

# Kontrollierte Kommunikation (2)

**Elektronische Post und Internet-Nutzungsfragen in einer Betriebs- oder Dienstvereinbarung zu regeln, erfordert sowohl einen Blick für das Große und Ganze, wenn es darum geht Perspektivisches einzubeziehen, wie auch Sorgfalt im Detail.**

**E**MAIL-KOMMUNIKATION und Internet-Nutzung gehören an immer mehr Arbeitsplätzen zur täglichen Routine. Wird hierbei der Internet-Anschluss nicht vom Einzelrechner aus hergestellt, sondern – wie üblich – über ein Intranet organisiert, laufen alle Daten

über einen zentralen Server und werden damit auch für eine Kontrolle der Leistung und des Verhaltens von Arbeitnehmern nutzbar. Der Automobilkonzern Ford hat kürzlich angekündigt, sogar alle Produktionsarbeiter mit einem häuslichen Computer auszustatten und auf Firmenkosten an sein Intranet anzubinden. Damit wären auch die (zum Teil ja sicherlich privaten) Aktionen am heimischen Ford-PC potenziell durch das Unternehmen zu kontrollieren ...

kommunikationsgesetzes (TKG) und des Teledienstedatenschutzgesetzes zum Fernmeldegeheimnis und dem Datenschutz bei Telekommunikations- und Multimediadiensten berücksichtigen (siehe dazu den ersten Teil dieses Artikel in cf 6/2000 ab Seite 12). Die folgenden Ausführungen sollen dabei eine Hilfe sein. Wobei natürlich zu beachten ist, dass sich Muster und Vorschläge für eine Betriebsvereinbarung üblicherweise nicht von Betrieb zu Betrieb übertragen lassen, sondern immer auf die konkreten Verhältnisse und Bedingungen des jeweiligen Betriebs zugeschnitten werden sollten.

**Intranet = Unternehmens-Netzwerk auf der Grundlage der Internet-Technik**

Also greift in jedem Fall die Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG. Ähnlich wie etwa bei der Einführung von Telefonanlagen sollten Betriebsräte in Betriebsvereinbarungen deshalb den notwendigen Persönlichkeitsschutz auch bei betrieblicher eMail- und Internet-Nutzung erzwingen. Diese Vereinbarung muss die Bestimmungen des Tele-

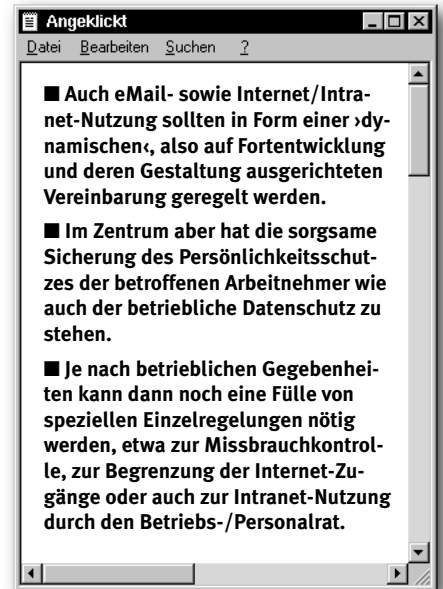
**Einige Vorabklärungen sind nötig**

ANGESICHTS DER GROSSEN Dynamik in der Entwicklung der Kommunikationstechnik und auch der Geschäftsprozesse stellt sich zunächst die Frage, ob heutzutage überhaupt noch eine *abschließende* Vereinbarung konkret bezogen auf einzelne technische Systeme oder Nutzungsarten getroffen werden sollte. Schon mehrfach wurde auch in dieser Zeitschrift auf die Vorteile ›dynamischer Vereinbarungen‹ verwiesen (siehe

›Intranet: Netz mit doppeltem Auftrag‹ in cf 2/2000 ab Seite 20 und cf 3/2000 ab Seite 16), die den rasanten technisch-organisatorischen Entwicklungen besser gerecht werden. Folgt man dieser Auffassung, dann würden in der Vereinbarung nicht – wie bisher zumeist üblich – technische Einrichtungen, verwendete Software und vor allem die erlaubte Datenerfassung und -auswertung im Detail und abschließend festgeschrieben, sondern es werden stattdessen lediglich Grundsätze für den Einsatz eines Systems und dazu noch Regeln und Verfahren der Konfliktlösung vereinbart.

Berücksichtigt man die stürmische Entwicklung der Geschäftsabwicklung übers Internet, das so genannte eBusiness, wäre eine solche dynamische, dieser Entwicklung folgende Vereinbarung sicher auch beim Thema eMail und Intranet das Gegebene.

Die elektronische Post wurde ursprünglich ja als flüchtiges Medium entwickelt. Verbunden mit dem Charme der



›Smileys‹ und reichlicher Tippfehler drückten eMails persönliche Stimmungen aus und bedurften allein schon deshalb des Schutzes persönlicher Kommunikation. Nach Etablierung des Gesetzes zur digitalen Signatur (= zertifizierte ›elektronische Unterschriften‹) und jüngst der Verabschiedung des ›Fernab-

satzgesetzes werden nun voraussichtlich aber auch »offizielle« Geschäftsbeziehungen zunehmend elektronisch abgewickelt werden. Manche eMails können dann nach wie vor der Sphäre flüchtiger persönlicher Kommunikation, andere aber eher der Sphäre offizieller Geschäftspost zugerechnet werden. Die strengen Maßstäbe an die Vertraulichkeit, wie sie vom Bundesverfassungsgericht für den Telefonverkehr entwickelt worden sind, wird zukünftig dann zwar noch für einen Teil der elektronischen Post in unveränderter Weise zu reklamieren sein, sie werden sich aber nur schwerlich auch für eMails als ausgesprochener Geschäftspost aufrecht erhalten lassen.

Gleiches gilt für die Nutzung von so genannten Tele-diensten (z. B. Informationsangebote über das Internet). Neben dem, was das »große« Internet hier zu bieten hat, gibt es auch immer öfter ähnliche Angebote von Unternehmen für die bei ihnen Beschäftigten (z. T. auch in deren Eigenschaft als Kunden). Zum Teil werden Telekommunikationsdienste (z. B. Telefon, eMail) wie auch Teledienste (z. B. Zugang zum Internet) von Konzernmüttern oder spezialisierten Konzern-töchtern für alle Beschäftigten eines Konzerns angeboten und abgewickelt. Je nach rechtlicher Konstruktion verschieben sich dabei auch die zu berücksichtigenden Telekommunikations- und Teledienste-Datenschutzbestimmungen. Auch um dieser Dynamik gerecht zu werden, empfehlen sich auf Entwicklung und Anpassung angelegte Vereinbarungen.

Nicht zuletzt entfele mit einer dynamischen Vereinbarung auch die Umständlichkeit, jede neue Nutzung betrieblicher Kommunikationsnetze mit einer neuen Vereinbarung regeln zu müssen (wenngleich diese Möglichkeit



letztlich – beispielsweise in massiven Konfliktfällen – natürlich immer offen bleibt).

Eine solche Vereinbarung könnte dann folgende Klauseln enthalten:

**(1) Dynamisierungsklausel**

*Bei Planungen hinsichtlich neuer oder zu ändernder Intranet-Anwendungen wird von Geschäftsleitung und Betriebsrat (BR) gemeinsam überprüft, ob die vereinbarten Grundsätze zum Daten- und Persönlichkeitsschutz eingehalten sind. Will die Geschäftsleitung von den vereinbarten Grundsätzen abweichen, oder macht der BR geltend, dass Abweichungen von diesen Grundsätzen zu erwarten sind, so wird hierüber mit dem Ziel einer einvernehmlichen Regelung verhandelt. Diese Regelung wird neuer Bestandteil der Vereinbarung. Systemnutzungen ohne Einvernehmensregelung sind unzulässig.*

**(2) Verpflichtung der Systemadministratoren**

*Die Systemadministratoren werden darauf verpflichtet, die bei der Nutzung des Intranets und Internets anfallenden Benutzerdaten nicht zum Zweck der Leistungs- und Verhaltenskontrolle der Beschäftigten zu nutzen. Sie haben eine entsprechende Verpflichtungserklärung zu unterschreiben. Sie werden hinsichtlich der Einhaltung des Fernmeldegeheimnisses und Datenschutzes nach TKG und TDDSG geschult und auf die strafrechtlichen Konsequenzen hingewiesen. Die Weitergabe von Benutzerdaten und jede Form personenbezogener Auswertung der Benutzerdaten bedarf der Zustimmung des BR bzw. einer Regelung nach (1). Der Betriebsrat kann die Abberufung eines Systemadministrators verlangen, wenn der begründete Verdacht auf Verstoß gegen die genannten Gesetze und die abgeschlossene Betriebsvereinbarung besteht. Im Streitfalle entscheidet die Einigungsstelle.*

**Grundsätze zum Daten- und Persönlichkeitsschutz**

UM DIE IM ERSTEN TEIL dieses Artikels (in CF 6/2000 ab Seite 12) vorgestellten Bestimmungen und Gesichtspunkte in die betriebliche Technikgestaltung einfließen zu lassen, empfiehlt es sich, in eine Vereinbarung zur eMail- und Internet-Nutzung folgende Grundsätze zum Daten- und Persönlichkeitsschutz aufzunehmen:

**(3) Ausschluss der Leistungs- und Verhaltenskontrolle**

*Die bei der Nutzung von eMail, der Intranet- und der Internet-Nutzung anfallenden personenbezogenen Daten (Protokoll- und Verbindungsdaten) dürfen nicht zur Leistungs- und Verhaltenskontrolle der Mitarbeiter verwendet werden. Personenbezogene Daten, die zur Sicherstellung eines ordnungsgemäßen*



Betriebs von Telekommunikations- und Telediensten erhoben und gespeichert werden, unterliegen der Zweckbindung nach § 31 BDSG.

### **(4) Erlaubte Nutzung der Protokoll Daten**

So nicht anders vereinbart, werden Protokoll Daten ausschließlich zur

- Abrechnung der Internet-Nutzung,
- Gewährleistung der Systemsicherheit,
- Steuerung der Lastverteilung im Netzwerk und Optimierung des Netzes und zur

tiertes Vertraulichkeit. Allen Mitarbeitern sind zu diesem Zweck persönliche Codes und Verschlüsselungsverfahren zur Verfügung zu stellen. Für unternehmensexterne Kommunikation ist grundsätzlich Verschlüsselung und damit Wahrung der Vertraulichkeit wie der Datensicherheit vorzusehen.

### **(8) Lösungsfristen**

Protokoll Daten, die für Abrechnungszwecke benötigt werden, sind spätestens 80 Tage nach Rechnungslegung zu löschen. Alle anderen personenbeziehbaren

zierten Rechtssituation im Einzelfall – der Betriebsrat je nach betrieblichen Umständen und Branche ganz unterschiedliche Schutzniveaus erreichen.

### **Zur nicht-geschäftlichen Internet-Nutzung**

In vielen Betrieben – gerade auch denen der IT-Branche – wird eine Unterscheidung zwischen dienstlicher oder privater Nutzung der eMail-Server und auch des Internet-Zugangs nicht gemacht. Hierin spiegelt sich die Haltung wieder, dass es allein auf die Ergebnisse der Arbeit ankomme, die Kosten für eine eventuell auch private Nutzung der betrieblichen Kommunikationsmöglichkeiten aber vernachlässigt werden könnten. Gibt es keine Unterscheidung zwischen privater und dienstlicher Nutzung, sollte eine Vereinbarung die Vertraulichkeit der Nutzung von eMail und Internet *umfassend* festschreiben. Ausnahmen hiervon – unter weitestgehender Wahrung der Persönlichkeitsrechte einzelner Beschäftigter – wären dann nur mit Zustimmung des Betriebsrats vorzusehen, und auch das nur dann, wenn zum Beispiel Fragen der Datensicherheit oder Wirtschaftlichkeit dies im Einzelfall erfordern. Eine (etwa aus Gründen der Reklamationsüberprüfung) eventuell notwendige Speicherung der elektronischen Post wäre dezentral (also z.B. am einzelnen Arbeitsplatz) zu organisieren und zu vereinbaren. Wünschenswert, aber sicher nicht in jedem Betrieb durchzusetzen, wäre folgende Festlegung:

## **Gibt es keine Unterscheidung zwischen privater und dienstlicher Nutzung sollte eine Vereinbarung doch die Vertraulichkeit der Nutzung von eMail und Internet/Intranet umfassend festschreiben.**

– Analyse und Korrektur von technischen Fehlern genutzt.

### **(5) Beweisverwertungsverbot**

Der Zugriff auf Protokoll Daten ist auf Systemadministratoren beschränkt; für diese gilt Regelung (2). Sofern zu Zwecken der Fehleranalyse und Analyse der Systemsicherheit in begründeten Fällen von den Systemadministratoren Auswertungen und Rückgriffe auf die einzelnen Protokollzeilen vorgenommen werden, sind personalrechtliche Konsequenzen aus den hierbei gewonnenen personenbezogenen Informationen ausgeschlossen.

### **(6) Ausschluss von der Protokollierung**

Unternehmensinterne eMails und unternehmensinterne Nutzung von Telediensten werden nicht protokolliert, bzw. umgehend automatisch gelöscht.

### **(7) Verschlüsselung**

Als Entwurf gekennzeichnete Ausarbeitungen sowie die Inhalte von eMails unterliegen auf Wunsch technisch garan-

tiertes Vertraulichkeit. Allen Mitarbeitern sind zu diesem Zweck persönliche Codes und Verschlüsselungsverfahren zur Verfügung zu stellen. Für unternehmensexterne Kommunikation ist grundsätzlich Verschlüsselung und damit Wahrung der Vertraulichkeit wie der Datensicherheit vorzusehen.

### **(9) Unbeschränkter Internet-Zugang**

Sofern ein Internet-Zugang betriebsbedingt benötigt oder auch vom Betrieb bereit gestellt wird, findet keine Beschränkung oder Kontrolle des Informationsverhaltens statt.

## **Regelungen bei unterschiedlichem Schutzanspruch**

DIE VORGENANNTE Grundsätze werden erfahrungsgemäß nicht in allen Betrieben durchzusetzen sein. Je nach Betrieb (zum Teil auch in Abhängigkeit von der Branchenzugehörigkeit) versuchen einzelne Geschäftsleitungen ausgesprochen einengende Regelungen zur eMail- und Internet-Nutzung durchzusetzen und umfassende Kontrollen zu etablieren. Wenn es also dem Betriebsrat nicht gelingt, die weitgehenden Schutzrechte des vorangegangenen Abschnitts durchzusetzen, wird es darauf ankommen, doch möglichst weitgehende Schutzrechte in einer Vereinbarung zu verankern. Dabei wird – wegen der kompli-

*Den Beschäftigten wird das Recht eingeräumt, Telekommunikations- und Teledienste für nicht geschäftliche Zwecke während der Arbeitszeit zu nutzen, sofern dadurch die beruflichen Aufgaben nicht beeinträchtigt werden.*

### **Zur Gebührenermittlung**

Kann eine solche großzügige Regelung betrieblich nicht durchgesetzt werden, könnte eine rein formale Trennung von dienstlicher und mehr privater Nutzung der betrieblichen elektronischen

Kommunikationseinrichtungen vorgenommen werden. Dies wäre möglich, indem zusätzlich zur dienstlichen noch eine private eMail-Adresse im Betrieb vorgehalten wird und indem für die Internet-Nutzung unterschiedliche Passwörter für privates und dienstliches ›Surfen‹ vergeben werden. Das bedeutet aber nicht, dass sich Daten- und Persönlichkeitsschutzfragen nur auf diese privaten Bereiche beziehen. Auch für dienstliche eMails wird ein generelles Mitlesen seitens der Vorgesetzten vom Betriebsrat nicht akzeptiert werden können – ähnlich wie eine generelle Video-Überwachung oder ein generelles Mithören dienstlicher Telefonate unzumutbar ist (geschweige denn erlaubt wäre). Dies macht dann allerdings Regelungen erforderlich, elektronische Dienstpost für den Fall des Falles verfügbar zu halten und – wenn nötig – zu archivieren. In einer Vereinbarung sollte dann beispielsweise beschlossen werden:

*Für die Gebührenermittlung privater Nutzung von Telekommunikations- und Telediensten können die Downloadzeiten und die übertragenen Datenmengen als Monatssumme pro Anschluss ausgegeben werden. Auf Wunsch des Beschäftigten können auch Protokollzeilen aufgeschlüsselt werden. Die Protokolldaten werden spätestens 80 Tage nach Rechnungslegung vollständig gelöscht.*

### **Zur ›kumulierten Nutzungsstatistik‹**

Rechtlich nicht zu beanstanden wäre, wenn in gewissem Umfang (etwa aus Kostengründen) auch die dienstlichen Anschlüsse einer Analyse unterzogen werden und kumulierte (zusammengerechnete) statistische Daten über die Kostenentwicklung in einzelnen Abteilungen oder sogar am einzelnen Arbeitsplatzrechner gesammelt werden. In diesem Falle könnte in der Vereinbarung festgeschrieben werden:

*Für interne Leistungsverrechnung der dienstlichen Anschlüsse dürfen Monatssummen der Download-Zeiten und -Datenmengen pro Anschluss erfasst werden, wobei die Wiedergabe der aufgesuchten Internet-Adressen ausgeschlossen wird.*

### **Zum Ausschluss willkürlicher Sanktionen**

Im Gegensatz zu den USA und vielen anderen Industrieländern wird in Deutschland von Seiten der Finanzämter ein unversteuertes Ermöglichen privater Internet-Nutzung im Betrieb als ›geldwerte Leistung‹ in Frage gestellt. Aus formalrechtlichen Gründen hat dies in vielen Betrieben dazu geführt, die private Nutzung dienstlicher Informations- und Telekommunikationsanlagen generell zu verbieten. Die betriebliche Praxis in solchen Betrieben sieht aber deren generelle oder weitgehende Duldung vor. Mit dem formalen Verbot erhöhen sich aber die zulässigen Zugriffs- und Kontrollmöglichkeiten der Vorge-

setzten und Geschäftsleitungen. Um plötzlichen Sanktionen, willkürlichem ›Mobbing‹ oder dem ›Abschießen‹ missliebiger gewordener Beschäftigter

*Im Falle des begründeten Verdachts der missbräuchlichen Nutzung betrieblicher Einrichtungen können personenbezogene Protokolldaten unter Zustimmung*

*gesetzt und ausgewertet werden. Sie sind unverzüglich zu löschen oder zu anonymisieren.*

## Bei Internet-Nutzung ist auch die Frage des (un-)kontrollierten Zugangs zu den Inhalten wichtig. Eine unbegrenzte Nutzung für beliebige Beschäftigte ist aber nicht erzwingbar.

vorzubeugen, könnte folgende Vereinbarung getroffen werden:

*Im Falle des begründeten Missbrauchsverdachts betrieblicher Einrichtungen wird der Beschäftigte auf den Verdacht hingewiesen. Im Wiederholungsfalle kann unter Beteiligung des Beschäftigten und eines zuständigen Betriebsrats das Protokoll der Internet-Nutzung des vergangenen Monats eingesehen und ausgewertet werden. Personalrechtliche Maßnahmen hieraus haben die betriebliche Praxis der Nutzung dieser Dienste zu berücksichtigen und bedürfen der Zustimmung des BR.*

### Zur Missbrauchskontrolle

Wenn Betriebe ein Verbot privater Nutzung betrieblicher Telekommunikationsdienste wie Internet-Zugänge aus betriebswirtschaftlicher Kosteneinsparung verfügt haben, wollen sie diese Verbote in der Regel auch strikt durchsetzen. Aber: Der Umstand, dass private Nutzung verboten ist, heißt durchaus nicht, dass eine generelle Überwachung und Kontrolle des Kommunikationsverhaltens einzelner Beschäftigter zulässig wäre. Verdachtskontrollen und Sanktionen für missbräuchliche Nutzung jedoch sind viel schwerer abzuwehren, wenn die private Nutzung prinzipiell untersagt ist. In diesem Falle bietet sich folgende Regelung an:

*mung des Betriebsrats bis zu drei Monate aufbewahrt werden. Verdächtige Mitarbeiter sind über die mögliche Auswertung der Protokolldaten zu informieren. Eine Auswertung der gespeicherten Daten erfolgt nur unter Zustimmung und im Beisein des Betriebsrats bei begründetem Verdacht auf wiederholten Missbrauch.*

### Zur Begrenzung von Internet-Zugängen

Bei Internet-Nutzung ist auch die Frage des (un-)kontrollierten Zugangs zu Inhalten wichtig. Eine unbegrenzte Internet-Nutzung für beliebige Beschäftigte ist allerdings im Wege der Mitbestimmung nicht erzwingbar. Abgeleitet aus dem Direktionsrecht steht es dem Unternehmen frei, die Freishaltung je nach Arbeitsaufgabe einzugrenzen oder durch Kontroll-Software das Herunterladen nicht benötigter oder unerwünschter Inhalte aus dem Internet automatisch zu sperren. Da auf diesem Wege aber das versuchte Aufrufen gesperrter Inhalte erfasst werden könnte, kommt also wieder die Möglichkeit der Verhaltenskontrolle ins Spiel, somit greift das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG. Für diesen Fall sollte in die Vereinbarung folgender Passus aufgenommen werden:

*Sperrungen oder Kontrollen entgegen dem Grundsatz (siehe Punkt 9) bedürfen der Zustimmung des BR. Bei Sperrungen aus arbeitsökonomischen Gründen dürfen die anfallenden Protokolldaten nicht zur individuellen Verhaltenskontrolle ein-*

## Weitere Vereinbarungen zu Einzelfragen

JEDE VEREINBARUNG WIRD natürlich den Geltungsbereich, den Gegenstand und die Zweckbestimmung, Definitionen, Inkrafttreten, Verfahren für Meinungsverschiedenheiten, Kündigung, Nachwirkung und einiges andere enthalten (ein Beispiel dafür kann die in CF 3/2000 abgedruckte ›klassische‹ Vereinbarung zur Einführung und Anwendung eines Intranets sein). Darüber hinaus sollten einige weitere Punkte in unserer Vereinbarung zur eMail- und Internet/Intranet-Nutzung geklärt werden:

### Information und Schulung der Beschäftigten

*Die Beschäftigten werden über die besonderen Datenschutz- und Datensicherheitsprobleme bei der Nutzung von Telekommunikations- und Telediensten unterrichtet. Sie werden für den sicheren und wirtschaftlichen Umgang mit dem Internet qualifiziert (Internet-Führerschein), über die einschlägigen Datenschutzvorschriften informiert, in der sicheren Nutzung von Verschlüsselungsverfahren geübt und auf die notwendige Netiquette [siehe auch den Beitrag ab Seite 35] verpflichtet.*

### Fehlerbehebung

Da Systemadministratoren technisch in der Lage sind, im Rahmen des Intranets auf die am Arbeitsplatzrechner verfügbaren Daten zuzugreifen und Konfigurationen zu ändern – und dies aus Systemsicherheitsgründen und zur Behebung von Fehlern und Ähnlichem gegebenenfalls auch ausüben – ist eine Regelung erforderlich, die die Beschäftigten über diese zulässigen Eingriffe aktuell informiert:

*Erfolgen notwendige Eingriffe der Systemadministratoren über das Intranet am Einzelplatzrechner, so ist dies vorher dem Beschäftigten anzuzeigen.*

### **Kontrolle der Einhaltung**

Es ist für den Betriebsrat nicht einfach, die Einhaltung dieser Vereinbarung zu kontrollieren und Verstöße von Geschäftsleitung und Systemadministratoren gegen die Bestimmungen der Vereinbarung zu bemerken. Dies gelingt in Zusammenarbeit mit dem betrieblichen Datenschutzbeauftragten oder durch Hinzuziehung von externen Sachverständigen möglicherweise besser. Auch hierzu sollte die Vereinbarung also Bestimmungen enthalten:

*Der BR kann zur Durchführung seiner Aufgaben nach Abstimmung mit der Geschäftsleitung Sachverständige seiner Wahl hinzuziehen. Diesem Sachverständigen sind alle für die Überwachung dieser BV notwendigen Unterlagen zugänglich zu machen und entsprechende Kontrollmöglichkeiten einzuräumen. Der BR hat auch das Recht, die Einhaltung dieser BV unter Hinzuziehung des betrieblichen Datenschutzbeauftragten personenbezogen zu überprüfen.*

### **Beweisverwertungsverbot**

Es empfiehlt sich auch, ein eigenes Beweisverwertungsverbot aufzunehmen. Kommt es zu personellen Maßnahmen und vielleicht auch zu Rechtsstreitigkeiten, so wird üblicherweise von einem Beweisverwertungsverbot für unrechtmäßig gewonnene personenbezogene Daten auszugehen sein. Eine Vereinbarungsbestimmung in diesem Sinne kann bereits im Vorfeld Klarheit verschaffen:

*Werden Erkenntnisse über Leistung und Verhalten von Beschäftigten unter Missachtung oder Verletzung der Bestimmungen der BV gewonnen, so sind sie zur Begründung personeller Maßnahmen als Beweismittel nicht zulässig.*

### **Nutzung des Intranets für Zwecke des Betriebsrats**

Um annähernde ›Waffengleichheit‹ herzustellen, ist es wichtig, die moder-

nen Informations- und Kommunikationstechniken auch für die Betriebsratsarbeit einsetzen zu können. Immer wieder machen Betriebsräte allerdings die Erfahrung, dass sie die ihnen nach BetrVG zustehende materielle Ausstattung erst vor Gericht einklagen müssen (siehe dazu ›Mit eMail und Internet‹ in CF 3/2000 ab Seite 33). Letztlich läuft es dabei darauf hinaus, dass unternehmensübliche Arbeitsmittel auch dem Betriebsrat zur Verfügung gestellt werden müssen:

*Der BR erhält auf Wunsch die gleichen eMail-Möglichkeiten zur Information der Beschäftigten wie die Geschäftsleitung. Der BR erhält unbeschränkten Zugang zu den Informationen des Internet. Der BR erhält auf Wunsch die Möglichkeit, in eigener Verantwortung Teledienste für die Beschäftigten zu entwickeln und vorzuhalten.*

Mit Letzterem ist zum Beispiel ein eigenes Informationsangebot des Betriebsrats für die Beschäftigten gemeint, das neben aktuellen Nachrichten aus der Betriebsratsarbeit auch Gesetzestexte und abgeschlossene Betriebsvereinbarungen enthalten könnte (siehe dazu ›Interessenvertretung im Intranet‹ in CF 5/2000 ab Seite 32).

---

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](mailto:kiper@btq.de)

---

