

MMR FOKUS

2. Festlegung von Verhaltensrichtlinien

Die Aufnahme dahingehender Verhaltensrichtlinien in den Arbeitsvertrag bzw. die Erweiterung einzel- oder kollektivvertraglicher Nebenpflichten würde die genannten Rechtsunsicherheiten jedenfalls verringern (vgl. zur Erweiterbarkeit des Pflichtenkreises *Reichold*, a.a.O., § 49 Rdnr. 16). Das gilt insbesondere für Verschwiegenheitspflichten oder die einheitliche und korrekte Darstellung von Unternehmensnamen und -gegenstand. Zu beachten bleiben ansonsten das Mitbestimmungsrecht des Betriebsrats sowie eine mögliche Inhaltskontrolle nach AGB-Recht und dabei – insbesondere, wo sonst Sanktionen drohen – Transparenz (vgl. *BAG NZA* 2008, 170, 172; *Reichold*, a.a.O., § 48 Rdnr. 31; *Diller*, *NZA* 2008, 574). Die Beschäftigten-Compliance dürfte auf diesem Wege deutlich erhöht werden können (zu Compliance-Richtlinien allgemein ausführlich *Schreiber*, *NZA* 2010, 617, 619), dies gilt wohl noch mehr für mit dem Betriebsrat getroffene Betriebsvereinbarungen nach § 77 BetrVG.

IV. Fazit

Arbeitnehmer anzuweisen, sich in einem sozialen Netzwerk anzumelden, ist kaum jemals zulässig, wenn nicht gerade ein deutlicher Bezug zwischen Arbeitsleistung und einem sozialen Netzwerk oder jedenfalls der öffentlichen Unternehmenspräsentation besteht. Auch der Weg über den Arbeitsvertrag oder eine Betriebsvereinbarung ist riskoreich, im Zweifel aber eher das Mittel der Wahl. Ist der Arbeitnehmer Mitglied eines sozialen Netzwerks, kann von ihm ein unternehmensunschädliches Verhalten verlangt werden. Im Zweifel kann man dem durch Weisung Nachdruck verleihen, die eine umfangreiche Interessenabwägung verlangt. Empfehlenswerter wäre insoweit die Regelung in einer arbeitsvertraglich einbezogenen Richtlinie.

■ Vgl. auch *Ott*, *MMR* 2009, 158; *Pröpper/Römermann*, *MMR* 2008, 514; *Weißnicht*, *MMR* 2003, 448.

Prof. Dr. Ulrich Gabriel

ist Rechtsanwalt in Kiel und Honorarprofessor an der Hochschule Wismar.

Stud. iur. Jann Hendrik Cornelis

ist wissenschaftlicher Mitarbeiter in der Kanzlei Gabriel Rechtsanwälte.

Axel Spies USA: Machine-to-Machine (M2M)-Kommunikation

MMR-Aktuell 2011, 317500

Unter Machine-to-Machine (M2M)-Kommunikation versteht man die Fähigkeit einer entsprechend ausgestatteten technischen Einrichtung („Maschine“), mit einer anderen technischen Einrichtung Daten auszutauschen, ohne dass die Teilhabe eines Menschen an diesem Prozess nötig ist. Da dieser Prozess üblicherweise über das Internet erfolgt, spricht man auch vom „Internet der Dinge.“ Meist erfolgt die Kommunikation unter den Maschinen über eine Mobilfunkverbindung, die auch die vom Menschen initiierte Mobiltelefonie nutzt.

Die M2M-Kommunikation kann erhebliche Auswirkungen auf die Frequenznutzung haben, da die entsprechenden Geräte billig sind und die Kommunikation in vielen Fällen nicht mehr von Menschen initiiert wird. TK-Experten vermuten, dass M2M-Kommunikation gerade bei der *ETSI* und anderen Koordinierungsgremien in naher Zukunft zu einem Top-Thema avancieren wird.

1. M2M-Nutzung und Ideen in den USA

Der Austausch von Daten der Maschinen kann über Cloud-Plattformen erfolgen, die speziell zu diesem Zweck eingerichtet werden. Die meisten M2M-Dienste in den USA stecken noch in der Anfangsphase und die WiFi-Verbindungen können in vielen Fällen den M2M-Markt nicht befriedigen, da sie weniger zuverlässig arbeiten als Mobilfunkverbindungen und weniger mobil sind. Ein Beispiel für eine solche Anwendung ist die Überwachung von medizinischem Gerät, darunter der Einsatz von HighTech-Pillendosen, die ihrem Besitzer eine Textnachricht auf sein Mobiltelefon schicken und ihn an seine Medikamenteneinnahme erinnern. Die größten Marktchancen für M2M-Technologien werden im Gesundheitsbereich gesehen, indem Systeme, die sich im Haus des Patienten befinden, dessen Gesundheitszustand überwachen und im Notfall Alarm geben sollen.

Ein anderer wichtiger Bereich für die M2M-Kommunikation ist der Verkehrssektor, z.B. für die Kontrolle eines Fuhrparks in Hinsicht auf Geoposition und Benzinverbrauch oder für Taxis in New York City, um deren Standort zu ermitteln

und dem Fahrgast auf einem Bildschirm die Route anzuzeigen. Gerade diesen Bereichen wird ein besonders großes Wachstumspotenzial zugesprochen.

Auch soll die M2M-Technologie in Elektroautos eingesetzt werden, um z.B. mit Ladestationen zu kommunizieren. Außerdem können Verkaufsautomaten melden, wenn sie leer sind und aufgefüllt werden müssen. Eine weitere Verwendung, die in der EU im Jahr 2020 umfassend durchgeführt werden soll, ist die Verwendung sog. Smart Meter (Messgeräte) in Geschäftsräumen und Privathaushalten, die den Energieverbrauch messen und diesen an den Strom- oder Heizungsanbieter übermitteln sollen. Die meisten Anwendungen sind allerdings noch lange nicht marktreif.

Einen weiteren Anwendungsbereich stellen „intelligente“ Bezahlssysteme dar: Laut einer Aussage des CEO von *KORE Telematics* ist die M2M-Technologie als Bezahlssystem anwendbar, wenn ein Kunde seine Kreditkarte beispielsweise für eine Waschanlage oder eine Parkuhr benutzt. Ein anderer wachsender Markt ist die Abwicklung von Transaktionen außerhalb von RFID via M2M-Kommunikation – so soll etwa ein Bezahlterminal in Parkhäusern den Kassierer dort ersetzen. Eher futuristisch ist das Beispiel eines Verkaufsautomaten, der den Preis der verkauften Waren an Umweltbedingungen wie Temperatur oder Niederschlag oder aber auch an die Zahl der Passanten knüpfen soll. Das Feld der möglichen Datenverknüpfungen ist schier endlos.

2. Allianzen entwickeln sich

Die Anbieter von M2M-Dienstleistungen sind die US-Mobilfunkanbieter (*AT&T*, *Verizon*, *T-Mobile* und *Sprint*), jedoch gibt es bereits in den USA Firmen, die ausschließlich M2M-Dienste über ein eigenes Netz anbieten. Die notwendigen Geräte, um eine M2M-Kommunikation zu ermöglichen (z.B. SIM-Karten, Sender etc.), können im Internet erworben werden. Beim Erwerb der SIM-Karte entscheidet sich der Käufer, welches Netz er nutzen will. Die einzelne „Kommunikation“ würde aber von dem Gerät initiiert und durchgeführt. Der Käufer könnte dies allenfalls auf seiner Telefonrechnung feststellen.

Einige Anbieter von Mobilfunknetzen haben sich zu Allianzen mit Firmen zusammengeschlossen, die auf M2M-Technologien spezialisiert sind: AT&T mit Jasper Wireless und Verizon und Vodafone mit nPhase, einem Verizon/Qualcom-Joint-Venture. Verizon ist kürzlich mit Sierra Wireless eine Partnerschaft eingegangen, um das von Sierra Wireless angebotene Produkt, eine M2M-Technologie, die sich des Cloud Computing bedient, im Verizon-Netz zu vermarkten. Im Rahmen von Cloud-basierter M2M-Kommunikation hat Ericsson die M2M-Sparte von Telenor Connexion erworben, um darauf i.R.d. Cloud Computing M2M-Services jenseits von Mobilfunkverbindungen und WiFi anzubieten.

3. Kritik

In den USA erfahren M2M-Systeme bisweilen Kritik durch Datenschützer, da diese Systeme, wie z.B. im Falle eines intelligenten Autos, nicht nur dessen Position, sondern auch Geschwindigkeit und Benzinverbrauch ermitteln, wodurch detaillierte Nutzerprofile erstellt werden könnten. Gerade die staatlichen Ermittlungsorgane sind an solchen Anwendungen zur Ergreifung von Kriminellen höchst interessiert.

Ein sensibler Bereich ist die Nutzung von Patientendaten bei der Überwachung des Gesundheitszustands. Es ist unklar, wie die Daten geschützt werden können. Das Mobilfunknetz selbst hingegen, über das die Daten übertragen werden, soll sicher sein.

Beim Einsatz von Cloud-Systemen besteht die Gefahr, dass die Daten, die von M2M-fähigen Maschinen übermittelt werden, nicht ausreichend verschlüsselt sind. Wie im Beck-Blog ausführlich diskutiert, ist es unklar, ob Daten, die innerhalb und aus Deutschland i.R.d. Cloud Computing übermittelt werden, trotz Verschlüsselung als personenbezogene Daten i.S.d. BDSG einzuordnen sind. Durch den bevorstehenden Kauf von T-Mobile durch AT&T wird befürchtet, dass damit das 2G-Netz, das viele M2M-Systeme nutzen, eingestellt wird.

4. Regulatorische Überlegungen und Diskussionen

International existiert bisher kein einheitlicher Standard für M2M-Kommunikation. Die Federal Communications Commission (FCC) hat bisher auch nicht re-

gelnd in den M2M-Markt eingegriffen. Die Bedenken, dass durch verstärkte Nutzung von M2M-Diensten die Bandbreiten im Mobilfunkbereich beschränkt werden, werden auch in den USA geteilt, weshalb die FCC das drahtlose Funkspektrum erweitern will. Darüber hinaus wird befürchtet, dass durch die Freigabe neuer Frequenzen, auf welchen auch M2M-Kommunikation abgewickelt wird, das GPS-Netz (Global Positioning) gestört werden könnte. Das Problem einer möglichen Überlastung der Bänder und Interferenzen durch M2M wird z.Zt. eher bandspezifisch adressiert.

Auch den sog. White Spaces (lukrative Frequenzbereiche zwischen den einzelnen TV-Bändern), in denen sich u.a. die drahtlosen Mikrophone befinden, drohen Interferenzen.

Nach den US-Gesetzen werden bestimmte Informationsdaten (Customer Proprietary Network Information – CPNI), die von Telefonanbietern erhoben werden, darunter Datum und Zeit des Anrufs,

Dauer des Gesprächs und die angerufene Nummer, geschützt. Diese Informationen dürfen z.B. nicht zu Marketingzwecken genutzt oder verkauft werden. Bislang sind aber keine Bestrebungen erkennbar, die von der M2M-Kommunikation erfasste Datenübertragung unter dem Gesichtspunkt CPNI zu thematisieren und die Datenweitergabe einzuschränken. Ungeklärt ist schließlich die Frage, wer die Kosten der Verbindungen zu tragen hat – der Anbieter der Leistung mit M2M-Funktion oder der Endverbraucher?

■ S.a. die weiteren Überlegungen im Beck-Blog mit Hinweis auf die BNetzA-Konsultation: „BNetzA: Überlastet Machine-to-Machine (M2M)-Kommunikation die TK-Netze?“, abrufbar unter: <http://blog.beck.de/2011/04/20/bnetza-ueberlastet-machine-to-machine-m2m-kommunikation-die-tk-netze/>; zu Smart Metering vgl. Wiesemann MMR 2011, 213 und Meldung MMR-Aktuell 2011, 316383 m.w.Nw.

Dr. Axel Spies

ist Rechtsanwalt in der Kanzlei Bingham McCutchen in Washington DC und Mitherausgeber der MMR.

Axel Spies USA: Zusammenschluss von AT&T und T-Mobile stößt auf Widerstand

MMR-Aktuell 2011, 316967

Die Genehmigung des Zusammenschlusses von AT&T und T-Mobile ist derzeit eines der wichtigsten kartellrechtlichen Verfahren in Washington DC. Der Schwerpunkt der Prüfung liegt beim US-Justizministerium, aber die Federal Communications Commission (FCC) hat ein gewichtiges Wort mitzureden. Der US-Handelsbeauftragte (USTR) hat zwischenzeitlich Deutschland auf die Schwarze Liste gesetzt. Wie und wann die Untersuchung der Behörden abgeschlossen sein wird, ist derzeit unklar.

FCC-Verfahren eingeleitet

Am 14.4.2011 erließ die FCC eine Vertrauensschutzanordnung (Protective Order) und veröffentlichte eine separate öffentliche Bekanntmachung über AT&T's vorgeschlagenen Kauf von T-Mobile. Die Behörde gab auch ein Aktenzeichen bekannt und erklärte, dass die FCC-Regeln über „ex parte“ eingreifen werden, sobald der offizielle Antrag auf Genehmigung der Transaktion bei der FCC eingeht. Die ex parte-Regeln dienen der Transparenz – z.B. muss jeder Verfahrens-

beteiligte öffentlich dokumentieren, wer sich wann mit Behördenvertretern in diesem Verfahren trifft und welche Dokumente und Informationen bei solchen Treffen ausgetauscht werden. AT&T und T-Mobile werden voraussichtlich um den 21.4.2011 förmlich um die FCC-Genehmigung ersuchen. Die Schutzanordnung würde den Unternehmen dann den Weg freimachen, um vertrauliche Informationen wie Geschäftsgeheimnisse mit der Anmeldung bei der FCC einzureichen. Die Unternehmen hatten die Transaktion am 20.3.2011 publik gemacht.

Die zuständigen FCC-Beamten haben noch nicht darüber entschieden, ob sie weitere Informationen über den Zustand der Branche von anderen TK-Anbietern einfordern sollen. Dies ist bei großen Merger-Verfahren in den USA die gängige Praxis. Im Jahr 2004 forderte das Justizministerium eine riesige Menge von Informationen von anderen Netzbetreibern an, als die Kartellbehörde den Zusammenschluss von AT&T mit dem Mobilfunkbetreiber Cingular zu prüfen hatte. Das Justizministerium ist bei der Geneh-