Manuel Kiper

Elektronische Kommunikation

Gläserne Betriebe – gläserne Belegschaften

Seit dem Bundesverfassungsgerichtsurteil vom 15. Dezember 1983 (Volkszählungsurteil) wird Datenschutz in Konkretisierung des Persönlichkeitsrechts des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG als Grundrecht auf informationelle Selbstbestimmung verstanden. Datenschutz als Schutz der Persönlichkeitsrechte korrespondiert heute aber auch mit der wirtschaftlichen Erfordernis der Datensicherheit, in der globalisierten Datenkommunikation die Integrität der Information und Kommunikation, die Vertraulichkeit, die Unbeobachtbarkeit, die Transparenz zur Beweissicherung etc. systematisch zu sichern.

Der Gesetzgeber hat seit 1996 mit dem Telekommunikationsgesetz, dem Teledienstedatenschutzgesetz wie mit dem Gesetz zur digitalen Signatur den rechtlichen Rahmen für Datenschutz und Datensicherheit weiter entfaltet und zugleich diesbezüglich Verschärfungen im Strafgesetzbuch vorgenommen. In den Unternehmen ist das Wissen um die neuen gesetzlichen Rahmensetzungen und Detailvorschriften auf seiten des Managements, der DV-Verantwortlichen wie auf seiten der Interessenvertretungen und der Beschäftigten höchstens in Ansätzen vorhanden. Gleichzeitig werden Datenschutz und Datensicherheit für den wirtschaftlichen Erfolg vieler Unternehmen wie für das funktionsfähige Handeln von Behörden immer wichtiger. Die Ausweitung von Mobil- und Telearbeit, die Durchsetzung von Telebanking und E-Kommerz wie die Entwicklung des gesamten Elektronischen Geschäftsverkehrs wird ohne entsprechende Verstärkung des persönlichen Datenschutzes wie der betrieblichen Datensicherheit nicht erfolgreich zu bewerkstelligen sein.

Das kürzliche Vorhaben von Mister Minit, die Mitarbeiter permanent mit Video zu überwachen, wurde zwar vom Kaufhof-Konzern abgeblockt. Eine solch offensichtliche lückenlose Überwachung des Verhaltens der Beschäftigten ist in Deutschland nicht zulässig. Die obersten Gerichte, Bundesarbeitsgericht wie Bundesverfassungsgericht schließen zwar im Einzelfall, insbesondere bei erheblicher Verdachtskontrolle, eine punktuelle und vorübergehende Video- wie auditive Überwachung nicht aus. Generalisierte Videobeobachtung oder Abhören haben sie aber grundsätzlich als mit dem Persönlichkeitsrecht und dem Recht auf informationelle Selbstbestimmung nicht vereinbare 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.[1] 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.[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.

Die in Computernetzen und digitalen Telefonanlagen mögliche unsichtbare Leistungs- und Verhaltenskontrolle wird dennoch immer ausgeklügelter. E-Mails können an verschiedenen Servern mitgelesen, das individuelle Aufrufen einzelner Web-sites lückenlos an anderen Rechnern kontrolliert, die Bildschirmarbeit eines Mitarbeiters mit geeigneter Software für sog. Screen-shots von Vorgesetzten zeitgleich transparent gemacht werden.[3] Nach einer Studie der American Management Association überwachen in den USA bereits 27% der Großunternehmen die Mail-Aktivitäten ihrer Mitarbeiter.[4] Wie wenig anonym das Arbeiten in einer qua Internet vernetzten Welt ist, zeigte nicht zuletzt die Verfolgung des jüngsten gefährlichen Virus Melissa. Durch Rückverfolgung des sich lawinenartig ausbreitenden Virus konnte innerhalb weniger Tage sein geistiger Urheber dingfest gemacht werden.[5] Jeder Computer firmiert im weltweiten Internet unter einer bestimmten codierten Adresse, die bei jedem Datentransfer automatisch mitübertragen wird. Dadurch werden enorme Datenspuren hinterlassen.

Die privatwirtschaftliche Auswertung solch individuell zuordenbarer Datenspuren, das Data mining, wurde inzwischen sogar ein eigener lukrativer Markt.[6] Zum gläsernen Bürger und gläsernen Mitarbeiter gesellt sich der gläserne Konsument. Durch zunehmendes Angebot von Telediensten in den Unternehmen auch für ihre eigenen Mitarbeiter werden Mitarbeiter nicht nur in ihrer Arbeitsleistung, sondern auch in ihrer Kundenqualität durchsichtig.

Datenschutz- und Datensicherheitsvorschriften in der neuen Telekommunikations- und Multimediagesetzgebung

Unverändert basiert der Datenschutz in Unternehmen auf dem Bundesdatenschutzgesetz (BDSG) und Betriebsvereinbarungen. Grundlage des betrieblichen Datenschutzes für die Telekommunikation sind jedoch Gesetze, die erst in den letzten Jahren im Zusammenhang mit der sogenannten Liberalisierung des Telekommunikations-Sektors erlassen wurden. Bei diesen Gesetzen 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.[7]

Telekommunikations- und Multimediagesetzgebung

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.

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 Nutzungs-

möglichkeiten der elektronischen Informations- und Kommunikationsdienste zu schaffen«. Zusätzlich wurden im ›Mediendienstestaatsvertrag‹ noch die an die Allgemeinheit gerichteten Informations- und Kommunikationsdienste, die sogenannten Mediendienste geregelt. Die folgende Übersicht gibt einen Überblick über Definitionen und Zuordnungen von Netzaktivitäten zu unterschiedlichen Gesetzesregelungen.

Erschwerend kommt zu dieser Vielfalt an Regelungen und Definitionen hinzu, dass es auch noch Überschneidungen gibt, weil bei der Nutzung von Telediensten z.B. gleichzeitig auch Telekommunikationsdienste genutzt werden.[8] Die in den aufgeführten Gesetzen enthaltenen Regelungen können für den betrieblichen Datenschutz im Einzelfall alle von Bedeutung sein.

Neben den gesetzlichen Regelungen des Telekommunikations- und Multimediarechts sind darüber hinaus bei der Datenverarbeitung auch die verschärften Bestimmungen des Strafgesetzbuchs (StGB) zu berücksichtigen. 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.

Telekommunikationsgesetz

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

Zunächst soll geklärt werden, 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 diejenigen, die – wie es in § 89 Abs. 1 TKG heißt – »geschäftsmäßig Telekommunikations-Dienste erbringen«. Und das 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 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«.[9]

Jedes Unternehmen, jede Stadtverwaltung oder Universität, jedes Krankenhaus oder Hotel, das seinen Angestellten (bei Privattelefonie) oder Kunden – also einem ›Dritten‹ – regelmäßig das Telefonieren erlaubt, erbringt also »geschäftsmäßig Telekommunikation« und unterliegt somit dem TKG. 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.

Fernmeldegeheimnis in der Telekommunikation

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 Telefonaten 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.

Zusammenfassend läßt sich sagen: Wenn und soweit vom Arbeitgeber die private Nutzung der betrieblichen Telekommunikations-Anlagen für interne oder externe Kommunikation gestattet wird, 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 Nutzung der Telekommunikationsanlagen durch die Beschäftigten entbindet dann nicht von der Verpflichtung zur Einhaltung des Fernmeldegeheimnisses und der Datenschutzvorschriften nach dem TKG, wenn eingehende Anrufe und E-Mails – die ja auch privaten Charakter haben könnten – automatisch an die Nebenstelle vermittelt werden (Durchwahl). Nur wenn der Arbeitgeber die strikte Nutzung der betrieblichen TK-Anlagen allein für dienstliche Zwecke erzwingt und organisatorisch sicherstellt, werden in Hinblick auf die Beschäftigten nicht mehr die Merkmale eines Telekommunikations-Dienstes ›für Dritte‹ erfüllt. Damit würden dann auch die Schutzbestimmungen des elften Teils des TKG entfallen.

Rechtsprechung zum Fernmeldegeheimnis

Gestützt wird die oben entwickelte weite Auslegung des Fernmeldegeheimnisses im TKG auch durch Entscheidungen höchster Gerichte. Entsprechende Rechtsprechung hat sich hinsichtlich der Kontrolle des Telefonierverhaltens herausgebildet. So hat das BVerfG in Korrektur einer anderslautenden Entscheidung des BAG festgehalten, dass ein heimliches Mithören oder Aufzeichnen des Inhalts eines Telefonats des Arbeitnehmers dessen Einwilligung voraussetzt und dass diese nicht stillschweigend als erteilt ange-

nommen werden kann, wenn der Arbeitnehmer um die Abhörmöglichkeit weiss.[10]

Entsprechend hat das BAG bei heimlichem Mithörenlassen von Telefongesprächen eine Persönlichkeitsrechtsverletzung erkannt. Heimliches Mithörenlassen von Telefongesprächen zwischen Arbeitnehmer und Arbeitgeber ist unzulässig. Auf diese Weise erlangte Beweismittel dürfen nicht verwertet werden. Bei Mithören ist der Gesprächspartner vorher darüber zu informieren. Gesprächspartner am Telefon müssen sich nicht ihrerseits vorher vorsorglich vergewissern, dass niemand mithört.[11]

So hat auch das Bundesarbeitsgericht im Oktober 1997 entschieden, dass auch im beruflichen Bereich das Recht am gesprochenen Wort als Teil des allgemeinen Persönlichkeitsrechts zu gewährleisten ist.[12] Nach Urteil des Bundesverfassungsgerichts stellt 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 dar.[13] 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.

Bereits seit dem sogenannten ›Fangschaltungsbeschluss‹ des BVerfG 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 Fernmeldegeheimnis« sind.[14] Insofern hat auch das BAG eine Betriebsvereinbarung, die es dem Arbeitgeber bei einer ACD-Anlage[15] erlaubt, externe Telefongespräche der Arbeitnehmer in deren Gegenwart zu Ausbildungszwecken mitzuhören, in diesem Fall für zulässig erklärt.[16] Die Praxis, dass Mitarbeiter wie Kunden in Call-Centern gängigerweise extern abzuhören sind, wie es von der Panoramaredaktion im September 1999 öffentlich gemacht wurde[17], dürfte damit allerdings unvereinbar sein.

Eine Kontrolle des Telefonierverhaltens der Beschäftigten in Hinblick auf Missbrauch und Kostenverursachung wird in der Rechtsprechung andererseits für zulässig gehalten. Von unteren Arbeitsgerichtsinstanzen werden hier z.T. drastische Urteile gefällt, die allerdings vor Landesarbeitsgerichten üblicherweise nicht 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.[18] 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.[19] Kündigungsgrund sah das Arbeitsgericht Frankfurt am Main auch bei unbezahlten Telefonaten mit Australien insbesondere, wenn die Arbeitnehmerin erst nach einem Computerausdruck bereit war, das Telefonat zu bestätigen.[20] Desgleichen sah das Gericht Kündigungsgrund, wenn ein Arbeitnehmer auf Kosten seines Arbeitgebers telefonisch einem Nebenjob nachgeht.[21] Andererseits hat jüngst das Arbeitsgericht Frankfurt am Main entschieden: »Ist einem ArbN 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 ArbN 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 Arbgeb. gerichteten Straftat und eine außerordentliche Kündigung des Arbgeb., wenn der ArbN ohne Aufforderung des Arbgeb. die durch die Privatgespräche entstanden Kosten (hier: DM 66,51) nicht von sich aus erstattet«.[22] Das Oberlandesgericht Hamm entschied, dass ein leitender Angestellter durch Inanspruchnahme von Telefonsexgesprächen in »nicht unbeträchtlicher Höhe für private Zwecke« seine ihm verliehene Vertrauensstellung im Betrieb missbraucht habe und damit ohne Abmahnung entlassen werden könne.[23]

Landesarbeitsgerichtsentscheidungen hingegen sind bislang für die Beschäftigten glimpflicher ausgefallen. So entschied das LAG Niedersachsen, dass auch bei erwiesener Vielzahl von Privattelefonaten auf Arbeitgeberkosten eine verhaltensbedingte Kündigung erst zu rechtfertigen sei, wenn der Mitarbeiter vorher abgemahnt worden sei.[24] Das Landesarbeitsgericht Köln befand sogar: Erlaubt ein Arbeitgeber seinen Beschäftigten, private 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.[25]

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

Wahrung des Fernmeldegeheimnisses bei Telefon, Telefax und eMail

Gesetzlich durch das Fernmeldegeheimnis geschützt ist – wie bereits dargelegt – 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 den Unternehmen stellt also einen Eingriff in den Schutzbereich des allgemeinen Persönlichkeitsrechts der Arbeitnehmer dar. Bei ausgesprochener Geschäftspost sind solche Eingriffe allerdings zu Kontrollzwecken zulässig. Persönlich adressierte oder z.B. an den Betriebs- oder Personalrat gerichtete oder verschickte eMails unterliegen hingegen einem Schutz vor Überwachung, nicht nur des Inhalts, sondern auch der Verbindungsdaten.

Im Hinblick darauf, dass Telefaxgeräte vielfach frei zugänglich sind und dass E-Mails 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 Tele-

kommunikationsdiensten dient«, zu »angemessenen technischen Vorkehrungen oder sonstigen Maßnahmen« zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten und zum Schutz programmgesteuerter Telekommunikations- und Datenverarbeitungs-Systeme gegen unerlaubte Zugriffe.

Dabei sind zum Schutz des Fernmeldegeheimnisses organisatorisch-technische Maßnahmen wie Zutritts- und Zugriffsbeschränkungen ebenso vorzusehen wie Anonymisierungs-Maßnahmen und auch Verschlüsselungen. Dies sicherzustellen dürfte in vielen Unternehmen 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.[26] So dürfen beispielsweise eMails an namensbezogene Adressen (wie ›WalterMüller@t-online.de‹) nicht protokolliert werden.

Allerdings darf der Arbeitgeber nach Auffassung des Berliner Datenschutzbeauftragten einzelne dienstliche E-Mails einsehen, auch wenn sie an einen bestimmten Arbeitnehmer gerichtet sind. »Der Arbeitnehmer hat dem Arbeitgeber den Zugang zu solchen E-Mails zu eröffnen. Dagegen ist eine Auswertung des gesamten E-Mail-Verkehrs (etwa durch automatisches Scannen) durch den Arbeitgeber jedenfalls im Regelfall nicht gestattet.«[27] Ist die Kennzeichnung privater E-Mails systemtechnisch nicht vorgesehen, erstreckt sich die Geheimhaltungspflicht nach dem TKG auch auf den betrieblichen E-Mail-Verkehr. Ist hingegen die Privatnutzung des E-Mail-Systems betriebsintern mengenmäßig oder zeitlich limitiert und diese Regelung den Beschäftigten bekanntgegeben worden, sind allerdings »Missbrauchskontrollen durch das Beschäftigungsunternehmen zulässig«.[28]

Datenschutz bei Telediensten

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

Das IuKDG ist – wie schon kurz erwähnt – ein Artikelgesetz, mit dem sehr unterschiedliche Fragen in einem Gesetz geregelt wurden. Anzuwenden ist das IuKDG auf Telediente. Das sind (Artikel 1 § 2 Abs. 2 IuKDG) Telebanking und Telespiele, Verkehrs- oder Börsendaten und manches andere. Vor allem aber sind Telediente Angebote zur Nutzung des Internets oder weiterer Netze. Demnach ist ein Arbeitgeber, der seinen Beschäftigten eine nicht ausschließlich dienstliche Internet-Nutzung ermöglicht, also ein Telediente-Anbieter. Gleiches gilt für weitere Netze, also auch für firmeninterne Computernetze wie etwa ein Intranet. Wird hingegen in einem Konzern von einem Konzernservicebetreiber die Internetnutzung den Konzernmitarbeitern nur für betriebliche Zwecke zur Verfügung gestellt, so ist nach Auffassung z.B. des Baden-Württembergischen Innenministeriums das einzelne Beschäftigungsunternehmen Nutzer und nicht der einzelne Beschäftigte, so dass – zwar unter Mitbestimmungsvorbehalt – aber »die Daten grundsätzlich auch zur Kontrolle des Verhaltens und der Leistung verwendet werden dürfen«.[29] Dem wird von anderer Seite allerdings widersprochen und die Gültigkeit des TDG auch für unternehmensinterne Telediente reklamiert, »gleichgültig ob dieser im einzelnen Unternehmen oder im Konzernverbund genutzt wird«.[30] Ein Zugriff des Arbeitgebers auf E-Mails kann auch »aus Gründen der Systemsicherheit, dem Schutz vor Viren und dem Schutz vor Kosten- und Netzüberlastung« nicht völlig ausgeschlossen werden.[31]

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 **§§ 3 – 6 TDDSG** festgeschrieben:

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

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 auszuwerten. »Die Protokollierung der privaten Nutzung ist nur – soweit diese vorgesehen ist – zu Abrechnungszwecken gestattet«.[33] Entsprechenden Befürchtungen kann und sollte mit klaren Regelungen zwischen Betriebsräten und Arbeitgebern entgegen getreten werden.[34] 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.

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, Filter oder andere technische Mittel einsetzen, um den Zugriff auf bestimmte

Dienste und Netzressourcen zu begrenzen.

Ist die private Internet-Nutzung von Arbeitnehmern am Arbeitsplatz entweder erlaubt oder wird geduldet und wird diese 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).[35] Deutlich sollte aber auch sein, dass ein Arbeitnehmer keinen Anspruch darauf hat, das Internet nach Belieben zu nutzen.

So müssen (und dürfen) auch strafbare Handlungen über E-Mail- oder Internet/Intranetnutzung nicht geduldet werden und sind insofern Missbrauchskontrollen und entsprechende Ahndung zulässig. Bei Verdacht auf strafrechtliche Vergehen von Mitarbeitern ist durch den Arbeitgeber ggf. die Polizei/Staatsanwaltschaft einzuschalten. Dies wäre z.B. 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.[36]
- unbefugt in fremde Dateien einzudringen,[37]
- beleidigende Inhalte auf seiner Web-Site anzubieten oder,[38]
- unkommentiert Links auf beleidigende oder sonstwie strafwürdige Inhalte setzt.[39]

Mitarbeiter verstoßen somit gegen ihre arbeitsvertraglichen Pflichten, wenn sie während der Arbeitszeit nicht-dienstliche Daten an ihrem Arbeitsplatz verarbeiten. So kann z.B. die Anlage von Dateien mit sexistischen oder rassistischen Witzen und deren Überspielung an Kollegen Grund für fristlose Kündigung sein.[40] 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.[41]

Zusammenfassung

Die systematische Überwachung, Kontrolle, Dokumentation und Auswertung des telekommunikativen Verhaltens von Mitarbeitern/innen ist weitgehend verboten, da das Fernmeldegeheimnis und das Persönlichkeitsrecht zu achten sind. Dies gilt, wenn und sofern private betriebliche Telekommunikation

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

Bezüglich dienstlicher Nutzung der betrieblichen Telekommunikationsanlagen gilt ein **Abwägungsprozess zwischen Direktionsrecht und Persönlichkeitsrecht.**

- Mithören ohne ausdrückliche Bekanntgabe ist nicht erlaubt.
- Mitlesen von E-Mails und Dateien durch Vorgesetzte ohne vorherige Bekanntgabe ist nicht erlaubt.
- Systematische Screen-shots (z.B. mit Cyber Patrol) sind nicht erlaubt.
- Für die Mailbox des BR/PR gilt weitgehende Meinungsfreiheit.
- Darüberhinaus gibt es besonders geschützte Personengruppen wie Betriebsärzte oder Mitarbeitervertretung, deren Rechte in besonderer Weise zu wahren sind.
- Jede Einführung oder zusätzliche Nutzung von technischen Einrichtungen unterliegt der Mitbestimmung des BR/PR. Ohne Zustimmung des BR/PR sind somit auch Sanktionen hinsichtlich des telekommunikativen Verhaltens der Beschäftigten hinfällig.
- Bei Verfehlungen sind Abmahnungen normalerweise nötig.

Eine **Mitarbeiterkontrolle** über Mithören bei Telefonnebenstellenanlagen, Mitlesen von E-Mails, Installieren von Videokameras oder Auswertung der Internetprotokolle ist allerdings nicht in jedem Fall dem Vorgesetzten untersagt. Überwachung, Kontrolle, Dokumentation und Auswertung des telekommunikativen Verhaltens ist erlaubt

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

Allerdings müssen auch bei dieser nach dem Direktionsrecht sanktionierten Kontrolle Persönlichkeitsrechte der Beschäftigten, die Rechte besonders geschützter Personengruppen und die Mitbestimmung des BR/PR geachtet werden. Bei Verdacht auf strafrechtliche Vergehen von Mitarbeitern ist eigenmächtige Überwachung durch den Arbeitgeber ohne Einschalten der Polizei/Staatsanwaltschaft nicht zulässig.

Zur Regelung der betrieblichen E-Mail- und Internetnutzung sollten Betriebsräte unbedingt auf den Abschluss von Betriebsvereinbarungen drängen. Eine Handlungshilfe hierzu kann von der BTQ Niedersachsen bezogen werden. In einer solchen Betriebsvereinbarung sollten auch Fragen der Verschlüsselung von E-Mails geregelt werden.

Persönlichkeitsdatenschutz und Verschlüsselung

Datensicherheit und Datenschutz sind nämlich für weitere Internetnutzung unabdingbare Voraussetzung. Konzerne wie Siemens, Enercon oder Boehringer hatten in der Vergangenheit unliebsame Erfahrungen mit der Schnüffelei des amerikanischen Geheimdienstes NSA gemacht.[42] Dass aber auch deutsche Geheimdienste internationalen Datenverkehr abhorchen, wurde einem größeren Publikum bekannt, als Ende letzten Jahres die Geldwäsche deutscher Banken

über Lichtenstein dokumentiert wurde. Die Daten waren vom Schwarzwald aus gewonnen worden. Mit 11.272 telefonüberwachten Anschlüssen[43] wurde – zu Strafverfolgungszwecken – in Deutschland 1998 sogar – gesetzlich sanktioniert – 10-mal soviel abgehört wie in den USA.

Eine Repräsentativuntersuchung privater und beruflicher Computernutzer ergab, dass lediglich 30 Prozent der Befragten sensible Daten in ihrem Computer ausreichend gegen einen Zugriff durch Unbefugte, z.B. über das Netz, geschützt hatten.[44] Untersuchungen des BSI zeichnen eine eher noch düstere Bilanz. Demnach würden lediglich vier Prozent der Unternehmen ihre E-Mails verschlüsseln. Datensicherheit ist aber zu einem ernstzunehmenden Faktor im globalen Wettbewerb geworden. Trotz erfreulicher Anstrengungen und Beschlüsse der Bundesregierung, Datenschutz und Datensicherheit in der Wirtschaft zu verbessern, verbleibt in Hinblick auf Persönlichkeitsschutz und Sicherung von Daten und Telekommunikation in den Betrieben Handlungsbedarf.

Die Enquete-Kommission des Deutschen Bundestags hatte nach zähem Ringen bereits einvernehmlich und mit den Stimmen der CDU/CSU entgegen der US-Politik und seinerzeitigen innenministeriellen Kryptoverbots-, Abhör- und Lauschplänen die Auffassung vertreten, »daß alle Maßnahmen und Hemmnisse, die einer breiten Nutzung von Verschlüsselungsverfahren entgegenwirken, vermieden und abgebaut werden müssen«.[45] Der amerikanische Sondergesandte David Aaron versuchte bereits kurz nach Regierungsantritt Bundesinnenminister Schily wie seinen Vorgänger auf die sogenannten Key-recovery-Initiative[46] einzuschwören, die es dem amerikanischen Geheimdienst NSA erlauben würde, u.a. von Bad Aibling in Bayern aus den gesamten europäischen auch verschlüsselten Datenverkehr für amerikanische militärische wie für wirtschaftliche Interessen mitzuhören und mitzulesen. Das Bundeskabinett hat demgegenüber am 2. Juni 1999 mit den »Eckpunkten der deutschen Kryptopolitik« zumindest in den kommenden zwei Jahren jede Beschränkung der Verschlüsselung ausgeschlossen.[47] Die Bundesregierung setzt sich jetzt dafür ein, dass »Verschlüsselungsverfahren und -produkte ohne Beschränkung entwickelt, hergestellt, vermarktet und genutzt werden dürfen«. Unter www.sicherheit-im-internet.de agiert jetzt die Initiative »Sicherheit in der Informationsgesellschaft« für die Bundesregierung.

Die Beschlusslage der G-8-Staaten zur gemeinsamen Spurensuche und Strafverfolgung im Datennetz, die Ende 1998 zufällig bekannt gewordenen Pläne der EU-Innen- und Justizminister für ein europaweites Abhören unter dem Stichwort Enfopol und die Weiterverfolgung der Verabschiedung einer Telekommunikationsüberwachungsverordnung[48] lassen die dargestellte wirtschaftlich motivierte Verbesserung der IT-Sicherheit seitens der Bundesregierung allerdings als halbherzig erscheinen.

Wenn so für Arbeitgeber wie Arbeitnehmer die Verschlüsselung der betrieblichen Kommunikation notwendig und wünschenswert ist, so sind doch auch hier Einbruchstellen nicht auszuschließen. Erst kürzlich offenbarte der Chaos-Computer Club, daß Microsoft mit seiner Verschlüsselungsschnittstelle Crypto-API in allen Windows-Betriebssystemen offensichtlich eine NSA-Hintertür einprogrammiert hat.[49] Im November 1999 musste das Bundesamt für Sicherheit in der Informationstechnik (BSI) sogar vor dem bekannten Verschlüsselungssystem PGP warnen. PGP wird heute als kommerzielles Produkt von der US-Firma Network Associates vertrieben, die eng mit der National Security Agency zusammenarbeitet. Das Bundesministerium für Wirtschaft und Technologie ist deshalb im November letzten Jahres dazu übergegangen, mit der OpenSource-Gemeinde[50] zu kooperieren und ein Verschlüsselungsprojekt ohne Geheimdienst-Hintertür zu fördern. Allerdings musste das Fazit gezogen werden: »Es gibt im Moment keine einfache und sichere Lösung der eMail-Kryptografiefrage für den Privatanwender.«[51]

Trotz amtlichem Segen für Verschlüsselung wird es eine hundertprozentige Sicherheit in der elektronischen Kommunikation auch zukünftig nicht geben. Fortschritte in der Kryptografie, die Gesetzgebung der letzten Jahre wie auch die Entwicklung der Rechtsprechung haben allerdings in den letzten Jahren dazu beigetragen, den Schutz und die Vertraulichkeit des elektronisch vermittelten Wortes und anderer Informationen erheblich zu verbessern. Hierzu gehört auch die strafrechtliche Bewehrung des Fernmeldegeheimnisses. Bis und ob aber Arbeitgeber wegen Verletzung des Fernmeldegeheimnisses durch Schnüffeln in E-Mails ihrer Mitarbeiter oder Mithören privater Gespräche am Arbeitsplatz mit strafrechtlichen Konsequenzen rechnen müssen, hängt auch davon ab, dass die neuen Bestimmungen breiter bekannt und in der betrieblichen Praxis umgesetzt werden. Das diffizile Abwägen zwischen Direktionsrecht einerseits und Persönlichkeitsschutz der Beschäftigten andererseits macht ein Aushandeln von Verfahrensregeln in Form von Betriebs- und Dienstvereinbarungen erstrebenswert, um manche Konflikte von vornherein auszuschalten. Die BTQ Niedersachsen gibt hierbei Hilfestellung und bietet eine ausführliche Handlungshilfe an.

Manuel Kiper u. Bruno Schierbaum: Arbeitnehmer-Datenschutz bei Internet- und E-M@ilnutzung – Handlungshilfe-; Edition BTQ Niedersachsen Nr. 3, 71 Seiten A4, April 2000, 25,- DM

---

1 Bundesarbeitsgericht, Urteil vom 29. Oktober 1997 – 5 AZR 508/96, siehe auch:. Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen, RDV 2/1998 S. 69-71
2 BVerfG Urteil vom 19.12.1991, BB 1992, S. 708
3 Vgl. hierzu: J. Haferkamp, Alles unter Kontrolle? in: Computer Fachwissen (CF) 12/98, S. 18-24
4 Unternehmen überwachen elektronische Post, in: Handelsblatt 3.2.00, S. 23
5 Müller, M., Vater gefunden, in: Handelsblatt 7.4.1999.
6 Vgl.: W. Fricke, Bergleute im Daten-Lagerhaus, Computer Fachwissen 4/99, S. 11-14
7 Vgl. hierzu: M. Kiper u. B. Schierbaum, Telekommunikationsgesetzgebung und Arbeitnehmerdatenschutz, in: Computer Fachwissen (CF) 8-9/99, S. 24-30
8 Vgl. G. Gounalakis u. L. Rhode, Elektronische Kommunikationsangebote zwischen Telediensten, Mediendiensten und Rundfunk, CR 8/1998, S. 487-492
9 BT-Drucks. 13/3609 vom 30.01.1996, S. 53
10 BVerfG. Beschluss vom 19.12.1991 – 1 BvR 382/85; vgl: RDV 1992, S. 128; ArbuR 5/1992, S. 158-160
11 BAG, Urteil vom 29.Oktober 1997 – 5 AZR 508/96; vgl.: Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen, RDV 2/1998 S. 69-71
12 Bundesarbeitsgericht, Urteil vom 29. Oktober 1997 – 5 AZR 508/96, siehe auch:. Persönlichkeitsrechtsverletzung durch heimliches Mithörenlassen von Telefongesprächen, RDV 2/1998 S. 69-71
13 BVerfG Urteil vom 19.12.1991, BB 1992, S. 708
14 BVerfGE 85,386, 396f
15 Automatic-Call-Distribution-Anlagen (wie sie in Call-Centern eingesetzt werden)
16 BAG, Beschluss vom 30. August 1995, – 1 ABR 4/95 – vgl: Mithören von Telefongesprächen zu Ausbildungszwecken, RDV 1/1996 , S. 30-33
17 vgl: Skript der PANORAMA-Sendung Nr. 579 vom 23.9.1999
18 Arbeitsgericht Frankfurt am Main, 18 Ca 7436/94
19 Arbeitsgericht Würzburg, 1 Ca 1326/97
20 Arbeitsgericht Frankfurt am Main, 11 Ca 5818/95
21 Arbeitsgericht Frankfurt am Main, 14 Ca 891/95
22 ArbG Frankfurt/Main v. 24.7.99, 2 Ca 8824/98
23 OLG Hamm, 8 U 194/98
24 LAG Niedersachsen, 13 Sa 1235/97
25 LAG Köln, 6 Sa 42/98
26 Vgl. z.B. E. G. Berger u. L. Gramlich, Corporate Networks im Telekommunikationsrecht, CR 3/1999, S. 150-159
27 Arbeitgeber als Anbieter von Telediensten, Jahresbericht 1998 des Berliner Datenschutzbeauftragten, zitiert nach: GDD-Mitteilungen 3-4/99, S.3-4
28 Innenministerium Baden-Württemberg, Hinweise zum Datenschutz für die Private Wirtschaft (Nr. 37), In: Staatsanzeiger Nr. 2 vom 18.1.99, S. 13; vgl.

Hinweise zum Datenschutz, RDV 3/1999, S. 131-135, hier S. 132

29 Innenministerium Baden-Württemberg, Hinweise zum Datenschutz für die Private Wirtschaft (Nr. 37), In: Staatsanzeiger Nr. 2 vom 18.1.99, S. 13; vgl. Hinweise zum Datenschutz, RDV 3/1999, S. 131-135

30 Marcus Kieper, Datenschutzrechtliche Bewertung von Proxy-Cache-Servern, in: Datenschutz und Datensicherheit 23 (1999) S. 591-593, hier 592

31 A. Müller, Datenschutz beim betrieblichen E-Mailing, RDV 5/1998, S. 205-212, hier S. 211

32 Landesbeauftragter für den Datenschutz Niedersachsen, Datenschutz bei Tele- und Mediendiensten, Hannover, 23.08.99

33 P. Gola, Neuer Tele-Datenschutz für Arbeitnehmer? Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MMR 6/1999, S. 322-330, hier S. 329

34 vgl.: Juristen empfehlen Firmen bei E-Mails eine klare Regelung, in: Handelsblatt 3.2.00, S. 23

35 Vgl. P. Gola, Neuer Tele-Datenschutz für Arbeitnehmer? in: MMR 6/1999, S. 322-330

36 Vgl..ArbG Braunschweig, Urteil vom 22.1.99 – 3 Ca 370/98; Ausserordentliche Kündigung wegen Kinderpornografie, Computer Fachwissen (CF) 10/99, S. 26

37 Vgl.: LAG Baden Württemberg, Urteil vom 11.1.1994 – 7 Sa 86/92; AG Osnabrück, Urteil vom 19.3.1997 – 1 Ca 639/96

38 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

39 Bay. OLG, Beschluss vom 11.11.1997, 4 St RR 232/97

40 Vgl.: LG Hamburg, Urteil vom 12.5.1998 – 312 O 85/98

41 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

42 vgl. U. Buse u. C. Schnibben, Der nackte Untertan, in: SPIEGEL 5.7.1999; O. Schröm, Verrat unter Freunden, in: DIE ZEIT, 30. 9.1999

43 J. Jacob, Telefonüberwachung evaluieren, in: Datenschutz und Datensicherheit 23 (1999), S. 666-667

44 H. W. Opaschowski, Der gläserne Konsument. Bestandsaufnahme und aktuelle Analysen zu den Themen Multimedia und Datenschutz. British American Tobacco (Germany), Freizeitforschungsinstitut, Hamburg 1998, S. 62

45 M. Kiper, M. Meister, J. Tauss, H.-O. Wilhelm, Sicherheit und Schutz im Netz, Enquete-Kommission, a.a.O., S. 173

46 dies bedeutet: Schlüsselhinterlegung beim NSA

47 R. Reimer, Deutsche Kryptopolitik: Endlich Klarheit, Datenschutz und Datensicherheit 23 (1999), S. 7

48 Mit Datum vom 12.4.99 ist ein Eckpunktepapier für eine neue gegenüber 1998 allerdings gemilderte Telekommunikationsüberwachungsverordnung (TKÜV) bekannt geworden; der 1998er Entwurf der TKÜV aus dem Hause Rexrodt hätte für die Wirtschaft Abhörmaßnahmen in Höhe von 40 Mrd. DM erforderlich gemacht, wurde aber nach massiven Protesten seitens der Grünen wie der Wirtschaft zurückgezogen.

49 D. Borchers, Das Vertrauen verschlüsselt sich, SZ 14.9.1999, S. V2/10

50 Softwareentwickler, die die Quell-Codes offenlegen (z.B. Linux)

51 www.sicherheit-im-internet.de, Pressemitteilung vom 22.11.1999