5401/01/DE/endg.
WP 55

Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten

Angenommen am 29. Mai 2002

Anmerkungen:

* Die Kapitel über die einzelnen Mitgliedstaaten können in Absprache mit den nationalen Vertretern noch geändert werden

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist das unabhängige Beratungsgremium der EU in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen durch die Direktion A (Funktionieren und Auswirkungen des Binnenmarktes - Koordinierung - Datenschutz) der Generaldirektion Binnenmarkt der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro Nr. C100-6/136.

Website: www.europa.eu.int/comm/privacy

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung und insbesondere Artikel 12 und 14 -

hat folgendes Arbeitsdokument angenommen:

[1] ABl. L 281 vom 23.11.1995, S. 31, verfügbar unter: http://europa.eu.int/comm/internal_market/de/dataprot/index.htm

ARBEITSDOKUMENT DER DATENSCHUTZGRUPPE NACH ARTIKEL 29[2] ZUR ÜBERWACHUNG UND KONTROLLE DER ELEKTRONISCHEN KOMMUNIKATION VON BESCHÄFTIGTEN

Zusammenfassung

Dieses Arbeitsdokument ergänzt die Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten[3] und leistet einen Beitrag zur einheitlichen Anwendung der einzelstaatlichen Maßnahmen, mit denen die Mitgliedstaaten die Datenschutzrichtlinie 95/46/EG[4] umgesetzt haben. Sie lässt die Anwendungen innerstaatlichen Rechts in mit dem Datenschutz verknüpften Bereichen unberührt.

Die Artikel 29-Datenschutzgruppe hat eine Untergruppe eingesetzt, die diese Frage prüfen soll[5], und ein **ausführliches Papier** angenommen, das im Internet unter folgender Adresse abrufbar ist[6]:

http://europa.eu.int/comm/internal_market/de/dataprot/wpdocs/index.htm

Die Artikel 29-Datenschutzgruppe hat in diesem Arbeitsdokument die Frage der Überwachung und Kontrolle der elektronischen Kommunikation am Arbeitsplatz durch den Arbeitgeber, mit anderen Worten die Überwachung des E-Mail-Verkehrs oder des Internetzugriffs von Arbeitnehmern untersucht.

---

2 Die Artikel 29-Datenschutzgruppe hat beratende Funktion, sie ist ein unabhängiges Gremium, das sich aus Vertretern der Datenschutzbehörden der Mitgliedstaaten zusammensetzt und unter anderem die Aufgabe hat, alle Fragen im Zusammenhang mit den zur Umsetzung der Datenschutzrichtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen.

3 Die am 13. September 2001 angenommene Stellungnahme ist unter folgender Internet-Adresse zu finden: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48de.pdf. Sie enthält eine gründliche Analyse der Anwendung der Vorschriften der Datenschutzrichtlinie (und insbesondere der Artikel 6, 7 und 8) zur Verarbeitung von Beschäftigtendaten.

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. ABl. L 281 vom 23.11.1995, S. 31.

5 Die Datenschutzbehörden folgender Länder haben an den Arbeiten dieser Untergruppe teilgenommen: AT, BE, DE, ES, FR, IR, IT, NL, UK.

6 Die Unterlage umfasst einen Anhang mit den wichtigsten Datenschutzvorschriften der Mitgliedstaaten, die für die Überwachung und Kontrolle der elektronischen Kommunikation am Arbeitsplatz von Bedeutung sind.

Vor dem Hintergrund der Rechtssprechung des Europäischen Gerichtshofs für Menschenrechte zu Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, anderer einschlägiger internationaler Rechtstexte und der Bestimmungen der Richtlinie 95/46/EG bietet dieses Arbeitsdokument Leitlinien und konkrete Beispiele für gesetzlich geregelte Überwachungsmaßnahmen und die annehmbaren Grenzen der Kontrolle der Arbeitnehmer durch den Arbeitgeber. Es sei darauf hingewiesen, dass in einigen Mitgliedstaaten die Rechtsvorschriften einen höheren Schutz vorsehen können als dieses Arbeitsdokument.

Arbeitnehmer geben ihr Recht auf Schutz der Privatsphäre und Datenschutz nicht allmorgendlich am Werkstor oder an der Bürotür ab. Sie haben eine berechtigte Erwartung, dass ihre Privatsphäre am Arbeitsplatz bis zu einem gewissen Grad gewahrt bleibt, da sie hier einen erheblichen Teil ihrer Beziehungen zu anderen Menschen entfalten. Dieses Recht muss jedoch gegen andere schutzwürdige Rechte und Interessen abgewogen werden. Dies gilt insbesondere für das Recht des Arbeitgebers, sein Geschäft bis zu einem gewissen Maß effektiv zu betreiben und vor allem für sein Recht, sich selbst vor der Haftung oder dem Schaden zu schützen, die das Verhalten seiner Arbeitnehmer verursachen kann. Diese Rechte und Interessen stellen einen legitimen Grund dar, der geeignete Maßnahmen zur Einschränkung des Rechts der Arbeitnehmer auf Schutz der Privatsphäre rechtfertigen kann. Das deutlichste Beispiel hierfür wären die Fälle, in denen der Arbeitgeber Opfer einer Straftat des Arbeitnehmers ist.

Beim Abwägen der verschiedenen Rechte und Interessen müssen jedoch einige Grundsätze berücksichtigt werden, insbesondere die Verhältnismäßigkeit. Es sollte klar sein, dass nicht jede Überwachungs- oder Kontrollmaßnahme, die als geeignet gilt, den Interessen des Arbeitgebers zu dienen, ein Eindringen in die Privatsphäre des Arbeitnehmers rechtfertigt. Jede Kontrollmaßnahme muss vor ihrer Einführung am Arbeitsplatz eine Reihe von Prüfungen durchlaufen, die in diesem Arbeitsdokument detailliert aufgeführt sind.

Die folgenden Fragen fassen die Art dieser Überprüfung zusammen:

a) Ist die Überwachungsmaßnahme für die Arbeitnehmer transparent?

b) Ist sie notwendig? Könnte der Arbeitgeber nicht mit traditionellen Überwachungsverfahren dasselbe Ergebnis erzielen?

c) Erfolgt die vorgeschlagene Verarbeitung personenbezogener Daten nach Treu und Glauben?

d) Entspricht sie den Bedenken, die sie zerstreuen soll?

Das Arbeitsdokument konzentriert sich auf die praktische Anwendung dieser Grundsätze. Daher gibt es Orientierungshilfen dafür, welche Inhalte die Verfahrensrichtlinien des Unternehmens für den Umgang mit E-Mail und Internet mindestens enthalten sollten. Diese können von Arbeitgebern und Arbeitnehmern als Basis verwendet und weiter ausgebaut werden (unter Berücksichtigung der Besonderheiten des jeweiligen Unternehmens, seiner Größe und der innerstaatlichen Rechtsvorschriften in mit dem Datenschutz verknüpften Bereichen).

Hinsichtlich der Nutzung des Internet für private Zwecke ist die Artikel 29-Datenschutzgruppe der Auffassung, dass **der Prävention Vorrang vor der Aufdeckung eingeräumt** werden sollte. Mit anderen Worten: Dem Interesse des Arbeitgebers ist besser gedient, wenn der Missbrauch des Internet verhindert wird, als wenn ein solcher Missbrauch aufgedeckt wird. In diesem Zusammenhang sind technische Lösungen besonders nützlich. Ein pauschales Verbot der privaten Internet-Nutzung durch Arbeitnehmer erscheint nicht angemessen und entspricht nicht dem Nutzen des Internet für das Alltagsleben der Arbeitnehmer.

Die Datenschutzgruppe möchte deutlich machen, dass es von wesentlicher Bedeutung ist, dass der Arbeitgeber die Arbeitnehmer informiert (i) über das Bestehen, die Nutzung und den Zweck jeglicher Kontrollvorrichtung, die an ihrem Arbeitsplatz eingerichtet wird, und (ii) über jeden aufgedeckten Missbrauch der elektronischen Kommunikation (E-Mail oder Internet), sofern nicht wichtige Gründe die Fortsetzung der verdeckten Kontrolle rechtfertigen[7], was normalerweise nicht der Fall ist. Die unverzügliche Information kann leicht über die Software erfolgen, wie zum Beispiel durch Fenster mit Warnhinweisen, die sich öffnen und den Arbeitnehmer darauf aufmerksam machen, dass das System eine unautorisierte Nutzung des Netzes festgestellt und/oder Maßnahmen zur Verhinderung einer solchen Nutzung eingeleitet hat.

Eine praktische Arbeitsgrundlage wäre die, dass Arbeitgeber beispielsweise Arbeitnehmern zwei E-Mail-Konten zur Verfügung stellen:

a) eines nur für berufliche Angelegenheiten, bei dem eine Überwachung innerhalb der Grenzen dieses Arbeitsdokuments möglich wäre,

b) ein weiteres Konto nur für rein private Zwecke (oder eine Autorisierung für die Nutzung von Internet-Mail), das nur Sicherheitsmaßnahmen sowie in Ausnahmefällen Überprüfungen auf Missbrauch unterzogen wird.

Die Artikel 29-Datenschutzgruppe hat in Bereichen, die mit dem Datenschutz in Zusammenhang stehen, einige Unterschiede zwischen den nationalen Rechtsvorschriften festgestellt, hauptsächlich bezüglich der zulässigen Ausnahmen vom Grundrecht auf das Briefgeheimnis sowie zu Ausmaß und Wirkung tariflicher Arbeitnehmervertretung und Mitbestimmung. Sie hat indessen keine Unterschiede zwischen den nationalen Rechtsvorschriften im Bereich des Datenschutzes festgestellt, die ein wesentliches Hindernis für ein gemeinsames Konzept darstellen könnten. Daher hat sie dieses Arbeitsdokument erstellt, das im Zeitraum 2002-2003 im Lichte der Erfahrungen und der weiteren Entwicklung in diesem Bereich überprüft werden wird.

---

[7] Fälle gerechtfertigter verdeckter Überwachung wären ein gutes Beispiel dafür.

1. ÜBERWACHUNG AM ARBEITSPLATZ - EINE HERAUSFORDERUNG FÜR DIE GESELLSCHAFT

Die Überwachung von Arbeitnehmern findet in jüngster Zeit großes Medieninteresse und ist gegenwärtig Gegenstand der öffentlichen Diskussion in der Gemeinschaft. Nachdem in der gesamten Gemeinschaft immer mehr Arbeitsplätze über einen E-Mail-Anschluss verfügen, werden sich Arbeitgeber wie Arbeitnehmer zunehmend der Gefahr eines Eindringens in die Privatsphäre der Beschäftigten bewusst.

Hinsichtlich der Frage der Kontrolle muss immer im Auge behalten werden, dass Arbeitnehmer zwar ein Recht darauf haben, dass ihre Privatsphäre am Arbeitsplatz bis zu einem gewissen Grad gewahrt bleibt, dieses Recht jedoch gegen das Recht des Arbeitgebers abgewogen werden muss, den Betriebsablauf in seinem Unternehmen zu kontrollieren und sich gegen Tätigkeiten der Arbeitnehmer zur Wehr zu setzen, die seine berechtigten Interessen verletzen könnten, zum Beispiel vor dem Hintergrund der Haftung des Arbeitgebers für die Handlungen seiner Beschäftigten.

Neue Technologien stellen zwar eine Bereicherung der den Arbeitgebern zur Verfügung stehenden Ressourcen dar, die Instrumente zur elektronischen Überwachung können jedoch auch in einer Art und Weise genutzt werden, die die Grundrechte und -freiheiten der Arbeitnehmer verletzt. Es muss beachtet werden, dass es angesichts der Entwicklung der neuen Informationstechnologien unabdingbar ist, dass Arbeitnehmer dieselben Rechte genießen, wenn sie online und wenn sie offline arbeiten.

Darüber hinaus ist zu betonen, dass sich die Arbeitsbedingungen in einer Weise verändert haben, dass es heute immer schwieriger wird, Arbeitszeit und Privatleben zu trennen. Insbesondere ist der "Heimarbeitsplatz" auf dem Vormarsch, viele Arbeitnehmer arbeiten zu Hause weiter und nutzen dabei die oder die nicht vom Arbeitgeber zu diesem Zweck zur Verfügung gestellte EDV-Infrastruktur.

Die Menschenwürde des Arbeitnehmers ist allen anderen Erwägungen übergeordnet. Es ist wichtig, diese Tatsache und die negativen Auswirkungen, die solche Maßnahmen auf die Qualität des Verhältnisses von Arbeitnehmern zu ihrem Arbeitgeber und ihrer Arbeit haben können, bei der Erörterung dieser Thematik zu berücksichtigen.

Angesichts all dieser Faktoren ist es wenig überraschend, dass dieses Thema im Mittelpunkt der öffentlichen Diskussion steht und das dringende Bedürfnis besteht, einen Beitrag zu einer einheitlichen Auslegung der Bestimmungen der Richtlinie 95/46/EG und der einzelstaatlichen Rechtsvorschriften zu deren Umsetzung zu leisten, und zwar vor dem Hintergrund der jüngsten Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte.

Die Datenschutzgruppe ist daher der Ansicht, dass es lohnend wäre, die folgenden Informationen und Arbeitsdokumente an den öffentlichen und den privaten Sektor weiterzugeben. Es sei darauf hingewiesen, dass sich dieses Arbeitsdokument auf alle Tätigkeiten bezieht, die die Überwachung der elektronischen Kommunikation am Arbeitsplatz betreffen, d. h. sowohl Echtzeit-Kontrolle und als auch Zugriff auf gespeicherte Daten.

2. INTERNATIONALE RECHTSVORSCHRIFTEN

2.1 ARTIKEL 8 UND 10 DER EUROPÄISCHEN KONVENTION ZUM SCHUTZE DER MENSCHENRECHTE UND GRUNDFREIHEITEN

Artikel 8.

1. *Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.*

2. *Der Eingriff einer **öffentlichen Behörde** in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.*

Artikel 10.

1. *Jeder hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein. Dieser Artikel schließt nicht aus, dass die Staaten Rundfunk-, Lichtspiel- oder Fernsehunternehmen einem Genehmigungsverfahren unterwerfen.*

2. *Da die Ausübung dieser Freiheiten Pflichten und Verantwortung mit sich bringt, kann sie bestimmten, vom Gesetz vorgesehenen Formvorschriften, Bedingungen, Einschränkungen oder Strafandrohungen unterworfen werden, wie sie vom Gesetz vorgeschrieben und in einer demokratischen Gesellschaft im Interesse der nationalen Sicherheit, der territorialen Unversehrtheit oder der öffentlichen Sicherheit, der Aufrechterhaltung der Ordnung und der Verbrechensverhütung, des Schutzes der Gesundheit und der Moral, des Schutzes des guten Rufes oder der Rechte anderer, um die Unparteilichkeit der Rechtsprechung zu gewährleisten, unentbehrlich sind.*

Alle Mitgliedstaaten und die Europäische Union sind an die Bestimmungen der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten gebunden. Diese Rechte werden traditionell vertikal ausgeübt (d. h. der Mensch gegenüber dem Staat), und die Diskussion darüber, inwieweit sie horizontal (d. h. zwischen den Menschen) ausgeübt werden können, wird fortgeführt. Es steht jedoch fest, dass diese Rechte allgemein existieren.

Die Arbeitsgruppe ist daher der Auffassung, dass es bei der Prüfung der Anwendbarkeit der einzelstaatlichen Maßnahmen, die gemäß der Richtlinie 95/46/EG getroffen wurden, mit Blick auf die einheitliche Anwendung dieser Maßnahmen notwendig ist, die wesentlichen Grundsätze der derzeit gültigen Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte bezüglich dieser Bestimmung und speziell bezüglich des Briefgeheimnisses in Erinnerung zu rufen.

In seinen bisherigen Urteilen hat der Gerichtshof eindeutig festgestellt, dass der in Artikel 8 verankerte Schutz des "Privatlebens" das Berufsleben als Arbeitnehmer nicht ausschließt und nicht auf das häusliche Leben beschränkt ist.

In der Sache **Niemitz gegen Deutschland** ging es um die Durchsuchung des Büros des Klägers durch eine staatliche Behörde. Die Regierung argumentierte, dass Artikel 8 keinen Schutz gegen die Durchsuchung von Büroräumen gewähre, da die Konvention eindeutig zwischen Privatleben und Wohnung einerseits und Berufs- und Geschäftsleben sowie den Räumlichkeiten, in denen dieses stattfindet, andererseits unterscheide.

Das Gericht lehnte diese Auffassung mit folgender Feststellung ab:

"Die Achtung des Privatlebens muss in gewissem Umfang auch das Recht beinhalten, Beziehungen zu anderen Menschen aufzubauen und zu entwickeln. ***Ferner scheint grundsätzlich nichts dafür zu sprechen, von diesem Verständnis des Begriffs des "Privatlebens" Tätigkeiten beruflicher oder geschäftlicher Art auszuschließen****, da die meisten Leute ja gerade in ihrem Berufsleben eine signifikante oder sogar die größte Möglichkeit zur Entwicklung der Beziehungen mit der Außenwelt haben. Diese Ansicht wird, wie die Kommission zu Recht betont hat, durch den Umstand bekräftigt, dass nicht immer eine klare Trennung möglich ist zwischen den Tätigkeiten eines Menschen, die zu seinem Berufs- oder Geschäftsbereich gehören, und denjenigen, bei denen das nicht der Fall ist."*[8]

Im Fall **Halford gegen das Vereinigte Königreich** entschied das Gericht außerdem, dass das Abhören von Telefongesprächen der Mitarbeiter am Arbeitsplatz einen Verstoß gegen Artikel 8 der Konvention darstellte. Interessanterweise verfügte Frau Halford über zwei Telefonapparate, von denen einer für die private Nutzung vorgesehen war. Bezüglich der Nutzung waren keine Einschränkungen ausgesprochen worden, und Frau Halford waren auch keine Richtlinien vorgegeben worden.

Frau Halford machte geltend, dass durch das Abhören ihrer Telefongespräche wiederholt gegen Artikel 8 der Konvention verstoßen worden sei. Die Regierung ihrerseits legte dar, dass die von Frau Halford von ihrem Arbeitsplatz aus getätigten Telefongespräche nicht unter den Schutz von Artikel 8 fielen, da sie diesbezüglich nicht begründeterweise von einer Privatheit habe ausgehen können. Bei der Anhörung vor Gericht vertrat der Anwalt der Regierung die Auffassung, dass es einem Arbeitgeber grundsätzlich und ohne vorherige Kenntnis des Arbeitnehmers erlaubt sein müsse, Anrufe des Letzteren, die dieser über die vom Arbeitgeber gestellten Telefonapparate tätige, zu überwachen.

Nach Auffassung des Gerichts allerdings *"geht aus der Rechtsprechung des Gerichts eindeutig hervor, dass Telefongespräche, die in Büroräumen getätigt werden ebenso wie Telefongespräche in der Wohnung unter die Begriffe "Privatleben" und "Korrespondenz"* im Sinne von Artikel 8 Absatz 1 fallen können (…).

Es liegt kein Beweis dafür vor, dass Frau Halford als Benutzerin des internen Telekommunikationssystems in irgendeiner Weise gewarnt worden wäre, dass Gespräche, die über dieses System getätigt werden, abgehört würden. Sie konnte damit nach Auffassung des Gerichts begründeterweise von der Privatheit derartiger Gespräche ausgehen..."[9].

---

[8] 23. November 1992, Reihe A Nr. 251/B, Absatz 29; Hervorhebung hinzugefügt.

[9] 27. Mai 1997.

Diese Auffassung von "Korrespondenz" schließt somit nicht nur Briefe auf Papier ein, sondern auch andere Formen elektronischer Kommunikation, die am Arbeitsplatz empfangen werden oder vom Arbeitsplatz getätigt werden, wie z. B. Telefongespräche, die in Büroräumen getätigt oder entgegengenommen werden oder E-Mail-Nachrichten, die an Computern am Arbeitsplatz empfangen oder von dort verschickt werden.

In einzelnen Auslegungen wird die Auffassung vertreten, dies impliziere offensichtlich auch, wenngleich dies im Urteil nicht so formuliert worden sei, dass, wenn ein Arbeitnehmer von einem Arbeitgeber im Voraus auf die Möglichkeit hingewiesen werde, dass seine Kommunikation abgehört werde, der Arbeitnehmer nicht mehr von deren Privatheit ausgehen könne und somit das Abhören keine Verletzung von Artikel 8 der Konvention darstelle. Die Datenschutzgruppe vertritt nicht die Ansicht, dass eine vorherige Unterrichtung des Arbeitnehmers ausreicht, um eine Verletzung seiner Datenschutzrechte zu rechtfertigen.

Auf allgemeinerer Ebene lassen sich von der Rechtsprechung zu Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten drei Grundsätze ableiten:

a) Arbeitnehmer haben die berechtigte Erwartung, dass ihre Privatsphäre am Arbeitsplatz gewahrt und nicht durch die Tatsache außer Kraft gesetzt wird, dass die Arbeitnehmer Kommunikationsgeräte oder andere geschäftliche Einrichtungen nutzen, die Eigentum des Arbeitgebers sind.

   Allerdings kann diese berechtigte Erwartung des Arbeitnehmers auf Schutz seiner Privatsphäre durch seine sachgerechte Unterrichtung durch den Arbeitgeber geschwächt werden.

b) Der allgemeine Grundsatz des Briefgeheimnisses gilt auch für die Kommunikation am Arbeitsplatz. Dies schließt wohl auch E-Mail-Nachrichten und daran angehängte Dateien ein.

c) Die Achtung des Privatlebens schließt bis zu einem gewissen Grad auch das Recht ein, Beziehungen zu anderen Menschen aufzunehmen und zu entwickeln. Die Tatsache, dass derartige Beziehungen zu einem großen Teil am Arbeitsplatz stattfinden, schränkt das berechtigte Interesse des Arbeitgebers an Überwachungsmaßnahmen ein.

Artikel 10 ist in geringerem Ausmaß ebenfalls relevant, da er den Anspruch auf freie Meinungsäußerung und Informationsfreiheit regelt und das Recht auf die Freiheit des Einzelnen zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden unterstreicht. Die Relevanz von Artikel 10 scheint in den oben angeführten Erwägungen des Gerichts in der Sache Niemitz gegen Deutschland deutlich zu werden. Wie das Gericht feststellte, entwickeln Menschen am Arbeitsplatz einen erheblichen Teil ihrer Beziehungen mit der Außenwelt. Daher würde ihr Recht auf die Freiheit auf Meinungsäußerung in diesem Zusammenhang sicherlich eine Rolle spielen.

2.2 ÜBEREINKOMMEN DES EUROPARATS ZUM SCHUTZ DES MENSCHEN BEI DER AUTOMATISCHEN VERARBEITUNG PERSONENBEZOGENER DATEN (ÜBEREINKOMMEN NR. 108)

Das Übereinkommen wurde am 28. Januar 1981 zur Unterzeichnung aufgelegt und ist das erste rechtlich bindende internationale Instrument im Bereich Datenschutz. Im Rahmen dieses Übereinkommens werden die Vertragsparteien aufgefordert, die notwendigen Schritte zu unternehmen, um die darin festgelegten Grundsätze in ihrer nationalen Gesetzgebung umzusetzen und so die Wahrung der Grundrechte aller Menschen im Hinblick auf die Verarbeitung personenbezogener Daten zu gewährleisten.[10]

Auch andere wichtige Dokumente, die einen Bezug zum Übereinkommen Nr. 108 haben, sind in diesem Zusammenhang relevant:

- Arbeitsdokument des Europarates (89) 2 zum Schutz personenbezogener Daten, die für Beschäftigungszwecke verwendet werden[11].
- Arbeitsdokument des Europarates (97) 5 zum Schutz medizinischer Daten[12].
- Arbeitsdokument des Europarates (86) 1 über den Schutz von Personendaten, die für Sozialversicherungszwecke verwendet werden[13].
- Empfehlung des Europarates (95) 4 über den Schutz von Personendaten im Bereich der Telekommunikation, unter besonderer Berücksichtigung von Telefondiensten

2.3. DIE CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION

Artikel 7. ***Achtung des Privat- und Familienlebens***

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Artikel 8. ***Schutz personenbezogener Daten***

1. Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

2. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

3. Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

---

[10] Siehe auch die Empfehlung des Europarates Nr. R (89) 2 zum Schutz personenbezogener Daten, die für Beschäftigungszwecke verwendet werden: http://cm.coe.int/ta/rec/1989/89r2.htm.

[11] http://cm.coe.int/ta/rec/1989/89r2.htm.

[12] http://cm.coe.int/ta/rec/1997/97r5.html.

[13] http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm

Die Charta der Grundrechte der Europäischen Union folgt damit offenkundig in wesentlichen Zügen der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), und der Begriff des "Briefgeheimnisses" wurde erweitert auf den neu entstandenen Begriff des "Kommunikationsgeheimnisses", mit dem das Ziel verfolgt wird, der elektronischen Kommunikation das gleiche Maß an Schutz zu gewähren wie dies in der Vergangenheit bereits bei Postsendungen der Fall war.

Darüber hinaus ergänzt Artikel 8 durch eine wesentliche Differenzierung des Datenschutzes den von Artikel 7 gewährten Schutz. Dieses Ergebnis ist für das Thema der Überwachung von E-Mail-Nachrichten von besonderer Bedeutung.

2.4. INTERNATIONALES ARBEITSAMT (ILO)

Verhaltenskodex des Internationalen Arbeitsamtes für den Schutz von Beschäftigtendaten (1997).

„5. Allgemeine Grundsätze

5.1. Personenbezogene Daten sollten rechtmäßig, nach Treu und Glauben und nur aus Gründen verarbeitet werden, die für die Beschäftigung des Arbeitnehmers relevant sind.

5.2. Personenbezogene Daten sollten im Prinzip nur für die Zwecke verwendet werden, für die sie ursprünglich erhoben wurden.

5.3. Wenn personenbezogene Daten für andere Zwecke verarbeitet werden sollen als die, für die sie erhoben wurden, sollte der Arbeitgeber sicherstellen, dass sie nicht in einer mit dem ursprünglichen Zweck nicht zu vereinbarenden Weise verwendet werden, und die Maßnahmen treffen, die erforderlich sind, um jegliche Fehlinterpretation aufgrund eines geänderten Kontexts zu vermeiden.

5.4. Personenbezogene Daten, die im Zusammenhang mit technischen oder organisatorischen Maßnahmen zur Gewährleistung der Sicherheit und des einwandfreien Funktionierens automatischer Informationssysteme erhoben werden, sollten nicht verwendet werden, um das Verhalten von Arbeitnehmern zu kontrollieren.

5.5. Entscheidungen über einen Arbeitnehmer sollten nicht ausschließlich auf die automatische Verarbeitung der personenbezogenen Daten dieses Arbeitnehmers gestützt werden.

5.6. Personenbezogene Daten, die mittels elektronischer Überwachung erhoben werden, sollten nicht die einzigen Faktoren zur Beurteilung der Leistung eines Arbeitnehmers sein (…)

6.14.(1) Wenn Arbeitnehmer überwacht werden, sollten Sie vorab über die Gründe der Überwachung, den Zeitplan, die eingesetzten Methoden und Techniken und die Daten, die erhoben werden sollen, informiert werden; außerdem muss der

Arbeitgeber das Eindringen in die Privatsphäre der Arbeitnehmer auf ein Minimum beschränken.

(2) Die heimliche Überwachung sollte nur zulässig sein:

a) wenn sie in mit den nationalen Rechtsvorschriften vereinbar ist oder

b) wenn der begründete Verdacht strafbarer Handlungen oder anderer ernsthafter Verfehlungen besteht.

(3) Eine ständige Überwachung sollte nur zulässig sein, wenn sie aus Gründen der Gesundheit und Sicherheit oder zum Schutze des Eigentums erforderlich ist (…)

12.2. Die Arbeitnehmervertreter sollten, wo eine solche Vertretung existiert, entsprechend der Praxis und den Rechtsvorschriften des Landes unterrichtet und gehört werden:

a) über die Einführung oder Änderung automatischer Systeme zur Verarbeitung der personenbezogenen Daten der Arbeitnehmer,

b) vor der Einführung einer elektronischen Überwachung des Verhaltens von Arbeitnehmern am Arbeitsplatz,

c) über Zwecke, Inhalte und Art der Verwaltung und Auslegung aller Fragebogen und Tests, die personenbezogene Daten des Arbeitnehmers betreffen“.

3. DIE ÜBERWACHUNG UND KONTROLLE DER ELEKTRONISCHEN KOMMUNIKATION DER BESCHÄFTIGTEN IM RAHMEN DER RICHTLINIE 95/46/EG

Grundlage des folgenden Arbeitsdokuments ist die Anwendung der Grundsätze von Richtlinie 95/46/EG auf die in Frage stehende Überwachung und Kontrolle unter Berücksichtigung von Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, der die Beachtung des Briefgeheimnisses ebenso fordert wie den Schutz der Privatsphäre.

Dem Arbeitgeber stehen zahlreiche Möglichkeiten der Überwachung am Arbeitsplatz zur Verfügung, von denen jede einzelne ihre spezifischen Probleme birgt. In dieser Empfehlung werden zwei Formen der Überwachung behandelt, auf die ähnliche Grundsätze anwendbar sind: die Überwachung von E-Mail-Nachrichten und die Kontrolle des Internetzugriffs.

Ausgangspunkt ist die Bestätigung des in der Stellungnahme 8/2001 vorgebrachten Arguments, dass die Richtlinie 95/46/EG auf die Verarbeitung personenbezogener Daten von Beschäftigten genauso anzuwenden ist wie in jedem anderen Kontext[14]. Neben der allgemeinen Richtlinie 95/46/EG kann auch die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation relevant sein. Sie spezifiziert und ergänzt die Richtlinie 95/46/EG hinsichtlich der Verarbeitung personenbezogener Daten in der Telekommunikation. Die Überwachung der elektronischen Kommunikation durch Arbeitgeber, einschließlich der Überwachung von E-Mail-Verkehr und Internetzugriff, fällt unter Umständen nicht nur unter Richtlinie 95/46/EG, sondern auch unter Richtlinie 97/66/EG. Diese wird gegenwärtig im Zuge der Novellierung des gemeinschaftlichen Rechtsrahmens für die Telekommunikation überarbeitet. In den Fällen, in denen diese Richtlinie anwendbar ist, können ihre Artikel 5 (Vertraulichkeit der Kommunikation) und Artikel 6 (Verkehrsdaten und Daten für die Gebührenabrechnung) eine besonders wichtige Rolle spielen.

3.1 ALLGEMEINE GRUNDSÄTZE FÜR DIE ÜBERWACHUNG DES E-MAIL-VERKEHRS UND DES INTERNETZUGRIFFS

Die folgenden Datenschutzgrundsätze sind aus der Richtlinie 95/46/EG abgeleitet und sollten bei der Erwägung der Verarbeitung personenbezogener Daten im Zusammenhang mit einer solchen Überwachung berücksichtigt werden. Alle folgenden Grundsätze müssen beachtet werden, wenn eine Überwachung rechtmäßig und gerechtfertigt sein soll.

3.1.1. ERFORDERLICHKEIT

Dieser Grundsatz besagt, dass der Arbeitgeber jegliche Form der Überwachung daraufhin prüfen muss, ob sie für einen festgelegten Zweck unbedingt erforderlich ist, bevor er Maßnahmen in dieser Hinsicht ergreift. Traditionelle Kontrollverfahren, mit denen nicht so

---

[14] http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48de.pdf.

stark in die Privatsphäre des Einzelnen eingedrungen wird, sollten sorgfältig in Erwägung gezogen werden, und wenn sie sich als geeignet erweisen, eingesetzt werden, bevor die elektronische Kommunikation in irgendeiner Form überwacht wird.

Nur in Ausnahmefällen würde die Überwachung des E-Mail-Verkehrs oder des Internetzugriffs eines Arbeitnehmers als notwendig angesehen. So könnte es notwendig werden, eine E-Mail-Nachricht eines Arbeitnehmers zu öffnen, um eine Bestätigung oder einen Beweis für bestimmte Tätigkeiten dieses Arbeitnehmers zu erhalten. Dies wären unter anderem kriminelle Handlungen des Arbeitnehmers, soweit der Arbeitgeber seine eigenen Interessen schützen muss, wenn er zum Beispiel für die Handlungen des Arbeitnehmers haftet. Darunter fiele außerdem die Entdeckung von Viren und allgemein jede Tätigkeit des Arbeitgebers, die die Gewährleistung der Sicherheit des Systems zum Ziel hat.

Es sollte erwähnt werden, dass das Öffnen der E-Mail eines Beschäftigten auch aus anderen Gründen als der Überwachung oder Kontrolle notwendig sein kann, z. B. um die Korrespondenz aufrechtzuerhalten, wenn der Beschäftigte nicht in seinem Büro ist (z. B. wegen Krankheit oder Urlaub) und dies nichts auf andere Art und Weise gewährleistet werden kann (z. B. durch automatische Rückantwort oder Weiterleitung).

Der Grundsatz der Erforderlichkeit bedeutet auch, dass ein Arbeitgeber Daten nicht länger aufbewahren darf, als es für den festgelegten Zweck der Überwachung notwendig ist.

3.1.2. ZWECKBINDUNG

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. In diesem Zusammenhang bedeutet der Grundsatz der „Vereinbarkeit“ zum Beispiel, dass, wenn die Datenverarbeitung auf der Basis der Systemsicherheit gerechtfertigt ist, diese Daten nicht außerdem zu einem anderen Zweck, wie zum Beispiel der Überwachung des Verhaltens des Arbeitnehmers, verarbeitet werden dürfen.

3.1.3. TRANSPARENZ

Dieser Grundsatz besagt, dass ein Arbeitgeber seine Tätigkeiten klar und deutlich offenlegen muss. Er besagt, dass eine verdeckte Überwachung des E-Mail-Verkehrs durch den Arbeitgeber nicht zulässig ist, mit Ausnahme der Fälle, in denen die Rechtsvorschriften des betreffenden Mitgliedstaates dies gemäß Artikel 13 der Richtlinie zulassen[15]. Das dürfte am ehesten der Fall sein, wo bestimmte kriminelle Handlungen festgestellt worden sind (und es erforderlich ist, einen Nachweis zu erbringen, und die Rechtsgrundsätze und Verfahrensvorschriften der Mitgliedstaaten einzuhalten sind.) oder in den Fällen, in denen nationale Rechtsvorschriften, die die erforderlichen Garantien beinhalten, es dem Arbeitgeber erlauben, bestimmte Maßnahmen zu ergreifen, um Verstöße am Arbeitsplatz festzustellen.

---

[15] Nach Artikel 13 der Richtlinie können die Mitgliedstaaten Rechtsvorschriften erlassen, die die Rechte und Pflichten bestimmter Artikel der Richtlinie beschränken, wenn eine solche Beschränkung notwendig ist zur Wahrung wichtiger öffentlicher Interessen wie der Sicherheit des Staates oder der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder zum Schutz der Betroffenen oder der Rechte und Freiheiten anderer Personen.

Ferner kann dieser Grundsatz in zwei Aspekte aufgeteilt werden:

3.1.3.1. DIE VERPFLICHTUNG, DIE BETROFFENE PERSON ZU UNTERRICHTEN

Dies ist vielleicht das wichtigste Beispiel für die praktische Umsetzung des Grundsatzes der Transparenz in diesem Zusammenhang. Der Arbeitgeber muss seinen Arbeitnehmern eine leicht zugängliche, klare und genaue Darstellung seiner Verfahrensrichtlinien für die Überwachung des E-Mail-Verkehrs und des Internetzugriffs zur Verfügung zu stellen.

Die Beschäftigten müssen umfassend über die konkreten Umstände, die eine derartige außerordentliche Maßnahme rechtfertigen würden, und über Reichweite und Umfang einer solchen Überwachung unterrichtet werden. Die Unterrichtung sollte folgende Angaben umfassen:

1. Verfahrensrichtlinien für den Umgang mit E-Mail und Internet in dem Unternehmen, die genaue Angaben darüber enthalten, in welchem Umfang die im Besitz des Unternehmens befindlichen Kommunikationseinrichtungen von den Beschäftigten für die persönliche/private Kommunikation genutzt werden dürfen (z. B. Einschränkung von Nutzungszeiten und Nutzungsdauer).

2. Gegebenenfalls Gründe und Zwecke einer Überwachung. Soweit der Arbeitgeber die Nutzung der unternehmenseigenen Kommunikationseinrichtungen für private Zwecke ausdrücklich erlaubt hat, kann unter sehr eingeschränkten Bedingungen eine Überwachung dieser privaten Kommunikation vorgenommen werden, z. B. um die Sicherheit des Informationssystems zu gewährleisten (Virenprüfung).

3. Die genauen Einzelheiten der Überwachungsmaßnahmen, d. h. Wer? Was? Wie? Wann?

4. Genaue Angaben über Durchsetzungsverfahren, aus denen hervorgeht, dass und wie die Mitarbeiter von Verstößen gegen die firmeninternen Verfahrensrichtlinien in Kenntnis gesetzt werden und die Möglichkeit erhalten, auf entsprechende, gegen sie erhobene Vorwürfe zu reagieren.

Die Datenschutzgruppe möchte an dieser Stelle deutlich machen, dass es aus praktischen Gründen ratsam ist, dass der Arbeitgeber den Arbeitnehmer unverzüglich über jeden aufgedeckten Missbrauch der elektronischen Kommunikation informiert, sofern nicht wichtige Gründe die Fortsetzung der verdeckten Kontrolle rechtfertigen[16], was normalerweise nicht der Fall ist. Die unverzügliche Information kann leicht über die Software erfolgen, wie zum Beispiel durch Fenster mit Warnhinweisen, die sich öffnen und den Arbeitnehmer darauf aufmerksam machen, dass das System eine unautorisierte Nutzung des Netzes festgestellt hat. Auf diese Weise können zahlreiche Missverständnisse ausgeräumt werden.

---

[16] Fälle gerechtfertigter verdeckter Überwachung wären ein gutes Beispiel dafür.

Ein weiteres Beispiel für den Grundsatz der Transparenz ist die Unterrichtung und/oder Anhörung der Arbeitnehmervertreter durch den Arbeitgeber vor Einführung von Maßnahmen, die die Arbeitnehmer betreffen. Es sei betont, dass für Entscheidungen über die Überwachung von Arbeitnehmern, einschließlich der Überwachung der elektronischen Kommunikation, die kürzlich verabschiedete Richtlinie 2002/14/EG gilt, wenn das betreffende Unternehmen in ihren Anwendungsbereich fällt. Diese Richtlinie schreibt insbesondere vor, dass die Arbeitnehmer über Entscheidungen unterrichtet werden müssen, die wesentliche Veränderungen der Arbeitsorganisation oder der Vertragsbeziehungen nach sich ziehen können, und dass sie zu solchen Maßnahmen gehört werden müssen. Nationale Rechtsvorschriften oder Tarifvereinbarungen können Bestimmungen enthalten, die für die Arbeitnehmer noch vorteilhafter sind.

Die Tarifvereinbarungen verpflichten den Arbeitgeber unter Umständen nicht nur dazu, die Arbeitnehmer zu unterrichten und anzuhören, bevor Überwachungssysteme eingerichtet werden. Sie können sogar die vorherige Zustimmung der Arbeitnehmervertreter zu einer solchen Maßnahme vorschreiben.

Tarifvereinbarungen können auch Bestimmungen über den Umfang der zulässigen Internet- und E-Mail-Nutzung durch Arbeitnehmer sowie Regelungen über die Überwachung dieser Nutzung enthalten.

3.1.3.2. DIE VERPFLICHTUNG, KONTROLLSTELLEN ZU INFORMIEREN, BEVOR EINE VOLLSTÄNDIG ODER TEILWEISE AUTOMATISIERTE VERARBEITUNG ODER EINE MEHRZAHL VON VERARBEITUNGEN DURCHGEFÜHRT WIRD

Dies ist eine weitere Möglichkeit, Transparenz herzustellen, da die Arbeitnehmer in den Datenschutzregistern zum Beispiel jederzeit überprüfen können, welche Kategorien personenbezogener Beschäftigtendaten der Arbeitgeber zu welchem Zweck und für welche Empfänger verarbeiten darf.

3.1.3.3 AUSKUNFTSRECHT

Wie alle anderen betroffenen Personen haben Arbeitnehmer nach der Richtlinie[17] einen Anspruch auf Auskunft über die sie betreffenden personenbezogenen Daten,

---

[17] Artikel 12: Die Mitgliedstaaten garantieren jeder betroffenen Person das Recht, vom für die Verarbeitung Verantwortlichen folgendes zu erhalten:

a) frei und ungehindert in angemessenen Abständen ohne unzumutbare Verzögerung oder übermäßige Kosten

- die Bestätigung, dass es Verarbeitungen sie betreffender Daten gibt oder nicht gibt, sowie zumindest Informationen über die Zweckbestimmungen dieser Verarbeitungen, die Kategorien der Daten, die Gegenstand der Verarbeitung sind, und die Empfänger oder Kategorien der Empfänger, an die die Daten übermittelt werden;

- eine Mitteilung in verständlicher Form über die Daten, die Gegenstand der Verarbeitung sind, sowie die verfügbaren Informationen über die Herkunft der Daten;

- Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne von Artikel 15 Absatz 1;

die von ihrem Arbeitgeber verarbeitet werden, und gegebenenfalls das Recht, die Berichtigung, Löschung oder Sperrung von Daten zu verlangen, die nicht den Vorschriften der Richtlinie genügen, insbesondere von unvollständigen oder unkorrekten Daten.

Der Anspruch auf freie und ungehinderte Auskunft über die Dateien des Arbeitgebers in angemessenen Abständen, ohne unzumutbare Verzögerung oder übermäßige Kosten ist ein äußerst wirkungsvolles Recht, das der Arbeitnehmer individuell wahrnehmen kann, um sicherzugehen, dass die Überwachungsmaßnahmen am Arbeitsplatz stets rechtmäßig und nach Treu und Glauben erfolgen. Die Auskunft aus Dateien des Arbeitgebers könnte sich indessen in Ausnahmefällen als problematisch erweisen, z. B. im Falle der so genannten Beurteilungsdaten.

Die Datenschutzgruppe sich hat schon einmal zu dieser Frage geäußert[18] und wird unter Umständen im Lichte der Erfahrungen weitere Leitlinien dazu vorlegen.

3.1.4. ZULÄSSIGKEIT

Dieser Grundsatz besagt, dass eine Verarbeitung personenbezogener Daten nur dann erfolgen darf, wenn sie einen rechtmäßigen Zweck gemäß Artikel 7 der Richtlinie und den nationalen Rechtsvorschriften zu deren Umsetzung verfolgt. Artikel 7 Buchstabe f der Richtlinie ist für diesen Grundsatz insofern besonders wichtig, als er festlegt, dass die Verarbeitung personenbezogener Daten von Beschäftigten gemäß der Richtlinie 95/46/EG nur dann zulässig ist, wenn sie zur Verwirklichung des berechtigten Interesses des Arbeitgebers erforderlich ist und die Grundrechte der Arbeitnehmer nicht verletzt.

Das Anliegen des Arbeitgebers, sein Unternehmen gegen ernsthafte Gefahren zu schützen, wie beispielsweise der Weitergabe vertraulicher Informationen an die Konkurrenz, kann ein solches berechtigtes Interesse darstellen.

Die Verarbeitung sensibler Daten in diesem Zusammenhang ist besonders problematisch, weil Artikel 8 der Richtlinie keine Interessenabwägung im Sinne von Artikel 7 Buchstabe f der Richtlinie vorsieht. Artikel 8 Buchstabe b sieht jedoch eine Ausnahme für den Fall vor, dass die Verarbeitung erforderlich ist, „um den Rechten und Pflichten des für die Verarbeitung Verantwortlichen auf dem Gebiet des Arbeitsrechts Rechnung zu tragen, sofern dies aufgrund von einzelstaatlichem Recht, das angemessene Garantien vorsieht, zulässig ist“.

---

b) je nach Fall die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen dieser Richtlinie entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind;

c) die Gewähr, dass jede Berichtigung, Löschung oder Sperrung, die entsprechend Buchstabe b) durchgeführt wurde, den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, sofern sich dies nicht als unmöglich erweist oder kein unverhältnismäßiger Aufwand damit verbunden ist.

[18] Siehe Empfehlung 1/2001 hinsichtlich der Daten in Beurteilungen von Arbeitnehmern.

Die Verarbeitung sensibler Daten im Zusammenhang mit Überwachungs- und Kontrollmaßnahmen ist eine schwierige Frage, die nicht nur im Zusammenhang mit Arbeitsverhältnissen von Bedeutung ist. Es handelt sich um eine allgemeine Problematik, zu der die Datenschutzgruppe unter Umständen Leitlinien vorlegen wird.

Soweit sie nämlich nicht durch nationale Rechtsvorschriften, die angemessene Garantien enthalten, ausdrücklich erlaubt sind, sind Überwachungsmaßnahmen, die direkt auf die Verarbeitung sensibler Daten von Arbeitnehmern zielen, nach den Vorschriften der Richtlinie 95/46/EG nicht zulässig und nicht akzeptabel. Es erscheint aber auch nicht akzeptabel, dass Überwachungsmaßnahmen (die in vielen Fällen nicht nur rechtmäßig, sondern auch wünschenswert sind, wie zum Beispiel Maßnahmen, die unmittelbar der Systemsicherheit dienen) allesamt verhindert oder extrem erschwert werden, allein deshalb, weil sie notgedrungen die Verarbeitung bestimmter sensibler Daten beinhalten könnten.

3.1.5. VERHÄLTNISMÄßIGKEIT

Dieser Grundsatz verlangt, dass alle personenbezogenen Daten, einschließlich der, die Überwachungsmaßnahmen unterliegen, dem angestrebten Zweck entsprechen, dafür erheblich sind und nicht darüber hinausgehen. Die Verfahrensrichtlinien des Unternehmens müssen in diesem Bereich auf Art und Umfang der Gefährdung des jeweiligen Unternehmens zugeschnitten sein.

Der Grundsatz der Verhältnismäßigkeit schließt demnach eine pauschale Überwachung einzelner E-Mail-Nachrichten und der Internetnutzung sämtlicher Mitarbeiter aus, wenn sie nicht zum Zwecke der Gewährleistung der Systemsicherheit erforderlich ist. Soweit das festgelegte Ziel auf einem Wege erreicht werden kann, der mit einem geringeren Eindringen in die Privatsphäre der Beschäftigten verbunden ist, sollte der Arbeitgeber diese Option in Erwägung ziehen (er/sie sollte zum Beispiel keine Systeme zur ständigen und automatischen Überwachung einsetzen).

Die Überwachung des E-Mail-Verkehrs sollte nach Möglichkeit auf die Erfassung von Verbindungsdaten über die Beteiligten und den Zeitpunkt der Kommunikation beschränkt bleiben und die Kommunikationsinhalte ausschließen, soweit dies ausreicht, um die Bedenken des Arbeitgebers zu zerstreuen. Wenn der Zugriff auf den Inhalt von E-Mail-Nachrichten absolut notwendig ist, sollte der Privatsphäre der Empfänger außerhalb der Organisation ebenso Rechnung getragen werden wie der Privatsphäre der Absender innerhalb der Organisation. So kann der Arbeitgeber beispielsweise die Einwilligung derjenigen außerhalb der Organisation, die E-Mails an seine Beschäftigten schickten, nicht einholen. Der Arbeitgeber sollte im Rahmen seiner Möglichkeiten versuchen, diejenigen außerhalb der Organisation über Überwachungsmaßnahmen zu informieren, soweit diese Personen außerhalb der Organisation betreffen können. Ein praktisches Beispiel wären Warnhinweise auf die Existenz von Überwachungssystemen in allen ausgehenden Mitteilungen der Organisation.

Es gibt genügend technische Hilfsmittel, mit denen der Arbeitgeber die Nutzung des E-Mail-Verkehrs durch die Beschäftigten feststellen kann, etwa durch Überprüfung der Zahl der eingegangenen oder versendeten E-Mail-Nachrichten oder des Formats von Anhängen. Daher ist das konkrete Öffnen von E-Mail-Nachrichten nicht verhältnismäßig. Darüber hinaus gibt es die technische Möglichkeit, durch den Einsatz von Sperren statt von Überwachungsmechanismen zu gewährleisten, dass die Verhältnismäßigkeit der vom

Arbeitgeber getroffenen Maßnahmen zur Sicherung des den Arbeitnehmern zur Verfügung gestellten Internet-Zugangs gegen Missbrauch gewahrt bleibt.[19]

Systeme für die Verarbeitung elektronischer Kommunikation sollten darauf ausgelegt sein, den Umfang der verarbeiteten personenbezogenen Daten auf ein absolutes Minimum zu beschränken[20].

Im Zusammenhang mit der Frage der Verhältnismäßigkeit sollte betont werden, dass Tarifverhandlungen sehr effektiv dafür genutzt werden können, darüber zu entscheiden, welche Maßnahmen für welche Gefährdung welches Arbeitgebers verhältnismäßig sind. Auf diese Weise kann zwischen Arbeitgeber und Arbeitnehmer Einvernehmen darüber erzielt werden, wie eine ausgewogene Berücksichtigung der Interessen erreicht werden kann.

3.1.6. SACHLICHE RICHTIGKEIT UND AUFBEWAHRUNG DER DATEN

Dieser Grundsatz verlangt, dass sämtliche vom Arbeitgeber rechtmäßig gespeicherte Daten (nach Erwägung aller anderen in diesem Kapitel aufgeführten Grundsätze), die aus dem E-Mail-Konto eines Arbeitnehmers oder dessen Internetzugriff stammen oder im Zusammenhang damit stehen, sachlich richtig und auf dem neuesten Stand sein müssen und nicht länger als notwendig aufbewahrt werden. Der Arbeitgeber sollte für E-Mails auf seinen zentralen Servern eine Aufbewahrungsfrist auf der Grundlage der geschäftlichen Erfordernisse festlegen. Es ist schwer vorstellbar, dass eine Aufbewahrungsfrist von mehr als drei Monaten normalerweise gerechtfertigt wäre.

3.1.7. SICHERHEIT

Dieser Grundsatz verpflichtet den Arbeitgeber, geeignete technische und organisatorische Maßnahmen umzusetzen, um zu gewährleisten, dass sämtliche von ihm aufbewahrten personenbezogenen Daten sicher vor einem externen Zugriff sind. Er erfasst ferner das Recht des Arbeitgebers, sein System vor Viren zu schützen, und kann das automatisierte Scannen von E-Mail-Nachrichten und Netzverbindungsdaten einschließen.

Die Datenschutzgruppe ist der Auffassung, dass mit Blick auf die Bedeutung der Systemsicherung ein solches automatisiertes Öffnen von E-Mail-Nachrichten nicht als eine Verletzung des Rechts des Arbeitnehmers auf Privatsphäre betrachtet werden sollte, sofern geeignete Garantien festgelegt wurden. So können Arbeitgeber zum Beispiel nun

---

[19] In der Praxis gibt es bereits viele Beispiele für diesen Einsatz der Technologie.

- Internet: Einige Unternehmen verwenden eine Software, die so konfiguriert werden kann, dass jede Verbindung zu bestimmten Websites verhindert wird. Der Arbeitgeber kann, nach Abgleichung mit der Liste der von seinen Angestellten besuchten Websites, beschließen, bestimmten Websites zur Liste der bereits blockierten hinzuzufügen (eventuell nachdem er die Beschäftigten davon unterrichtet hat, dass die Verbindung blockiert wird, wenn nicht ein Mitarbeiter die Notwendigkeit einer Verbindung zu diesen Websites nachweist).

- E-Mail: andere Unternehmen verwenden eine automatische Weiterleitungsfunktion zu einem isolierten Server für alle E-Mails, die einen bestimmten Umfang überschreiten. Der Adressat wird automatisch darüber informiert, dass eine verdächtige E-Mail zu diesem Server umgeleitet worden ist und dort geöffnet werden kann.

[20] Richtlinienentwurf 97/66, Erwägungsgrund 30.

automatisierte Techniken nutzen, die ihren Sicherheitsinteressen dienen, ohne das Recht der Arbeitnehmer auf den Schutz ihrer Privatsphäre zu verletzen.

Die Artikel 29-Datenschutzgruppe weist auf die Rolle der Systemverwalter hin; es handelt sich hierbei um Arbeitnehmer, die aus datenschutzrechtlicher Sicht große Verantwortung tragen. Es ist von größter Bedeutung, dass der Systemverwalter und andere Personen, die im Zuge von Überwachungsmaßnahmen Zugriff auf personenbezogene Daten über Arbeitnehmer erhalten, sich in bezug auf die ihnen zugänglichen vertraulichen Informationen streng an das Berufsgeheimnis halten müssen.

4. ÜBERWACHUNG VON E-MAIL-NACHRICHTEN

4.1 DAS BRIEFGEHEIMNIS

Wie in diesem Arbeitsdokument bereits dargelegt, ist die Datenschutzgruppe der Auffassung, dass Online- und Offline-Kommunikation nicht grundlos unterschiedlich behandelt werden dürfen, und damit für E-Mail-Nachrichten derselbe Schutz grundlegender Rechte gilt wie für herkömmliche Postsendungen auf Papier[21]. Die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte hat in gewissem Umfang Vorgaben für die Anwendung des Grundsatzes des Briefgeheimnisses in einer demokratischen Gesellschaft geliefert. Die Rechtsysteme der Mitgliedstaaten weichen indessen bei der Auslegung dieses Grundsatzes etwas voneinander ab, insbesondere beim Geltungsumfang für die berufliche Kommunikation, sowohl bezüglich des Inhalts als auch bezüglich der Verbindungsdaten. Unter dem Aspekt des Datenschutzes hat das erhebliche Konsequenzen, wenn es um den Grad des tolerierbaren Eindringens in den E-Mail-Verkehr der Beschäftigten geht.

Die Artikel 29-Datenschutzgruppe vertritt die Auffassung, dass elektronische Kommunikation aus Geschäftsräumen unter die Begriffe „Privatleben" - „Korrespondenz" im Sinne von Artikel 8 Absatz 1 der Europäischen Menschenrechtskonvention fallen kann. Diesbezüglich gibt es wenig Auslegungsspielraum, wie das Gericht in der obengenannten Sache **Halford gegen das Vereinigte Königreich** deutlich gemacht hat.

Zu prüfen bleibt, und hier besteht ein gewisser Auslegungsspielraum, in welchem Umfang Ausnahmen von diesem Grundsatz oder Beschränkungen des Prinzips möglich sind, insbesondere wenn ihm die Rechte und Freiheiten anderer gegenüberstehen, die ebenfalls in der Konvention verankert sind (z. B. rechtmäßige Interessen der Arbeitgeber). **Auf jeden Fall schließen Ort und Eigentum an den benutzten elektronischen Mitteln das in Rechtsgrundsätzen und Verfassungen enthaltene Kommunikations- und Briefgeheimnis nicht aus.**

Die Datenschutzgruppe möchte dennoch daran erinnern, dass es sich hier nicht um ein spezifisches Problem bei der Verarbeitung personenbezogener Daten am Arbeitsplatz handelt, sondern um ein Problem allgemeiner Art, das darauf zurückzuführen ist, das Datenschutzrecht und -vorschriften nicht abstrakt anwendbar sind. Datenschutzrechte sollen in verschiedenen Rechtssystemen gelten, zusammen mit anderen Gesetzen, die

---

[21] In einer der ersten Empfehlungen der Datenschutzgruppe, Empfehlung 3/97 „Anonymität im Internet" wurde gesagt, Online- und Offline-Situationen sollten gleich behandelt werden.

Siehe http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp6de.pdf

In Kapitel III Ziffer 3 des Papiers der Internet-Taskforce, des wichtigsten Papiers zur Frage des Datenschutzes im Internet, das die Datenschutzgruppe verabschiedet hat, wurde diese Forderung nachdrücklich bekräftigt:

See http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37de.pdf

andere Rechte und Pflichten für den Einzelnen festlegen (z. B. das Arbeitsrecht). Die Artikel 29-Datenschutzgruppe ist indessen überzeugt, dass die in diesem Arbeitsdokument vorgeschlagenen Lösungen bei dieser schwierigen Interessenabwägung hilfreich sein können.

4.2. ZULÄSSIGKEIT GEMÄß DER RICHTLINIE 95/46/EG

E-Mail-Nachrichten enthalten personenbezogene Daten, die durch die Bestimmungen der Richtlinie 95/46/EG geschützt sind. Daher muss ein Arbeitgeber einen legitimen Grund für die Verarbeitung dieser Daten nachweisen. Wie schon in der Stellungnahme 8/2001 ausführlich erläutert, muss die Einwilligung von dem Beschäftigten freiwillig und in vollständiger Kenntnis der Sachlage erteilt werden, und der Arbeitgeber sollte nicht versuchen, diese Verarbeitung generell auf die Einwilligung der betroffenen Person zu stützen.

Die wahrscheinlichste Rechtfertigung für die Überwachung des E-Mail-Verkehrs findet sich in Artikel 7 Buchstabe f der Richtlinie: die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden. Bevor die Anwendbarkeit dieser Vorschrift auf die hier diskutierten Maßnahmen erörtert wird, muss darauf hingewiesen werden, dass eine solche Rechtfertigung nicht den Grundrechten und Grundfreiheiten des Arbeitnehmers übergeordnet werden darf. Diese beinhalten gegebenenfalls auch das Grundrecht des Briefgeheimnisses.

Die Datenschutzgruppe hat bereits ihrer Auffassung Ausdruck gegeben, dass[22]:

"es in den Fällen, in denen ein Arbeitgeber zwangsläufig aufgrund des Beschäftigungsverhältnisses personenbezogene Daten verarbeiten muss, irreführend ist, wenn er versucht, diese Verarbeitung auf die Einwilligung der betroffenen Person zu stützen. Die Einwilligung der betroffenen Person sollte nur in den Fällen in Anspruch genommen werden, in denen der Beschäftigte eine echte Wahl hat und seine Einwilligung zu einem späteren Zeitpunkt widerrufen kann, ohne dass ihm daraus Nachteile erwachsen.

In Anbetracht der Tatsache, dass E-Mail-Nachrichten personenbezogene Daten sowohl des Absenders als auch des Empfängers enthalten und Arbeitgeber im Allgemeinen nur die Einwilligung einer dieser Parteien ohne größere Schwierigkeiten einholen können (soweit es sich nicht um Korrespondenz zwischen Beschäftigten handelt), ist die Möglichkeit der Legitimierung der Überwachung von E-Mail-Nachrichten auf der Grundlage einer solchen Einwilligung sehr begrenzt. Ähnliche Überlegungen treffen auf Artikel 7 Buchstabe b der Richtlinie zu, da eine der Parteien des Schreibens keinesfalls in einem Vertragsverhältnis mit dem für die Verarbeitung im Sinne dieser Bestimmung, d. h. zur Überwachung der E-Mail-Nachricht, Verantwortlichen steht.

---

22 Siehe den umrahmten Abschnitt auf Seite 28 der Stellungnahme 8/2001.

An diesem Punkt muss klargestellt werden, dass, wenn ein Arbeitnehmer ein privates E-Mail-Konto zur rein privaten Nutzung oder Zugang zu einem Internet-Mail-Konto erhält, das Öffnen von E-Mail-Nachrichten dieses Kontos durch den Arbeitgeber (ausgenommen zur Viruskontrolle) nur unter ganz bestimmten Umständen[23] gerechtfertigt werden kann. Unter normalen Umständen kann es nicht auf der Grundlage von Artikel 7 Buchstabe f gerechtfertigt werden, da der Arbeitgeber kein berechtigtes Interesse an einem Zugang zu derartigen Daten hat. Hier hat vielmehr das Grundrecht auf das Briefgeheimnis Vorrang.

Daher ist das Ausmaß, bis zu dem Artikel 7 Buchstabe f die Überwachung des E-Mail-Verkehrs gestattet, von Fall zu Fall von der Anwendung der in Kapitel 3.2 erläuterten Grundprinzipien abhängig. Wie bereits unter Punkt 3.1.4 (Zulässigkeit) dargelegt wurde, sollte bei der Abwägung auch die Privatsphäre derjenigen außerhalb der Organisation berücksichtigt werden, die von der Überwachung betroffen sind.

4.3 EMPFEHLUNGEN ZUM MINDESTMAß AN INFORMATIONEN, DIE DAS UNTERNEHMEN SEINEN ARBEITNEHMERN ZUR VERFÜGUNG STELLEN SOLLTE

Bei der Ausarbeitung ihrer Verfahrensrichtlinien müssen Arbeitgeber im Lichte der Erfordernisse und der Größe der Organisation die in Kapitel 3.1.3 im Rahmen des allgemeinen Grundsatzes der Transparenz genannten Grundsätze einhalten[24].

Im Hinblick auf den E-Mail-Verkehr im Besonderen sollten die folgenden Aspekte berücksichtigt werden:

a) Ob ein Arbeitnehmer befugt ist, ein E-Mail-Konto zur rein privaten Nutzung zu haben, ob die Nutzung von Internet-Mail-Konten am Arbeitsplatz gestattet ist und ob der Arbeitgeber die Nutzung eines privaten Internet-Mail-Kontos für rein private Zwecke durch die Arbeitnehmer empfiehlt (vgl. Kapitel 4.4).

b) Die Absprachen mit den Arbeitnehmern für den Zugriff auf den Inhalt einer E-Mail-Nachricht, z. B. wenn der Arbeitnehmer unerwartet abwesend ist, und die spezifischen Zwecke eines solchen Zugriffs.

---

[23] Dies wären unter anderem kriminelle Handlungen von Seiten des Arbeitnehmers, soweit der Arbeitgeber seine eigenen Interessen schützen muss, wenn er zum Beispiel für die Handlungen des Arbeitnehmers haftet oder Opfer der kriminellen Handlung ist.

[24]

1. Verfahrensrichtlinien für den Umgang mit E-Mail und Internet in dem Unternehmen, die genaue Angaben darüber enthalten, in welchem Umfang die im Besitz des Unternehmens befindlichen Kommunikationseinrichtungen von den Beschäftigten für die persönliche/private Kommunikation genutzt werden dürfen (z. B. Einschränkung von Nutzungszeiten und Nutzungsdauer).

2. Gegebenenfalls Gründe und Zwecke einer Überwachung. Soweit der Arbeitgeber die Nutzung der unternehmenseigenen Kommunikationseinrichtungen für private Zwecke ausdrücklich erlaubt hat, kann unter sehr eingeschränkten Bedingungen eine Überwachung dieser privaten Kommunikation vorgenommen werden, z. B. um die Sicherheit des Informationssystems zu gewährleisten (automatische Virenprüfung).

3. Die genauen Einzelheiten der Überwachungsmaßnahmen, d. h. Wer? Was? Wann?

4. Genaue Angaben über Durchsetzungsverfahren, aus denen hervorgeht, dass und wie die Mitarbeiter umgehend von Verstößen gegen die firmeninternen E-Mail-Verfahrensrichtlinien in Kenntnis gesetzt werden und die Möglichkeit erhalten, auf entsprechende, gegen sie erhobene Vorwürfe zu reagieren.

c) Wenn Sicherheitskopien von Nachrichten angelegt werden, wie lange diese gespeichert werden.

d) Angaben darüber, wann E-Mail-Nachrichten endgültig vom Server gelöscht werden.

e) Sicherheitsfragen.

f) Die Einbeziehung von Arbeitnehmervertretern in die Ausarbeitung der Verfahrensrichtlinien.

Es muss festgestellt werden, dass der Arbeitgeber verpflichtet ist zu gewährleisten, dass seine Verfahrensrichtlinien gemäß den technologischen Entwicklungen und der Standpunkte seiner Arbeitnehmer stets auf den neuesten Stand gebracht werden.

4.4 INTERNET-MAIL[25]

Die Datenschutzgruppe ist der Auffassung, dass derartige Verfahrensrichtlinien, die den Arbeitnehmern die Nutzung eines privaten E-Mail-Kontos oder von Internet-Mail erlauben, zu einer pragmatischen Lösung des genannten Problems beitragen könnten. Ein derartiges Arbeitsdokument des Arbeitgebers würde eine eindeutige Unterscheidung zwischen E-Mail-Nachrichten für geschäftliche und für private Zwecke ermöglichen und die Möglichkeit verringern, dass Arbeitgeber in die Privatsphäre ihrer Beschäftigten eindringen. Darüber hinaus würde sie dem Arbeitgeber keine bzw. minimale zusätzliche Kosten verursachen.

Durch die Einführung solcher Verfahrensrichtlinien hätte ein Arbeitgeber die Möglichkeit, in bestimmten Fällen, in denen ein ernsthafter Verdacht bezüglich des Verhaltens eines Mitarbeiters besteht, zu kontrollieren, in welchem Umfang dieser Arbeitnehmer seinen PC für persönliche Zwecke nutzt, indem er die Nutzungszeiten der Internet-Mail-Konten registriert. Auf diese Weise wären die Interessen des Arbeitgebers gewahrt, ohne dass die Gefahr bestünde, dass personenbezogene und insbesondere sensible Daten von Arbeitnehmern offengelegt werden.

Solche Verfahrensrichtlinien könnten auch für die Beschäftigten von Nutzen sein, da sie Gewissheit über den Grad an Privatheit hätten, den sie erwarten können, was bei komplizierteren und weniger eindeutigen Verhaltensregeln möglicherweise nicht der Fall wäre. In diesem Zusammenhang muss allerdings auch deutlich gemacht werden, dass

a) **die Tatsache, dass die Nutzung von Internet-Mail oder privaten E-Mail-Konten erlaubt ist, die umfassende Anwendbarkeit der vorstehenden Abschnitte dieses Kapitels auf andere E-Mail-Konten am Arbeitsplatz nicht einschränkt;**

b) sich die Unternehmen, wenn sie die Nutzung von Internet-Mail gestatten, bewusst sein müssen, dass diese die Sicherheit der Unternehmensnetze beeinträchtigen kann, insbesondere im Hinblick auf die Verbreitung von Viren;

---

[25] Internet-Mail ist ein E-Mail-System, das über das Internet das Abrufen von E-Mail-Nachrichten von jedem beliebigen POP- oder IMAP-Server ermöglicht und in der Regel durch Benutzerkennung und Passwort geschützt ist.

c) den Arbeitnehmern bewusst sein muss, dass Internet-Mail-Server in Drittländern stationiert sein können, in denen kein angemessener Schutz von personenbezogenen Daten besteht.

Es ist zu beachten, dass diese Überlegungen sich auf normale Arbeitgeber-Arbeitnehmer-Verhältnisse beziehen. Für die Kommunikationen von Arbeitnehmern, die an ein Berufsgeheimnis gebunden sind, sind unter Umständen spezielle Regelungen erforderlich.

5. ÜBERWACHUNG DES INTERNETZUGRIFFS

5.1 PRIVATE INTERNET-NUTZUNG AM ARBEITSPLATZ

Zunächst sollte betont werden, dass es Sache der Unternehmen ist, zu entscheiden, ob und in welchem Umfang sie ihren Beschäftigten die Nutzung des Internet für private Zwecke gestatten.

Allerdings vertritt die Datenschutzgruppe hierzu die Auffassung, dass ein pauschales Verbot der privaten Internet-Nutzung durch Arbeitnehmer unpraktisch und auch etwas unrealistisch erscheinen könnte, da es nicht dem Nutzen des Internet für das Alltagsleben der Arbeitnehmer entspricht.

5.2. GRUNDSÄTZE FÜR DIE ÜBERWACHUNG DES INTERNETZUGRIFFS

Es gibt einige Grundsätze, die in der Diskussion über die Überwachung des Internetzugriffs der Arbeitnehmer berücksichtigt werden sollten:

Soweit als möglich sollte **der Prävention Vorrang vor der Aufdeckung** eingeräumt werden. Mit anderen Worten: Dem Interesse des Arbeitgebers ist besser gedient, wenn der Missbrauch des Internet mit technischen Mitteln verhindert wird, als wenn Ressourcen eingesetzt werden, um Missbrauch aufzudecken. Statt das Mitarbeiterverhalten zu überwachen sollten sich Internet-Verfahrensrichtlinien nach Möglichkeit auf technische Mittel stützen, die den Zugriff einschränken, wie z. B. das Sperren bestimmter Websites oder die Installation automatischer Zugangs-Warnsysteme.

Die unverzügliche Unterrichtung des Arbeitnehmers über die Feststellung eines verdächtigen Internetzugriffs ist wichtig, um die Probleme möglichst gering zu halten. Selbst wenn eine Überwachung notwendig ist, muss sie eine **angemessene Reaktion** des Arbeitgebers auf die Risiken sein, mit denen er konfrontiert ist. In den meisten Fällen kann eine missbräuchliche Nutzung des Internet festgestellt werden, ohne dass es erforderlich wäre, den Inhalt der besuchten Seiten zu analysieren. So dürfte zum Beispiel die Überprüfung der Online-Zeiten oder der am häufigsten besuchten Websites auf Abteilungsebene genügen, um den Arbeitgeber Gewissheit zu verschaffen, dass seine Einrichtungen nicht missbräuchlich genutzt werden. Wenn bei diesen allgemeinen Überprüfungen eine möglicherweise missbräuchliche Nutzung des Internet festgestellt wird, kann der Arbeitgeber eine zusätzliche Überwachung des Gefährdungsbereichs in Betracht ziehen.

Bei der Beurteilung der Internet-Nutzung durch ihre Mitarbeiter **sollten die Arbeitgeber versuchen, mit Schlussfolgerungen vorsichtig zu sein,** und in Betracht ziehen, wie leicht es zu einem unbeabsichtigten Zugriff auf Websites durch das versehentliche Aktivieren von Antworten in Suchmaschinen, nicht eindeutige Hypertext-Links, irreführende Banner-Werbung und Eingabefehler kommen kann. In jedem Fall müssen den Arbeitnehmern die Fakten vorgelegt werden, und sie müssen umfassende Gelegenheit haben, den vom Arbeitgeber behaupteten Missbrauch zu widerlegen.

5.3 EMPFEHLUNGEN ZUM MINDESTINHALT DER INTERNET-VERFAHRENSRICHTLINIEN EINES UNTERNEHMENS

1. Die in Kapitel 3.1.3 im Rahmen des Grundsatzes der Transparenz angeführten Informationen[26].

   Im Hinblick auf die Internet-Nutzung sollten insbesondere die folgenden Aspekte berücksichtigt werden;

2. Der Arbeitgeber muss gegenüber den Arbeitnehmern eindeutig die Bedingungen darlegen, unter denen die private Nutzung des Internet zulässig ist. Ferner muss er festlegen, welche Inhalte nicht betrachtet oder kopiert werden dürfen. Diese Bedingungen und Einschränkungen müssen den Arbeitnehmern erläutert werden.

3. Die Arbeitnehmer müssen über die Systeme unterrichtet werden, die eingeführt wurden, um den Zugang zu bestimmten Websites zu verhindern und Missbrauch aufzudecken. Der Umfang einer derartigen Überwachung sollte definiert werden, z. B. ob Einzelpersonen oder bestimmte Bereiche des Unternehmens überwacht werden oder ob unter bestimmten Umständen die Inhalte der besuchten Websites vom Arbeitgeber betrachtet oder aufgezeichnet werden. Ferner sollten die Verfahrensrichtlinien festlegen, ob und zu welchem Zweck die Daten verwendet werden, die Informationen darüber liefern, welcher Mitarbeiter welche Seiten besucht hat.

4. Die Arbeitnehmer müssen über die Mitwirkung ihrer Vertreter sowohl an der Erstellung der Verfahrensrichtlinien als auch an der Untersuchung vermeintlicher Verstöße gegen die Verfahrensrichtlinien unterrichtet werden.

SCHLUSSFOLGERUNG

Die Datenschutzgruppe möchte mit diesem Arbeitsdokument einen Beitrag leisten zur einheitlichen Anwendung der nationalen Umsetzungsmaßnahmen zu Richtlinie 95/46/EG auf die Überwachung und Kontrolle der elektronischen Kommunikation am Arbeitsplatz. (Siehe Zusammenfassung in der nationalen Rechtsvorschriften im Anhang).

26

1. Verfahrensrichtlinien für den Umgang mit E-Mail und Internet in dem Unternehmen, die genaue Angaben darüber enthalten, in welchem Umfang die im Besitz des Unternehmens befindlichen Kommunikationseinrichtungen von den Beschäftigten für die persönliche/private Kommunikation genutzt werden dürfen (z. B. Einschränkung von Nutzungszeiten und Nutzungsdauer).

2. Gegebenenfalls Gründe und Zwecke einer Überwachung. Soweit der Arbeitgeber die Nutzung der unternehmenseigenen Kommunikationseinrichtungen für private Zwecke ausdrücklich erlaubt hat, kann unter sehr eingeschränkten Bedingungen eine Überwachung dieser privaten Kommunikation vorgenommen werden, z. B. um die Sicherheit des Informationssystems zu gewährleisten (automatische Virenprüfung).

3. Die genauen Einzelheiten der Überwachungsmaßnahmen, d. h. Wer? Was? Wann?

4. Genaue Angaben über Durchsetzungsverfahren, aus denen hervorgeht, dass und wie die Mitarbeiter umgehend von Verstößen gegen die firmeninternen E-Mail-Verfahrensrichtlinien in Kenntnis gesetzt werden und die Möglichkeit erhalten, auf entsprechende, gegen sie erhobene Vorwürfe zu reagieren.

Die Datenschutzgruppe hat einige Unterschiede zwischen den nationalen Rechtsvorschriften festgestellt, vor allem in mit dem Datenschutz verwandten Bereichen; sie betreffen Ausnahmen vom Grundrecht des Briefgeheimnisses und den Umfang und die Wirkungen von Arbeitnehmervertretung und Mitbestimmung. Die Datenschutzgruppe möchte jedoch betonen, dass Unterschiede zwischen den Maßnahmen der Mitgliedstaaten zur Umsetzung der Richtlinie 95/46/EG keine größeren Hindernisse für einen gemeinsamen Ansatz sind, wie ihn die Grundsätze und Modelllösungen darstellen, die in diesem Arbeitsdokument aufgezeigt werden.

Die Untergruppe für Beschäftigungsfragen wird dieses Arbeitsdokument im Lichte der Erfahrung und der weiteren Entwicklung dieses Bereichs im Zeitraum 2002-2003 überprüfen.

Brüssel, den 29. Mai 2002

Für die Gruppe

Der Vorsitzende

Stefano RODOTA