MANUEL KIPER, BRUNO SCHIERBAUM

Telekommunikations-gesetzgebung und Arbeitnehmerdatenschutz

Durch gleich eine ganze Reihe neuer Gesetze zum Themenbereich Telekommunikation und Multimedia ist die Rechtslage zwar nicht unbedingt übersichtlicher geworden, aber dennoch ist es – auch unter dem Gesichtspunkt Arbeitnehmerdatenschutz – nötig, sich damit zu befassen.

Telekommunikation wird heute am Arbeitsplatz in vielfältiger Weise genutzt. Zum Arbeitsalltag gehören neben dem Telefonieren auch immer mehr die Nutzung von Telefax, elektronischer Post und Mailing-Listen, das Lesen und Schreiben in Newsgroups und nicht zuletzt die Nutzung des WWW (World Wide Web). Zudem hat sich der Einsatz von Telekommunikation am Arbeitsplatz auch qualitativ verändert. Der elektronische Austausch von Daten oder das gemeinsame Bearbeiten von Dokumenten in Verbindung mit neuen Formen der Arbeitsorganisation (wie etwa Telearbeit oder Workflow-Management) stellen Betriebs- wie Personalräte vor neue Aufgaben. Vor diesem Hintergrund sollen die weitgehenden datenschutzrechtlichen Bestimmungen der neuen Telekommunikations- und Multimedia-Gesetzgebung in Bezug auf den Arbeitnehmerdatenschutz hier nun näher betrachtet werden.

Mailing-Liste = eine Art öffentlicher Briefverkehr auf Basis der elektronischen Post zu einem bestimmten Thema. Newsgroup = Diskussionsforum im Internet; ähnliche Einrichtung wie die Mailing-Liste, aber diskussionsorientierter.

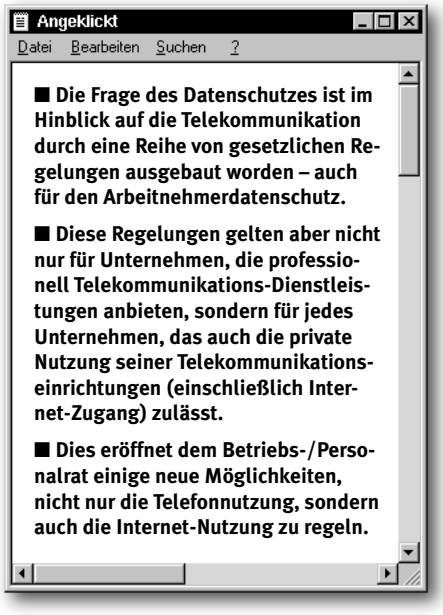
Workflow-Management = Unterstützung von Arbeitsprozessen (workflows) durch spezielle Software. Typisch ist z.B., dass die Software gleich nach Abschluss eines Arbeitsschritts Datei und Programm für den nächsten Arbeitsschritt automatisch auf den Bildschirm bringt, Arbeitsergebnisse sofort weiterleitet usw.

Neue Grundlagen des betrieblichen Datenschutzes

Unverändert basiert der Datenschutz in Unternehmen auf dem Bundesdatenschutzgesetz (BDSG), auf Tarifverträgen und Betriebsvereinbarungen. Grundlage des betrieblichen Datenschutzes *für die Telekommunikation* sind jedoch Gesetze, die erst in den letzten Jahren im Zusammenhang mit der ›Liberalisierung‹ des Telekommunikations-Sektors erlassen wurden. Bei diesen Gesetzen (siehe info-Kasten auf Seite 25) handelt es sich um *vorrangige* Rechtsvorschriften des Bundes im Sinne des Bundesdatenschutzgesetzes (§ 1 Abs. 4 BDSG), um Vorschriften also, die dem BDSG gegenüber Vorrang haben.

Den Anfang machte im Juli 1996 das ›Telekommunikationsgesetz‹ (TKG), das den Wettbewerb im Telekommunikations-Sektor fördern und das flächendeckende Angebot angemessener und ausreichender Dienstleistungen gewährleisten soll. Ergänzt wird das TKG durch das Anfang 1998 in Kraft getretene ›Telekommunikations-Begleitgesetz‹ (TKBeglG), das vorrangig beamtenrechtliche Fragen im Zusammenhang mit der Post-Privatisierung regelt, aber auch Strafverschärfungen bei Verstößen gegen das Fernmeldegeheimnis vorsieht.

Dazu kam im August 1997 das ›Informations- und Kommunikationsdienste-Gesetz‹ (IuKDG) als ein Artikelgesetz – gewissermaßen ein Gesetzesbündel –, das als Artikel 1 das ›Teledienstegesetz‹ und als Artikel 2 das ›Teledienstedatenschutzgesetz‹ enthält und dessen Ziel es



ist, »einheitliche wirtschaftliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen«. Zusätzlich wurden im ›Mediendienstestaatsvertrag‹ noch die an die Allgemeinheit gerichteten Informations- und Kommunikationsdienste, die sogenannten Mediendienste geregelt (zur Definition der wichtigsten Begriffe siehe info-Kasten auf Seite 26).

Erschwerend kommt zu dieser Vielfalt hinzu, dass es auch noch Überschneidungen gibt, weil bei der Nutzung von Telediensten gleichzeitig auch Telekommunikationsdienste genutzt werden und so weiter. Es hilft also alles nichts: Die in den aufgeführten Gesetzen enthaltenen Regelungen können für den betrieblichen Datenschutz im Einzelfall *alle* von Bedeutung sein.

Darüber hinaus sind bei der Datenverarbeitung auch die verschärften Bestimmungen des Strafgesetzbuchs (StGB) zu beachten. Der neu geschaffene § 206 StGB stellt den Bruch des Fernmeldegeheimnisses unter Strafe. Verboten sind auch verschiedene Eingriffe in den Datenverkehr. § 202 a StGB stellt das Ausspähen von Daten unter Strafe. Dies umfasst nach Absatz 2 dieses Paragrafen auch die Übermittlung von Daten, also auch das ›Ausspähen‹ von eMails oder persönlichen Identifikations-Nummern. Nach § 303 a schließlich wird die Veränderung von Daten und nach § 303 b die Computer-Sabotage unter Strafe gestellt.

Datenschutz als Aufgabe des Betriebs-/Personalrats

Für die Umsetzung der Datenschutzbestimmungen in die Praxis ist der Unternehmer (oder in der öffentlichen Verwaltung die Dienststellenleitung) zuständig. Betriebs- und Personalräte haben allerdings nach Betriebsverfassungsgesetz und Personalvertretungsgesetzen die Aufgabe, die Einhaltung (auch) dieser Gesetze zu kontrollieren.

Darüber hinaus greifen natürlich Mitbestimmungsrechte, etwa bei Einführung und Anwendung von »technischen Einrichtungen, die zur Leistungs- oder Verhaltenskontrolle« geeignet sind. Telefonanlagen dürften ebenso wie die Telefax-, eMail- oder Internet-Nutzung in und aus Unternehmensnetzen heraus regelmäßig dazu gehören. Die sozialverträgliche Gestaltung und Nutzung dieser technischen Einrichtungen kann also in Betriebs- und Dienstvereinbarungen sichergestellt werden. Deshalb ist es – wie gesagt – für Betriebs- und Personalräte unumgänglich, die datenschutzrechtlichen Bestimmungen der neuen Telekommunikations- und Multimedia-Gesetzgebung zur Kenntnis zu nehmen.

info

Übersicht

Die neuen ›Tele-Gesetze‹ ...

TKG – Telekommunikationsgesetz (vom 25. 7. 1996)
Zweck: Regulierung der Telekommunikation unter anderem mit dem Ziel, das Fernmeldegeheimnis und den Datenschutz bei Telekommunikationsdiensten zu wahren.

TDSV – Telekommunikationsdienstunternehmen-Datenschutzverordnung (vom 12. 7. 1996)
Zweck: Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten sicherstellen.

TDG – Teledienstegesetz (Art. 1 des IuKDG – Informations- und Kommunikationsdienstegesetz vom 22. 7. 1997)
Zweck: Rahmenbedingungen schaffen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste (Teledienste)

TDDSG – Teledienstedatenschutzgesetz (Art. 2 des IuKDG – Informations- und Kommunikationsdienstegesetz vom 22. 7. 1997)
Zweck: Schutz personenbezogener Daten bei Telediensten sicherstellen.

Mediendienstestaatsvertrag (vom 12. 2. 1997)
Zweck: Einheitliche Rahmenbedingungen für Mediendienste schaffen.

Datenschutz bei betrieblicher Telekommunikation

Das TKG befasst sich auch mit datenschutzrechtlichen Fragen. Es regelt in seinem elften Teil (info-Kasten Seite 27) den Schutz des Fernmeldegeheimnisses, den Datenschutz sowie den staatlichen Zugriff auf die bei der Telekommunikation anfallenden Daten.

Klären wir zunächst einmal, was nach dem TKG unter Telekommunikation verstanden wird. Telekommunikation wird dort definiert als der »technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikations-Anlagen.« (§ 3 Nr. 16 TKG). Damit unterliegt also auch die Kommunikation über das Internet (oder ein unternehmensinternes Intranet) den Bestimmungen des TKG.

Nun könnte vielleicht die Meinung aufkommen, die Regelungen des TKG bezögen sich nur auf spezielle Telekommunikations-Unternehmen, nicht aber auf ›normale‹ Firmen. Tatsächlich jedoch bezieht sich das TKG durchaus nicht nur auf das gewerbliche Angebot von Telekommunikation. Vielmehr unterliegen den Datenschutzbestimmungen des TKG all jene, die – wie es in § 89 Abs. 1 heißt – »geschäftsmäßig Telekommunikations-Dienste erbringen«. Und das wiederum wird in § 3 Nr. 5 TKG definiert als »das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht« (nachhaltig ist das Angebot immer dann, wenn es nicht nur einmalig, sondern auf Wiederholung oder auf Dauer angelegt ist).

Die Ausweitung des Geltungsbereichs des TKG über den gewerblichen und gewinnorientierten Sektor der Telekommunikation hinaus ist also vom Gesetzgeber ausdrücklich gewollt. Dies zeigt auch die Gesetzesbegründung. Dort heißt es unter anderem: »Dem Fernmeldegeheimnis [unterliegen] damit

info

Definitionen:

Informationstechnische Dienste

Telekommunikationsdienstleistungen **sind das gewerbliche Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte.**

Geschäftsmäßiges Erbringen von Telekommunikationsdiensten **ist das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht.**

Teledienste **sind für die individuelle Nutzung bestimmte elektronische Informations- und Kommunikationsdienste (z. B. Telebanking, Datenaustausch, Internet-Nutzung und Datendienste auch über Waren und Dienstleistungsangebote, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht).**

Mediendienste **sind an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste (z. B. Verteildienste in Form von direkten Angeboten an die Öffentlichkeit für den Fernseheinkauf, Verteildienste in Form von Textdiensten und Multimedia-Abrufdienste)**

z. B. Corporate Networks, Nebenstellenanlagen in Hotels und Krankenhäusern, Clubtelefone und Nebenstellenanlagen in Betrieben und Behörden, soweit sie den Beschäftigten zur privaten Nutzung zur Verfügung gestellt sind«.

Geschäftsmäßige Telekommunikation

Jedes Unternehmen, jede Stadtverwaltung oder Universität, jedes Krankenhaus oder Hotel, das seinen Angestellten (bei privatem Telefonieren) oder Kunden – das heißt: irgendeinem ›Dritten‹ – regelmäßig das Telefonieren erlaubt, erbringt also »geschäftsmäßig Telekommunikation« und unterliegt somit dem TKG. Damit gelten die datenschutzrechtlichen Vorschriften des TKG auch für ›geschlossene Benutzergruppen‹, wie etwa die Belegschaft eines Unternehmens. Und dies gilt nicht nur für die Telefonanlage eines Betriebs, sondern auch für firmeninterne Computer-Netzwerke. Dem entspricht es, dass die im TKG angeführten strafrechtlichen Regelungen zum Schutz des Fernmeldegeheimnisses ausdrücklich durch das Anfang 1998 in Kraft getretene Telekommunikations-Begleitgesetz (TKBeglG) auch auf den Bereich firmeninterner Netze ausgedehnt worden sind.

Der § 85 TKG bestimmt nun, dass »der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikations-Vorgang beteiligt ist oder war«, dem Fernmeldegeheimnis unterliegen. Weiterhin erstreckt sich das Fernmeldegeheimnis auf »die näheren Umstände erfolgloser Verbindungsversuche«. Geschützt sind damit zum Beispiel auch die Verbindungsdaten eines Kommunikationsvorgangs – also wer wann, mit wem, wie lange, von wo, wohin und auf welche Weise kommuniziert hat. Damit stellt eine detaillierte Liste von Verbindungsdaten – beispielsweise über Telefonate zu Kontrollzwecken erstellt – einen Verstoß gegen das Fernmeldegeheimnis dar. Dies gilt unstrittig immer dann, wenn die Telekommunikations-Dienste geschäftsmäßig, also regelmäßig (nachhaltig) für Dritte erbracht werden.

Fassen wir zusammen: Wenn und so weit der Arbeitgeber die private Nutzung der betrieblichen Telekommunikations-Anlagen für interne oder externe Kommunikation gestattet, gelten sowohl das Fernmeldegeheimnis wie auch die datenschutzrechtlichen Bestimmungen des TKG. Unerheblich ist dabei, ob die Telekommunikations-Anlagen entgeltlich oder unentgeltlich zu privaten Zwecken genutzt werden dürfen. Selbst das Untersagen privater Anrufe durch die Beschäftigten entbindet nicht von der Verpflichtung zur Einhaltung des Fernmeldegeheimnisses und der Datenschutzvorschriften nach dem TKG, jedenfalls dann nicht, wenn *eingehende* Anrufe – die ja auch privaten Charakter haben können – automatisch an die Nebenstelle vermittelt werden (Durchwahl). Nur die strikte Nutzung der betrieblichen TK-Anlagen allein für dienstliche Zwecke erfüllt die Merkmale eines Telekommunikations-Dienstes ›für Dritte‹ nicht und unterliegt damit auch nicht den Schutzbestimmungen des elften Teils des TKG.

Höchstrichterliche Entscheidungen

Gestützt wird das alles auch durch Entscheidungen höchster Gerichte. So hat das Bundesarbeitsgericht im Oktober 1997 entschieden, dass auch im beruflichen Bereich das Recht am gesprochenen Wort als Teil des allgemeinen Persönlichkeitsrechts zu gewährleisten ist…[1]. Und zuvor schon hatte das Bundesverfassungsgericht geurteilt, dass ein Telefon-Überwachungssystem, 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…[2]. 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. Und seit dem ›Fangschaltungsbeschluss‹ des BVerfG ist auch 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 Fernmeldegeheimnis« sind…[3].

Insofern ist alles in allem von einem weitreichenden Schutz des Fernmelde-

1…Bundesarbeitsgericht vom 29. 10 1997, Aktenzeichen: 5 AZR 508/96

2… Bundesverfassungsgericht vom 19. 12. 1991, in: ›Betriebs-Berater‹ 1992, Seite 708

3… Amtliche Sammlung der Bundesverfassungsgerichts-Entscheidungen 1985, Seite 386 und 396 f.

geheimnisses und des Datenschutzes bei Telekommunikationsvorgängen auszugehen. Nicht zuletzt sind die Mitgliedsstaaten der EU durch – hier zu Lande noch nicht umgesetzte – EG-Richtlinien dazu verpflichtet, »das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikationen durch andere Personen als die Benutzer« zu untersagen.

Fernmeldegeheimnis bei Telefax und eMail

Gesetzlich durch das Fernmeldegeheimnis geschützt ist – wie wir gesehen haben – nicht nur das Telefonieren, sondern jede Art der individuellen Nachrichtenübermittlung, einschließlich eMail und Telefax. Auch die Einführung eines generellen Überwachungssystems für den elektronischen Postverkehr in einem Unternehmen stellt also einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts der Arbeitnehmer dar. Ausgesprochene Geschäftspost ist hiervon nicht betroffen. Persönlich adressierte oder z. B. an den Betriebs- oder Personalrat gerichtete oder verschickte eMails unterliegen hingegen einem Schutz vor Überwachung – und zwar nicht nur der Inhalt, sondern auch die Verbindungsdaten.

Etwa im Hinblick darauf, dass Telefaxgeräte vielfach frei zugänglich sind und dass eMails zwischengespeichert werden, gewinnen hier auch die Vorschriften des § 87 TKG Bedeutung, die den Arbeitgeber zu technischen Schutzmaßnahmen zwingen, um so das Fernmeldegeheimnis zu sichern. Zwar haben Angestellte, die eingegangene Telefaxe dem Gerät – zum Beispiel einem Etagen-Telefaxgerät – entnehmen, 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 räumliche und organisatorische Maßnahmen ebenso vorzusehen wie Anonymisierungs-Maßnahmen und auch Verschlüsselungen. Dies sicherzustellen dürfte in vielen Unternehmen 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 (etwa wie ›WalterMüller@t-online.de‹) nicht protokolliert werden ...

Datenschutz im Telekommunikationsrecht

In § 89 TKG wird in Ergänzung des Bundesdatenschutzgesetzes der Datenschutz spezialgesetzlich für den Telekommunikations-Sektor geregelt. Dabei werden die zentralen Grundsätze des Datenschutzes zur Verarbeitung personenbezogener Daten kurz aufgeführt:

- der Grundsatz der Verhältnismäßigkeit,
- das Minimierungsgebot,
- der Grundsatz der Zweckbindung
- Höchstfristen für die Speicherungsdauer der Daten.

Im Weiteren werden im § 89 TKG detaillierte Regelungen über zulässige Datenaufnahme, Datenverarbeitung und Datenspeicherung getroffen. Eine personenbezogene Datenverarbeitung ist demnach erlaubt zum Zwecke ...

- der Abwicklung des Vertragsverhältnisses,
- Herstellung und Aufrechterhaltung einer Telekommunikations-Verbindung,
- Abrechnung und Erfassung erbrachter Leistungen,
- Erkennung und Beseitigung von Störungen und
- Ahndung von Missbrauch.

Weitere Einzelheiten des Telekommunikations-Datenschutzes regeln die dann folgenden Absätze des § 89 TKG und auch die ›Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen‹ (TDSV). Weil diese Verordnung aber noch vor dem TKG erlassen wurde, baut sie auf einer veralteten Rechtsgrundlage auf. Das bedeutet, dass die TDSV gemäß § 1 Abs. 1 in Verbindung mit § 2 Nr. 2 und Nr. 6 nur für das *öffentliche, gewerbliche* Angebot von Telekommunikations-Leistungen gilt, also nur für Telekommunikations-Unternehmen im engeren Sinne (im Gegensatz zu den Bestimmungen des TKG selber, das für alle Unternehmen gilt, die ›geschäftsmäßig‹

info

Regelungsbereiche im elften Teil des TKG:

Fernmeldegeheimnis, Datenschutz, Sicherung

§ 85 – Fernmeldegeheimnis

§ 86 – Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen

§ 87 – Technische Schutzmaßnahmen

§ 88 – Technische Umsetzung von Überwachungsmaßnahmen

§ 89 – Datenschutz

§ 90 – Auskunftsersuchen der Sicherheitsbehörden

§ 91 – Kontrolle und Durchsetzung von Verpflichtungen

§ 92 – Auskunftspflicht

§ 93 – Staatstelekommunikationsverbindungen

Telekommunikations-Dienste erbringen – siehe oben).

Konkret heißt das: Solange keine neue Datenschutzverordnung zum TKG erlassen ist, gelten für alle Unternehmen, die *nicht* gewerbsmäßig und nicht öffentlich Telekommunikations-Dienste erbringen, ausschließlich die Datenschutzbestimmungen des TKG, die für diese Unternehmen also nicht durch eine Datenschutzverordnung konkretisiert werden. So dürfen etwa die Steuersignale (mit denen der Datentransport im Netz geregelt wird) im Falle eines Missbrauchs maschinell erhoben werden. Davon sind allerdings die Regulierungsbehörde und der Betroffene zu unterrichten. Das Aufschalten auf bestehende Verbindungen – also das Mithören – ist nur bei Funktionsstörungen erlaubt, nicht jedoch zur Missbrauchsbekämpfung. Ein solches Aufschalten ist den Beteiligten in jedem Fall durch ein spezielles Signal kenntlich zu machen (z.B. regelmäßiger Signalton, Blinken einer Lampe). Nachrichten*inhalte* (ob Sprache, Dateien, eMails oder Telefaxe) dürfen nur dann aufgezeichnet werden, soweit sie Gegenstand oder aus verarbeitungstechnischen Gründen notwendiger Bestandteil des Dienstes sind, beispielsweise bei Mailboxen.

Nach § 89 Abs. 2 Nr. 3 a TKG und § 6 Abs. 7 TDSV sind bei Telefon-, Telefax- und eMail-Anschlüssen in Betrieben und Behörden Einzelverbindungsnachweise nur zulässig, wenn der Kunde (= Unternehmen/Dienststelle) gegenüber dem Diensteanbieter schriftlich erklärt hat, dass die Beschäftigten informiert worden sind (auch künftige Beschäftigte informiert werden) und dass der Betriebs- oder Personalrat entsprechend den gesetzlichen Vorschriften beteiligt wurde.

Internet- und Intranet-Nutzung

Das IuKDG ist – wie schon kurz erwähnt – ein ›Artikelgesetz‹, mit dem sehr unterschiedliche Fragen in einem Gesetz geregelt wurden. Anzuwenden ist das IuKDG auf ›Teledienste‹. Das sind (Artikel 1 § 2 Abs. 2 IuKDG) Telebanking und Telespiele, Verkehrs- oder Börsendaten und manches andere. Vor allem aber sind Teledienste »Angebote zur Nutzung des Internets oder weiterer Netze«. Demnach ist ein Arbeitgeber, der seinen Beschäftigten eine nicht ausschließlich dienstliche Internet-Nutzung ermöglicht, ein Teledienste-Anbieter. Gleiches gilt für ›weitere Netze‹, also auch für firmeninterne Computernetze wie etwa ein Intranet.

Nutzungsdaten von Telekommunikationseinrichtungen einschließlich Internet müssen unverzüglich gelöscht werden und Nutzungsprofile sind unzulässig.

Den Datenschutz regelt das IuKDG in seinem Artikel 2, dem ›Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz – TDDSG)‹. Wobei auch das TDDSG nicht zwischen firmeninterner oder -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 Paragrafen 3 bis 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.

Im Unterschied zu anderen Datenschutzgesetzen und -vorschriften bleibt der Datenschutz im IuKDG aber trotz dieser Regelungen wirkungsschwach, da das TDDSG nicht vorsieht, Datenschutzverstöße als Ordnungswidrigkeit zu bestrafen.

Nutzungsprofile und Datenlöschung

Fest steht aber: Weil Arbeitgeber, die ihren Beschäftigten den Zugang zum Internet nicht nur ausschließlich für dienstliche Zwecke ermöglichen, Teledienste-Anbieter sind, gilt nicht nur das TKG, sondern auch das IuKDG. Denn nach § 3 Nr. 1 TDG sind Teledienstean-bieter »natürliche oder juristische Personen oder Personenvereinigungen, die eigene oder fremde Teledienste zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln«.

Das heißt: 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 zu erfassen und aus-

zuwerten. Entsprechenden Befürchtungen kann und sollte mit klaren Regelungen zwischen Betriebsräten und Arbeitgebern entgegen getreten werden.

Dies heißt nun allerdings nicht, dass der Arbeitgeber jedwede Internet-Nutzung seiner Beschäftigten dulden muss. Zugangsbeschränkungen, Ahndung von Missbrauch oder Geheimnisverrat und Ähnliches sind dem Arbeitgeber 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‹ (siehe CF 4/99 ab Seite 16), Filter oder andere technische Mittel einsetzen, um den Zugriff auf bestimmte Dienste und Netzressourcen zu begrenzen.

Fassen wir zusammen: Ist die private Internet-Nutzung von Arbeitnehmern am Arbeitsplatz erlaubt oder doch geduldet und wird sie auch nicht abgerechnet, darf der Arbeitgeber keine Daten über die Internet-Nutzung seiner Beschäftigten sammeln. Hervorzuheben ist auch, dass – soweit technisch möglich und zumutbar – dem Nutzer die Möglichkeit einzuräumen ist, Teledienste anonym oder unter Pseudonym zu nutzen (bei Pseudonymen sind dann allerdings Nutzungsprofile zulässig). Deutlich sollte aber auch sein, dass ein Arbeitnehmer keinen Anspruch darauf hat, das Internet nach Belieben zu nutzen.

Beteiligungsrechte von Betriebsräten

Bei der Einführung und Nutzung von Telekommunikations-Einrichtungen bestehen neben den vorgestellten gesetzlichen Regelungen auch Beteiligungsrechte des Betriebsrats nach dem BetrVG (Entsprechendes gilt für Personalräte). Hierbei handelt es sich insbesondere um Überwachungs-, Informations- und Mitbestimmungsrechte.

Eine grundsätzliche Vorgabe in Bezug auf den Schutz der Persönlichkeitsrechte der Beschäftigten enthält § 75 Abs. 2 BetrVG. Danach haben der Arbeitgeber und der Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern.

Bereits nach Art. 2 Abs. 1 GG hat jeder Beschäftigte das Recht auf freie Entfaltung der Persönlichkeit. Rechtswidrige Eingriffe in die Persönlichkeitssphäre können insbesondere im Zusammenhang mit betrieblichen Kontrollmaßnahmen vorkommen. Dabei sind bestimmte Kontrollmaßnahmen von vornherein unzulässig. Es ist also nicht etwa möglich, solche Kontrollmaßnahmen im Zuge der Mitbestimmung durch den Betriebsrat ›abzusegnen‹. So ist in jedem Falle eine Überwachung der Arbeitnehmer durch Abhörgeräte oder Tonbandaufzeichnungen unzulässig. Das Gleiche gilt für das Abhören oder heimliche Mithören von Telefongesprächen oder für die heimliche Video-Überwachung (CF 2/99 ab Seite 4).

Betriebsvereinbarungen anstreben

Betriebsräte sollten ihr Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG allerdings so oder so nicht durch schlichte Zustimmung wahrnehmen, sondern die Einführung und Anwendung der technischen Systeme durch den Abschluss von Betriebsvereinbarungen regeln. Der Betriebsrat kann dabei unterschiedliche Wege wählen. Zum einen besteht die Möglichkeit, eine alle Systeme übergreifende Rahmenvereinbarung zur Verarbeitung und Nutzung personenbezogener Arbeitnehmerdaten abzuschließen. Zum anderen kann der Betriebsrat Einzelvereinbarungen für die Anwendung der einzelnen technischen System wie Telefonanlage, eMail, Internet- und Intranet-Nutzung anstreben. Auch eine Kombination beider Möglichkeiten kommt in Frage (einen umfassenden Überblick gibt dazu CF 6-7/98).

Unabhängig von dieser Grundsatzfrage sollen hier nun die wichtigsten Inhalte betrieblicher Regelungen grob skizziert werden. Dabei wird allerdings ausschließlich auf den Arbeitnehmerdatenschutz eingegangen.

Folgende Punkte sollten dabei abschließend geregelt werden:

- die eingesetzte Hard- und Software,
- die gespeicherten personenbezogenen Daten,
- die Auswertungen, die jeweils erstellt werden,
- die zugriffberechtigten Personen und die Löschungsfristen.

Im Detail sind vor allem folgende personenbezogene Daten festzulegen:

- *Bestandsdaten* ... Das sind die Daten, die bei einem Kommunikationssystem oder -netz dauerhaft gespeichert werden, um den Betrieb zu gewährleisten; dieses sind bei Netzwerken z.B. Passwörter oder die IP-Adresse als Identifikations-Nummer eines Rechners, bei Telefonanlagen die Nebenstellen, bei eMail-Systemen die eMail-Adressen.
- *Verbindungsdaten* ... Das sind Angaben über den jeweiligen Kommunikationspartner (z.B. Zielnummer oder eMail-Adresse); weiter fallen darunter Angaben über Zeitpunkt und Dauer einer Verbindung, in Anspruch genommene Systemleistungen, benutzte Anschlüsse und Leitungen.
- *Inhaltsdaten* ... Das sind die zum Beispiel über Telefon oder eMail übertragenen Informationen und Nachrichten, die über ihre Zuordnung an einen bestimmten Absender und Empfänger ebenfalls personenbezogene Daten sind; sie sind einem besonderen Schutz zu unterwerfen, so dass nur Sender und Adressat Zugang zu diesen Informationen haben sollten.

Vor allem: Datensparsamkeit

Da der Umfang der gespeicherten personenbezogenen Daten die Basis für die Auswertung des Kommunikationsprozesses bildet, sollte die Speicherung dieser Daten abschließend festgelegt

und dabei auf das notwendige Minimum beschränkt werden. Welche Auswertungen aus der Verarbeitung der so übrig gebliebenen personenbezogenen Daten zugelassen werden, sollte ebenfalls Bestandteil der Vereinbarung sein, zusätzlich die Löschungsfristen und die zugriffsberechtigten Personen. Vereinbart werden sollte auch, dass eMails grundsätzlich nur vom Sender und Empfänger gelesen werden dürfen, so dass ein heimliches Lesen von eMails ausgeschlossen ist, ebenso wie das heimliche Mithören von Telefongesprächen.

Darüber hinaus sind technische und organisatorische Maßnahmen nach den Vorgaben von § 9 BDSG und § 87 TKG zu vereinbaren.

Dr. Manuel Kiper, Bruno Schierbaum; Kontaktadresse: BTQ Niedersachsen, Donnerschweer Straße 84, 26123 Oldenburg, Telefon 0441/8 20 68; eMail: **kiper@btq.de, schierbaum@btq.de**