

19.11.2008 AH/MJ/BM

mj\seminar\schwetzingen\081103-skript[7]

Internet am Arbeitsplatz

Dr. Alexander Hoff

Rechtsanwalt
Fachanwalt für Arbeitsrecht

Lehrbeauftragter der Universität Karlsruhe für Arbeitsrecht
am Zentrum für Angewandte Rechtswissenschaften
der Fakultät für Informatik

I. Einführung

Die Nutzung moderner Kommunikationsmittel am Arbeitsplatz ist heute Standard. Auch im Bereich der Unternehmensverwaltung und –organisation haben sich die neuen Medien durchgesetzt, wenngleich diese Entwicklung noch nicht vollständig abgeschlossen ist. Dem gegenüber hinkt die rechtssichere Gestaltung der betriebsinternen Rahmenbedingungen der technischen Entwicklung hinterher. Häufig fehlt in den Unternehmen das Verständnis dafür, dass mit dem Wechsel von Papier zur elektronischen Datenspeicherung nicht nur das Speichermedium gewechselt wurde, sondern zahlreiche Arbeitsabläufe und Standards revolutioniert werden – und zwar unabhängig davon, ob dies intendiert ist oder nicht. Informationstechnologie macht es möglich, dass jenseits der bloßen gespeicherten Information (z. B. ein Schreiben) zahlreiche weitere Informationen zwangsläufig vorhanden sind (Wer hat wann dieses Schreiben verfasst, wer hat es gelesen, wer hat es korrigiert usw.).

Es liegt auf der Hand, dass Arbeitsrecht als Arbeitnehmerschutzrecht auf diese Herausforderungen eine Antwort finden muss ohne das berechtigte Interesse des Arbeitgebers an der Sicherung seines Know How und seiner Kommunikationsfähigkeit aus dem Blick zu verlieren. Dabei sind die Bereiche, in denen das Arbeitsrecht Berührung zu Rechtsfragen der Informationstechnologie hat, weit. Neben dem Datenschutz sind hier unter anderem das Recht der Arbeitnehmererfindungen (z. B. Software), das Outsourcing und rechtliche Fragen im Zusammenhang mit dem Einsatz von Internet und E-Mail am Arbeitsplatz zu nennen. Um letzteres soll es in dieser kurzen Einführung gehen. Zahlreiche andere rechtliche Aspekte, z.B. strafrechtliche (z. B. §§ 201 ff StGB) oder steuerrechtliche Gesichtspunkte (z. B. § 3 Nr. 45 EStG) müssen unberücksichtigt bleiben, soll der Rahmen der Veranstaltung nicht gesprengt werden.

II. Technische Grundzüge

Eine interessengerechte rechtliche Wertung der einzelnen Sachverhalte wird schwer möglich sein, ohne einige grundlegende Kenntnisse der technischen Zusammenhänge.

1. Datenwege

Wenn ein Sender eine E-Mail an einen Empfänger verschickt, sendet er sie technisch zunächst lediglich an seinen Provider, also denjenigen, der seinen Netzzugang organisiert. Der Provider löst die E-Mail-Adresse des Empfängers (z. B. empfänger@firma-mueller.de) auf. Das heißt, er übersetzt die Domain (firma-mueller.de) in die dahinter liegende IP-Adresse (eine Zahlenkombination, über die jeder Domain-Inhaber identifizierbar ist). Der Provider des Senders sendet die E-Mail sodann an den Provider des Empfängers, der die Domain des Empfängers verwaltet (hostet). Die Weiterleitung der E-Mail (in Form kleiner Datenpakete) erfolgt über unterschiedliche Router. Der Provider des Empfängers hält die E-Mail vor, bis sie vom Empfänger abgerufen wird. Dies geschieht bei Privatanutzern in der Regel durch das E-Mail-Programm (z. B. Outlook, Lotus notes, thunderbird), bei gewerblichen Nutzern in der Regel in regelmäßigen Abständen automatisch.

Ist der Empfänger ein Arbeitnehmer, der die E-Mail an seine Firmenadresse geschickt bekommt, wird die an ihn gerichtete E-Mail vom Empfänger-Provider zunächst auf dem Server des Arbeitgebers gespeichert, wo sie der Empfänger von seinem Arbeitsplatz aus abrufen kann. Die E-Mail muss dabei, bevor sie den Arbeitgeberserver erreicht, in der Regel eine Firewall passieren, die die eingehenden Daten auf Viren und ähnliche Angriffe untersucht.

Bevor der Empfänger die E-Mail also zur Kenntnis nehmen kann, werden die Daten der Nachricht beim Sender-Provider, beim Empfänger-Provider und beim Server des Arbeitgebers (Firewall) erfasst, gespeichert und weitergeleitet (nicht jedoch bei den eingeschalteten Routern – dort ist eine Inhaltskontrolle der weitergeleiteten Daten aufgrund des gewählten Protokolls nicht möglich). An jeder dieser Stellen (Provider und Client) können die Daten kontrolliert und ausgewertet werden. Für das Arbeitsverhältnis ist naturgemäß die Kontrolle auf dem Arbeitgeberserver bzw. an der Firewall von besonderer Bedeutung.

2. Datenqualität

Hinsichtlich der Qualität der erfassten Daten ist zu unterscheiden:

- Als **Verkehrsdaten** oder **Verbindungsdaten** werden solche Daten bezeichnet, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (Legaldefinition in § 3 Nr. 30 TKG). Dazu gehört zum Beispiel der in Anspruch genommene Telekommunikationsdienst, die Nummer oder die Kennung der beteiligten Anschlüsse und Beginn und Ende der Datenverbindung.
- **Bestandsdaten** sind die Daten, die ein Vertragsverhältnis zwischen einem Diensteanbieter und einem Nutzer bestehen und für die Begründung, Ausgestaltung oder Änderung des Vertragsverhältnisses von Bedeutung sind (vgl. z.B. § 14 TMG, beispielsweise E-Mail-Adresse, Vertragslaufzeit). Sie haben keinen Bezug zur konkreten Netznutzung.
- **Nutzungsdaten** sind die **einem konkreten Nutzer zugeordneten Verbindungsdaten** (vgl. § 15 TMG). Aus den Nutzungsdaten lässt sich ein **Nutzungsprofil** erstellen, durch Auswertung so genannter Ereignisprotokolle. Kombiniert man die hierdurch gewonnenen Daten zusätzlich mit den Inhaltsdaten zum Beispiel der aufgerufenen Internetseiten oder der E-Mail-Inhalte, lässt sich nicht nur ein Nutzungsprofil, sondern sogar ein **Persönlichkeitsprofil** erstellen.

III. Maßgebliche Normen (Auszug)

1. Grundgesetz

Art. 1 Abs. 1: *Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.*

Art. 2 Abs. 1: *Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.*

Das Bundesverfassungsgericht hat aus dem Persönlichkeitsrecht in Art. 2 Abs. 1 GG das Recht auf informationelle Selbstbestimmung entwickelt (Volkszählungsurteil, **BVerfG, 19.12.1983, Az. 1 BvR 209/83**) und dies in weiteren Entscheidungen konkretisiert (z. B. **BVerfG, 23.10.2006, Az. 1 BvR 2027/02; 27.12.2006, Az. 2 BvR 803/05**). Zwar binden Grundrechte zunächst den Staat gegenüber dem Bürger. Es ist aber allgemein anerkannt, dass Grundrechte ge-

rade im Arbeitsrecht Ausstrahlungswirkung entfalten (st. Rspr. **BAG, 15.01.1955, Az. 1 AZR 305/54 = BAGE 1, 258**). Die Ausprägung dieser mittelbaren Grundrechtswirkung im Arbeitsrecht wird z.B. in § 75 Abs. 2 BetrVG konkretisiert.

2. Betriebsverfassungsgesetz

§ 75 Abs. 2 BetrVG: *Arbeitgeber und Betriebsrat haben die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern. Sie haben die Selbständigkeit und Eigeninitiative der Arbeitnehmer und Arbeitsgruppen zu fördern.*

§ 80 Abs. 1 Nr. 1 BetrVG: *Der Betriebsrat hat folgende allgemeine Aufgaben: 1. darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, Unfallverhütungsvorschriften, Tarifverträge und Betriebsvereinbarungen durchgeführt werden,*

§ 81 Abs. 4 BetrVG: *Der Arbeitgeber hat den Arbeitnehmer über die aufgrund einer Planung von technischen Anlagen, von Arbeitsverfahren und Arbeitsabläufen oder der Arbeitsplätze vorgesehenen Maßnahmen und ihre Auswirkungen auf seinen Arbeitsplatz, die Arbeitsumgebung sowie auf Inhalt und Art seiner Tätigkeit zu unterrichten.*

§ 87 Abs. 1 Nr. 1 BetrVG: *Der Betriebsrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, in folgenden Angelegenheiten mitzubestimmen: [.....] Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb...*

§ 87 Abs. 1 Nr. 6 BetrVG: *Der Betriebsrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, in folgenden Angelegenheiten mitzubestimmen: [.....] Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. ...*

§§ 75 Abs. 2 und 81 Abs. 4 BetrVG konkretisieren das Recht des Arbeitnehmers auf informationelle Selbstbestimmung (s.o.). (§ 81 Abs. 4 BetrVG ist insoweit systemwidrig, als dort ein Anspruch begründet wird, der keinen kollektivrechtlichen Bezug hat und besser im Zusammenhang mit §§ 617, 618 BGB (Fürsorgepflichten des Arbeitgebers) geregelt worden wäre.)

Gesetze im Sinne des § 80 Abs. 1 Nr. 1 BetrVG sind auch das BDSG und die Arbeitnehmer schützenden Vorschriften des TKG und des TMG.

3. Bundesdatenschutzgesetz (BDSG) (Auswahl)

§ 1 Abs. 1 BDSG: Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

§ 1 Abs. 2 BDSG: Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch [...] nicht öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

§ 1 Abs. 3 BDSG: Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor [...].

§ 2 Abs. 4 BDSG: Nicht öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Abs. 1 – 3 fallen [...].

§ 3 BDSG: Enthält zahlreiche Begriffsbestimmungen über personenbezogene Daten, Erheben, Verarbeiten und Nutzen von Daten usw.

§ 3 a BDSG: Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 4 Abs. 1 BDSG: Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

§ 4 Abs. 3 BDSG: Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, soweit er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über die Identität der verantwortlichen Stelle, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Kategorien von Empfängern nur, so-

weit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss, zu unterrichten [...].

§ 4 a Abs. 1 BDSG: *Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.*

§ 5 BDSG: *Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.*

§ 13 BDSG: Hier ist geregelt, wann das Erheben personenbezogener Daten zulässig ist.

§ 14 BDSG: Hier ist geregelt, wann das Speichern, Verändern oder Nutzen personenbezogener Daten zulässig ist.

§ 19 BDSG: Hier ist ein umfassendes Auskunftsrecht des Betroffenen über die über ihn gespeicherten Daten, den Empfänger der Daten und den Zweck der Speicherung geregelt.

Das BDSG gilt subsidiär gegenüber anderen Regelungen, §§ 1 Abs. 3 und 4 Abs. 1 BDSG. Andere Regelungen im Sinne dieser Normen sind nicht nur die Regelungen des TKG und des TMG, sondern z. B. auch Regelungen in Betriebsvereinbarungen. Gerade im Hinblick auf das Informationsrecht der Betroffenen gemäß § 19 f. BDSG kann der Abschluss einer Betriebsvereinbarung für den Arbeitgeber von Interesse sein.

4. Telemediengesetz (TMG)

§ 1 Abs. 1 TMG

Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste [es folgen Ausnahmen]. Dieses Gesetz gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

§ 2 TMG

Im Sinne dieses Gesetzes ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereit hält oder den Zugang zur Nutzung vermittelt, [...] ist Nutzer jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen [...]

5. Telekommunikationsgesetz (TKG)

§ 3 TKG: Enthält zahlreiche Begriffsbestimmungen, unter anderem eine Bestimmung der Bestandsdaten (§ 3 Nr. 3 TKG), des Endnutzers (§ 3 Nr. 8 TKG) und des geschäftsmäßigen Erbringens von Telekommunikationsdiensten (§ 3 Nr. 10 TKG) als das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht.

§ 88 Abs. 1 TKG: *Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.*

§ 88 Abs. 2 TKG: *Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.*

§ 91 Abs. 1 TKG: *Dieser Abschnitt regelt den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken. Dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbarer juristischen Person oder Personengesellschaft, sofern sie mit der Fähigkeit ausges-*

tattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, stehen den personenbezogenen Daten gleich.

IV. Grundsätzliche Weichenstellung: Private Nutzung erlaubt oder verboten?

Für die Frage, welche Befugnisse der Arbeitgeber bei der Kontrolle von Internet- und E-Mail-Verkehr der Arbeitnehmer ein Arbeitgeber hat, ist es von entscheidender Bedeutung, ob die private Nutzung des Internets und der E-Mail-Funktionen gestattet ist.

1. Grundsatz

Rechner, Server und Bürokommunikationsmittel sind in der Regel Eigentum des Arbeitgebers. Er bestimmt, **ob** die Arbeitnehmer diese Arbeitsmittel auch privat nutzen dürfen. Er ist bei dieser Frage in seiner Entscheidung frei und an eine Mitwirkungshandlung eines ggf. bestehenden Betriebsrates nicht gebunden (vgl. z. B. **LAG Hamm 07.04.2006 MMR 2006, 700**).

2. Zustimmung zur privaten Nutzung

Die Zustimmung zur privaten Nutzung der Kommunikationsmittel kann (idealerweise) im **Arbeitsvertrag** geregelt werden. Die Privatnutzung kann aber auch Gegenstand einer **Betriebsvereinbarung** sein. Besondere Vorsicht ist im Hinblick auf eine möglicherweise entstehende **betriebliche Übung** geboten. Auch dadurch kann die Erlaubnis zur privaten Nutzung gegeben werden. Die Lösung des Arbeitgebers von einem durch betriebliche Übung entstandenen Anspruch ist bekanntermaßen schwer.

3. Folgen der Zulassung privater Nutzung

Unabhängig davon, ob der Arbeitgeber die private Nutzung des Internets gestattet, hat der Betriebsrat bestimmte **Mitbestimmungsrechte** – im Falle der privaten Nutzung ist der Umfang dieser Rechte jedoch erweitert (dazu unten V.)

Ist die private Nutzung der Kommunikationsmittel erlaubt, wird der Arbeitgeber außerdem zum **Dienstleiter im Sinne des TKG** (vgl. § 3 Nr. 10 TKG – hierzu unten VI.) und **Diensteanbieter im Sinne des TMG** (vgl. § 2 Nr. 1

TMG – hierzu unten VII.). Ist die private Nutzung nicht gestattet, sind die Vorschriften des TKG und des TMG für den Arbeitgeber ohne Belang. Es bleibt bei den insoweit subsidiär geltenden Regelungen des BDSG (vgl. §§ 1 Abs. 3 und 4 Abs. 1 BDSG).

V. Mitbestimmungsrechte des Betriebsrates

1. Mitbestimmungsrechte unabhängig von privater Nutzung

Neben der allgemeinen Verpflichtung des Betriebsrats, die zugunsten des Arbeitnehmers geltenden Gesetze, also auch Datenschutzvorschriften, zu überwachen (§ 80 Abs. 1 Nr. 1 BetrVG), kommt vor allem der Regelung in § 87 Abs. 1 Nr. 6 BetrVG besondere Bedeutung zu. Dem Wortlaut nach besteht das Mitbestimmungsrecht nur bei der Einführung und Anwendung von technischen Einrichtungen, die dazu *bestimmt sind*, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Es besteht aber Einigkeit, dass es nicht entscheidend auf die Intension des Arbeitgebers bei Einführung der technischen Einrichtung ankommt, sondern auf ihre generelle Geeignetheit zur Überwachung. Schon dann besteht das Mitbestimmungsrecht des Betriebsrates (ständige Rechtsprechung seit **BAG 09.09.1975, AP Nr. 2 zu § 87 BetrVG 1972 Überwachung**).

Überwachung im Sinne des § 87 Abs. 1 Nr. 6 BetrVG ist jeder Vorgang, durch den Informationen über das Verhalten oder die Leistung von Arbeitnehmern dokumentiert wird. Daraus folgt zwingend, dass selbst die Einführung standardisierter Software mitbestimmungspflichtig ist. Auch diese Softwareprogramme ermöglichen nämlich eine Auswertung protokollierter Informationen über die Nutzung.

Zwar ist Software für sich allein genommen noch keine „technische Einrichtung“. Eine solche isolierte Betrachtung entspräche allerdings nicht dem Schutzzweck der Norm. Jedenfalls im Zusammenhang mit dem jeweiligen Arbeitsplatz (Hardware und Software) stellt auch die Einrichtung einer neuen Software die Einführung einer technischen Einrichtung dar, die der Mitbestimmung gemäß § 87 Abs. 1 Nr. 6 BetrVG unterliegt.

2. Erweiterte Mitbestimmungsrechte bei privater Nutzung

Gestattet der Arbeitgeber die private Nutzung des Internets und des E-Mail-Verkehrs, erweitert dies die Mitbestimmungsrechte des Betriebsrates. Da der Betriebsrat gemäß § 87 Abs. 1 Nr. 1 BetrVG auch bei Fragen der Ordnung des Betriebs und des Verhaltens der Arbeitnehmer im Betrieb mitzubestimmen hat, ist die Frage des **Wie** der Internetnutzung mitbestimmungspflichtig. Will der Arbeitgeber also z. B. die private Internetnutzung auf bestimmte Zeiten beschränken (z. B. nur in den Pausen), bestimmte Nutzungsarten unterbinden (z. B. das Herunterladen von Dateien) oder Seiten bestimmten Inhalts grundsätzlich sperren (z. B. Seiten mit pornografischen Inhalten), bedarf er der Zustimmung des Betriebsrats.

VI. Vorschriften des TKG bei zulässiger privater Nutzung

Wenn ein Arbeitgeber die private Nutzung des Internets gestattet – und sei es unentgeltlich – ist er geschäftsmäßiger Anbieter von Telekommunikationsdiensten im Sinne des TKG (§ 3 Nr. 6 TKG). Der Arbeitnehmer ist Dritter im Sinne des Gesetzes. Den Arbeitgeber treffen deshalb weitgehende Verpflichtungen: Der Arbeitgeber ist verpflichtet, das **Fernmeldegeheimnis** zu wahren (§ 88 TKG). Dem Fernmeldegeheimnis unterfallen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Geschützt sind also alle Inhalts- und Verbindungsdaten. Zu Reichweite und Umfang des Fernmeldegeheimnisses im Hinblick auf E-Mails gibt es noch keine Rechtsprechung. Die Rechtsprechung zum Fernmeldegeheimnis im Hinblick auf die Verbindungsdaten im Mobilfunkverkehr kann jedoch entsprechend herangezogen werden (vgl. **BVerfG, 02.03.2006, Az. 2 BvR 2099/04**).

Der Arbeitgeber hat aber nicht nur das Fernmeldegeheimnis zu wahren. Er hat gemäß § 109 TKG auch die **technischen Voraussetzungen** dafür zu schaffen, dass das Fernmeldegeheimnis gewahrt werden kann. Die technischen Vorkehrungen zum Schutz des Fernmeldegeheimnisses müssen angemessen sein, um das Ziel zu erreichen (Schutz des Fernmeldegeheimnisses). Die mit der Einführung entsprechender technischer Einrichtung verbundenen Kosten und der damit verbundene Aufwand sind kein Argument gegen die Einführung der gesetzlich geforderten Maßnahmen. Es findet insoweit keine Abwägung zwischen dem Aufwand des Arbeitgebers einerseits und dem Schutz des Fernmeldegeheimnisses andererseits

statt (**streitig** –zum Teil wird vertreten, dass hier eine Interessenabwägung stattzufinden habe, da das TKG in erster Linie gewerbliche Betreiber im Blick habe, nicht den „normalen“ Arbeitgeber, der lediglich die private Internetnutzung ermögliche).

Der Arbeitgeber darf in das Fernmeldegeheimnis nur insoweit eingreifen, als der Eingriff erforderlich ist, um das Entgelt für die Telekommunikationsdienste zu ermitteln (§ 97 TKG) oder um Störungen und Fehler der TK-Anlage zu beheben oder die rechtswidrige Nutzung des Internets zu unterbinden (vgl. § 100 TKG).

Insbesondere der zuletzt genannte Eingriffsgrund (Aufklären rechtswidriger Internetnutzung) wird in der Praxis gerne bemüht, um Eingriffe in das Fernmeldegeheimnis zu rechtfertigen. Dabei wird meist übersehen, dass **konkrete Anhaltspunkte** für einen Internetmissbrauch bestehen müssen, um einen Eingriff in das Fernmeldegeheimnis zu rechtfertigen (§ 100 Abs. 3 TKG). Soweit das TKG anwendbar ist, verdrängt es insoweit die Regelungen des BDSG.

VII. Vorschriften des TMG bei zulässiger privater Nutzung

Gemäß § 11 Abs. 1 Nr. 1 TMG gelten die Vorschriften des TMG nicht in den Fällen, in denen die private Nutzung des Internets nicht gestattet ist. Daraus folgt, dass die Regelungen des TMG nur Anwendung finden, wenn der Arbeitgeber die Privatnutzung des Internets oder **den privaten E-Mail-Verkehr und die private Internet-Nutzung gestattet**.

Der Arbeitgeber ist verpflichtet, dem Arbeitnehmer Internet- und E-Mail-Nutzung anonym oder unter einem fremden Namen (Pseudonym) zu ermöglichen (§ 13 Abs. 6 TMG), soweit dies technisch möglich und zumutbar ist. Der Arbeitnehmer ist über diese Möglichkeit zu informieren. Gespeicherte Daten sind nach der zulässigen Verwendung (z. B. zur Abrechnung) zu löschen. Dies folgt aus der enumerativen Aufzählung in §§ 14 und 15 TMG, zu welchem Zweck und wie lange Daten erhoben und verwendet werden dürfen. Auch hier gilt, dass die Vorschriften des BDSG subsidiär sind.

VIII. Vorschriften des BDSG bei zulässiger privater Nutzung

Die Vorschriften des BDSG finden bei zulässiger privater Nutzung nur eingeschränkt Anwendung, da vorrangig die Regelung des TKG und des TMG anzuwenden sind. Die Vorschriften des BDSG erlangen jedoch eigenständige Bedeutung in den Fällen, in denen die private Nutzung von Internet und E-Mail durch die Arbeitnehmer nicht gestattet ist. In diesen Fällen sind TKG und TMG nicht einschlägig. Allerdings ist zu beachten, dass auch **Betriebsvereinbarungen Regelungen im Sinne des § 4 Abs. 1 BDSG** sein können. Soweit danach die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig ist, geht diese Regelung vor.

Betriebsvereinbarungen werden allerdings in der Regel **im Vorfeld** der konkreten Datenerhebung, Nutzung und Verarbeitung greifen, nämlich bei der Implementierung entsprechender Systeme (vgl. oben). Demgegenüber betrifft das BDSG wie auch die Regelungen des TMG und des TKG **den konkreten Vorgang** der Datenerhebung, Verarbeitung und Verwendung (wenngleich auch TMG und TKG über den konkreten Fall hinaus Vorgaben zur Datensicherheit machen).

IX. Kontrollmöglichkeiten des Arbeitgebers bei zulässiger privater Nutzung

1. Berechtigtes Interesse an Kontrolle

Der Arbeitgeber hat ein berechtigtes Interesse daran, seine Daten, seine Datenverwaltungsstrukturen und den Zugang zum Netz zu kontrollieren. Dabei geht es nicht lediglich um die mit der Internetnutzung gegebenenfalls verbundenen Kosten, sondern vor allem um die Know-How-Sicherung und die Sicherung des Datenbestandes. Soweit der Gesetzgeber dem Arbeitgeber Verpflichtungen auferlegt, z. B. zur effektiven Sicherung des Fernmeldegeheimnisses gemäß § 109 TKG, handelt der Arbeitgeber bei Kontrolle und Überwachung des E-Mail- und Internetverkehrs insoweit auch zur Erfüllung seiner gesetzlichen Verpflichtung zu effektivem Schutz des Fernmeldegeheimnisses. Nicht zu vergessen ist die ggf. mit einem Missbrauch von E-Mail und Internet einhergehende Rufschädigung für das Unternehmen, wenn z. B. aus dem Netz des Arbeitgebers Angriffe auf Datenbestände und -strukturen Dritter verübt werden (Hacker, Virenangriffe) oder die Netzstruktur des Arbeitgebers als

Plattform für illegale Tätigkeiten dient (Betrügereien, Versendung pornografischer oder extremistischer Inhalte).

2. Geeignete rechtliche und technische Strukturen schaffen

Der Arbeitgeber ist gut beraten, in den **Arbeitsverträgen** explizit zu regeln, ob er die private Nutzung von Internet und E-Mail gestattet oder nicht. Angesichts des Umstandes, dass E-Mail als Kommunikationsmittel auch innerhalb des Betriebes genutzt wird und der Arbeitgeber den persönlichen Kontakt der Arbeitnehmer untereinander nicht unterbinden darf, erscheint eine vollständige Untersagung der Nutzung zunehmend problematisch. Die zeitliche Begrenzung (z. B. Internetnutzung nur während der Mittagspause oder nach Dienst) oder die Untersagung bestimmter Nutzungsarten (Verbot des Herunterladens von Musikdateien u. ä.) ist deshalb sinnvoll, weil die Regelung hinreichend konkret ist, um Verstöße klar zu erkennen und zu sanktionieren.

Darüber hinaus sind alle Mitarbeiter, die in Kontakt mit Datenverarbeitungssystemen kommen, zumindest **gemäß § 5 BDSG zum Datenschutz zu verpflichten**. Soweit die Vorschriften des TMG und des TKG einzuhalten sind, ist auf die Einhaltung des Fernmeldegesetzes zu achten. Auch dies sollte in den Verträgen erwähnt sein.

Schwieriger gestaltet sich die Schaffung einer **technischen Struktur** zur Missbrauchsverhinderung. Die Errichtung einer **Firewall** ohne gesetzliche oder in einer Betriebsvereinbarung niedergelegter Rechtfertigung ist bei zugelassener Privatnutzung des Internets ein rechtswidriger Eingriff in das Persönlichkeitsrecht. Dies folgt schon daraus, dass über die Firewall Nutzungs- und Inhaltsdaten aufgezeichnet werden, die grundsätzlich zur Auswertung geeignet sind. Es empfiehlt sich daher, für die private Nutzung getrennte Accounts anzulegen, damit der Arbeitgeber auf die dienstlichen Accounts zugreifen kann. Sollte er dort wider Erwarten auf private Korrespondenz stoßen, hat er diese unverzüglich an den Arbeitnehmer weiterzuleiten und in dem dienstlichen Account zu löschen, ohne den Inhalt der Nachricht zur Kenntnis zu nehmen. Für Vertretungsfälle (Urlaub, Krankheit) ist individual-vertraglich oder durch Betriebsvereinbarung die Rechtsgrundlage zu schaffen, um den E-Mail-Verkehr einsehen zu können.

3. Konkrete Kontrolle

Wenn der Arbeitgeber die **Privatnutzung des Internets nicht gestattet**, darf er zumindest stichprobenartig prüfen, ob das Verbot der Privatnutzung auch eingehalten wird. So wirkt er auch dem Entstehen einer betrieblichen Übung entgegen. Eine lückenlose und ständige Überwachung des E-Mail- und Internetverkehrs ist auch bei der rein dienstlichen Nutzung nicht zulässig, weil damit Nutzungsprofile erstellt werden können, was das informationelle Selbstbestimmungsrecht der Arbeitnehmer verletzt (str).

Dienstliche E-Mails darf der Arbeitgeber ebenso lesen wie Akten auf konventionellen Datenträgern (Papier). Problematisch ist allerdings ein unbeschränkter Zugriff auf die Postfächer der Arbeitnehmer, da nicht ausgeschlossen ist, dass unternehmensinterne Kommunikation zwischen den Arbeitnehmern stattfindet, die nicht für den Vorgesetzten bestimmt ist. Da gemäß § 28 Abs. 1 Nr. 1 BDSG die Kontrolle der Verbindungs- und Inhaltsdaten aber zulässig ist, wenn die Verwendung der Daten im Rahmen der Zweckbestimmung einer Vertragsverhältnisses liegt, bestehen gegen die grundsätzliche Nutzung der E-Mail- und Internetdaten keine Bedenken, wenn die Privatnutzung untersagt ist. Ob eine konkrete Maßnahme des Arbeitgebers noch zulässig oder wegen Unverhältnismäßigkeit unzulässig ist, ist eine Frage der Einzelfallbewertung.

Schwieriger gestaltet sich die Situation, wenn der Arbeitgeber die **private Nutzung von Internet und E-Mail gestattet** hat. Eine Protokollierung der Internet- und E-Mail-Nutzung kann – einmal abgesehen von einer ausdrücklichen Einwilligung der Arbeitnehmer – nur erfolgen, wenn dies der Datenschutzkontrolle, der Datensicherung oder der Sicherung des ordnungsgemäßen Betriebes oder zu Abrechnungszwecken erforderlich ist oder der Verdacht auf eine strafrechtlich relevante Nutzung vorliegt. Jede weitergehende Kontrolle ist unzulässig.

Problematisch ist in diesem Zusammenhang die automatisierte Filterung und Löschung von unerwünschten E-Mail-Botschaften (Spam-Mails). Ein solches Beseitigen der an einen anderen gerichteten elektronischen Post kann strafrechtlich relevant sein (§§ 206 Abs. 3, 303 a StGB –streitig).

- Leitfaden für umfassende, regelkonforme, sichere und abgesicherte E-Mail-Korrespondenz, Webnutzung und Webinhalte für Unternehmen“, www.e-policyinstitute.com
- Hanau, Peter; Hoeren, Thomas (Hrsg.) „Private Internetnutzung durch Arbeitnehmer“ Verlag C.H. Beck, Schriftenreihe Information und Recht, Band 34, 2003
- Hassemer, Ines M.; Witzel, Michaela „Filterung und Kontrolle des Datenverkehrs – Ist die Filterung von E-Mails im Unternehmen rechtmäßig?“, ITRB 2006, S. 139 ff
- Koch, Frank (Hrsg.) „Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel“, NZA 2008, S. 911 ff.
- Krauß, Claudia (Hrsg.) „Internet am Arbeitsplatz“, JurPC webdog 14/2004, Abs. 1 - 52
- Lehmann, Michael; Meents, Geert (Hrsg.) Handbuch des Fachanwalts für Informationstechnologierecht:
S. 375 ff.: Arbeitsrechtliche Aspekte beim IT-Outsourcing
S. 717 ff.: Arbeitnehmererfindungsrecht
S. 895 ff.: Datenschutzrecht
- Möller, Reinhard „Privatnutzung des Internets am Arbeitsplatz“, ITRB 2005, S. 142
- Möller, Reinhard „Betriebsvereinbarungen zur Internetnutzung“ ITRB 2008 (noch nicht veröffentlicht)