MANUEL KIPER

Kontrollierte Kommunikation (1)

›Mitarbeiterorientierung‹ hin, ›Vertrauenskultur‹ her, wenn die Möglichkeiten für eine mehr oder weniger lückenlose Kontrolle des Komunikationsverhaltens da sind, dann sind Vor(aus)sicht und klare Regelungen immer noch die Mutter der Porzellankiste.

Das letztjährige Vorhaben von ›Mister Minit‹, Beschäftigte permanent mit Video zu überwachen, wurde vom ›Kaufhof‹-Konzern abgeblockt. Eine so offensichtliche und lückenlose Überwachung des Verhaltens von Beschäftigten ist in Deutschland nicht zulässig (›Alles sehen, alles kontrollieren – und mehr ...‹ in CF 2/99 ab Seite 4). Weniger offensichtliche Formen der Verhaltenskontrolle erfreuen sich aber auch in Deutschland wachsender Beliebtheit. Vorgesetzte und Unternehmensleitungen nutzen Informations- und Kommunikationstechniken wie eMail und Internet-Surfen, um die Arbeit und das Verhalten von Beschäftigten transparent zu machen. Ein- und ausgehende eMails werden gelesen, über das möglicherweise dienstfremde Internet-Surfen einzelner Arbeitnehmer werden ›Rennlisten‹ geführt. Im Einzelfall kommt es zu Sanktionen bis hin zu Kündigungen.

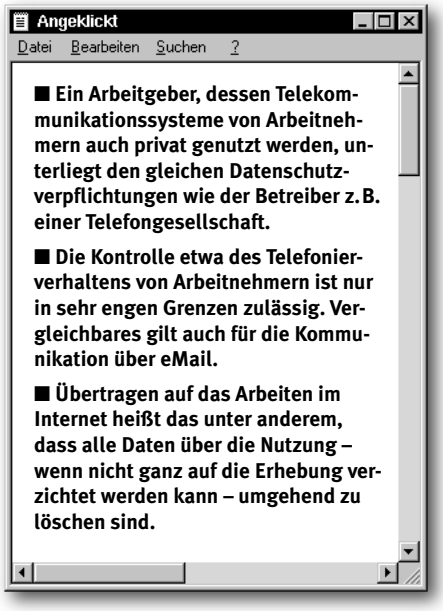
Was sich da in einigen Betrieben als Kontroll-Praxis etabliert, ist deshalb aber längst noch nicht rechtens. Höchstrichterliche Entscheidungen zur eMail-Kommunikation oder zum Surfen im Internet stehen zwar aus und die obersten Gerichte, Bundesarbeitsgericht wie Bundesverfassungsgericht, schließen im Hinblick auf andere betriebliche Kontrolltechniken eine punktuelle und vorübergehende Video- oder Abhör-Überwachung im Einzelfall (insbesondere bei Vorliegen erheblicher Verdachtsgründe) auch nicht aus. Eine generelle Video- oder Abhör-Überwachung aber haben sie grundsätzlich als eine mit dem Persönlichkeitsrecht und dem Recht auf ›informationelle Selbstbestimmung‹ nicht zu vereinbarende Kontrolle für unzulässig erklärt.

Unübersichtliche Rechtslage

Die Rechtslage insgesamt allerdings ist eher unübersichtlich. Zusammenfassend lässt sich sagen:

Wenn und soweit vom Arbeitgeber die private Nutzung der betrieblichen Telekommunikations-Anlagen für interne oder externe Kommunikation gestattet oder nicht ausgeschlossen wird, gelten sowohl das Fernmeldegeheimnis wie auch die datenschutzrechtlichen Bestimmungen des Telekommunikationsgesetzes (TKG).

Der Grund: In dem Moment, in dem der Arbeitgeber seine TK-Einrichtungen für den privaten Gebrauch durch Arbeitnehmer öffnet, wird er als jemand tätig, der ›Dritten‹ (in diesem Fall: seinen Arbeitnehmern) Telekommunikations-Dienstleistungen anbietet. Und weil er das tut, wird er den TK-Dienstleistern gleichgestellt und fällt als ›geschäftsmäßiger‹ Anbieter von TK-Diensten unter die gleichen gesetzlichen Regelungen wie beispielsweise eine Telefongesellschaft. Unerheblich ist dabei, ob die TK-Anlagen entgeltlich oder unentgeltlich zu privaten Zwecken genutzt werden dürfen. Selbst das ausdrückliche Untersagen privater Nutzung der TK-Anlagen durch die Beschäftigten entbindet nicht von der Verpflichtung zur Einhaltung des Fernmeldegeheimnisses und der Datenschutzvorschriften nach dem TKG, wenn *eingehende* Anrufe und eMails – die ja auch privaten Charakter haben könnten – *automatisch* an die Nebenstelle vermittelt werden (Durchwahl). Nur wenn der Arbeitgeber die strikte Nutzung der betrieblichen TK-Anlagen allein für dienstliche Zwecke erzwingt und dies auch organisatorisch sicherstellt, wären im Hinblick auf die Beschäftigten die Merkmale eines Telekommunikations-Dienstes *für Dritte* nicht mehr erfüllt und damit würde dann auch die Verpflichtung entfallen, die Schutzbestimmungen des TKG zu beachten (siehe dazu ›Telekommunikationsgesetz-



gebung und Arbeitnehmerdatenschutz‹ in CF 8-9/99 ab Seite 24).

Diese – zugegeben – weite Auslegung des Fernmeldegeheimnisses im TKG war vom Gesetzgeber gewollt und wird gestützt durch Entscheidungen höchster Gerichte, bezogen vor allem auf die Kontrolle des Telefonierverhaltens. So hatte das Bundesverfassungsgericht 1991 geurteilt, dass ein Telefonüberwachungs-System, mit dessen Hilfe der Arbeitgeber alle dienstlichen wie privaten Telefongespräche seiner Arbeitnehmer aufzeichnen und abhören kann, einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts darstellt (BverfG, Urteil vom 19. 12. 1991, BB 1992, Seite 708). Allein die Tatsache, dass ein Telefongespräch »in der Sphäre eines Arbeitsverhältnisses« geführt wird, erlaubt es einer weiteren Person (z. B. dem Personalchef oder dem Abteilungsleiter) also keineswegs, ohne Zustimmung des Gesprächspartners mitzuhören oder mithören zu lassen. Damit hat das BVerfG (in Korrektur übrigens einer anders lautenden Entscheidung des Bundesarbeitsgerichts) festgehalten, dass ein Mithören oder Aufzeichnen des Inhalts eines Telefonats die Einwilligung des betreffenden Arbeitnehmers voraussetzt und dass diese nicht etwa stillschweigend als erteilt angenommen werden kann, nur weil der Arbeitnehmer um die Abhörmöglichkeit weiß (siehe dazu den Beitrag ab Seite 20).

Auch das Bundesarbeitsgericht (BAG) hat dann im Oktober 1997 entschieden, dass im beruflichen Bereich das Recht am gesprochenen Wort als Teil des allgemeinen Persönlichkeitsrechts zu gewährleisten ist. Entsprechend hat das BAG bei heimlichem Mithören(lassen) von Telefongesprächen eine Persönlichkeitsrechtsverletzung erkannt. Heimliches Mithören(lassen) von Telefongesprächen zwischen Arbeitgeber und Arbeitnehmer ist also unzulässig. Auf diese Weise erlangte Beweismittel dürfen nicht verwertet werden. Hört bei einem Telefongespräch eine dritte Person mit, ist der Gesprächspartner vorher darüber zu informieren. Gesprächspartner am Telefon müssen sich nicht vorsorglich vergewissern, dass niemand mithört.

Bereits seit dem so genannten Fangschaltungsbeschluss des BVerfG 1985 war entschieden, dass *betriebsbedingte* Einblicke eines Betreibers von Telekommunikations-Anlagen (und dazu gehört, wie gesagt, auch der Arbeitgeber, der eine Telefonanlage oder ein Intranet betreibt) in Inhalte und Umstände elektronischer Kommunikation »rechtfertigungsbedürftige Eingriffe in das Fernmeldegeheimnis« seien. Konkretisierend hat denn auch das BAG 1995 eine Betriebsvereinbarung für zulässig erklärt, die es dem Arbeitgeber bei einer ACD-Anlage erlaubt, externe Telefongespräche der Arbeitnehmer in deren Gegenwart speziell zu Ausbildungszwecken mitzuhören. Die Praxis, dass Beschäftigte und Kunden in Call-Centern vom Betreiber sogar von außerhalb des Betriebs abzuhören sind, wie es von der ›Panorama‹-Redaktion im September 1999 öffentlich gemacht wurde, dürfte damit allerdings unvereinbar sein.

Andererseits wird in der Rechtsprechung eine Kontrolle des Telefonierverhaltens der Beschäftigten im Hinblick auf Missbrauch und Kostenverursachung für zulässig gehalten – mit den entsprechenden arbeitsrechtlichen Konsequenzen. Von unteren Arbeitsgerichtsinstanzen werden hier z. T. drastische Urteile gefällt (die allerdings vor Landesarbeitsgerichten üblicherweise nicht Bestand haben). Arbeitnehmer etwa, die in erheblichem Umfang auf Kosten ihres Arbeitgebers privat telefonieren, könnten demnach ohne Abmahnung entlassen werden, so entschied 1994 das Arbeitsgericht Frankfurt am Main. Auch das Arbeitsgericht Würzburg sah 1997 eine Kündigung ohne vorherige Abmahnung wegen vollendeten Betrugs gerechtfertigt, wenn ein Arbeitnehmer häufig auf Kosten seines Arbeitgebers telefoniert, ohne die Gespräche zu bezahlen.

Kündigungsgrund sah das Arbeitsgericht Frankfurt am Main auch bei unbezahlten Telefonaten mit Australien, insbesondere weil die betroffene Arbeitnehmerin erst nach Vorlegen eines Computerausdrucks bereit war, das Telefonat zu bestätigen. Desgleichen sah das Gericht Grund für eine Kündigung, wenn ein Arbeitnehmer auf Kosten seines Arbeitgebers telefonisch einem Nebenjob nachgehe. Und auch das Oberlandesgericht Hamm entschied 1998, dass ein leitender Angestellter durch Inanspruchnahme von Telefonsex-Gesprächen in

info

Übersicht:

Kontroll-Software im Internet

CyberPatrol	**http://www.cyberpatrol.com/**
Disk Tracy	**http://www.disktracy.com/**
Little Brother	**http://www.charred.com/**
NetNanny	**http://www.netnanny.com/**
NetSnitch	**http://www.netsnitch.com/**
Spector	**http://www.spectorsoft.com/**
SurfControl	**http://www.jsb.com/**
SurfWatch	**http://www.surfwatch.com/**
WinGuardian	**http://www.webroot.com/**
WinWhatWhere	**http://www.winwhatwhere.com/**

»nicht unbeträchtlicher Höhe für private Zwecke« seine ihm verliehene Vertrauensstellung im Betrieb missbraucht habe und damit ohne Abmahnung entlassen werden könne.

1999 hingegen entschied das Arbeitsgericht Frankfurt am Main: »Ist einem Arbeitnehmer die Nutzung der betrieblichen Telefonanlage zu Privatgesprächen in bestimmtem Umfang gegen Kostenerstattung erlaubt, schließt eine derartige Gestattung auch kurze Anrufe zu privaten Zwecken während der Arbeitszeit ein, solange nicht ausdrücklich etwas anderes festgelegt wurde und der Arbeitnehmer nicht mit der ihm obliegenden Arbeitsleistung in Rückstand gerät. Die Ausübung eines solchen Rechts rechtfertigt auch dann nicht ohne Weiteres den Vorwurf einer gegen den Arbeitgeber gerichteten Straftat und eine außerordentliche Kündigung des Arbeitgebers, wenn der Arbeitnehmer ohne Aufforderung des Arbeitgebers die durch die Privatgespräche entstanden Kosten (hier: DM 66,51) nicht von sich aus erstattet.«

Und einschlägige Entscheidungen der Landesarbeitsgerichte sind im Vergleich zu den Arbeitsgerichten generell glimpflicher für die Beschäftigten ausgegangen. So entschied 1997 das LAG Niedersachsen, dass auch bei erwiesener Vielzahl von Privattelefonaten auf Arbeitgeberkosten eine verhaltensbedingte Kündigung erst zu rechtfertigen sei, wenn der betroffene Arbeitnehmer vorher abgemahnt worden sei. Das LAG Köln befand 1998 sogar: Erlaubt ein Arbeitgeber seinen Beschäftigten, private Telefonate von seiner Anlage aus zu führen, so darf er einem Arbeitnehmer, der davon »ausschweifend« Gebrauch macht, nicht kündigen, insbesondere dann nicht, wenn er durch eine »unzureichende Organisation« erst spät darauf aufmerksam wird und damit rechtzeitige Ermahnungen unterblieben sind.

Insofern ist alles in allem von einem weitreichenden Schutz des Fernmeldegeheimnisses und des Datenschutzes bei Telekommunikations-Vorgängen auszugehen. Nicht zuletzt sind die Mitgliedsstaaten der EU durch die – hierzulande noch nicht umgesetzte – EG-Telekommunikations-Datenschutzrichtlinie von 1997 generell dazu verpflichtet, »das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikationen durch andere Personen als die Benutzer« zu untersagen.

Umgang mit der elektronischen Post regeln

Durch das Fernmeldegeheimnis ist aber – wie bereits dargelegt – nicht nur das Telefonieren geschützt, sondern *jede Art* der individuellen Nachrichtenübermittlung, einschließlich eMail und Telefax. Auch die Einführung eines allgemeinen Überwachungssystems für den elektronischen Postverkehr im Unternehmen stellt deshalb einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts der Arbeitnehmer dar. Bei ausgesprochener Geschäftspost sind solche Eingriffe zu Kontrollzwecken zwar zulässig, persönlich adressierte oder zum Beispiel an den Betriebs- oder Personalrat gerichtete oder verschickte eMails jedoch unterliegen einem Schutz vor Überwachung nicht nur des Inhalts, sondern auch der Verbindungsdaten.

Im Hinblick darauf, dass Telefax-Geräte vielfach frei zugänglich sind und dass eMails auch auf anderen als dem Rechner des Empfängers zwischengespeichert werden, gewinnen hier auch die Vorschriften des § 87 TKG Bedeutung, die den Arbeitgeber zu technischen Schutzmaßnahmen zwingen, soweit diese nötig sind, um das Fernmeldegeheimnis zu sichern. Zwar haben Angestellte, die eingegangene Telefaxe einem Gerät – zum Beispiel einem Abteilungs-Telefaxgerät – entnehmen, persönlich das Fernmeldegeheimnis zu wahren und Gleiches gilt auch für den Ausdruck von Sende- und Empfangsprotokollen an einem Telefaxgerät, das von mehreren Personen genutzt wird. § 87 Abs. 1 TKG verpflichtet aber darüber hinaus den Arbeitgeber, »der eine Telekommunikationsanlage betreibt, die dem geschäftsmäßigen Erbringen von Telekommunikationsdiensten dient«, zu »angemessenen technischen Vorkehrungen oder sonstigen Maßnahmen« zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten und zum Schutz programmgesteuerter Telekommunikations- und Datenverarbeitungs-Systeme gegen unerlaubte Zugriffe.

Dabei sind zum Schutz des Fernmeldegeheimnisses organisatorisch-technische Maßnahmen wie Zutritts- und Zugriffsbeschränkungen ebenso vorzusehen wie Anonymisierungs-Maßnahmen und auch Verschlüsselungen. Dies sicherzustellen dürfte in vielen Unternehmen allerdings eine Umorganisation notwendig machen, um so zum Beispiel Verbindungsprotokolle, die zur Auswertung häufig in gedruckter Form vorliegen, vor unbefugter Einsichtnahme zu schützen. Elektronische Posteingangsbücher und die Dokumentation der betriebsinternen eMail-Bearbeitung haben ebenfalls das Fernmeldegeheimnis zu wahren. So dürfen beispielsweise eMails an namensbezogene Adressen (also etwa: **manuel.kiper@#####.de**)nicht protokolliert werden.

Nur in Einzelfällen darf der Arbeitgeber auch persönlich adressierte eMails einsehen – zumindest nach Auffassung des Berliner Datenschutzbeauftragten: »Der Arbeitnehmer hat dem Arbeitgeber den Zugang zu solchen eMails zu eröffnen. Dagegen ist eine Auswertung des gesamten eMail-Verkehrs (etwa durch automatisches Scannen) durch den Arbeitgeber jedenfalls im Regelfall nicht gestattet.«

Ist eine spezielle Kennzeichnung privater eMails systemtechnisch nicht vorgesehen, erstreckt sich die Geheimhaltungspflicht nach dem TKG auf den gesamten betrieblichen eMail-Verkehr. Ist hingegen die Privatnutzung des eMail-Systems betriebsintern mengenmäßig oder zeitlich limitiert und diese Regelung den Beschäftigten bekanntgegeben worden, sind nach Auffassung der Baden-Württembergischen Datenschützer »Missbrauchskontrollen durch das Beschäftigungsunternehmen zulässig«. Klar ist, dass ein Zugriff des Arbeitgebers auf eMails aus Gründen der Systemsicherheit, des Schutzes vor Viren und des Schutzes vor Kosten- und Netzüberlastung nicht völlig ausgeschlossen werden kann.

Datenschutz bei Telediensten

Weil Arbeitgeber, die ihren Beschäftigten den Zugang zum Internet nicht ausschließlich für dienstliche Zwecke ermöglichen, definitionsgemäß Teledienste-Anbieter sind, gilt für sie nicht nur das TKG, sondern auch das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG). Teledienste sind Telebanking und Telespiele, Verkehrs- oder Börsendaten und manches andere. Vor allem aber sind Teledienste Angebote zur Nutzung des Internet oder weiterer Netze, also auch für firmeninterne Computernetze wie etwa ein Intranet.

Wird hingegen in einem Konzern den Konzernbeschäftgten von einem Konzern-Service-Betreiber die Internet-Nutzung nur für betriebliche Zwecke zur Verfügung gestellt, so ist nach Auffassung z. B. des Baden-Württembergischen Innenministeriums das einzelne *Beschäftigungsunternehmen* der Nutzer und *nicht* der einzelne *Beschäftigte*, so dass in diesem Fall »die Daten grundsätzlich auch zur Kontrolle des Verhaltens und der Leistung verwendet werden dürfen« – vorbehaltlich natürlich der Mitbestimmung durch den Betriebsrat (so es denn einen gibt). Dem wird von anderen Datenschutzexperten allerdings widersprochen und die Gültigkeit des TDG auch für unternehmensinterne

info

Die wichtigsten rechtlichen Grundsätze ...

... zur eMail- und Internet-Nutzung

Die individuell zuzuordnende systematische Überwachung, Kontrolle, Dokumentation und Auswertung des Telekommunikations-Verhaltens von Beschäftigten ist weitgehend verboten, da das Fernmeldegeheimnis und das Persönlichkeitsrecht zu achten sind. Dies gilt, wenn und sofern private betriebliche Telekommunikation:

- **nicht verboten, sondern geduldet oder erlaubt ist;**
- **nicht unentgeltlich erfolgt, sondern gesondert abgerechnet wird oder**
- **bei unentgeltlicher Nutzung nur geringfügig genutzt wird.**

Im Falle rein dienstlicher Nutzung betrieblicher Telekommunikations-Anlagen gilt es im Einzelfall zwischen Direktionsrecht und Persönlichkeitsrecht abzuwägen. Dabei kann von folgenden Grundsätzen ausgegangen werden:

- **Mithören ohne ausdrückliche Bekanntgabe ist nicht erlaubt.**
- **Mitlesen von eMails und Dateien durch Vorgesetzte ist ohne vorherige Bekanntgabe nicht erlaubt.**
- **Systematisches Speichern von Bildschirminhalten (Screenshots), z. B. mit CyberPatrol, ist nicht erlaubt.**
- **Für die Mailbox des Betriebs-/Personalrat gilt weitgehende Meinungsfreiheit.**
- **Darüber hinaus gibt es besonders geschützte Personengruppen wie Betriebsärzte oder Mitarbeitervertretung, deren Rechte in besonderer Weise zu wahren sind.**
- **Jede Einführung oder zusätzliche Nutzung technischer Einrichtungen unterliegt der Mitbestimmung des Betriebs-/Personalrat. Ohne seine Zustimmung sind somit auch Sanktionen hinsichtlich des Telekommunikation-Verhaltens der Beschäftigten hinfällig.**
- **Bei Verfehlungen sind normalerweise Abmahnungen nötig, ehe an rechtswirksame Kündigungen auch nur gedacht werden kann.**

Nicht in jedem Fall allerdings ist eine Kontrolle durch Vorgesetzte etwa durch Mithören bei Telefonnebenstellen-Anlagen, durch das Mitlesen von eMails, das Installieren von Videokameras oder durch Auswertung der Internet-Protokolle untersagt. Gelegentliche Überwachung, Kontrolle, Dokumentation und Auswertung des telekommunikativen Verhaltens ist erlaubt:

- **zu Ausbildungszwecken;**
- **zur Kostenreduktion;**
- **aus Sicherheitsgründen (z. B. bei Netzüberlastung, Spionageverdacht, Virenbefall);**
- **bei begründetem Verdacht auf Diebstahl, Störung des Betriebsfriedens, Nutzung unlizenzierter Software, Suchen oder Speichern verbotener Inhalte (z. B. Kinderpornografie);**
- **bei begründetem Verdacht auf Verrat von Betriebsgeheimnissen oder auf nichtdienstliche Beschäftigungen am Arbeitsplatz (Tätigkeit im Nebenjob auf Kosten des Arbeitgebers, ›Rotlicht‹-Surfen usw.)**

Allerdings müssen auch in diesen Fällen die Persönlichkeitsrechte der Beschäftigten, die Rechte besonders geschützter Personengruppen und die Mitbestimmung des Betriebs-/Personalrats geachtet werden. Bei Verdacht auf strafrechtliche Vergehen von Beschäftigten ist eine eigenmächtige Überwachung durch den Arbeitgeber ohne Einschalten der Polizei/Staatsanwaltschaft nicht zulässig.

Teledienste reklamiert, »gleichgültig ob dieser im einzelnen Unternehmen oder im Konzernverbund genutzt wird«.

Arbeitnehmerdatenschutz bei Multimedia-Diensten

»Die Privatsphäre der Arbeitnehmer in Unternehmen, die Multimedia-Dienste anbieten oder nutzen, ist sorgfältig zu schützen. Dazu gehört, dass keine Verknüpfung der Daten der Beschäftigten in seiner Stellung als Arbeitnehmer mit den Daten in seiner Rolle als Kunde stattfindet. Der Anbieter hat technische und organisatorische Lösungen zur getrennten Speicherung und Verarbeitung der dienstlichen und privaten Nutzungs- und Abrechnungsdaten zur Verfügung zu stellen. Ist dies technisch nicht trennbar, muss der Dienstherr entweder eine private Nutzung untersagen oder den gesamten Telekommunikationsvorgang wie private Nutzung behandeln.« (Landesbeauftragter für den Datenschutz Niedersachsen, 1999)

Den Datenschutz bei Telediensten regelt – wie erwähnt – das Teledienstedatenschutzgesetz (TDDSG). Wobei auch das TDDSG nicht zwischen firmeninterner bzw. -externer Kommunikation unterscheidet. Und es gilt – wie im Bundesdatenschutzgesetz – ein Verbot mit ›Erlaubnisvorbehalt‹. Das heißt in diesem Fall: Jede Datenverarbeitung ist verboten, wenn sie nicht ausdrücklich gesetzlich erlaubt ist.

Folgende einzelne Datenschutzvorschriften sind in den §§ 3 – 6 TDDSG festgeschrieben:

- das Gebot der Datensparsamkeit;
- die Datenerhebung ist von der Zustimmung des Nutzers abhängig;
- der Nutzer ist von Art und Umfang der Datenerhebung zu unterrichten;
- die Nutzung ist – so weit technisch möglich und zumutbar – anonym oder pseudonym (mit einem ›Decknamen‹) zu ermöglichen;
- Nutzungsdaten, die zur Abrechnung nicht benötigt werden, sind nach Beendigung der Verbindung umgehend zu löschen;
- Abrechnungsdaten sind 80 Tage nach Rechnungslegung zu löschen;
- personenbezogene Nutzerprofile sind unzulässig und nur bei Pseudonymen erlaubt;
- eine Datenschutzkontrolle nach § 38 BDSG durch die zuständige Aufsichtsbehörde ist auch dann erlaubt, wenn keine Anhaltspunkte für eine Verletzung der Datenschutzvorschriften vorliegen.

Ist die private Internet-Nutzung am Arbeitsplatz erlaubt oder wird sie geduldet und auch nicht abgerechnet, dürfen darüber keine Daten der Beschäftigten gesammelt werden!

Die in unserem Zusammenhang wichtigsten Regeln sind:

- Nutzungsdaten (Daten über die Benutzung einer Telekommunikations-Einrichtung) und andere nicht benötigte Daten von im Internet surfenden Arbeitnehmern müssen unverzüglich gelöscht werden;
- Nutzungsprofile sind unzulässig; und das wiederum bedeutet, dass Arbeitgebern untersagt ist, Daten über die Netzbenutzung ihrer Beschäftigten auszuwerten.

»Die Protokollierung der privaten Nutzung ist nur - soweit diese vorgesehen ist - zu Abrechnungszwecken gestattet.« Entsprechenden Befürchtungen kann und sollte mit klaren Regelungen zwischen Betriebsräten und Arbeitgebern entgegen getreten werden (eine Auffassung, die im Januar dieses Jahres sogar im Handelsblatt vertreten wurde). Im Unterschied zu anderen Datenschutzgesetzen und -vorschriften bleibt der Datenschutz im TDDSG aber trotz dieser Regelungen wirkungsschwach, da dieses Gesetz nicht vorsieht, Datenschutzverstöße als Ordnungswidrigkeit zu bestrafen.

Dass Nutzungsdaten zu löschen und Nutzungsprofile verboten sind, heißt allerdings nicht, dass der Arbeitgeber jedwede Internet-Nutzung seiner Beschäftigten dulden muss. So ist dem Arbeitgeber beispielsweise das Verhängen von Zugangsbeschränkungen oder die Ahndung von Missbrauch und Geheimnisverrat nicht verwehrt. Die praktische Durchführung aber muss immer auch dem weitestgehenden Schutz des Persönlichkeitsrechts der Beschäftigten Rechnung tragen. So kann der Arbeitgeber zum Beispiel Firewalls, Filter-Software oder andere technische Mittel einsetzen, um den Zugriff auf bestimmte Dienste und Daten zu begrenzen.

Um es noch einmal ganz deutlich zu sagen: Ist die private Internet-Nutzung von Arbeitnehmern am Arbeitsplatz entweder erlaubt oder wird geduldet und wird sie auch nicht gesondert abgerechnet, darf der Arbeitgeber keine Daten über die Internet-Nutzung seiner Beschäftigten sammeln! Hervorzuheben ist auch, dass – soweit technisch möglich und zumutbar – dem einzelnen Nutzer die Möglichkeit einzuräumen ist, Teledienste anonym oder unter Pseudonym zu nutzen (bei Pseudonymen wären dann allerdings Nutzungsprofile zulässig).

Ebenso deutlich muss aber auch gesagt werden, dass strafbare Handlungen mit Hilfe von eMail- oder Internet/Intranet nicht geduldet werden müssen und dürfen. Insofern sind *bei begründetem Verdacht* Missbrauchskontrollen und Ahndung des Missbrauchs zulässig. Bei Verdacht auf strafrechtliche Vergehen von Beschäftigten ist durch den Arbeitgeber die Polizei/Staatsanwaltschaft einzuschalten.

Dies wäre zum Beispiel dann der Fall, wenn ein Beschäftigter in den Verdacht gerät, an seinem Arbeitsplatz (verbotene) Kinderpornografie aus dem Netz zu

laden und innerbetrieblich auf seinem Computer zu speichern. Das Arbeitsgericht Braunschweig hat in einem solchen Fall mit Urteil vom 22. 1. 99 eine außerordentliche Kündigung für gerechtfertigt gehalten.

Ebenfalls strafbar ist es, ...

- unbefugt in fremde Dateien einzudringen,
- beleidigende Inhalte auf seiner Website anzubieten oder
- unkommentiert Links auf beleidigende oder sonstwie strafwürdige Inhalte anderer Websites zu setzen.

Auch verstoßen Arbeitnehmer gegen ihre arbeitsvertraglichen Pflichten, wenn sie während der Arbeitszeit nichtdienstliche Daten an ihrem Arbeitsplatz verarbeiten. So kann zum Beispiel die Anlage von Dateien mit sexistischen oder rassistischen Witzen und deren Überspielung an Kollegen Grund für eine fristlose Kündigung sein (so sah es das LAG Köln 1998).

Aber: Eine *systematische* Überwachung und personenbezogene Auswertung von Internet-Aktivitäten, wie sie die Filterprogramme von CyberPatrol, Little Brother, Spector, SurfControl und andere Software zulassen (siehe ›Alles unter Kontrolle?‹ in: CF 12/98 ab Seite 18), ist in den USA zwar üblich, in Deutschland aber unzulässig!

Persönlichkeitsschutz und Verschlüsselung

Statt Bespitzelung der Beschäftigten wäre für die Unternehmen ohnehin eine Erhöhung der Datensicherheit sehr viel wichtiger und produktiver. Vor allem die Verschlüsselung von Daten wäre hierzu ein wichtiger Baustein. Die Erhöhung der Datensicherheit ist auch für die weitere wirtschaftliche Internet-Nutzung unabdingbare Voraussetzung.

Dies betrifft indirekt auch den Persönlichkeitsschutz der Arbeitnehmer, vor allem aber die wirtschaftlichen Interessen von Firmen. Konzerne wie Siemens, Enercon oder Boehringer hatten in der Vergangenheit beispielsweise unliebsame Erfahrungen mit der Schnüffelei des amerikanischen Geheimdienstes NSA gemacht, der offensichtlich Wirtschaftsgeheimnisse an konkurrierende amerikanische Firmen weitergegeben hat. Dass aber auch deutsche Geheimdienste internationalen Datenverkehr abhorchen, wurde einem größeren Publikum bekannt, als Ende letzten Jahres die Geldwäsche deutscher Banken über Liechtenstein dokumentiert wurde – die Daten waren vom Schwarzwald aus gewonnen worden.

Eine Repräsentativ-Untersuchung privater und beruflicher Computer-Nutzer ergab 1998, dass lediglich 30 Prozent der Befragten sensible Daten in ihrem Computer für ausreichend gegen einen Zugriff durch Unbefugte (z.B. über das Netz) geschützt halten. Untersuchungen des Bundesamts für Sicherheit in der Informationstechnlogie (BSI) zeichnen eine eher noch düsterere Bilanz. Demnach verschlüsseln lediglich vier Prozent der Unternehmen ihre eMails. Datensicherheit ist aber zu einem ernst zu nehmenden Faktor im globalen Wettbewerb geworden. Parteienübergreifend kam die Multimedia-Enquete-Kommission des Deutschen Bundestags denn auch zu der Auffassung, »dass alle Maßnahmen und Hemmnisse, die einer breiten Nutzung von Verschlüsselungsverfahren entgegenwirken, vermieden und abgebaut werden müssen«. Und letztes Jahr hat das Bundeskabinett mit den ›Eckpunkten der deutschen Kryptopolitik‹ für Deutschland vorläufig jede Beschränkung der Verschlüsselung ausgeschlossen. Die Bundesregierung setzt sich jetzt dafür ein, dass »Verschlüsselungsverfahren und -produkte ohne Be-

schränkung entwickelt, hergestellt, vermarktet und genutzt werden dürfen«.

Wenn also auch für Arbeitgeber wie Arbeitnehmer die Verschlüsselung der betrieblichen Kommunikation notwendig und wünschenswert ist, so sind hier doch Einbruchstellen nicht auszuschließen. Erst kürzlich offenbarte der ›Chaos-Computer Club‹, dass Microsoft mit seiner Verschlüsselungsschnittstelle Crypto-API in alle Windows-Betriebssysteme offensichtlich auch eine Hintertür einprogrammiert hat, durch die die Spionageaktionen der NSA erst möglich waren. Im November 1999 musste das Bundesamt für Sicherheit in der Informationstechnik (BSI) sogar vor dem bekannten Verschlüsselungssystem PGP warnen.

PGP wird heute als kommerzielles Produkt von der US-Firma Network Associates vertrieben, die eng mit der US-amerikanischen National Security Agency zusammenarbeitet. Das Bundesministerium für Wirtschaft und Technologie ist deshalb im November letzten Jahres dazu übergegangen, mit der Open-Source-Gemeinde zu kooperieren und ein Verschlüsselungsprojekt ohne Geheimdienst-Hintertür zu fördern. In Hinblick auf Schutz und Verschlüsselung der innerbetrieblichen wie externen Unternehmens-Kommunikation besteht aber noch großer Handlungsbedarf.

In jedem Falle auch sollten Betriebs-/Personalräte zur Regelung der betrieblichen eMail- und Internet-Nutzung unbedingt auf den Abschluss von Betriebs-/Dienstvereinbarungen drängen – damit wird sich die zweite Folge dieses Beitrags beschäftigen.

Dr. Manuel Kiper ist Technologie- und Arbeitsschutzberater bei der BTQ Niedersachsen. Kontaktadresse:
BTQ Niedersachsen, Donnerschweer Str. 84, 26123 Oldenburg, Telefon 04 21 / 8 20 68
eMail: **kiper@btq.de**

Eine ausführliche Handlungshilfe ist hierzu von der BTQ Niedersachsen entwickelt worden. Siehe dazu die Besprechung auf der gegenüberliegenden Seite.