

MANUEL KIPER

Spione im Büro

Überwachung am Arbeitsplatz

Überwachung von Leistung und Verhalten im Betrieb ist keine Erfindung des elektronischen Zeitalters. Eine unbemerkte Fernüberwachung gewinnt aber an vernetzten Computerarbeitsplätzen eine neue Qualität. Hier können alle Arbeitsschritte automatisiert erfasst, ausgewertet und diese Kontrolldaten zur Steuerung von Verhalten und Leistung eingesetzt werden. Hierzu ist nicht einmal Videokontrolle notwendig, die unter dem Slogan »Big Brother is Watching You« frühere bedrohliche Überwachungsszenarien dominierte.

Das kürzliche Vorhaben von »Mister Minit«, die Mitarbeiter permanent mit Video zu überwachen, wurde sogar vom Kaufhof-Konzern abgeblockt: eine solch offensichtliche lückenlose Überwachung des Verhaltens der Beschäftigten ist in Deutschland nämlich nicht zulässig. Bundesarbeitsgericht wie Bundesverfassungsgericht erlauben zwar im Rahmen erheblicher Verdachtskontrolle eine punktuelle Videoüberwachung am Arbeitsplatz, verbieten aber eine generalisierte Videobeobachtung oder ein permanentes Abhören von Telefongesprächen. Eine solch generelle Überwachung ist nach Auffassung der obersten Gerichte mit dem in den Grundrechten verankerten Persönlichkeitsrecht und dem im Volkszählungsurteil 1983 erkannten Recht auf informationelle Selbstbestimmung nicht vereinbar.

1. Überwachung im firmeninternen Intranet

In welchem Ausmaß hingegen nunmehr unbemerkt in Firmennetzwerken die zentralen E-Mail- oder Internetserver zur Kontrolle der Beschäftigten herangezogen werden, machen Umfrageergebnisse und Arbeitskämpfe insbesondere in den USA deutlich, wo weder Datenschutz noch Mitbestimmung ein Niveau erreichen, wie es hier zu Lande gesetzlich festgeschrieben ist. Nach einer Studie der »American Management Association« überwachten 1997 14,9 Prozent der Firmen die E-Mails, 1999 waren es 27 Prozent, im Jahre 2000 stieg der Anteil auf 38,2 Prozent.¹ Auf Grund dieser Aktivitäten sind aus US-Firmen wie Xerox, der New York Times, auch aus britischen Firmen wie Merrill Lynch und Edward Jones & Co richtige Entlassungswellen bekannt ge-

worden. Nach einer kürzlichen Untersuchung der US-amerikanischen Purdue-Universität kontrollierten 63 Prozent der befragten amerikanischen Unternehmen auch, welche Webseiten sich ihre Mitarbeiter ansahen.²

In Deutschland wird zwar aus einzelnen Firmen ebenfalls von E-Mail-Kontrolle berichtet, arbeitsrechtliche Konsequenzen sind allerdings nur in wenigen Einzelfällen bekannt geworden.³ Allerdings gibt es auch Fälle wie Xerox in Deutschland, die im März 2001 den E-Mail-Verkehr zwischen Beschäftigten, Betriebsräten und der Gewerkschaft HBV in ver.di in allen elf Geschäftsstellen fadenscheinig wegen interner Netzüberlastung sperrten. Hintergrund der Blockade dürfte der intensive Abwehrkampf gegen die Entlassungswelle bei Xerox gewesen sein. Gleichzeitig wurde nämlich auch der betriebsinterne Zugriff auf eine von Betriebsräten und Gewerkschaft eingerichtete Internetseite gesperrt, auf der über Aktionen und Neuigkeiten berichtet wurde.

In den USA greift darüber hinaus offensichtlich die Praxis um sich, sogar anonyme Kritiker (seien es Kunden oder Arbeitnehmer) im Netz zu enttarnen und zu verfolgen.⁴ Diese Praxis dürfte in Deutschland durch die Gültigkeit des Teledienstedatenschutzgesetzes unterbunden sein, welches im Internet auf Wunsch Anonymität und hohen Datenschutz garantiert.

2. Kontrollsoftware

Moderne Kontrollsoftware macht die unmerkliche Steuerung, Überwachung und Auswertung des Mitarbeiterverhaltens am vernetzten Computerarbeitsplatz möglich. Schon auf den Mitarbeiterrechnern protokollieren die Browser automatisch die aufgerufenen Internetseiten. Zwar kann diese Protokollierung deaktiviert werden, die Protokollierung am Zentralrechner wird damit aber keineswegs außer Kraft gesetzt. Die dort anfallenden Log-Files geben nicht nur Auskunft über die aufgerufenen Websites, sondern auch über die Uhrzeit und Dauer. Durch zusätzliche komfortable Überwachungsprogramme, installiert am Zentralserver oder bei der Geschäfts- oder Dienstleitung, könnten hier beliebig detaillierte Auswertungen und weitere Schnüffeleien vorgenommen werden.

Die Software TotalView zum Beispiel wirbt gerade damit, einen »Überblick über den Datenbestand der einzelnen Arbeitsplätze zu geben, auch wenn hierfür keine Freigabe existiert«. TotalView kann ohne besondere IT-Kenntnisse installiert werden und erlaubt Screenshots (Istzeitbilder) der überwachten Bildschirme zentral anzusehen, den Mitarbeiter-Besuch bestimmter betrieblich unerwünschter Internetseiten der Überwachungsstelle aktuell zu melden oder alle abgelaufenen Arbeitsprozesse an einem Computerarbeitsplatz rückwirkend nachzuvollziehen und zu analysieren.

Ohne Softwareinstallation erlaubt ein kleiner Adapter namens Keyghost der Firma Orth aus Kürten (einrichtbar auch bei ausgeschaltetem und mit

Kontroll-Software

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/
TotalView	http://totalview.de
WinGuardian	http://www.webroot.com/
WinWhatWhere	http://www.winwhatwhere.com/
siehe auch www.surfcontrol.com/products/superscout-for-business/categorylist/index.html	

Passwort geschütztem PC) als eine – vom Flugzeug bekannte – Blackbox des PCs bis zu zwei Millionen Tastatureingaben aufzuzeichnen und auf einem anderen beliebigen Computer nachzuvollziehen.⁵ Die Software Eblaster kontrolliert ebenfalls alles, was auf dem Computer abläuft und schickt zur idealen Fernüberwachung eine Auswertung an eine gewünschte E-Mail-Adresse.

Software unter bezeichnenden Namen wie Surfcontrol, Winwhatwhere, Spector, Cyberpatrol, Little Brother oder SurfWatch erlauben üblicherweise nicht nur die nachträgliche Auswertung des Arbeits- und Surfverhaltens am Computerarbeitsplatz, sondern auch die beliebige Sperrung von Sachgebieten des World Wide Web wie Spiele oder Sport und von Stichworten wie Aktien oder Sex. Festgelegt werden kann damit auch eine entsprechende zeitliche Dosierung, so dass zum Beispiel nur nach Dienstschluss oder in festgelegten Pausen diese vergnüglichen Netzinhalte am Einzelarbeitsplatz aufrufbar sind.

Die zentrale Überwachung und Filterung ein- und ausgehender E-Mails ist technisch eine Leichtigkeit, werden im Rahmen eines Netzwerks doch alle E-Mails am zentralen E-Mail-Server gespiegelt. Durch entsprechende Filtersoftware können zum Beispiel alle ausgehenden E-Mails mit unerwünschtem Vokabular, unhöflicher Form oder anstößigen oder geheim zu haltenden Inhalten zurückgehalten, an namensgleiche oder beliebig anders aussortierbare E-Mail-Adressen blockiert und eingehende thematisch – oder wegen des Absenders – unerwünschte E-Mails abgefangen werden.

Nach einer Umfrage der Zeitschrift Capital werden in Deutschland »nur« in 13 Prozent der befragten Unternehmen grundsätzlich ausgehende E-Mails kontrolliert. In den USA kontrolliert hingegen fast jedes zweite Unternehmen den E-Mail-Verkehr. Erlaubt ist dies in Deutschland wegen des strengen Schutzes des Fernmeldegeheimnisses (§ 85 Telekommunikationsgesetz) übrigens nur bei strikter Untersagung oder besonderer Kennzeichnung (und damit

Schutz) privater E-Mails in den betreffenden Firmen. Dienstliche E-Mails nehmen dabei eine Zwitterstellung zwischen Brief und flüchtigem Telefongespräch ein. Dienstpost unterliegt im Prinzip dem Zugriff der Geschäftsleitung. Telefonate dürfen andererseits nicht mitgehört werden. E-Mails hingegen können Dienstpost sein (zum Beispiel im papierlosen Büro), können aber auch flüchtige geschützte Kommunikation sein, die nicht unmittelbar dem Direktionszugriff unterliegt.

Wie wenig anonym das Arbeiten in einer qua Internet vernetzten Welt ist, zeigte nicht zuletzt die Verfolgung gefährlicher Viren namens Melissa oder des I-Love-You-Virus. Durch Rückverfolgung des sich lawinenartig ausbreitenden

Spione im Büro

Nach einer Umfrage der Zeitschrift Capital vom September 2001 ist die private Nutzung des Internets am Arbeitsplatz in nahezu jeder zweiten Firma erlaubt oder geduldet (drei von 5 Firmen wollten allerdings nicht genannt werden oder antworteten nicht).

Die private Nutzung des Internets am Arbeitsplatz

ist erlaubt bei Ericsson, Fiat, Intel, Intershop, Lycos Europe, Otto Versand, Volkswagen;

wird toleriert bei Adidas-Salomon, Alcatel Deutschland, American Express, AOK Bundesverband, Bausparkasse Schwäbisch-Hall, BMW, Brauerei Beck, CA Computer Associates, Cap Gemini Ernst & Young, Celanes, Coca-Cola, Compaq, Davev, Deutsche Renault, Deutsche Telekom, E-Plus Mobilfunk, Gehe, Henkel, Hochtief, Hoffmann-La Roche, Hypovereinsbank, Kraft Foods Deutschland, Lekkerland Tobaccoland, Lexware, Melitta, Metro, MLP, Pixelpark, Quelle, RWE, SAP, T-Mobil, Thyssenkrupp, Web.de;

ist verboten bei 3 M Deutschland, ABB, Allianz, Audi, Axa Colonia, B. Braun Melsungen, BASF, Bayer, Bertelsmann, Boehringer Ingelheim, Brokat, Buderus, Commerzbank, Daimler-Chrysler, DAK, Deutsche Lufthansa, Deutsche Post, Dresdner Bank, EADS Deutschland, Epcos, Faber-Castell, Fresenius, Gesellschaft für Nuklear-Service, Giesecke & Devrient, Heidelberger Druck, HUK Coburg, Hutchison Telecom, Infineon, Kaufhof, Kienbaum, Linde, MAN, Merck, Motorola, Münchner Rück, Obi, Osram, Panasonic Deutschland, Philips, Preussag, Puma, Schering, Siemens, Stinnes, Talkline, Thomas Cook, TUI, Würth, Wüstenrot, Xerox, ZF Friedrichshafen.

Virus können innerhalb weniger Tage die geistigen Urheber dingfest gemacht werden.⁶ Jeder Computer firmiert nämlich im weltweiten Internet unter einer bestimmten codierten Adresse, die bei jedem Datentransfer automatisch mitübertragen wird. Dadurch werden enorme Datenspuren hinterlassen, die im Bedarfsfall bei den Providern ausgewertet werden können.

Die privatwirtschaftliche Nutzung solch individuell zuzuordnender Datenspuren, das Data-Mining, wurde inzwischen sogar ein eigener lukrativer Markt.⁷ Zum gläsernen Bürger und gläsernen Mitarbeiter gesellt sich der gläserne Konsument. Durch die – mit Einwilligung durchaus erlaubte – Über-

tragung und Installation von kleinen Cookies des Datenanbieters auf dem Einzelrechner wird die Verknüpfung vieler Einzelkundendaten zum durchsichtigen Klienten noch erleichtert. Der Klient kann sofort mit Namen angesprochen werden, sein bisheriges Informations- oder Kaufverhalten kann zur individuellen extrapolierten Betreuung nutzbar gemacht werden.

Da Unternehmen auch für ihre eigenen Mitarbeiter zunehmend Teledienste anbieten, könnten Mitarbeiter nicht nur in ihrer Arbeitsleistung, sondern auch in ihrer privaten Kundenqualität durchsichtig gemacht werden. Das Teledienstedatenschutzgesetz setzt hier in Deutschland allerdings erhebliche Schranken. Zutreffend schreibt der Niedersächsische Landesbeauftragte für den Datenschutz: »Die Privatsphäre der Arbeitnehmer in Unternehmen, die Multimediadienste 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.«⁸

3. Biometrie

Big Brother stützt sich neuerdings auch auf die Biologie. Die Gen-Analyse erlaubt heute die Entschlüsselung und personelle Zuordnung geringster Spuren biologischen Materials, was in der forensischen Medizin zur Überführung von Tätern genutzt wird. Andere messbare Körperdaten wie Stimme, Gesicht, Iris oder Fingerkuppen werden heute zunehmend ausgewertet und so genannte biometrische Identifikationen vorgenommen, systematisch Zugangskontrollen installiert und Identität und Anwesenheit automatisiert kontrolliert. Aus diesen zusätzlichen digitalen und zukünftig vermutlich auch genetischen Datenspuren werden heutzutage Persönlichkeitsprofile gewinnbar und Überwachungsszenarien machbar, die die Visionen von »Brave New World« und »Big Brother is Watching You« in den Schatten stellen.⁹

Biometrische Identifikationsverfahren

Fingerabdruck: Siemens präsentierte schon auf der Computermesse CEBIT 1997 einen Chip, der mittels 65000 winzigen Sensoren die Fingerkuppen abtastete, womit ein lebendes Schlüsselsystem der Zukunft beispielsweise mit dem Handy möglich wurde. Bio-Prox heißt eine bereits vermarktete Schließtechnik für Chefetagen und Gefängnisse. Von der Firma Deister-Electronic in Barsinghausen wird dieses System angeboten, das aus einer Kombination von Chipkarte und Lesegerät besteht. Die mitgeführte Chipkarte sagt dem Gerät, wie der persönliche Fingerabdruck aussehen soll. Einlass bekommt nur, wer den

richtigen Fingerabdruck auf das Lesegerät hält. Nach einer halben Sekunde ist die Identitätsprüfung abgeschlossen, da die Fingerabdrücke nicht in einer Datenbank gesucht werden müssen. Seit Jahren sind solche automatisierten Zugangssysteme auch schon an Flughäfen zum Beispiel in New York installiert.

Gesichtserkennungssysteme: Am Markt werden von der Bochumer ZN GmbH das Produkt ZN-Face, das Produkt Phantomas, welches eine automatisierte Durchsicht großer Bilddatenbestände ermöglicht, oder das Produkt FaceVACS der Firma Siemens-Nixdorf bereits angeboten. »Fratze schneiden? Zwecklos. Brille auf? Keine Chance. Dreitagebart? Aussichtslos. Dem computergesteuerten Türsteher ZN-Face macht niemand etwas vor«, begeisterte sich die Zeitschrift Wirtschaftswoche. Mit neuen Systemen zum Beispiel der Software PersonSpotter lassen sich Gesichter auch im Halbprofil aus einer größeren Menge heraus automatisch verfolgen und identifizieren.

Irismustererkennung: Mit einem Iris-Scanner sind schon Zugangskontrollen für Gebäude, Sicherheitszonen, die Verifikation persönlicher Dokumente, KFZ-Diebstahlsicherungen, Codeschlüssel zur Sicherung von Telekommunikation und anderes entwickelt worden. Im Gefängnis von Cook County/Illinois müssen die Häftlinge bereits in jedem Trakt die Augenlesegeräte passieren. Auch am Amsterdamer Flughafen Schiphol ersetzt der Iris-Scanner bereits für Vielflieger die Passkontrolle.

Typ- und Unterschriftsverhalten: Die Analyse von Schreibrhythmus, Anschlagverhalten und weiteren charakteristischen Merkmalen des Tippverhaltens können eine Person über die Tastatur identifizieren.

Wärmeabstrahlungsmuster der Blutgefäße in der Gesichtshaut dienen der Identifizierung.

Spracherkennung: Das unter Federführung des Forschungszentrums Saarbrücken für Künstliche Intelligenz mit einem Aufwand von bisher 100 Millionen Mark entwickelte so genannte Verbmobil erlaubt nicht nur Spracherkennung sondern gleichzeitig die Übersetzung. Solche Systeme müssen sich erst systematisch auf die feinen individuellen Sprachmodulationen eines Sprechers einstellen. Umgekehrt sind die Schwingungsspektren und Modulationen der Stimme ein individueller Stimmabdruck und können zur Personenidentifizierung eingesetzt werden.

Schweißgeruch: Die englische Firma »Bloodhound Sensors« entwickelt sogar Erkennungssysteme für individuellen Schweißgeruch.

Schritterkennung: Am US-amerikanischen MIT wie an der englischen Universität Southampton sind Programme zur Personenidentifizierung am Schritt entwickelt worden.

DNA-Profilung: Mit dieser Technik kann aus einer winzigen Spur Erbsubstanz, einem Haar, dem Speichel an einer Zigarette etc. ein für jeden Menschen charakteristisches Bandenmuster erzeugt werden, welches als Strichcode sichtbar gemacht werden kann. Dieses kann als Zahlenreihe gespeichert und mit anderen Proben verglichen werden. Die Beschleunigung und Miniaturisierung der genetischen Identifikationssysteme schreitet allerdings in großen Sprüngen voran, so dass zukünftig mit dieser Methode nicht nur eine nachträgliche Identifikation, sondern auch eine Istzeitauthentifizierung möglich werden könnte.

Den biometrischen Identifizierungsverfahren liegt ein statisches biologisches Merkmal wie die Iris zu Grunde. Mit weit über 200 zu differenzierenden Strukturmerkmalen ist sie dem seit langem bekannten Identifizierungsverfahren, dem Fingerabdruck mit nur etwa 40 Strukturmerkmalen, erheblich überlegen. Das BioID-Verfahren des Berliner Unternehmens DCS arbeitet sogar multimodal; sowohl statische als auch dynamische biologische Merkmale der zu identifizierenden Person werden genutzt. Konkret wird das Gesicht, die Stimme und die Lippenbewegung beim Sprechen zur Erstellung eines biometrischen Datensatzes und zur eindeutigen Identifikation genutzt. Dieses System ist gewissermaßen die Fortentwicklung des multimodalen Identifikationssystems der Sieben Geißlein der Gebrüder Grimm, die mit Schlüsselnachricht (»Eure Mutter ist wieder da«), hoher Stimme und weißer Pfote arbeiteten. Bezeichnenderweise nennt sich ein ähnliches multimodales System, was als High-tech-Pförtner von der Fraunhofer-Gesellschaft in Erlangen entwickelt wurde, Sesam (Synergetische Erkennung durch Standbild, Akustik und Motorik).

Bereits über zwei Millionen Lichtbilder umfasst immerhin die Kartei der erkennungsdienstlich behandelten Personen beim BKA. Deutsche Firmen haben andere Länder wie Indonesien, Brasilien oder Ägypten in die Lage versetzt, die Fingerabdrücke aller Bürger elektronisch zu erfassen und mit dem automatisierten Erkennungssystem für Fingerabdrücke auszuwerten.

Auch das Ausmaß der Videoüberwachung steigt ständig. 1976 führte Hannover als erste deutsche Stadt mit 25 ferngesteuerten schwenkbaren stationären Zoom-Kameras den Dauereinsatz der Videotechnik ein, auch zur Überwachung von »Rand- und Problemgruppen«. Videokameras zeichnen heute Personen in Bahnhöfen und U-Bahnstationen, an Müllablageplätzen und Schulhöfen, in Warenhäusern und Einkaufspassagen, an Geldautomaten und in Spielbanken auf. Sie können beliebig mit am Markt käuflicher Software zur automatischen Personenerkennung gekoppelt werden. Die vorhandenen automatischen Personenidentifizierungstechniken könnten heute, so eine Untersuchung an der Universität Hull, die britische Regierung in die Lage versetzen, jeden einzelnen Menschen zu kontrollieren, zumal zusätzlich zu den heutigen elektronischen Personenerkennungssystemen auch Programme entwickelt werden, um normales von verdächtigem Verhalten zu unterscheiden. Ganz zu schweigen davon, dass moderne Videokameras Infrarotansicht, Fernbedienung, Zoom und automatische Verfolgung im Repertoire haben. Wenn auch in Deutschland der betrieblichen Videoüberwachung von Mitarbeitern erhebliche datenschutzrechtliche Hürden entgegenstehen und die Gerichte heimliche Überwachung nur als letztes Mittel innerbetrieblicher Kontrolle anerkennen, entwickelt sich vor allem in Kaufhäusern und Spielbanken die Videoüberwachung lückenlos.

Die technisch mögliche Zusammenführung all dieser verfügbaren Bewegungsbilder mit individuellen Konsumentendaten und Bilddaten über das häusliche Wohnen, wie es heute auch in Deutschland am Markt angeboten wird, ließe bei Bewerbern im Arbeitsleben bereits im Vorfeld die Erstellung

von umfassenden Persönlichkeitsprofilen zu. Dies verheißt intensivierete Überwachung von Verhalten und Leistung im Betrieb, wenn der Einsatz biometrischer Verfahren nicht durch Gesetzesrahmen und Mitbestimmung beschränkt wird.

Ein Verbot der Biometrie steht dabei nicht zur Diskussion, da nach heutigem Wissensstand gerade die Biometrie wohl am besten geeignet ist, zuverlässig automatisch zu bestätigen, dass der Anwesende oder Signierende tatsächlich der ist, der er zu sein vorgibt. Der biometrischen Authentifizierung sollte deshalb zukünftig zum Beispiel bei Kauf, Zeugnis, Testament und anderen rechtsverbindlichen Akten eine wesentliche Rolle zukommen. Sicherzustellen ist aber, dass biometrische Daten nicht unbemerkt erhoben und auch nicht ohne Erfordernis gespeichert werden.

4. Keine schrankenlose Überwachung

Da in Bezug auf Telefonanlagen das Bundesverfassungsgericht bereits 1991 klargestellt hat, dass sogar dienstliche Telefongespräche des Arbeitnehmers von einem Dienstapparat dem verfassungsrechtlichen Schutz des allgemeinen Persönlichkeitsrechts unterliegen,¹⁰ sind hier zu Lande einer Überwachung enge Grenzen gesetzt. Das Bundesverfassungsgericht schließt zwar im Einzelfall, insbesondere bei erheblichem Verdacht, eine punktuelle und vorübergehende Überwachung des Telekommunikationsverkehrs nicht aus. Eine generalisierte Überwachung hat es aber grundsätzlich als mit dem Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung nicht zu vereinbarende Kontrolle für unzulässig erklärt. Entsprechend hat das Bundesarbeitsgericht im Oktober 1997 entschieden, dass im beruflichen Bereich auch das Recht am gesprochenen Wort als Teil des allgemeinen Persönlichkeitsrechts zu gewährleisten ist.¹¹ Und zuvor schon hatte das Bundesverfassungsgericht geurteilt, dass ein Telefonüberwachungssystem, 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.¹² Allein die Tatsache, dass ein Telefongespräch »in der Sphäre eines Arbeitsverhältnisses« geführt wird, erlaubt es einer weiteren Person wie dem Personalchef oder dem Abteilungsleiter also keineswegs, ohne Zustimmung des Gesprächspartners mitzuhören oder mithören zu lassen.

Das Bundesverfassungsgericht hat auch festgehalten, dass ein heimliches Mithören oder Aufzeichnen des Inhalts eines Telefonats des Arbeitnehmers dessen Einwilligung voraussetzt und dass diese nicht stillschweigend als erteilt angenommen werden kann, wenn der Arbeitnehmer um die Abhörmöglichkeit weiß.¹³ Heimliches Mithörenlassen von Telefongesprächen zwischen Arbeitnehmer und Arbeitgeber ist unzulässig. Auf diese Weise erlangte Beweis-

mittel dürfen nicht verwertet werden. Beim Mithören ist der Gesprächspartner vorher darüber zu informieren. Gesprächspartner am Telefon müssen sich nicht ihrerseits vorher vorsorglich vergewissern, dass niemand mithört.¹⁴

Auch die Auswertung des gesamten E-Mail-Verkehrs (etwa durch automatisches Scannen) durch den Arbeitgeber wäre deshalb nach Auffassung der Länderdatenschutzbeauftragten »jedenfalls im Regelfall nicht gestattet«.¹⁵ Ist die Kennzeichnung privater E-Mails systemtechnisch nicht vorgesehen, erstreckt sich das Fernmeldegeheimnis nach dem Telekommunikationsgesetz auch auf den betrieblichen E-Mail-Verkehr.¹⁶ Ist hingegen die Privatnutzung des E-Mail-Systems betriebsintern mengenmäßig oder zeitlich limitiert und diese Regelung den Beschäftigten bekannt gegeben worden, sind allerdings »Missbrauchskontrollen durch das Beschäftigungsunternehmen zulässig«.¹⁷

Bereits seit dem so genannten »Fangschaltungsbeschluss« des Bundesverfassungsgerichts war entschieden, dass betriebsbedingte Einblicke eines Diensteanbieters oder Betreibers (und dazu gehört auch das Unternehmen, das eine Telefonanlage oder ein Intranet betreibt) in Inhalte und Umstände elektronischer Kommunikation »rechtfertigungsbedürftige Eingriffe in das

Arbeitsrechtliche Entscheidungen zur Überwachung

Abhören dienstlicher Telefongespräche ist unzulässig

Auch dienstliche Telefongespräche des Arbeitnehmers von einem Dienstapparat unterliegen dem verfassungsrechtlichen Schutz des allgemeinen Persönlichkeitsrechts (Recht am eigenen Wort) nach Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG. Dieser grundrechtliche Schutz kann nicht durch bloße Kenntnis von der Mithörmöglichkeit beseitigt werden. In der gerichtlichen Verwertung von Kenntnissen und Beweismitteln, die unter Verstoß gegen das Persönlichkeitsrecht erlangt sind, liegt regelmäßig ein Eingriff in die genannten Grundrechte.

(BverfG vom 19.12.1991 – Az 1 BvR 382/85)

Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen

Das heimliche Mithörenlassen von Telefongesprächen zwischen Arbeitnehmer und Arbeitgeber ist im Allgemeinen unzulässig. Es verletzt das Persönlichkeitsrecht des Gesprächspartners. Auf diese Weise erlangte Beweismittel dürfen nicht verwertet werden. Wer jemanden mithören lassen will, hat seinen Gesprächspartner vorher darüber zu informieren. Dieser ist nicht gehalten, sich seinerseits vorsorglich zu vergewissern, dass niemand mithört.

(BAG vom 29. 10. 1997 – Az 5 AZR 508/96)

Nebenjob auf (Telefon-)Firmenkosten kostet den Hauptjob

Wer vom Telefon seines Arbeitgebers aus einem Nebenjob nachgeht (hier: für ein Meinungsforschungsinstitut), der kann entlassen werden.

(Arbeitsgericht FfM – Az 14 Ca 891/95)

Telefonsex auf Betriebskosten kostet den Job

Führt eine leitender Angestellter (hier ein GmbH-Geschäftsführer) mehrfach auf Firmenkosten Telefonsexgespräche und nimmt er dadurch Firmengelder von nicht unbeträchtlicher Höhe für private Zwecke in Anspruch, so missbraucht er

damit die ihm verliehene Vertrauensstellung und kann ohne vorherige Abmahnung entlassen werden. (OLG Hamm – Az 8 U 194/98)

Kündigung wegen unzulässigen privaten E-Mail-Versands

Ein gegen die Anweisung des Arbeitgebers verstoßender privater E-Mail-Verkehr berechtigt in der Regel erst nach vorausgegangener Abmahnung zur Kündigung des Arbeitsverhältnisses.

(Arbeitsgericht FfM vom 20. 3. 2001 – Az 5 Ca 4459/00)

Kündigung wegen Beleidigung des Arbeitgebers im Internet

Wer seinen Arbeitgeber öffentlich beleidigt, dem droht eine verhaltensbedingte Kündigung auch dann, wenn er als Medium das Internet benutzt.

(LAG Schleswig-Holstein vom 4. 11. 1998 – Az 2 Sa 330/98)

Meinungsfreiheit in der Mailbox

Verbreitet ein Betriebsrat elektronisch einen Text über Mitarbeiteransprüche im Unternehmen, so handelt er zumindest in engem Zusammenhang mit seiner Betriebsratstätigkeit. Weist ein solches Schreiben auf Rechtsbruch der Unternehmensleitung hin, so ist dies keine Beleidigung. Unternehmensöffentliche Kritik an der Geschäftsführung ist für sich genommen kein Grund für eine außerordentliche Kündigung, auch wenn sie in zugespitzter und provozierender Weise geübt wird.

(LAG Hamburg vom 4. 11. 1996 – Az 4 TaBV 10/95)

Fristlose Kündigung bei rassistischer Witzesammlung

Es stellt einen wichtigen Grund für eine außerordentliche Kündigung gem. § 54 BAT dar, wenn ein Angestellter der Bundeswehr eine so genannte Witzesammlung, die zu einem erheblichen Teil Judenwitze, Ausländerwitze und sexistische Frauenwitze von eklatant die Menschenwürde verachtendem Charakter enthält, über ein dienstliches MEMO-System in Kenntnis des Inhalts weiterverbreitet.

(LAG Köln vom 10. 8. 1999 – Az 3 Sa 220/99)

Außerordentliche Kündigung wegen Kinderpornografie

Wenn ein Kindergartenleiter kinderpornografische Bilddateien besitzt, so rechtfertigt dies eine außerordentliche Kündigung wegen Verdachts auf pädophile Neigungen. Eine vorangegangene Abmahnung erübrigt sich in einem solchen Fall.

(ArbG Braunschweig vom 22. 1. 1999 – Az 3 Ca 370/98)

Verletzung des Persönlichkeitsrechts durch lückenlose Überwachung

Eine Verletzung der Persönlichkeitsrechte eines Arbeitnehmers kann vorliegen, wenn er einem ständigen lückenlosen Überwachungsdruck dadurch unterworfen wird, dass der Arbeitgeber sich vorbehält, jederzeit ohne konkreten Hinweis den Arbeitsplatz durch versteckt aufgestellte Videokameras zu beobachten. Eine Maßnahme der vorbezeichneten Art kann allerdings gerechtfertigt sein, wenn überwiegende schutzwürdige Interessen des Arbeitgebers sie erfordern. Hierzu bedarf es eines substantiierten Sachvortrages.

(BAG vom 7. 10. 1987 – Az 5 AZR 116/86)

Elektronisches Überwachungsprogramm mit verdeckten Videokameras ist unzulässig auch bei Zustimmung

Eine nicht durch besondere Sicherheitsinteressen des Arbeitgebers ausnahmsweise gerechtfertigte heimliche Überwachung der Arbeitnehmer per Videokamera kann nicht durch Zustimmung des Betriebs- oder Personalrats legitimiert werden.

(BAG vom 15. 5. 1991 – Az 5 AZR 115/90)

Fernmeldegeheimnis« sind.¹⁸ Insofern hat auch das Bundesarbeitsgericht eine Betriebsvereinbarung, die es dem Arbeitgeber bei einer ACD-Anlage¹⁹ erlaubte, externe Telefongespräche der Arbeitnehmer in deren Gegenwart zu Ausbildungszwecken mitzuhören, für zulässig erklärt.²⁰ Die Praxis, dass Mitarbeiter wie Kunden in Call-Centern gängigerweise extern abgehört sind, wie es von der „Panorama“-Redaktion im September 1999 aufgedeckt wurde,²¹ dürfte damit allerdings unvereinbar sein.

Eine Kontrolle des Telefonierverhaltens der Beschäftigten in Hinblick auf den Missbrauch und die Kostenverursachung wird in der Rechtsprechung andererseits für zulässig gehalten. Von unteren Arbeitsgerichtsinstanzen werden hier zum Teil drastische Urteile gefällt, die allerdings vor Landesarbeitsgerichten üblicherweise keinen Bestand haben. Arbeitnehmer, die in erheblichem Umfang auf Kosten ihres Arbeitgebers privat telefonieren, können ohne Abmahnung entlassen werden, so die Entscheidung des Arbeitsgerichts Frankfurt am Main.²² Auch das Arbeitsgericht Würzburg sah eine Kündigung ohne vorherige Abmahnung wegen vollendeten Betrugs gerechtfertigt, wenn ein Arbeitnehmer häufig auf Kosten seines Arbeitgebers telefoniert, ohne die Gespräche zu bezahlen.²³ Einen Kündigungsgrund sah das Arbeitsgericht Frankfurt am Main auch bei unbezahlten Telefonaten nach Australien insbesondere, wenn die Arbeitnehmerin erst angesichts eines Computerausdrucks bereit war, das Telefonat zu bestätigen.²⁴ Desgleichen sah das Gericht einen Kündigungsgrund, wenn ein Arbeitnehmer auf Kosten seines Arbeitgebers telefonisch einem Nebenjob nachgeht.²⁵ Andererseits hat jüngst das Arbeitsgericht Frankfurt am Main entschieden: »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 entstandenen Kosten (hier: 66,51 Mark) nicht von sich aus erstattet.«²⁶ Das Oberlandesgericht Hamm entschied, dass ein leitender Angestellter durch Inanspruchnahme von Telefonexgesprächen in »nicht unbeträchtlicher Höhe für private Zwecke« seine ihm verliehene Vertrauensstellung im Betrieb missbraucht habe und damit ohne Abmahnung entlassen werden könne.²⁷

Landesarbeitsgerichtsentscheidungen hingegen sind bislang für die Beschäftigten glimpflicher ausgefallen. So entschied das Landesarbeitsgericht Niedersachsen, dass auch bei erwiesener Vielzahl von Privattelefonaten auf Arbeitgeberkosten eine verhaltensbedingte Kündigung erst zu rechtfertigen sei, wenn der Mitarbeiter vorher abgemahnt worden sei.²⁸ Das Landesarbeitsgericht Köln befand sogar: Erlaubt ein Arbeitgeber seinen Beschäftigten, pri-

vate Telefonate von seiner Anlage aus zu führen, so darf er einem Mitarbeiter nicht kündigen, der davon »ausschweifend« Gebrauch macht, insbesondere dann nicht, wenn er durch eine »unzureichende Organisation« erst spät darauf aufmerksam wird und damit rechtzeitige Ermahnungen unterblieben sind.²⁹

In Hinblick auf Surfen im Internet bewies auch jüngst das Arbeitsgericht Wesel Verständnis für die Situation der Arbeitnehmer. Ein Arbeitgeber hatte einer Buchhalterin während eines Jahres rund 100 Stunden privates Surfen im Internet während der Arbeitszeit nachgewiesen. Die Firma hatte ihr ohne Abmahnung fristlos gekündigt. Die Richter sahen die Schuld beim Arbeitgeber. Dieser hatte das private Surfen weder verboten, noch zeitlich begrenzt. Die Richter hielten die Aufstellung klarer Regeln für unerlässlich. Ohne klare Regeln könne unterstellt werden, dass das private Surfen geduldet werde.³⁰

Insofern ist alles in allem von einem weit reichenden Schutz des Fernmeldegeheimnisses und des Datenschutzes bei Telekommunikationsvorgängen jedweder Art auszugehen.

5. Kontrolle unter Wahrung des Fernmeldegeheimnisses

Dies heißt nun jedoch nicht, dass der Arbeitgeber jedwede Internet-Nutzung seiner Beschäftigten dulden muss. Zugangsbeschränkungen, Ahndung von Missbrauch oder Geheimnisverrat und Ähnliches sind dem Arbeitgeber keineswegs 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 oder andere technische Mittel einsetzen, um den Zugriff auf bestimmte Dienste und Netzressourcen zu begrenzen. Auch hat ein Arbeitnehmer keinen Anspruch darauf, das Internet nach Belieben zu nutzen.

So müssen (und dürfen) auch strafbare Handlungen über E-Mail- oder Internet/Intranetnutzung nicht geduldet werden. Insofern sind Missbrauchskontrollen und entsprechende Ahndung zulässig bzw. geboten. Bei Verdacht auf strafrechtliche Vergehen von Mitarbeitern ist durch den Arbeitgeber ggf. die Polizei oder Staatsanwaltschaft einzuschalten. Dies wäre zum Beispiel gegeben, wenn ein Mitarbeiter in den Verdacht gerät, von seinem Arbeitsplatz

- (verbotene) Kinderpornografie aus dem Netz zu laden und innerbetrieblich auf seinem Computer zu speichern,³¹
- unbefugt in fremde Dateien einzudringen,³²
- beleidigende Inhalte auf seiner Website anzubieten³³ oder
- unkommentiert Links auf beleidigende oder sonstwie strafwürdige Inhalte zu setzt.³⁴

Mitarbeiter verstoßen somit gegen ihre arbeitsvertraglichen Pflichten, wenn sie während der Arbeitszeit nicht-dienstliche Daten an ihrem Arbeitsplatz verarbeiten. So kann zum Beispiel die Anlage von Dateien mit sexistischen oder

rasstistischen Witzen und deren Überspielung an Kollegen ein Grund für eine fristlose Kündigung sein.³⁵ Eine systematische Überwachung der Internetaktivitäten von Mitarbeitern, wie sie die Filterprogramme von CyberPatrol, Little Brother, Spector, SurfControl und andere Software zulassen, ist zwar in den USA üblich, in Deutschland aber unzulässig.³⁶ Jede systematische und insbesondere jede heimliche Überwachung ist in Deutschland verboten. So heißt es auch explizit in der gültigen Bildschirmarbeitsverordnung von 1996 im Anhang Pt. 22 über an Bildschirmarbeitsplätze zu stellende Anforderungen: »Ohne Wissen der Benutzer darf keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden.«

6. Umstrittene Missbrauch-Kosten betrieblicher Einrichtungen

Moderne Informations- und Kommunikationstechnik soll die Produktivität erhöhen. Durch die Medien geistern hingegen vorrangig Horrorzahlen darüber, welche immensen Kosten beziehungsweise welchen Verlust an Arbeitszeit die missbräuchliche Nutzung dienstlicher Geräte verursacht. Millionenfach wurde per Internet das Moorhuhnspiel heruntergeladen, durchschnittlich wurde das Online-Game während der Arbeitszeit angeblich 20 Minuten gespielt. Eine Online-Umfrage der Jobware Online-Service GmbH ermittelte, dass 93 Prozent aller vernetzten Arbeitnehmer privat am Arbeitsplatz surfen, 48 Prozent würden dies bis zu 50 Minuten wöchentlich und 37 Prozent noch länger tun.³⁷ 30 Prozent der Firmen unterstützen privates Surfen am Arbeitsplatz. Viele Firmen machen hingegen die Auflage, privates Surfen außerhalb der Arbeitszeit zu legen. Nach einer Umfrage des Wirtschaftsmagazins »Bizz« unter 1300 Beschäftigten greift jeder vierte Mitarbeiter mit Internetanschluss im Schnitt wöchentlich 5,8mal jeweils 11,4 Minuten auf das Web zu, um das Börsengeschehen zu verfolgen.³⁸ Der private Aktienhandel während der Arbeitszeit koste somit rund 5 Milliarden Euro. Gar über 50 Milliarden Euro Verluste durch private Internetnutzung am Arbeitsplatz ermittelte die Agentur »Denkfabrik« bei einer Umfrage unter 1000 Firmen im Jahre 2000.³⁹ Der Wunsch nach exzessiver Kontrolle aus Angst vor Missbrauch, vergeudeter Arbeitszeit und ausufernden Kosten bestimmt denn auch viele Debatten um die Einführung von Internetzugang in der öffentlichen Verwaltung.

Wie geringfügig die realen zusätzlichen Telekommunikationskosten auch bei Internetnutzung ausfallen, machten die Arbeitgeberverbände geschlossen im Zusammenhang mit der zeitweilig geplanten Internetbesteuerung deutlich. In einer Eingabe an das Bundesfinanzministerium wurden von den Unternehmerverbänden die Kosten pro Beschäftigten durch Internetnutzung auf 15 Mark beziehungsweise 7,50 Euro veranschlagt.⁴⁰ Die Besteuerung eines angeblich kostenwerten Vorteils lehnten sie dennoch rigoros ab, um keine Kostenlawine loszutreten. Durch Flatrates oder die Nutzung von Standleitungen

entstehen zusätzliche Kosten erst bei erheblichem Datentransfer. Die vielfach zusätzlich beklagte angeblich verlorene Arbeitszeit kann wiederum nur im Zusammenhang und in Abwägung mit der jeweiligen Erfüllung der Aufgabenstellung und notwendigen Erholungspausen berechnet werden. Zu berücksichtigen wären dabei auch positive Auswirkungen auf steigende Informationstechnikkompetenz, soziale Kommunikation und Betriebsklima. Bei der Einführung von E-Mail- und Internetnutzung im Betrieb sollten Arbeitnehmer sich deshalb restriktiven Nutzungsregeln und ausufernder Kontrolle unter vermeintlichen Kostengesichtspunkten entgegenstellen. Dies ist dank wirksamer Mitbestimmungsregelungen durch Betriebs- und Personalräte tatsächlich möglich.

7. Schutz der Arbeitnehmer durch Mitbestimmung

Der Aufbau betriebs- und behördeninterner Intranets und die Einführung von E-Mail- und Internetnutzung im Betrieb ist mitbestimmungspflichtig⁴¹ und kann in Betriebs- und Dienstvereinbarungen geregelt werden. Vielfach wird in solchen Betriebsvereinbarungen die technisch kaschierte Leistungs- und Verhaltenskontrolle ausdrücklich ausgeschlossen. Andererseits können trotzdem Regelungen gefunden werden, um angesichts bekannt gewordener Fälle von Missbrauch betrieblicher oder dienstlicher IuK-Technik durch Arbeitnehmer für private Firmen, verbotener Kinderpornografie oder Verbreitung rassistischer Hetze eine wirksame Missbrauchskontrolle zu gewährleisten.

Schon früh wurden ausgesprochen liberale Regelungen in Hochschulen und Forschungseinrichtungen getroffen. So wurde Anfang 1995 an der Ruhr-Universität Bochum eine Dienstvereinbarung über den Betrieb eines hochschuleigenen Rechnernetzes, und damit unter anderem auch die E-Mail- und Internetnutzung, abgeschlossen. Mit dieser Dienstvereinbarung wurde unter sagt, Überwachungsprogramme zu installieren oder zu nutzen, die Einsicht in die transportierten oder gespeicherten Informationsinhalte ermöglichen.⁴² In einer norddeutschen Stadt ist Ende August 2001 vereinbart worden, die Nutzung des Internet-, Intranet- und E-Mail-Zugangs auch zur gelegentlichen privaten Nutzung zuzulassen, »soweit der Betriebsablauf dadurch nicht gestört wird«. Die Dienstvereinbarung »Internet« der Stadt Erlangen vom 31. 10. 2000 beschränkt sich darauf, individuelle Leistungs- und Verhaltenskontrollen weitgehend zu unterbinden: »Individuelle Leistungs- oder Verhaltenskontrollen finden mittels der erfassten Daten nicht statt. Dies gilt nicht, wenn Tatsachen bekannt werden, die den Verdacht einer erheblichen Verletzung der Dienst- und Arbeitspflichten begründen und die Personalvertretung einer entsprechenden Auswertung vorher zugestimmt hat.«⁴³

Eine entsprechende E-Mail-Geschäftsanweisung der Stadt Mannheim erklärt private E-Mails unter 2 MB durchaus für zulässig: »Private E-Mails

sind zulässig, außerhalb des städtischen Intranets (ins Internet) allerdings nur ohne Attachments (Dateianlagen) und ohne jegliche Verschlüsselung. Sie sind grundsätzlich außerhalb der regelmäßigen Arbeitszeit abzufassen und als »Privat« zu kennzeichnen, damit sie (zum Beispiel im Vertretungsfall) vom Empfänger als solche erkennbar werden.«⁴⁴

Unter Kosten-Nutzen-Gesichtspunkten sind solche liberalen Regelungen nicht nur vertretbar, sondern geradezu geboten. Moderne Verwaltung ist gerade auch auf moderne Informations- und Kommunikationstechnik für Marketing und Partizipation angewiesen.⁴⁵ Nicht von ungefähr konstatiert die Erlanger Dienstvereinbarung »Internet«: »Die Stadt Erlangen wünscht die umfassende Nutzung des neuen Mediums Internet und stellt deshalb allen Mitarbeiterinnen und Mitarbeitern mit Zugang zum PC-Netz einen Internetzugang zur Verfügung.« Routinierte Beherrschung setzt allerdings angstfreie Nutzung und Motivation voraus, auf die neuen Medien umzusteigen. Engmaschige Verbote und Begrenzung dienstlicher Freiräume und Selbstverantwortung würden in Hinblick auf das Internet die Gestaltungschancen der Öffentlichen Verwaltung höchst unproduktiv blockieren.

Im Zeitalter von Internet und Telearbeit, virtuellen Betrieben und Arbeitszeitflexibilisierung kann auch gewerkschaftliche Information im Betrieb und Transport gewerkschaftlicher Ziele nur noch unter Zuhilfenahme elektronischer Medien funktionieren. Die Verbreitung gewerkschaftlicher Informationen über das Intranet, die Einstellung gewerkschaftlicher Informationen auf Betriebsrats-Homepages oder Links von diesen zu den Gewerkschaften werden zum Teil von Arbeitgebern massiv bekämpft und zuwiderhandelnde Kollegen arbeitsrechtlich belangt. Das Bundesverfassungsgericht hat indes seit Ende 1995 die Rechtsprechung des Bundesarbeitsgerichts korrigiert, die die betriebliche Werbung und Präsenz der Gewerkschaften auf einen engen Kernbereich beschnitten hatte.⁴⁶ Der geschützte Kernbereich erfasst nunmehr alle koalitionspezifischen Verhaltensweisen, also auch Information, und steht jedem einzelnen Gewerkschaftsmitglied zu. Gibt es ein betriebliches Intranet, so darf seitdem den Gewerkschaften in Wahrnehmung ihrer Aufgaben das Recht, eigene unzensurierte Homepages im betrieblichen Intranet einzurichten oder Links zu setzen, nicht genommen werden.

Elektronische Mitgliederwerbung übers Intranet steht nicht nur der Gewerkschaft zu, sondern auch dem einzelnen Gewerkschaftsmitglied im Betrieb.⁴⁷ Das Landesarbeitsgericht Schleswig-Holstein hat bezüglich solcher Gewerkschaftswerbung über betriebliche E-Mail-Verteiler eine richtungweisende Entscheidung getroffen.⁴⁸ Mit Urteil vom 1. 12. 2000 verfügte das Gericht die Rücknahme einer Abmahnung wegen Gewerkschaftswerbung über einen innerbetrieblichen E-Mail-Verteiler. Da die E-Mails von dem betreffenden Kollegen außerhalb seiner Arbeitszeit von zu Hause aus verschickt wurden, hatte er gegen seine Arbeitspflicht unstrittig nicht verstoßen. Ob er es auch während der Arbeitszeit hätte machen dürfen, hatte das Gericht nicht zu entscheiden und offen gelassen.

8. Fazit

Lässt man die neueren digitalen Möglichkeiten Revue passieren, so wird deutlich, dass technisch gesehen am Bildschirmarbeitsplatz ein umfassendes Regime der Verhaltens- und Leistungskontrolle aufgebaut werden könnte. Selbst unter Kostengesichtspunkten sind allerdings solche Vorhaben umstritten, scheinen sogar eher kontraproduktiv zu sein. In Deutschland greifen darüber hinaus wirksame Persönlichkeitsschutz- und Mitbestimmungsrechte. Statt auf umfassende Überwachung zu setzen, würden Unternehmen und Behörden deshalb besser fahren, auf Selbstverantwortung und ergänzende Missbrauchskontrolle zu setzen.

Anmerkungen

- 1 Vgl. Konrad Lischka, Klick, klick – und weg ist der Job, in: Spiegel Online 30. 10. 2000; vgl. http://www.amanet.org/press/research/check_email.htm
- 2 Vgl. 87 Prozent der Chefs in den USA überwachen E-Mails ihrer Mitarbeiter, in: bild der wissenschaft online, Newsticker 29. 5. 2001.
- 3 Vgl. Gillies, Privates Surfen gefährdet den Arbeitsplatz, in: VDI-Nachrichten 8. 10. 99.
- 4 W. Müller, Freie Meinung im Internet?, in: CF 12/2000, S. 8–9.
- 5 Die Tastatur als Blackbox, NetworkWorld, 28. 5. 2001.
- 6 Müller, M., Vater gefunden, in: Handelsblatt 7. 4. 1999.
- 7 Vgl.: W. Fricke, Bergleute im Daten-Lagerhaus, in: Computer Fachwissen 4/99, S. 11–14.
- 8 Landesbeauftragter für den Datenschutz Niedersachsen, Datenschutz bei Tele- und Mediendiensten, 23. August 1999.
- 9 Vgl. M. Kiper, Biometrische Identifikation, in: Computer Fachwissen 8-9/99, S. 46–51; N. Pohlmann, Biometrie, in: IT-Sicherheit 2/2001, S. 13–21; F. Büllingen/ A. Hillebrand, Biometrie als Teil der Sicherungsinfrastruktur, in: DuD 24 (2000), S. 339–343.
- 10 BVerfG Beschluss vom 19. 12. 1991 – 1 BvR 2382/85
- 11 Bundesarbeitsgericht, Urteil vom 29. Oktober 1997 – 5 AZR 508/96, vgl. auch: Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen, RDV 2/1998 S. 69-71.
- 12 BVerfG Urteil vom 19. 12. 1991, BB 1992, S. 708.
- 13 BVerfG. Beschluss vom 19. 12. 1991 – 1 BvR 382/85; vgl. RDV 1992, S. 128; ArbuR 5/1992, S. 158-160.
- 14 BAG, Urteil vom 29. Oktober 1997 – 5 AZR 508/96; vgl. Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen, in: RDV 2/1998 S. 69-71.
- 15 Arbeitgeber als Anbieter von Telediensten, Jahresbericht 1998 des Berliner Datenschutzbeauftragten, zitiert nach: GDD-Mitteilungen 3–4/99, S. 3–4.
- 16 vgl. Kiper/Schierbaum, Telekommunikationsgesetzgebung und Arbeitnehmerdatenschutz, in: Computer Fachwissen 8-9/99, S. 24–29.
- 17 Innenministerium Baden-Württemberg, Hinweise zum Datenschutz für die Private Wirtschaft (Nr. 37), in: Staatsanzeiger Nr. 2 vom 18. 1. 99, S. 13.

- 18 BVerfGE 85, 386, 396 f.
- 19 Automatic-Call-Distribution-Anlagen, wie sie in Call-Centern eingesetzt werden.
- 20 BAG, Beschluss vom 30. August 1995, – 1 ABR 4/95 – vgl. Mithören von Telefongesprächen zu Ausbildungszwecken, in: RDV 1/1996, S. 30–33.
- 21 Vgl. Skript der Panorama-Sendung Nr. 579 vom 23. 9. 1999.
- 22 Arbeitsgericht Frankfurt am Main, 18 Ca 7436/94.
- 23 Arbeitsgericht Würzburg, 1 Ca 1326/97.
- 24 Arbeitsgericht Frankfurt am Main, 11 Ca 5818/95.
- 25 Arbeitsgericht Frankfurt am Main, 14 Ca 891/95.
- 26 Arbeitsgericht Frankfurt am Main vom 24. 7. 99, 2 Ca 8824/98.
- 27 OLG Hamm, 8 U 194/98.
- 28 LAG Niedersachsen, 13 Sa 1235/97.
- 29 LAG Köln, 6 Sa 42/98.
- 30 ArbG Wesel AZ 5 Ca 4021/00 vom 21. 3. 2001; vgl. C. Tödtmann, Heißes Eisen, in: Handelsblatt 24. 9. 2001 S. N 5.
- 31 Vgl. ArbG Braunschweig, Urteil vom 22. 1. 1999 – 3 Ca 370/98; Außerordentliche Kündigung wegen Kinderpornografie, in: Computer Fachwissen (CF) 10/99, S. 26.
- 32 Vgl. LAG Baden Württemberg, Urteil vom 11. 1. 1994 – 7 Sa 86/92; AG Osnabrück, Urteil vom 19. 3. 1997 – 1 Ca 639/96.
- 33 Kündigung wegen Sammlung und Verbreitung rassistischer und sexistischer Witze per dienstlichem PC, LAG Köln, Urteil vom 14. 12. 1998 – 12 Sa 896/98; LAG Schleswig-Holstein, Urteil vom 4. 11. 1998 – 2 Sa 330/98.
- 34 Bay. OLG, Beschluss vom 11. 11. 1997, 4 St RR 232/97.
- 35 Vgl. LG Hamburg, Urteil vom 12. 5. 1998 – 312 O 85/98.
- 36 Vgl. D. Sauer, Der Chef als Detektiv, in: Internet World, März 2000, S. 60–63; Vgl. J. Haverkamp, Alles unter Kontrolle? in: Computer Fachwissen (CF) 12/98, S. 18–24.
- 37 Vgl. Surfen kann ins Aus führen, in: Hannoversche Allgemeine Zeitung, 6. 10. 2001.
- 38 <http://www.handel.de/service/news/archivjan01>
- 39 Vgl. Privates Surfen im Büro kostet Firmen Milliarden, in: Frankfurter Rundschau, 26. 8. 2000.
- 40 Vgl. Anm. 39 in T. Klebe/P. Wedde, Gewerkschaftsrechte auch per E-Mail und Intranet? In: AuR 11/2000, 401–407.
- 41 Vgl. Schierbaum, in: PersR 2000, 499 (503 f.).
- 42 <http://www.slf.uni-bochum.de/wpr/dv-netz.htm>
- 43 http://www.erlangen.de/news.asp?folder_id=1579&mainfolder_id=1579&news_id=29086
- 44 Besondere Geschäftsanweisung der Stadt Mannheim über die Benutzung und Behandlung elektronischer Post (BGA – E-Mail) vom 3. 7. 1999.
- 45 Vgl. Groß, Öffentliche Verwaltung im Internet, in: Die öffentliche Verwaltung 2001, S. 159–164.
- 46 BVerfG, Beschluss vom 14.11.1995 DB 1996, 1627, in: AuR 1996, 151.
- 47 Vgl. T. Klebe, P. Wedde, Gewerkschaftsrechte auch per E-Mail und Intranet? in: AuR 11/2000, S. 401–407.
- 48 LAG Schleswig-Holstein, Az 6 Sa 562/99 – 3 Ca 653a/99 ArbG Elmshorn.