzlich auch reglementieren. Er kann die Nutzung von Social Media etwa nur beschränkt zulassen oder nur bestimmte Seiten oder bestimmte Blogs erlauben. In diesem Fall kann der Arbeitgeber die rechtmäßige Nutzung auch unbeschränkt kontrollieren.

Allerdings erfasst der Arbeitgeber damit nur das Verhalten während der Arbeitszeit, nicht aber die Fälle, in denen der Mitarbeiter außerhalb der Arbeitszeit und mit seinem privaten Rechner im Web 2.0 aktiv ist. Das private Verhalten eines Mitarbeiters ist grundsätzlich nicht regelbar und Web 2.0 Aktivitäten in der Freizeit mit eigenem Rechner zählen erst einmal zum Privatbereich.

Ebenso ist dem Arbeitgeber die Kontrolle der Internetnutzung durch den Mitarbeiter weitgehend entzogen, wenn er die private Internetnutzung am Arbeitsplatz erlaubt, der Beschäftigte also soziale Netzwerke zum Austausch mit anderen Mitgliedern während der Arbeitszeit nutzen darf. Denn in diesem Fall ist der Arbeitgeber Dienstanbieter i. S. v. § 3 Nr. 6 TKG und es gilt somit das Telekommunikationsgeheimnis des § 88 TKG.

Eine Ausnahme gilt nur, wenn außerdienstliches oder vom TKG geschütztes Verhalten auf den betrieblichen Bereich durchschlägt. Ohne Zweifel sind deshalb Äußerungen des Mitarbeiters bzw. Daten, mit denen der Mitarbeiter Verschwiegenheitspflichten bricht oder Betriebsgeheimnisse offenbart, relevant.
Ein solcher dienstlicher Bezug liegt zumindest dann vor, wenn der Mitarbeiter unter Offenlegung seines Namens und seiner Unternehmenszugehörigkeit bloggt und den Eindruck erweckt, mit der Stimme des Unternehmens zu sprechen. In dem Fall stellt sich daher die Frage, ob der Mitarbeiter genau dazu verpflichtet werden kann, nämlich seinen Namen und die Unternehmenszugehörigkeit stets zu nennen. Hier wird man unterscheiden müssen: Sobald der Account vom Unternehmen selbst unterhalten wird (firmeneigener Blog), ist die Pflicht zur Offenlegung von Name und Zugehörigkeit zum Unternehmen zulässig, denn das Unternehmen entscheidet über die „Spielregeln“. Davon wird man auch ausgehen können, wenn ein Mitarbeiter auf Anregung seines Arbeitgebers an einem Blog oder Chat etwa als Experte teilnimmt oder auf einer Bewerberplattform seine Arbeit beschreibt.
Ist der Mitarbeiter indes privat im Netz unterwegs, kann er wohl nicht verpflichtet werden, aus dem privaten Verhalten durch Identifizierung als Mitarbeiter des Unternehmens einen dienstlichen Bezug herzustellen und damit die Regelbarkeit erst zu ermöglichen. Das Gleiche gilt, wenn ein Unternehmen die Regelungen allein daran festmachen möchte, das der Mitarbeiter beiläufig angibt, bei einem bestimmten Unternehmen beschäftigt zu sein, etwa in seinem Xing oder Monster-Profil oder in einem sozialen Netzwerk. Die Bekanntmachung der Tatsache, dass man bei einem bestimmten Unternehmen arbeitet, lässt sich noch dem Privatbereich zuordnen, stellt also keinen dienstlichen Bezug dar.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

Der Maßstab bei Web 2.0 Aktivitäten im privaten Bereich ist der geschützte Bereich der Meinungsfreiheit nach Art 5 Abs. 1 GG. Dieses Grundrecht gilt auch mittelbar im Verhältnis Arbeitgeber/Arbeitnehmer. Der Arbeitgeber kann nämlich (auch private) negative Äußerungen über betriebliche Belange verbieten, die von der Meinungsfreiheit nicht mehr gedeckt sind. Außerdem kann der Arbeitgeber sein grundrechtlich mit der Berufsfreiheit geschütztes Interesse entgegensetzen, nur mit solchen Mitarbeitern zu arbeiten, die die Ziele des Unternehmens fördern und es vor Schäden bewahren. Auch die Rücksichtnahmepflicht nach § 241 Abs. 2 BGB stärkt den Arbeitgeber in dieser Rechtsposition.

Zu beachten ist außerdem, dass unter der derzeitigen Rechtslage der Arbeitgeber nach § 28 Absatz 1 Nr. 3 BDSG nur auf allgemein zugängliche Daten zugreifen darf, es sei denn, Belange der Mitarbeiter überwiegen offensichtlich. Die Grenze ist aber in jedem Fall bei Daten erreicht, die ein Arbeitnehmer bewusst nur privaten Kontakten zugänglich macht. Ein solches Netzwerk darf der Arbeitgeber nicht nach Inhalten ausforschen.

Schwieriger zu bewerten sind kritische oder nachteilige Äußerungen im Web 2.0, wenn sie von der Meinungsfreiheit nicht mehr gedeckt sind. Nach heutigem Diskussionsstand können für rechtmäßiges Social Media Verhalten in etwa folgende Grenzen beschrieben werden:

Unzulässig sind ehrverletzende Äußerungen, wahrheitswidrige Tatsachenbehauptungen, in grobem Maße unsachliche Angriffe auf Mitarbeiter, Kollegen und Vorgesetzte oder Äußerungen, die den Betriebsfrieden stören.

Jedoch ist Kritik am Unternehmen und der Geschäftspolitik grundsätzlich auch dann zulässig, wenn sie überspitzt und polemisch geäußert wird, es sei denn die (berechtigte) Kritik am Unternehmen stellt den Arbeitgeber bloß. Soweit reicht die Meinungsfreiheit nicht. Stattdessen muss ein Mitarbeiter für Kritik gegebenenfalls innerbetriebliche Abhilfemöglichkeiten in Anspruch nehmen.

Beispiele noch zulässiger Äußerungen:

- Bezeichnung des Arbeitgebers als „Mafia“ (Arbeitsgericht Herford vom 12.11.2009, Ga 26/09; a.A. im Grundsatz wohl LAG BW vom 07.05.2007, 4 Sa 107/07)
- Bezeichnung von nicht namentlich genannten Kollegen als „brauner Mob“ (BAG vom 26.04.2004, 2 AZR 63/03)
- „Wenn der Chef so weitermacht, macht er die Firma kaputt“ (BAG vom 17.02.2000, 2 AZR 927/98)

Sonderfälle: Mitarbeiter mit Repräsentationsfunktion oder mit besonderem Zugang zu Betriebs- und Geschäftsgeheimnissen haben eine gesteigerte vertragliche Rücksichtnahmepflicht; ähnliches dürfte für leitende Angestellte allgemein gelten.

ISBN 978-3-88579-286-4

Nach rechtlicher Bewertung verlangt auch der Wunsch des Arbeitgebers, Social Media zwecks Kundenpflege durch seine Beschäftigten zu nutzen. In diesem Fall sind diese sogar gehalten, das Unternehmen oder sich selbst im Netz zu präsentieren und Produkte oder Dienstleistungen anzubieten, um so Kontakte mit Kunden zu pflegen oder neue Kunden hinzuzugewinnen. Hat der Beschäftigte während seines Arbeitsverhältnisses über das soziale Netzwerk Kundenkontakte geknüpft und in den Benutzeraccount des Netzwerks eingepflegt, stellt sich die Frage, wem der Benutzeraccount zuzuordnen ist und ob der Beschäftigte seinem Arbeitgeber die Zugangsdaten mitteilen oder die Kundendaten an ihn herausgeben muss. Denn ist dies nicht der Fall, läuft der Arbeitgeber Gefahr, die Kundendaten zu verlieren. In der Literatur wird eine differenzierte Lösung vertreten [vgl. Bi11, S. 110ff.]:

Hat der Arbeitgeber die Kosten der Mitgliedschaft getragen oder den Benutzeraccount zur Verfügung gestellt, soll der Beschäftigte bei Beendigung des Beschäftigungsverhältnisses verpflichtet sein, den Account wie ein ihm sonst zur Verfügung gestelltes Arbeitsmittel herauszugeben. Andernfalls wird ein Herausgabeanspruch verneint. Lediglich die Daten, die der Arbeitgeber zur Fortführung der vom ausscheidenden Beschäftigten getätigten Geschäfte benötigt, soll dieser dem Arbeitgeber auch bei Fehlen eines Herausgabeanspruchs überlassen müssen. Erfolgt die Nutzung eines Accounts jedoch mit Duldung des Arbeitgebers auch für private Zwecke, dann gilt das Telekommunikationsgeheimnis des § 88 TKG und der Arbeitgeber kann sich sogar strafbar machen, wenn er auf den Account ohne die erforderliche Einwilligung zugreift.

Die Verwertung von recherchierten Informationen im Arbeitsverhältnis durch den Arbeitgeber ist also nur unter engen Voraussetzungen möglich. Zudem sieht die geplante BDSG-Neuregelung vor, dass eine Verwertung solcher Informationen nur zulässig ist, soweit Art und Ausmaß der Informationserlangung im Hinblick auf den Zweck nicht unverhältnismäßig sind.

3.3 Schutz der Mitarbeiter

Die Artikel-29-Datenschutzgruppe, ein unabhängiges Beratungsgremium der EU in Datenschutzfragen, nahm Mitte 2009 zur Nutzung sozialer Online-Netzwerke Stellung [DS08]. Darin äußerten die Autoren besorgniserregende Sicherheitsbedenken bei der Verbreitung und Verwendung von Informationen, die über soziale Netzwerkdienste verfügbar sind, zu anderweitigen, sekundären und unbefugten Zwecken. Die Ausnutzung von personenbezogenen Daten für unterschiedliche, so auch kommerzielle, Zwecke und Vorhaben, berge mitunter größere Gefahren und Risiken wie z.B. Identitätsdiebstahl, finanzielle Einbußen, Nachteile für Geschäfts- oder Erwerbsmöglichkeiten und Beeinträchtigung der körperlichen Unversehrtheit. Die Gruppe fordert deshalb von den Betreibern sozialer Netzwerkdienste neben umfassender Aufklärung und Information der Nutzer auf der technischen Seite auch datenschutzfreundliche Standardeinstellungen. Die Nutzer sollten uneingeschränkt ihre Rechte als betroffene Person im Sinne der EU-Datenschutzrichtlinie genießen.

ISBN 978-3-88579-286-4

Seit der Schuldrechtsreform von 2002 ist § 241 Abs. 2 BGB für Arbeitsverhältnisse zu entnehmen, dass jedem Vertragspartner die arbeitsvertragliche Nebenpflicht der Rücksichtnahme obliegt. Dieser entspricht inhaltlich dem oftmals noch verwendeten Begriff der allgemeinen Fürsorgepflicht des Arbeitgebers. Wenn man die sich daraus ergebenden drei Gruppen betrachtet, nämlich die Schutzpflichten, die Informationspflichten sowie bestimmte Mitwirkungspflichten, so liegt es nahe, dem Arbeitgeber auch entsprechende Nebenpflichten aufzuerlegen, wenn er seinen Mitarbeiter technische Möglichkeiten zu Social Media-Verhalten überlässt oder ein solches gar erwartet. Kritische Stimmen sehen in der gleichzeitigen Fülle der Informationen, die für den Einzelnen verfügbar sind und denen er sich zunehmend aussetzt eine extreme Form der Überforderung. Es erwachse eine Informationsgier, die zu einem Kreativitätsverlust führe und Stress verursache, solange die Informationen nur durch einen hindurch laufen, ohne verarbeitet und verankert zu werden [Pö11]. Auch wegen dieser Risiken ist ein Arbeitgeber gut beraten, die Grenzen des Zugangs seiner Mitarbeiter sorgfältig abzuwägen, zumindest aber seine Mitarbeiter sich im Netz nicht ohne unterstützend-beratende Begleitung bewegen zu lassen.

4 Umsetzung der Rechtslage im Unternehmen

Bei Bewerbungs- und Einstellungsprozessen muss sich der Arbeitgeber sorgfältig auf die zuvor dargestellte Gesetzeslage einstellen, indem er seinen Mitarbeitern klare Handlungsanweisungen, z.B. bei Hintergrundchecks von Stellenbewerbern, vorgibt.

Bei Recherchen über seine eigenen Beschäftigten muss der Arbeitgeber die gleichen o. g. Regelungen beachten.

Gegenüber den Mitarbeitern und deren richtigen Umgang mit Web 2.0 Anwendungen beschränken sich die Unternehmen heute mangels weitergehender Regelungskompetenz oftmals auf Verhaltensempfehlungen und Richtlinien. Soweit sie verbindlichen Charakter haben, müssen sie stets einen betrieblichen Bezug aufweisen. Zudem können die Mitarbeiter mit Geheimhaltungs- und Vertraulichkeitsregeln zu einem sensitiven Umgang mit Betriebsinterna angehalten werden. Das wird aber im Allgemeinen bereits über den Arbeitsvertrag geregelt. Eine Reglementierung des privaten Web 2.0 Verhaltens scheidet grundsätzlich aus. Die üblichen Empfehlungen, oft verbunden mit einer breiten Aufklärungskampagne, lassen sich in folgenden Punkten zusammenfassen:

- **Netiquette**: Respekt der Internetgemeinschaft, Achtung der Regeln von Communities und der üblichen Gebote von Anstand und Respekt, verantwortlicher Umgang mit Kritik
- **Geistiges Eigentum**: keine Verletzung von Urheberrechten
- **Internes bleibt intern**: Wahrung von Betriebsgeheimnissen und Verschwiegenheitsverpflichtungen
- **Authentizität**: persönliche Meinungen nicht als Unternehmensmeinung darstellen, für sich selbst sprechen unter eigenem Namen
- **Wettbewerb respektieren**: sachlich bleiben und als persönliche Meinung deutlich machen

- **Anzeigepflichten**: aus Social Media bekannt gewordene Kritik am Unternehmen ist zu melden

Fazit

Wegen der vielfältigen Möglichkeiten und den damit verbundenen Chancen lassen heute die meisten Unternehmen die arbeitnehmerseitige Nutzung von sozialen Netzwerken zu. Dabei ist der Arbeitgeber – neben eindeutigen Verbots- oder Verhaltensnormen (§ 17 UWG, § 22 KunstUrhG) – auf die arbeitsrechtlichen Instrumente beschränkt, die sich ihm heute schon bieten.

Im Übrigen ist die rechtliche Erfassung dieser Entwicklungen noch lückenhaft: Auf supranationaler Ebene liegt lediglich ein Bericht mit Empfehlungen der sogenannten Artikel-29-Datenschutzgruppe vor. Die Datenerhebung in Web 2.0 Anwendungen durch den Arbeitgeber orientiert sich an den Wertungen des AGG, des BDSG sowie des Art. 5 GG. Das Bundesdatenschutzgesetz schützt bislang unzureichend das Verhalten in sozialen Netzwerken. Regelungsansätze gibt es hingegen in der im Parlamentsverfahren befindlichen Novelle zum BDSG. Deshalb bleibt heute zur Risikoabwehr lediglich eine breite Aufklärung verbunden mit innerbetrieblichen Regelungen, die arbeitsrechtlichen Grundsätzen stand halten.

Vor dem Hintergrund der bekannten Gefahren und Risiken bei der Nutzung von sozialen Netzwerkdiensten im Arbeitsalltag, sollten die Unternehmen aus eigenem Sicherheitsinteresse und auch wegen ihrer Pflicht zur Rücksichtnahme auf ihre Mitarbeiter sorgfältig die Grenzen des Internet-Zugangs abwägen.

Literaturverzeichnis

ISBN 978-3-88579-286-4

[Bi11] Bierekoven, C.: Social Networks am Arbeitsplatz, Einsatzmöglichkeiten, Regelungsbedarf und Lösungsansätze. In: ITRB 05/2011, S. 110 - 113

[BCM11] Bughin, J.; Chuhi, M.; Miller, A.: McKinsey Global Survey Results: How Companies are benefiting from Web 2.0. http://www.mckinseyquarterly.com/How_companies_are_benefiting_from_Web_20_Kinsey_Global_Survey_Results_2432, zuletzt abgerufen am 20.06.2011

[Dä09] Däubler, W.; Klebe, T.; Wedde, P.; Weichert, T.: Bundesdatenschutzgesetz, 3. Auflage, 2009

[DS08] O. V.: Stellungnahme der Artikel – 29 – Datenschutzgruppe 5/2009 zur Nutzung sozialer Online-Netzwerke vom 12. Juni 2009, http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm, zuletzt abgerufen am 25.06.2011

[Dein11] siehe www.deinguterruf.de

[Fo10] Forst, G.: Bewerberauswahl über soziale Netzwerke im Internet? In: NZA 8/2010, S. 427 - 433

[Myim11] siehe www.myimagecontrol.de

[Ob08] Oberwetter, C.: Bewerberprofilerstellung durch das Internet – Verstoß gegen das Datenschutzrecht? In: Betriebs-Berater 29/2008, S. 1562 – 1566

[Pö11] Pöppel, E.: Facebook ist Selbstprostitution. FAZ-net vom 10. Mai 2010, www.faz.net/-01ry8w, zuletzt abgerufen am 20.06.2011

[Rom08] O. V.: Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten – „Rom Memorandum“ – vom 4. März 2008, International Working Group on Data Protection in: Telecommunications, http://www.berlin-privacy-group.org, zuletzt abgerufen am 22.06.2011

[RR11] Rolf, C.; Riechwald, J.: Betriebliche Social Media Richtlinien auf dem arbeitsrechtlichen Prüfstand, RDV 2010

[Ta11] Taylor, C.(Hrsg.): Web2.0@Work. http://www.websense.com/assets/reports/Websense_Web2.0atWork_US_April_2009.pdf, zuletzt abgerufen am 20.06.2011

ISBN 978-3-88579-286-4