

FORUM Wirtschaftsrecht

Band 2

Herausgegeben vom
Institut für Wirtschaftsrecht an der Universität Kassel

Internet- und E-Mail-Überwachung am Arbeitsplatz

Dennis Hoss

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen
Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar

ISBN print: 978-3-89958-726-5

ISBN online: 978-3-89958-727-2

URN: urn:nbn:de:0002-7271

© 2009, kassel university press GmbH, Kassel
www.upress.uni-kassel.de

Druck und Verarbeitung: Unidruckerei der Universität Kassel
Umschlaggestaltung: Heike Arend, Unidruckerei der Universität Kassel
Printed in Germany

Vorwort

Die vom Institut für Wirtschaftsrecht der Universität Kassel herausgegebene Publikationsreihe „FORUM Wirtschaftsrecht“ soll u. a. auch dem wissenschaftlichen Nachwuchs als Plattform zur Verfügung stehen. Besonders erfreulich ist es, wenn von Studierenden Abschlussarbeiten auf so hohem Niveau vorgelegt werden, dass sie in die Reihe aufgenommen werden und somit der wirtschaftsrechtlichen Praxis durch die Aufarbeitung aktueller Fragestellungen dienen können.

Trotz der wissenschaftsfreundlichen Preisgestaltung durch den Verlag können sich in einem solchen Fall die Publikationskosten als nicht zu unterschätzende Hürde erweisen. Daher dankt das Institut für Wirtschaftsrecht der Juristischen Gesellschaft zu Kassel sehr für die Stiftung eines Absolventinnen- und Absolventenpreises, in dessen Rahmen die Druckkosten übernommen werden. Preisträger des Studienjahres 2007/08 ist Herr *Dennis Hoss, LL.M.*, der für seine im Sommer 2008 vorgelegte und von mir betreute Masterarbeit „Internet- und E-Mail-Überwachung am Arbeitsplatz“ ausgezeichnet wurde.

Das Thema der prämierten Masterarbeit ist zugleich theoretisch anspruchsvoll und von großer praktischer Relevanz: Längst ist das Internet zum unverzichtbaren Hilfsmittel für viele Arbeitsplätze geworden, aus Büroumgebungen ist es gar nicht mehr wegzudenken. Sein vernünftiger Einsatz vermag die Produktivität und die Qualität der Arbeit zu fördern, während übermäßiges oder gar unerlaubtes „Surfen“ ebenso schädliche Folgen nach sich ziehen kann wie der missbräuchliche Einsatz der E-Mail-Kommunikation.

Daher ist die Kontrolle des Surf- und E-Mail-Verhaltens der Belegschaft inzwischen betrieblicher Alltag. Beim unreflektierten Einsatz – aus technischer Sicht – leicht zu realisierender Überwachungsmaßnahmen ist dabei längst nicht nur an Supermarkketten und Konzernunternehmen zu denken. Auch Behörden, ja selbst Universitäten, strecken begehrliche Finger nach den Kommunikationsdaten ihrer Mitarbeiterinnen und Mitarbeiter aus, ohne sich in jedem Fall der Rechtmäßigkeit ihres Tuns sicher sein zu können.

Wegen des Fehlens eines speziellen Arbeitnehmerdatenschutzgesetzes wird der rechtliche Rahmen für eine Überwachung des Internet- und E-Mail-Verkehrs durch die allgemeinen Vorgaben des Bundesdatenschutzgesetzes, des Telekommunikationsgesetzes und des Telemediengesetzes gebildet. Vieles ist dabei noch unklar; die vergleichsweise spärliche Judikatur konnte bislang wenig zur Verbesserung der Rechtssicherheit beitragen. In der rechtswissenschaftlichen Literatur wird die Problematik zwar seit Längerem diskutiert, eine zugleich inhaltlich überzeugende und wegen ihrer Übersichtlichkeit und Vollständigkeit für die unternehmerische Praxis taugliche Aufbereitung der drängenden Fragen wurde jedoch bislang nicht vorgelegt.

Herrn *Hoss* ist es durchwegs gelungen, die mit dem anspruchsvollen Thema verbundenen Rechtsfragen zutreffend zu identifizieren und an Hand der bisher vorliegenden Literaturstimmen überzeugend zu beantworten. Selbst komplexe Zusammenhänge stellt er dabei in klarer, gut lesbarer Sprache dar. Das besondere Verdienst der von Herrn *Hoss* vorgelegten Arbeit ist darin zu sehen, dass sie die wesentlichen Fragen der Internet- und E-Mail-Überwachung am Arbeitsplatz in einer auch als Handreichung für die unternehmerische Praxis gut geeigneten Weise beantwortet. Dazu trägt nicht zuletzt der Anhang mit seinen nützlichen Formulierungsvorschlägen bei.

Dass dieser zweite Band der Publikationsreihe „FORUM Wirtschaftsrecht“ zum reflektierten und rechtlich abgesicherten Umgang mit unseren Kommunikationsdaten beitragen möge, hoffe ich zuversichtlich.

Kassel, im Mai 2009

Prof. Dr. Dr. *Walter Blocher*
Gf. Direktor des Instituts für Wirtschaftsrecht

Inhaltsverzeichnis

Literatur- und Quellenverzeichnis	VII
Abbildungsverzeichnis	XVIII
1 EINFÜHRUNG UND AUFBAU DER ARBEIT	1
2 TECHNISCHE GRUNDLAGEN.....	5
2.1 Internet und E-Mail	5
2.2 Überwachungsmöglichkeiten	9
2.2.1 Überwachung des Internets.....	9
2.2.2 Überwachung von E-Mail.....	12
3 GEGENÜBERSTELLUNG VON ARBEITGEBER- UND ARBEIT- NEHMERINTERESSEN.....	14
3.1 Überwachungsinteressen des Arbeitgebers.....	15
3.1.1 Überprüfung der geschuldeten Arbeitsleistung.....	15
3.1.2 Schutz vor Malware.....	16
3.1.3 Verhinderung des Entstehens zusätzlicher Kosten.....	17
3.1.4 Ausschluss der Mithaftung.....	17
3.1.5 Verhinderung einer Systemüberlastung	18
3.1.6 Vermeidung eines Imageschadens	19
3.1.7 Unterbinden strafbarer Handlungen.....	19
3.1.8 Schutz vor Wirtschaftsspionage.....	20
3.2 Schutzinteressen des Arbeitnehmers.....	21
3.2.1 Vermeidung der Schaffung eines gläsernen Mitarbeiters	22
3.2.2 Schutz vor technikimmanenten Gefahren.....	23
4 RECHTLICHER RAHMEN	26
4.1 Europäische Vorschriften	26
4.2 Deutsche Vorschriften.....	28
4.2.1 Verfassungsrechtliche Ebene.....	28

4.2.1.1	Tangierte Grundrechte auf Arbeitgeberseite	29
4.2.1.1.1	Allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG.....	29
4.2.1.1.2	Berufsfreiheit aus Art. 12 Abs. 1 GG	29
4.2.1.1.3	Eigentumsrecht aus Art. 14 GG	30
4.2.1.2	Tangierte Grundrechte auf Arbeitnehmerseite.....	30
4.2.1.2.1	Allgemeines Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG.....	30
4.2.1.2.2	Fernmeldegeheimnis aus Art. 10 GG	32
4.2.2	Ebene der einfachen Gesetze und Rechtsverordnungen	33
4.2.2.1	Datenschutz-, Telekommunikations- und Telemedi- recht.....	33
4.2.2.1.1	Bundesdatenschutzgesetz	36
4.2.2.1.2	Telekommunikationsgesetz	37
4.2.2.1.3	Telemediengesetz	37
4.2.2.2	Arbeitsrecht	38
4.2.2.2.1	Betriebsverfassungsgesetz.....	38
4.2.2.2.2	Bildschirmarbeitsverordnung.....	38
5	ÜBERWACHUNG DER INTERNET- UND E-MAIL- KOMMUNIKATION NACH AKTUELLER RECHTSLAGE.....	40
5.1	Abgrenzung zwischen betrieblicher und privater Nutzung	40
5.1.1	Erlaubnis zur privaten Nutzung	42
5.1.1.1	Ausdrückliche Erlaubnis.....	42
5.1.1.2	Konkludente Erlaubnis.....	43
5.1.1.3	Betriebliche Übung	44
5.1.1.4	Einschränkung der Erlaubnis	45
5.1.1.5	Rücknahme der Erlaubnis.....	45
5.1.2	Konsequenzen der erlaubten Privatnutzung.....	46
5.2	Überwachung des Internets	51
5.2.1	Überwachung bei unerlaubter Privatnutzung bzw. bei betrieblicher Nutzung	51
5.2.1.1	Gesetzliche Ermächtigung	52
5.2.1.1.1	Äußere Umstände	55
5.2.1.1.2	Inhaltsdaten	57
5.2.1.2	Prüfung von Erweiterungsmöglichkeiten der Überwachungsbefugnis	58
5.2.1.2.1	Einwilligung der Arbeitnehmer	58

5.2.1.2.2	Regelung durch Betriebsvereinbarung oder Tarifvertrag	61
5.2.2	Überwachung bei erlaubter Privatnutzung	63
5.2.2.1	Beurteilung nach dem Telekommunikationsgesetz	65
5.2.2.1.1	Bestandsdaten	66
5.2.2.1.2	Verkehrsdaten	68
5.2.2.1.3	Inhaltsdaten	69
5.2.2.2	Beurteilung nach dem Telemediengesetz	70
5.2.2.3	Prüfung von Erweiterungsmöglichkeiten der Überwachungsbefugnis	73
5.2.2.3.1	Einwilligung der Arbeitnehmer	73
5.2.2.3.2	Regelung durch Betriebsvereinbarung oder Tarifvertrag	76
5.2.3	Überwachung bei Mischnutzung	77
5.3	Überwachung von E-Mail	78
5.3.1	Überwachung bei unerlaubter Privatnutzung bzw. betrieblicher Nutzung	78
5.3.1.1	Äußere Umstände	82
5.3.1.2	Inhaltsdaten	82
5.3.2	Überwachung bei erlaubter Privatnutzung	85
5.3.2.1	Beurteilung nach dem Telekommunikationsgesetz	85
5.3.2.2	Beurteilung nach dem Telemediengesetz	85
5.3.3	Überwachung bei Mischnutzung	86
5.4	Überwachung bei besonderen Berufsgruppen	87
5.5	Folgen einer unerlaubten Privatnutzung	90
5.5.1	Ermahnung	91
5.5.2	Sperrung des Internet-Zugangs	91
5.5.3	Abmahnung	92
5.5.4	Kürzung der Vergütung	93
5.5.5	Ordentliche Kündigung	94
5.5.6	Außerordentliche Kündigung	95
5.5.7	Schadenersatzansprüche	97
5.5.8	Strafanzeige	98
5.6	Folgen einer rechtswidrigen Überwachung	99
5.6.1	Unterlassungsanspruch	99
5.6.2	Beseitigungsanspruch	100
5.6.3	Löschungsanspruch	100
5.6.4	Verwertungsverbot	101
5.6.5	Zurückbehaltungsrecht	101

5.6.6	Schadenersatzansprüche.....	102
5.6.7	Strafbarkeit	103
5.6.7.1	Ausspähen von Daten	104
5.6.7.2	Abfangen von Daten.....	105
5.6.7.3	Verletzung des Fernmeldegeheimnisses	105
5.6.7.4	Datenveränderung.....	107
5.6.7.5	Sonstige Straftatbestände	108
5.6.8	Ordnungswidrigkeit.....	108
5.7	Rechte der Arbeitnehmer bei Verwendung personen- bezogener Daten durch den Arbeitgeber.....	109
6	BETRIEBSVERFASSUNGSRECHTLICHE ASPEKTE	112
6.1	Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG	113
6.2	Ausübung der Mitbestimmung	116
7	RECHTSPRECHUNG	118
8	FAZIT UND AUSBLICK.....	123
	Anlagenverzeichnis.....	127

Literatur- und Quellenverzeichnis

Altenburg, Stephan/Reinersdorff, Wolfgang von/Leister, Thomas,
Telekommunikation am Arbeitsplatz, MMR 2005, 135-139.

Dies.,
Betriebsverfassungsrechtliche Aspekte der Telekommunikation
am Arbeitsplatz, MMR 2005, 222-226.

Barton, Dirk-M.,
Risiko-Management und IT-Sicherheit. Der europäische
Gesetzgeber will die Überwachung des Internetarbeitsplatzes
weitgehend einschränken, K&R 2004, 305-312.

Ders.,
(Mit-)Verantwortlichkeit des Arbeitgebers für rechtsmissbräuch-
liche Online-Nutzungen durch den Arbeitnehmer, CR 2003, 592-
598.

Ders.,
Betriebliche Übung und private Nutzung des Internetarbeits-
platzes – „Arbeitsrechtliche Alternativen“ zur Wiedereinführung
der alleinigen dienstlichen Verwendung, NZA 2006, 460-466.

Beck'scher Online-Kommentar Arbeitsrecht,
hrsg. v. Rolfs, Christian/Giesen, Richard/Kreikebohm, Ralf u. a., (Ed.
7, Stand: 1.3.2008) (zitiert: *Bearbeiter*, in: Beck'scher Online-
Kommentar Arbeitsrecht).

Beck'scher Online-Kommentar Grundgesetz,
hrsg. v. Epping, Volker/Hillgruber, Christian, (Ed. 1, Stand:
1.2.2008) (zitiert: *Bearbeiter*, in: Beck'scher Online-Kommentar
GG).

Beck'scher TKG-Kommentar,
hrsg. v. Geppert, Martin/Piepenbrock, Hermann-Josef/Schütz,
Raimund u. a., 3. Aufl., München 2006 (zitiert: *Bearbeiter*, in:
Beck'scher TKG-Kommentar).

Beckschulze, Martin,

Internet-, Intranet- und E-Mail-Einsatz am Arbeitsplatz. Rechte der Beteiligten und Rechtsfolgen bei Pflichtverletzungen, DB 2003, 2777-2786.

Beckschulze, Martin/Henkel, Wolfram,

Der Einfluss des Internets auf das Arbeitsrecht, DB 2001, 1491-1506.

Bender, Rolf/Kahlen, Christine,

Neues Telemediengesetz verbessert den Rechtsrahmen für Neue Dienste und Schutz vor Spam-Mails, MMR 2006, 590-594.

Bernhardt, Marion/Barthel, Thomas,

Beispiel unerlaubte Internetnutzung. Die außerordentliche Tat- und Verdachtskündigung, AuA 2008, 150-153.

Besgen, Nicolai/Prinz, Thomas,

Dienstliche und private Nutzung von Internet, Intranet und E-Mail – Individualarbeitsrecht, in: *Besgen, Nicolai/Prinz, Thomas* (Hrsg.), *Neue Medien und Arbeitsrecht. Internet, E-Mail und andere moderne Kommunikationsmittel*, Bonn 2006, S. 37-82.

Dies.,

Internet, Intranet und E-Mail – Kollektives Arbeitsrecht, in: *Besgen, Nicolai/Prinz, Thomas* (Hrsg.), *Neue Medien und Arbeitsrecht. Internet, E-Mail und andere moderne Kommunikationsmittel*, Bonn 2006, S. 83-118.

Böker, Karl-Hermann/Kamp, Lothar,

Betriebliche Nutzung von Internet, Intranet und E-Mail. Analyse und Handlungsempfehlungen, Frankfurt 2003.

Borchers, Detlef/Benning, Maria/Kuri, Jürgen,

“Hätt ich dich heute erwartet...“. Das Internet hat Geburtstag – oder nicht?, c’t 21/1999, 128-133.

Busse, Julia,

Datenschutz, in: *Besgen, Nicolai/Prinz, Thomas* (Hrsg.), *Neue Medien und Arbeitsrecht. Internet, E-Mail und andere moderne Kommunikationsmittel*, Bonn 2006, S. 341-399.

Däubler, Wolfgang,

Internet und Arbeitsrecht, 2. Aufl., Frankfurt 2002.

Ders.,

Nutzung des Internet durch Arbeitnehmer, *K&R* 2000, 323-327.

Ders.,

Das neue Bundesdatenschutzgesetz und seine Auswirkungen im Arbeitsrecht, *NZA* 2001, 874-881.

Dickmann, Roman,

Inhaltliche Ausgestaltung von Regelungen zur privaten Internetnutzung im Betrieb, *NZA* 2003, 1009-1013.

Elschner, Günter,

Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, *Lohmar*, Köln 2004.

Erfurter Kommentar zum Arbeitsrecht,

hrsg. v. *Müller-Glöge, Rudi/Preis, Ulrich/Schmidt, Ingrid*, 8. Aufl., Bd. 51, München 2008 (zitiert: *ErfK/Bearbeiter*).

Erler, Andreas,

Die private Nutzung neuer Medien am Arbeitsplatz, München 2003.

Ernst, Stefan,

Der Arbeitgeber, die E-Mail und das Internet, *NZA* 2002, 585-591.

Ders.,

Privates Surfen am Arbeitsplatz als Kündigungsgrund. Folgerungen aus dem BAG-Urteil vom 7. Juli 2005, *DuD* 2006, 223-225.

Fischer, Ulrich,

„Surfen“ im Internet, AuR 2006, 206-208.

Freund, Ferdinand/Knoblauch, Rolf/Eisele, Daniela,

Praxisorientierte Personalwirtschaftslehre, 6. Aufl., Stuttgart 2003.

Frey, Hartmut,

E-Mail: Revolution im Unternehmen. Wie sich Motivation, Kommunikation und Innovationsgeist der Mitarbeiter wandeln. Studie im Auftrag des Bundesforschungsministeriums mit einer Befragung von 50 Unternehmen, Neuwied, Kriftel 1999.

Gerling, Rainer W.,

Betrieb von WWW-Servern. Rechtliche und technische Aspekte, IT-Sicherheit 3/2001, 18-22.

Ders.,

Betriebsvereinbarung E-Mail und Internet. Ein kommentierter Entwurf für die Praxis, DuD 1997, 703-708.

Gliss, Hans/Kramer, Philipp,

Arbeitnehmerdatenschutz. Aktionsfelder für Betriebsräte, Frankfurt 2006.

Gola, Peter,

Datenschutz und Multimedia am Arbeitsplatz, Frechen 2006.

Ders.,

Neuer Tele-Datenschutz für Arbeitnehmer? Die Anwendung von TKG und TDDSG im Arbeitsverhältnis, MMR 1999, 322-330.

Hanau, Peter/Hoeren, Thomas,

Private Internetnutzung durch Arbeitnehmer. Die arbeits- und betriebsverfassungsrechtlichen Probleme, München 2003.

Hase, Karl von,

Fristlose Kündigung und Abmahnung nach neuem Recht, NJW 2002, 2278-2283.

Haußmann, Katrin/Krets, Jérôme,
EDV-Betriebsvereinbarungen im Praxistest, NZA 2005, 259-264.

Heidrich, Joerg/Tschoepe, Sven,
Rechtsprobleme der E-Mail-Filterung, MMR 2004, 75-80.

Henke, Jens,
IT und Datenschutz im Unternehmen. Was Arbeitgeber prüfen dürfen und wo das Kontrollrecht endet, Saarbrücken 2006.

Hilber, Marc D./Frik, Roman,
Rechtliche Aspekte der Nutzung von Netzwerken durch Arbeitnehmer und den Betriebsrat, RdA 2002, 89-97.

Höld, Florian,
Die Überwachung von Arbeitnehmern. Nicht-technische Überwachungsmethoden, technische Überwachungsmethoden und ärztliche Untersuchungen, Hamburg 2006.

Hoeren, Thomas,
Grundzüge des Internetrechts. E-Commerce, Domains, Urheberrecht, 2. Aufl., München 2002.

Ders.,
Internetrecht (Stand: März 2008), http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz2008.pdf (Zugriff 30.4.08).

Ders.,
Das Telemediengesetz, NJW 2007, 801-806.

Ders.,
Virenscreening und Spamfilter – Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co., NJW 2004, 3513-3517.

Holenstein, Christoph,
Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, Bern 2002.

Hornung, Gerrit,

Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das WWW, MMR 2004, 3-8.

Hunold, Wolf,

Die Rechtsprechung zur Abmahnung, NZA-RR 2000, 169-175.

Kiper, Manuel,

Spione im Büro. Überwachung am Arbeitsplatz, in: *Schulzki-Haddouti* (Hrsg.), Bürgerrechte im Netz, Bonn 2003, S. 92-108.

Klasen, Evelyn,

Unternehmensinterne Datennetze im Lichte der Betriebsverfassung. Neue betriebliche Kommunikationstechnologien (Intranet) als Gegenstand der Zusammenarbeit zwischen Arbeitgeber und Betriebsrat, Berlin 2005.

Köhler, Markus/Arndt, Hans-Wolfgang,

Recht des Internet, 4. Aufl., Heidelberg 2003.

Kömpf, Nicola/Kunz, Holger,

Kontrolle der Nutzung von Internet und E-Mail am Arbeitsplatz in Frankreich und in Deutschland, NZA 2007, 1341-1346.

Koeppen, Thomas,

Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz. Deutschland, Großbritannien und USA im Vergleich, Hamburg 2007.

Kramer, Stefan,

Internetnutzung als Kündigungsgrund, NZA 2004, 457-464.

Ders.,

Kündigung wegen privater Internetnutzung, NZA 2006, 194-197.

Ders.,

BAG zur Kündigung wegen privater Internetnutzung, NZA 2007, 1338-1341.

Langner, Sören/Witt, Boris,

Aktuelles zur Verdachtskündigung, DStR 2008, 825-830.

Mattl, Tina,

Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz: unter besonderer Berücksichtigung der Vorgaben des Telekommunikationsgesetzes, Hamburg 2008.

Mengel, Anja,

Kontrolle der E-mail- und Internetkommunikation am Arbeitsplatz. Wege durch einen juristischen Irrgarten, BB 2004, 2014-2021.

Mester, Britta Alexandra,

Datenschutzrechtliche Aspekte bei der Nutzung von E-Mail am Arbeitsplatz, in: *Hammermeister, Jörg/Reich, Bettina/Rose, Edgar* (Hrsg.), Information – Wissen – Kompetenz, Oldenburg 2004, S. 35-64.

Michalke, Reinhart,

Wenn der Staatsanwalt klingelt – Verhalten bei Durchsuchung und Beschlagnahme, NJW 2008, 1490-1494.

Mühlbauer, Peter,

Trojaner vom Chef, <http://www.heise.de/tp/r4/artikel/22/22268/1.html> (Zugriff 27.3.2008).

Münz, Stefan/Nefzger, Wolfgang,

HTML Handbuch. WWW-Projekte richtig planen – Style Sheets, Frames, Layer – Grafik richtig einsetzen – Java-Applets und JavaScripts – Tips und Tricks zu HTML, Feldkirchen 1997.

Nägele, Stefan/Meyer, Lars,

Internet und E-Mail am Arbeitsplatz: Rechtliche Rahmenbedingungen der Nutzung und Kontrolle sowie der Reaktion auf Missbrauch, K&R 2004, 312-317.

Ohlenburg, Anna,

Der neue Telekommunikationsdatenschutz – eine Darstellung von Abschnitt 7 Teil 2 TKG, MMR 2004, 431-440.

- o. V.,
http://www.bitkom.de/de/markt_statistik/46261_38546.aspx
(Zugriff 23.3.2008).
- o. V.,
<http://www.internetrecht-rostock.de/betriebsvereinbarung.pdf>
(Zugriff 29.3.2008).
- o. V.,
<http://www.linux-hamburg.de/thintelligent/compnetz2.gif>
(Zugriff 5.4.2008).
- o. V.,
http://www.arbeitsrecht.de/arbeitsrecht/RechtKompakt/Rechtsprechung/2008/2008_04_10_kuendigung_wegen_privater_nutzung_eines_dienst-pcs_erfordert_abmahnung.php?navid=1
(Zugriff 13.5.2008).
- o. V.,
<http://www.heise.de/newsticker/meldung/109190> (Zugriff 9.6.2008).
- o. V.,
<http://www.tse.de/vereinbarungen/internet%20und%20netze/policy.html> (Zugriff 18.6.2008).
- o. V.,
http://www.bfdi.bund.de/cln_027/nn_530440/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/Arbeitnehmerdatenschutzgesetz.html (Zugriff 19.6.2008).

Panzer, Andrea,
Mitarbeiterkontrolle und neue Medien, Frankfurt, Berlin, Bern,
Brüssel, New York, Oxford, Wien 2004.

Raffler, Andrea/Hellich, Peter,
Unter welchen Voraussetzungen ist die Überwachung von
Arbeitnehmer-e-mails zulässig?, NZA 1997, 862-868.

Rath, Michael/Karner, Sophia,

Private Internetnutzung am Arbeitsplatz – rechtliche Zulässigkeit und Kontrollmöglichkeiten des Arbeitgebers, K&R 2007, 446-452.

Roßnagel, Alexander,

Das Telemediengesetz – Neuordnung für Informations- und Kommunikationsdienste, NVwZ 2007, 743-748.

Ders.,

Datenschutz in einem informatisierten Alltag, Berlin 2007.

Sassenberg, Thomas/Bamberg, Niclas,

Betriebsvereinbarung contra BDSG?, DuD 2006, 226-229.

Schmidl, Michael,

Private E-Mail-Nutzung – Der Fluch der guten Tat. § 206 StGB als Folge der Gestattung privater E-Mail-Nutzung am Arbeitsplatz, DuD 2005, 267-271.

Ders.,

E-Mail-Filterung am Arbeitsplatz, MMR 2005, 343-348.

Schönfeld, Anja/Strese, Franziska/Flemming, Anne,

Ausgewählte Probleme der Nutzung des Internet im Arbeitsleben, MMR 2001, 8-13.

Scholz, Christian,

Personalmanagement. Informationsorientierte und verhaltens-theoretische Grundlagen, 5. Aufl., München 2000.

Schuster, Heidi,

Haftung für Malware im Arbeitsverhältnis. Haftung für Schäden, die Mitarbeitern aus der erlaubten privaten Nutzung der IT-Infrastruktur des Arbeitgebers entstehen, DuD 2006, 424-432.

Spindler, Gerald,

Das neue Telemediengesetz – Konvergenz in sachten Schritten, CR 2007, 239-245.

Steidle, Roland,

Multimedia-Assistenten im Betrieb. Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme, Wiesbaden 2005.

Tinnefeld, Marie-Theres,

Die Novellierung des BDSG im Zeichen des Gemeinschaftsrechts, NJW 2001, 3078-3083.

Dies.,

Arbeitnehmerdatenschutz in Zeiten des Internet, MMR 2001, 797-800.

Tinnefeld, Marie-Theres/ Viethen, Hans Peter,

Arbeitnehmerdatenschutz und Internet-Ökonomie. Zu einem Gesetz über Information und Kommunikation im Arbeitsverhältnis, NZA 2000, 977-983.

Tuchbreiter, Stephan,

Beteiligungsrechte des Betriebsrats bei der Einführung und Anwendung moderner Kommunikationsmittel, Hamburg 2007.

Waltermann, Raimund,

Anspruch auf private Internetnutzung durch betriebliche Übung?, NZA 2007, 529-533.

Weißgerber, Michael,

Das Einsehen kennwortgeschützter Privatdaten des Arbeitnehmers durch den Arbeitgeber, NZA 2003, 1005-1009.

Ders.,

Arbeitsrechtliche Fragen bei der Einführung und Nutzung vernetzter Computerarbeitsplätze, Berlin 2003.

Weißnicht, Elmar,

Die Nutzung des Internet am Arbeitsplatz, MMR 2003, 448-453.

Worzalla, Michael (Hrsg.),

Internet am Arbeitsplatz. Arbeitsrechtliche Grundlagen zur Vermeidung von unerwünschter Privatnutzung und Missbrauchsfällen, Berlin 2006 (zitiert: *Lelley*, in: *Worzalla*).

Zilkens, Martin,

Datenschutz am Arbeitsplatz, DuD 2005, 253-261.

Zscherpe, Kerstin A.,

Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, 723-727.

Abbildungsverzeichnis

Abb. 1	Drei Ebenen der Telekommunikation	S. 33
--------	-----------------------------------	-------

1 EINFÜHRUNG UND AUFBAU DER ARBEIT

Die Nutzung von Computern am Arbeitsplatz ist heutzutage aus dem betrieblichen Alltag nicht mehr wegzudenken. Eine Studie von BITKOM¹ aus dem Jahre 2006 belegt, dass nunmehr 56 Prozent aller Beschäftigten in Deutschland mit einem Computer arbeiten². Nicht weniger bahnbrechend als die Einführung moderner EDV-Systeme war die Entstehung des Internets mit all seinen Diensten, u. a. E-Mail, und der Einzug dieser Informationstechnik in Unternehmen. Die Vorteile der modernen IuK-Systeme liegen auf der Hand: Erhebliche Effizienzsteigerungen resultieren aus der komfortablen Suche z. B. nach Informationen über Märkte, Produkte von Wettbewerbern und technischen Entwicklungen. Die Vielfalt, Aktualität und sofortige Verfügbarkeit der Daten sind die wesentlichen Vorzüge im Vergleich zu herkömmlichen, meist zeit- und kostenaufwändigen Methoden der Informationsbeschaffung³. Auch der unternehmenseigene Internet-Auftritt spielt oftmals eine große Rolle, wenn es um die Generierung von Neukunden geht. Der E-Mail-Dienst ermöglicht den virtuellen Schriftwechsel in nahezu Echtzeit und bietet darüber hinaus auch die Möglichkeit, Dateianhänge, sog. Attachments, der eigentlichen Nachricht anzufügen. Überdies ist der Versand von E-Mail-Nachrichten - je nach Ausgestaltung der Zugangsmöglichkeit zum Internet - praktisch kostenfrei oder mindestens zu nur einem winzigen Bruchteil der Kosten des herkömmlichen Briefverkehrs zu realisieren. Als weiterer Vorzug von Internet und E-Mail lässt sich die gesteigerte Kommunikationsflexibilität durch die Möglichkeit der ortsunabhängigen Nutzung der Medien nennen.

¹ BITKOM, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

² Vgl. o. V., http://www.bitkom.de/de/markt_statistik/46261_38546.aspx (23.3.08).

³ Vgl. *Elschner*, Rechtsfragen der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2004, S. 3.

Den zahlreichen Positiveffekten eines Arbeitsplatzes mit Online-Zugang stehen jedoch auch Risiken gegenüber: Allzu oft ist die Versuchung für Mitarbeiter zu groß, auch private Angelegenheiten über den Internet-Anschluss des Arbeitgebers zu Lasten der Arbeitszeit zu erledigen. Neben der eher „harmlosen“ Inanspruchnahme von Web-Diensten, wie Wettervorhersagen oder Routenplaner, treten missbräuchliche und damit u. U. auch für den Arbeitgeber selbst strafrechtlich relevante Nutzungsaktivitäten. Um einerseits diesen Gefahren vorzubeugen und andererseits rückwirkend – im Falle einer bereits vollzogenen missbräuchlichen Nutzung – die erforderlichen Maßnahmen treffen zu können, hat die Arbeitgeberseite ein berechtigtes Interesse daran, die Internet- und E-Mail-Aktivitäten der Mitarbeiter zu kontrollieren.

Die vorliegende Arbeit befasst sich mit den zentralen Fragen, inwieweit eine Überwachung des Internet- und E-Mail-Verkehrs der Mitarbeiter durch den Arbeitgeber zulässig ist und innerhalb welcher rechtlichen Grenzen sich solche Kontrollmaßnahmen bewegen müssen. Im Fokus der Betrachtung stehen dabei insbesondere die Datenschutzbestimmungen des allgemeinen Datenschutzrechts sowie des Telekommunikations- und Telemedienrechts.

Im zweiten Kapitel, **Technische Grundlagen**, wird der technische „Hintergrund“ der Internet- und E-Mail-Technologie kurz dargestellt; ferner werden Möglichkeiten zu deren Überwachung aufgezeigt. Technische Grundkenntnisse sind für die rechtliche Beurteilung der Thematik unabdingbar.

Kapitel 3, **Gegenüberstellung von Arbeitgeber- und Arbeitnehmerinteressen**, verdeutlicht das Spannungsverhältnis der Arbeitsvertragsparteien im Hinblick auf die Kontrolle der Internet- und E-Mail-Nutzung; den Überwachungsinteressen des Arbeitgebers stehen die Schutzinteressen der Arbeitnehmer gegenüber.

Die im vierten Kapitel, **Rechtlicher Rahmen**, skizzierten Rechtsvorschriften auf europäischer und nationaler Ebene bilden das Gerüst der von der Themenstellung tangierten Normen. Insbesondere die auf einfachgesetzlicher Ebene vorzunehmende Differenzierung zwischen dem allgemeinen Datenschutzrecht, dem Telekommunikations- und dem Telemedienrecht sowie die Frage nach der Eröffnung des jeweiligen Anwendungsbereichs sind hier von erheblicher Relevanz.

Den eigentlichen Kern der Abhandlung bildet Kapitel 5, **Überwachung der Internet- und E-Mail-Kommunikation nach aktueller Rechtslage**. Darin wird die Zulässigkeit der Überwachung des Internet- und E-Mail-Verkehrs jeweils danach unterschieden, ob den Arbeitnehmern die Privatnutzung gestattet oder untersagt ist. Berufsgruppen, die einen Sonderstatus genießen, werden gesondert behandelt. Sanktionsmöglichkeiten des Arbeitgebers auf Pflichtverletzungen durch Arbeitnehmer werden ebenso aufgezeigt wie denkbare Konsequenzen für die Arbeitgeberseite, falls die Internet- und E-Mail-Überwachung in rechtswidriger Weise erfolgt ist. Die abschließenden Ausführungen dieses Kapitels beschäftigen sich mit Rechten, die Arbeitnehmern zustehen, wenn der Arbeitgeber mit ihren personenbezogenen Daten umgeht.

Kapitel 6, **Betriebsverfassungsrechtliche Aspekte**, behandelt ein zentrales Mitbestimmungsrecht des Betriebsrats, mit welchem er auf die Ausgestaltung der Kontrollmaßnahmen des Arbeitgebers Einfluss zu nehmen vermag. Darüber hinaus erfolgt die Darstellung der Ausübung dieses Mitbestimmungsrechts in Form einer Betriebsvereinbarung.

Im siebten Kapitel, **Rechtsprechung**, wird anhand des jüngsten Urteils im Zusammenhang mit der unerlaubten Internet-Nutzung erörtert, welche Pflichtverletzungen ein kündigungsrelevantes Verhalten darstellen können.

Schließlich sind in Kapitel 8, **Fazit und Ausblick**, wichtige Aussagen und Erkenntnisse zusammengefasst, die aus den vorangegangenen Ausführungen resultieren. Es wird ferner versucht, einen Blick auf das zukünftige Feld des Arbeitnehmerdatenschutzes zu werfen.

Im **Anhang** ist ein praxistauglicher Leitfaden für Arbeitgeber abgedruckt, mit dem sich die Zulässigkeit geplanter oder bereits vollzogener Überwachungsmaßnahmen beurteilen lässt (Anlage 1). Überdies sind in diesem Teil exemplarische Mustervereinbarungen und ergänzende Informationen zur Arbeit enthalten.

Anmerkungen:

- Die Ausführungen in der vorliegenden Arbeit beziehen sich ausschließlich auf nichtöffentliche Unternehmen.
- Aufgrund der einfacheren Lesbarkeit wird auf die Differenzierung zwischen weiblicher und männlicher Form verzichtet; die jeweilige Nennung der männlichen Form umfasst stets beide Geschlechter.

2 TECHNISCHE GRUNDLAGEN

Um zum besseren Verständnis der vorliegenden Arbeit beizutragen, sollen in diesem Kapitel technische Grundlagen über die Funktionsweise von Internet und E-Mail vermittelt werden; erst ein gewisses Grundlagenwissen ermöglicht die rechtliche Einschätzung der Problematik. Zunächst wird aufgezeigt, welche Dienste unter dem Begriff „Internet“ zu subsumieren sind. Anschließend wird die Funktionsweise von E-Mail erläutert.

Daran anknüpfend erfolgt eine kurze Darstellung der verschiedenen technischen und organisatorischen Maßnahmen, welche die Überwachung der Internet- und E-Mail-Aktivitäten von Mitarbeitern ermöglichen.

2.1 Internet und E-Mail

Das Internet⁴ wurde in den 1960er-Jahren aus militärischen Gründen in den USA entwickelt. Primäres Ziel, welches mit dem Aufbau des Internets verfolgt wurde, war die Schaffung eines dezentralen Datennetzes, bei dem der Informationsfluss nicht durch Ausfälle einzelner Netzknoten unterbrochen werden konnte⁵. Das damalige sog. ARPANET (United States Advanced Research Projects Agency) sollte auch im Falle eines Atomkriegs funktionsfähig bleiben⁶. Die 1970er- und 1980er-Jahre brachten politische Entspannung und das Netz verlor seine Bedeutung für das Militär. Im Jahre 1983 wurde das Netz in einen militärischen Teil – das sog. MILNET – und einen zivilen

⁴ Zur Entstehung und geschichtlichen Entwicklung des Internets siehe bspw. *Borchers/Benning/Kuri*, c't 21/1999, 128-133.

⁵ Vgl. *Münz/Nefzger*, HTML Handbuch, 1997, S. 25.

⁶ Vgl. *Köhler/Arndt*, Recht des Internet, 4. Aufl. (2003), S. 2.

aufgeteilt; aus dem zivilen Teil entwickelte sich allmählich das heutige Internet.⁷

Das Internet versteht sich als weltweiter Verbund von Einzelcomputern und Netzwerken, die über Leitungen gleichrangig miteinander verbunden sind. Es bildet die technische Infrastruktur zur Übertragung von Informationen in digitaler Form.⁸ Heute werden verschiedene Dienste über das Internet angeboten. Die derzeit wichtigsten Dienste sind:

- World Wide Web (WWW): Das WWW stützt sich auf ein Hyperlinksystem, das durch seine grafische Benutzeroberfläche sehr einfach zu bedienen ist. Per Tastendruck kann von einer zur nächsten Internet-Seite gesprungen („gesurft“) werden.⁹ Unter Zuhilfenahme eines Suchdienstes im WWW lässt sich praktisch jegliche gesuchte Information auffinden¹⁰.
- Electronic Mail (E-Mail)¹¹.
- Internet Relay Chat (IRC): Dieser Dienst ermöglicht die direkte Kommunikation zwischen Anwendern in Echtzeit. Die Server, die das Chat-System bereitstellen, bieten i. d. R. eine Vielzahl verschiedener Themenkanäle an, über die sich die User textuell unterhalten können.¹² Darüber hinaus besteht mittels spezieller Chat-Systeme auch die Möglichkeit zu telefonieren und Videokonferenzen abzuhalten¹³.

⁷ Vgl. *Koeppen*, Rechtliche Grenzen der Kontrolle der E-Mail- und Internetnutzung am Arbeitsplatz, 2007, S. 8.

⁸ Vgl. *Koeppen* (o. Fußn. 7), S. 10.

⁹ Vgl. *Hornung*, MMR 2004, 3 (4).

¹⁰ Vgl. *Hoeren*, Grundzüge des Internetrechts, 2. Aufl. (2002), S. 12.

¹¹ Ausführlich im vorliegenden Kapitelunterpunkt, S. 8.

¹² Vgl. *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer, 2003, S. 10.

¹³ Vgl. *Holenstein*, Die Benutzung von elektronischen Kommunikationsmitteln (Internet und Intranet) im Arbeitsverhältnis, 2002, S. 13.

- Diskussionsgruppen: Diskussionsforen existieren in Form von Mailinglisten, bei denen man seine Beiträge an einen Zentralrechner sendet. Dieser verschickt die Nachricht anschließend automatisch an sämtliche angemeldete Nutzer des Systems. Daneben bestehen Newsgroups, zu deren Nutzung keine Anmeldung erforderlich ist. Hierbei werden die neuen Artikel der Foren vom jeweiligen Provider bereitgestellt. Der wesentliche Unterschied zu Mailinglisten besteht darin, dass Newsgroups öffentlich sind¹⁴ und deren Nutzer deshalb regelmäßig pseudonym auftreten.
- File Transfer Protocol (FTP): Der Internet-Dienst FTP lässt die Übertragung von Dateien eines Rechners auf einen anderen zu¹⁵. Der Benutzer kann auf einen FTP-Server zugreifen, um bereitgestellte Dateien herunter zu laden bzw. Dateien hoch zu laden¹⁶.
- Telnet: Mit dem Dienst Telnet lassen sich räumlich entfernte, über das Netz zugängliche Rechner fernsteuern. Bspw. kann auf diese Weise Software abgespielt werden, die auf dem eigenen Computer nicht lauffähig ist.¹⁷

Wird in den folgenden Ausführungen die Bezeichnung „Internet“ verwendet, so handelt es sich dabei um die Nutzung des WWW, da davon auszugehen ist, dass der am Arbeitsplatz verursachte Datenverkehr durch die Internet-Nutzung nahezu ausschließlich, neben der Nutzung des E-Mail-Dienstes, durch die - wie auch immer geartete - Nutzung des WWW verursacht wird.

Vom Internet abzugrenzen ist das sog. Intranet. Als Intranet wird ein konzern-, unternehmens- oder betriebsinternes Netzwerk bezeichnet,

¹⁴ Vgl. *Hoeren* (o. Fußn. 10), S. 15 f.

¹⁵ Vgl. *Hoeren* (o. Fußn. 10), S. 17.

¹⁶ Vgl. *Holenstein* (o. Fußn. 13), S. 13.

¹⁷ Vgl. *Hoeren* (o. Fußn. 10), S. 17.

auf welches nur eine bestimmte Benutzergruppe, namentlich die Mitarbeiter, zugreifen kann. Im Grunde genommen handelt es sich beim Intranet um das Internet des Unternehmens, da eine vergleichbare Struktur vorliegt.¹⁸ Das Intranet ist demnach eine begrenzte Zusammenlegung von Rechnern, auf die der Zugriff von außen – also bspw. aus dem Internet – nicht bzw. nicht ohne weiteres möglich ist¹⁹. Im Normalfall bieten die Webseiten eines Intranets Informationen vom Unternehmen und weitere Dienstleistungen²⁰, welche zumeist im engen Zusammenhang mit der Erfüllung der Arbeitsaufgaben stehen. Eine Grafik, die den strukturellen Zusammenhang zwischen Internet, Firewall bzw. Server und Intranet veranschaulicht, befindet sich im Anhang (Anlage 2).

E-Mail bezeichnet persönliche, über Netzwerke digital übertragene Nachrichten. Zu den Vorzügen des E-Mail-Dienstes zählen die weltweite Kommunikation in kürzester Zeit zu minimalen Kosten²¹ und eine enorme Mobilität. Eine E-Mail kann versendet werden, ohne dass der Absender wissen muss, wo sich der Empfänger zu diesem Zeitpunkt aufhält. Darüber hinaus sind E-Mails asynchron und am Computer lesbar.²²

Eine E-Mail-Nachricht besteht aus einer Kopfzeile („Header“), dem eigentlichen Nachrichtentext („Body“) und evtl. aus einer oder mehreren Anlagen („Attachment(s)“). Die Kopfzeile enthält Informationen zum Absender, zum Empfänger oder zu den Empfängern sowie eine Betreffzeile und den Sendezeitpunkt.²³ Als Anlagen können einer E-Mail sämtliche Dateien²⁴ beigelegt werden.

¹⁸ Vgl. *Erler*, Die private Nutzung neuer Medien am Arbeitsplatz, 2003, S. 4.

¹⁹ Vgl. *Lelley*, in: *Worzalla*, S. 6 Rdnr. 10.

²⁰ Ebda.

²¹ Vgl. *Mattl*, Die Kontrolle der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2008, S. 9.

²² Vgl. *Frey*, E-Mail: Revolution im Unternehmen, 1999, S. 31.

²³ Vgl. *Mattl* (o. Fußn. 21), S. 9.

²⁴ Eine Restriktion kann in einigen Fällen die Größe der Dateien darstellen. Insbesondere sog. Web-Mail-Dienste schränken ihre Nutzer oftmals dahingehend ein, dass nicht E-Mails beliebiger Größe verschickt und empfangen werden können.

2.2 Überwachungsmöglichkeiten

Dem Arbeitgeber steht eine Vielzahl von Möglichkeiten zur Verfügung, den Internet- und E-Mail-Verkehr seiner Mitarbeiter zu überwachen. Grundsätzlich von einander zu unterscheiden sind einerseits Kontrollmöglichkeiten durch die Analyse der durch die Nutzung des Internet-Anschlusses ohnehin anfallenden Protokolldateien, der sog. Logfiles; andererseits existieren Kontrollmöglichkeiten durch den Einsatz spezieller Überwachungssoftware, welche die auf einem Arbeitsplatzrechner oder die im Netzwerk anfallenden Daten auswertet. Für erstgenannten Vorgang bedarf es keiner speziellen Software.²⁵

2.2.1 Überwachung des Internets

Einen Ansatzpunkt für die Überwachung der Internet-Aktivitäten bietet das Firewall-System. Es dient dazu, das unternehmensinterne Intranet vor unberechtigten Zugriffen von außen zu schützen; es kann auch nicht autorisierten Mitarbeitern den Kontakt zum Internet teilweise oder vollständig verwehren²⁶. Eine Firewall protokolliert alle Zugriffe auf das Internet sowie alle versuchten Zugriffe, die aufgrund einer Sperrung blockiert wurden. In der Auswertung der Firewall-Protokolle besteht ein hohes Überwachungspotenzial für den Arbeitgeber.²⁷

Eine weitere Überwachungsalternative existiert in der Untersuchung der im Proxy-Server gespeicherten Dateien. Der Proxy-Server hat u. a. die Aufgabe, häufig im Internet aufgerufene Webseiten bzw. Dateien abrufbereit zu halten.²⁸ Der Proxy-Server erzeugt darüber hinaus

²⁵ Vgl. Koeppen (o. Fußn. 7), S. 16 f.

²⁶ Däubler, Internet und Arbeitsrecht, 2. Aufl. (2002), § 4 Rdnr. 213; vgl. Koeppen (o. Fußn. 7), S. 18.

²⁷ Vgl. Hanau/Hoeren (o. Fußn. 12), S. 17; vgl. Koeppen (o. Fußn. 7), S. 18.

²⁸ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 213.

– ohne dass es ein Nutzer des Unternehmensnetzwerks bemerkt – Protokolldateien, die es anhand geeigneter Auswertungsprogramme erlauben, umfassende Nutzungsprofile über jeden einzelnen Mitarbeiter, der das Unternehmensnetzwerk nutzt, zu erstellen²⁹. Es lässt sich also genau rekonstruieren, welcher Mitarbeiter zu welcher Zeit welche Internet-Seite aufgerufen hat³⁰. Ein exemplarischer Auszug aus einem Logfile ist im Anhang der vorliegenden Arbeit abgedruckt (Anlage 3).

Möglichkeiten zur Überwachung bietet auch Standardsoftware, bspw. der zur Internet-Nutzung verwendete Browser. Die Benutzung des Internet-Browsers hinterlässt bei jedem „Streifzug“ durchs Netz Spuren auf der Festplatte des Computers, anhand derer die Kontrolle erfolgen kann.³¹ Für eine Auswertung können Cache-Dateien herangezogen werden. Cache-Dateien erfüllen den gleichen Zweck wie ein Proxy-Server: Bereits aufgerufene Webseiten werden auf der lokalen Festplatte gespeichert, um bei einem erneuten Zugriff diese Seiten schneller laden zu können.³² Der versierte Nutzer kann die Cache-funktion des Browsers allerdings abschalten, sodass diese Kontrollmöglichkeit nicht immer besteht³³. Noch einfacher gestaltet sich die Feststellung der Internet-Seiten, auf denen sich ein Arbeitnehmer bewegt, durch das Untersuchen der im Verlauf des Browsers gespeicherten Internet-Adressen³⁴. Der Verlauf ist eine Funktion, die aufgerufene Internet-Adressen für eine beliebig einstellbare Dauer im Web-Browser abspeichert³⁵. Jedoch lässt sich im Regelfall auch der Verlauf durch den Nutzer löschen³⁶. Ferner kann der Arbeitnehmer durch

²⁹ Vgl. *Elschner* (o. Fußn. 3), S. 12.

³⁰ Vgl. *Koeppen* (o. Fußn. 7), S. 18 f.

³¹ Vgl. *Koeppen* (o. Fußn. 7), S. 19.

³² Vgl. *Elschner* (o. Fußn. 3), S. 12 Fußn. 3.

³³ Vgl. *Koeppen* (o. Fußn. 7), S. 19.

³⁴ Vgl. *Nägele/Meyer*, K&R 2004, 312 (313); vgl. *Mühlbauer*, Trojaner vom Chef, <http://www.heise.de/tp/r4/artikel/22/22268/1.html> (27.3.08).

³⁵ Vgl. *Koeppen* (o. Fußn. 7), S. 20; vgl. *Rath/Karner*, K&R 2007, 446 (450).

³⁶ Vgl. *Kiper*, in: *Schulzki-Haddouti* (Hrsg.), Bürgerrechte im Netz, S. 92 (93); vgl. *Elschner* (o. Fußn. 3), S. 12 f.

Analyse der auf dem Arbeitsplatzrechner abgespeicherten Cookies überwacht werden. Cookies sind automatisch erstellte Datensätze, die beim Aufruf einer Webseite vom Web-Server interaktiv erzeugt, an den Internet-Browser gesendet und im Computer lokal auf der Festplatte in einer Cookie-Datei gespeichert werden. Cookies enthalten nutzungsrelevante Daten wie Layout-Einstellungen oder Kundendaten.³⁷ Sie werden häufig im Bereich des E-Commerce eingesetzt, um dort z. B. einen virtuellen Warenkorb bereitzustellen. Die Abspeicherung von Cookies kann allerdings verhindert werden.³⁸

Für den Arbeitgeber gestaltet sich der Einsatz spezieller Überwachungssoftware weitaus komfortabler als die eben aufgezeigten Überwachungsmethoden³⁹. Je nach Ausgestaltung des eingesetzten Programms können u. U. sämtliche Vorgänge am Computer – egal, ob online oder offline – aufgezeichnet werden⁴⁰. Die Bandbreite der verfügbaren „Schnüffelsoftware“⁴¹ reicht von Programmen, die ausschließlich die Web-Nutzung aufzeichnen, über Programme, die Aktivitätsprotokolle über den Computergebrauch anfertigen, bis hin zu Tastaturmitschnitten und Screenshots⁴². Darüber hinaus existieren Filter, welche die Sperrung von Schlüsselbegriffen wie „Sex“ oder „Streik“ bieten und jeden Zugriffsversuch auf eine gesperrte Seite protokollieren⁴³. Es ist vorstellbar, sämtliche ermittelten Daten in Form von Tabellen oder grafisch darzustellen und nach unterschiedlichen Kriterien zu sortieren. So kann exakt analysiert werden, welcher Arbeitnehmer welche Internet-Seite wie oft und zu welchem Zeitpunkt aufgerufen hat, welche Datenmenge übertragen wurde und

³⁷ Vgl. *Elschner* (o. Fußn. 3), S. 12 Fußn 5.

³⁸ Vgl. *Koeppen* (o. Fußn. 7), S. 20 f.

³⁹ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 215.

⁴⁰ Vgl. *Koeppen* (o. Fußn. 7), S. 17.

⁴¹ Eine umfassende Überwachung der Computer- und Internet-Aktivitäten erlaubt bspw. das Programm Spector Pro des Herstellers SpectorSoft (<http://www.spectorsoft.de>).

⁴² Vgl. *Mühlbauer* (o. Fußn. 34), <http://www.heise.de/tp/r4/artikel/22/22268/1.html> (27.3.08); vgl. *Rath/Karner* (o. Fußn. 35), 446 (450).

⁴³ Vgl. *Kiper*, in: *Schulzki-Haddouti* (o. Fußn. 36), S. 94; vgl. *Mühlbauer* (o. Fußn. 34), <http://www.heise.de/tp/r4/artikel/22/22268/1.html> (27.3.08).

bspw. welcher Dienst – WWW oder E-Mail – in Anspruch genommen wurde. Insofern könnte man bei Nutzung der potenziellen Kontrollmechanismen den gläsernen Mitarbeiter „erzeugen“.⁴⁴

2.2.2 Überwachung von E-Mail

Eine nahezu lückenlose Kontrolle ist ebenso bei der E-Mail-Kommunikation durchführbar. Der Systemadministrator verfügt über uneingeschränkte Zugriffsmöglichkeiten auf die E-Mail-Postfächer der einzelnen Mitarbeiter, die zumeist auf einem Netzwerk-Server hinterlegt sind. Somit hat auch der Arbeitgeber Gelegenheit, die eingegangenen E-Mails und die lokal abgespeicherten Kopien versendeter Nachrichten zu lesen.⁴⁵ Außerdem kann der Mail-Server so konfiguriert werden, dass von allen ein- und ausgehenden E-Mails der Arbeitnehmer eine Kopie direkt an den Arbeitgeber gesendet wird. Der Einsatz von Filterprogrammen, die gezielt nach E-Mails suchen, welche bestimmte Schlüsselwörter beinhalten (Content Searcher), mindern dabei den Aufwand für den Arbeitgeber.⁴⁶ Daneben stehen noch die bereits bei der Internet-Überwachung genannten „allgemeinen“ Spionageprogramme, wie Software zur Anfertigung von Screenshots, zur Verfügung.

Ein denkbares Hindernis für zumindest die inhaltliche Kontrolle stellt die Verschlüsselung der E-Mails durch den Arbeitnehmer dar. Fraglich ist allerdings, ob der Arbeitgeber überhaupt gestattet, dass Arbeitnehmer Kryptographiesoftware auf ihrem betrieblichen Computer installieren und verwenden. Jedoch kann selbst der Einsatz von Verschlüsselungsprogrammen nicht verhindern, dass mindestens die äußeren Verbindungsdaten der E-Mails, namentlich der Absender, der Empfänger, der Nachrichtenbetreff, das Datenvolumen und der Sen-

⁴⁴ Vgl. *Koeppen* (o. Fußn. 7), S. 17.

⁴⁵ Vgl. *Elschner* (o. Fußn. 3), S. 13.

⁴⁶ Vgl. *Koeppen* (o. Fußn. 7), S. 21 f.

de- bzw. Empfangszeitpunkt verfügbar sind.⁴⁷ Im Ergebnis lässt sich festhalten, dass – genau wie bei der Web-Nutzung – vollumfängliche Überwachungsmöglichkeiten vorliegen, die es ermöglichen, das gesamte Verhalten der Mitarbeiter im Umgang mit der modernen IuK-Technik nachzuvollziehen.

⁴⁷ Vgl. *Elschner* (o. Fußn. 3), S. 13 f.; vgl. *Koeppen* (o. Fußn. 7), S. 22.

3 GEGENÜBERSTELLUNG VON ARBEITGEBER- UND ARBEITNEHMERINTERESSEN

Arbeitsplatzrechner, die mit einem Zugang zum Internet ausgestattet sind, beherbergen ein hohes Missbrauchspotenzial durch die Mitarbeiter. Für viele Arbeitnehmer ist die Versuchung groß, sich – freilich während der Arbeitszeit – in privatem Interesse im WWW aufzuhalten oder E-Mails an private Kontakte zu versenden. Die Inhalte des Internets sind geradezu verlockend: Egal, ob Online-Auktion, Wettervorhersage oder Nachrichtendienst – das mannigfache Angebot der verschiedenen Web-Inhalte bietet immer etwas für jeden Interessenschwerpunkt.

Ein Ansatz, diese Problematik zu entschärfen, liegt in der inhaltlichen Beschränkung des Internet-Zugangs. Verschiedene Möglichkeiten, z. B. Black Lists⁴⁸, White Lists⁴⁹ sowie voll- und halbautomatische Filterverfahren stehen dazu grundsätzlich zur Verfügung. Der Einsatz dieser Verfahren ist jedoch problembehaftet, bzw. sie sind technisch nicht ausgereift und können dazu führen, dass auch auf unternehmensrelevante Informationen nicht zugegriffen werden kann.⁵⁰

Ebenso wenig sinnvoll ist die Beschränkung des E-Mail-Accounts. Einerseits könnten dadurch neue Kommunikationspartner, also auch potenzielle Kunden, die Mitarbeiter des Unternehmens nicht mehr erreichen, da ihre noch nicht freigeschalteten E-Mail-Adressen am Filter hängen blieben. Andererseits könnte eine Kontaktaufnahme zu neuen Geschäftspartnern erst dann stattfinden, wenn der Arbeitgeber diese Kommunikation als betrieblich relevant autorisiert hat. In Frage

⁴⁸ Durch eine Black List wird der Zugriff auf bestimmte Internet-Inhalte gesperrt. Es liegt eine grundsätzliche Freigabe des Internets mit explizit gesperrten Seiten vor (vgl. *Elschner* (o. Fußn. 3), S. 5).

⁴⁹ Die White List verkörpert den Gegensatz zur Black List: Durch sie sind grundsätzlich alle Internet-Seiten gesperrt, bis auf die in der White List enthaltenen (vgl. *Elschner* (o. Fußn. 3), S. 5).

⁵⁰ Vgl. *Elschner* (o. Fußn. 3), S. 4-6.

kommt eine Einschränkung des E-Mail-Dienstes allenfalls dann, wenn sie als Reaktion auf bereits vollzogene Missbrauchsfälle erfolgt. Ein solcher Fall wäre dann gegeben, wenn bekannt wurde, dass ein Mitarbeiter häufig mit einem bestimmten Kommunikationspartner privat über E-Mail kommuniziert.⁵¹

Festzustellen bleibt, dass der Arbeitgeber ein berechtigtes Interesse hat, die Internet- und E-Mail-Aktivitäten der Mitarbeiter zu kontrollieren, um bei unerlaubten Nutzungen durch die Mitarbeiter ggf. erforderliche Konsequenzen ziehen zu können. Den Interessen an einer Überwachung des Internet- und E-Mail-Verkehrs durch den Arbeitgeber stehen die Schutzinteressen des Arbeitnehmers gegenüber. Diese Schutzinteressen beschränken die Zulässigkeit einer Überwachung. Nachfolgend werden die Interessen beider Parteien aufgezeigt.

3.1 Überwachungsinteressen des Arbeitgebers

3.1.1 Überprüfung der geschuldeten Arbeitsleistung

Ein gewichtiger Grund, der für das Überwachungsinteresse des Arbeitgebers spricht, liegt in der Kontrolle der Erledigung von Arbeitsaufgaben⁵². Der Arbeitnehmer ist gem. § 611 Abs. 1 BGB verpflichtet, seine versprochenen Dienste – also Arbeitsleistung – zu erbringen. Der Arbeitgeber muss die Möglichkeit haben, die Aufgabenerfüllung durch seine Mitarbeiter kontrollieren zu können; es ist jedoch fraglich, ob er überhaupt technische Mittel dazu einsetzen darf, und falls ja, welche⁵³. Auch die Einhaltung von betriebsinternen Richtlinien für den Umgang mit modernen Kommunikationsmitteln, sofern solche Richtlinien bestehen, begründet ein Kontrollinteresse des Ar-

⁵¹ Vgl. *Elschner* (o. Fußn. 3), S. 9.

⁵² Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 217.

⁵³ Vgl. *Ernst*, NZA 2002, 585 (588).

beitgebers⁵⁴, da die betriebliche Praxis oftmals zur Erkenntnis geführt hat, dass Regelungen nur dann eingehalten werden, wenn auch kontrolliert wird⁵⁵.

Bei einer exzessiven, d. h. einer über das übliche Maß hinausgehenden⁵⁶ privaten Nutzung des bereitgestellten Internet-Anschlusses ist zu befürchten, dass die Arbeitsleistung massiv beeinträchtigt wird⁵⁷.

Im Übrigen lässt sich durch die Überwachung der Kommunikation mit Dritten feststellen, ob z. B. Kunden oder Geschäftspartner fachgerecht bedient und freundlich behandelt werden⁵⁸.

3.1.2 Schutz vor Malware

Weiterhin ist ein gesteigertes Gefahrenpotenzial durch das Einschleusen von Viren, Trojanern und sonstiger Malware⁵⁹ vorhanden. Die genannte Malware kann dazu beitragen, dass Geschäftsgeheimnisse an Dritte geraten. Etwa der unvorsichtige Umgang der Arbeitnehmer mit eingehenden E-Mails und deren Attachments birgt das Risiko, dass unerwünschte Schadsoftware ins Unternehmensnetzwerk gelangt⁶⁰. Mit einer Zunahme von Spam-Mails und Cookies ist ebenso zu rechnen; deshalb müssen kostenträchtige Gegenmaßnahmen, wie die Einrichtung von Firewalls und Datenverschlüsselungsmechanismen, ergriffen werden.⁶¹

⁵⁴ Vgl. Koeppen (o. Fußn. 7), S. 29.

⁵⁵ Vgl. Höld, Die Überwachung von Arbeitnehmern, 2006, S. 5.

⁵⁶ Vgl. Besgen/Prinz, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, § 1 Rdnr. 118.

⁵⁷ Vgl. Zilkens, DuD 2005, 253 (256).

⁵⁸ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 218.

⁵⁹ Zur Frage, ob derjenige, der eine IT-Infrastruktur auch zur privaten Nutzung vorhält, der rechtlichen Verpflichtung unterliegt, diese durch geeignete technische und/oder organisatorische Maßnahmen vor dem Zugriff von Malware zu schützen und ob durch fahrlässiges Tun bzw. Unterlassen Schadenersatzansprüche der Nutzer entstehen können, siehe Schuster, DuD 2006, 424-432.

⁶⁰ Vgl. Elschner (o. Fußn. 3), S. 11.

⁶¹ Vgl. Koeppen (o. Fußn. 7), S. 29; vgl. Beckschulze/Henkel, DB 2001, 1491 (1492).

3.1.3 Verhinderung des Entstehens zusätzlicher Kosten

Kosten, die durch die private Nutzung des Internet-Anschlusses entstehen, sind in erster Linie Kosten für die unproduktiv genutzte Arbeitszeit⁶²; insofern kann auf den Kapitelunterpunkt 3.1.1 verwiesen werden. Überdies verursacht das Herunterladen größerer Datenmengen sowie das Herstellen und Aufrechterhalten einer Verbindung zum Internet u. U. Kosten⁶³.

Eine zusätzliche Kostenbelastung des Unternehmens kann aus der Inanspruchnahme entgeltlicher Internet-Dienste, wie dem Herunterladen von Gerichtsentscheidungen bei Juris, resultieren⁶⁴.

3.1.4 Ausschluss der Mithaftung⁶⁵

Für die Begründung einer Haftung des Unternehmens kommt z. B. § 831 BGB, in dem die Haftung für den Verrichtungsgehilfen geregelt ist, in Betracht. Dieser Haftung kann sich der Unternehmer nur entziehen, wenn er den sog. Exkulpationsbeweis erbringt. Jener setzt voraus, dass der Mitarbeiter sorgfältig ausgewählt bzw. in Verrichtung seiner Tätigkeit mit gebotener Sorgfalt beobachtet worden ist. Weiterhin sind Mittäterschaft bzw. Beihilfe gem. § 830 BGB denkbare

⁶² Vgl. *Mester*, in: *Hammermeister/Reich/Rose* (Hrsg.), *Information – Wissen – Kompetenz*, 2004, S. 35 (36).

⁶³ Vgl. *Elschner* (o. Fußn. 3), S. 6.

In der Literatur (so z. B. *Dickmann*, NZA 2003, 1009) wird hierzu oft ins Feld geführt, dass diese Kostenbelastung durch das Vorhandensein von pauschal abgerechneten Flatrates aktuell entfiele. Dabei bleibt jedoch unberücksichtigt, dass solche Breitbandanschlüsse nur in und in der Nähe von Ballungsgebieten zur Verfügung stehen. Unternehmen in ländlichen Gegenden beklagen allzu oft, sich mit einer Kanalbündelung des ISDN-Anschlusses begnügen zu müssen. Insoweit hält dieses Argument stand.

⁶⁴ Vgl. *Däubler*, K&R 2000, 323 (324).

⁶⁵ Siehe dazu ausführlich *Barton*, CR 2003, 592-598, der sich insbesondere mit der Frage einer Verantwortlichkeitsprivilegierung gem. ehemaligem § 9 Abs. 1 TDG auseinandersetzt.

Tatbeiträge des Unternehmens, die eine gesamtschuldnerische Haftung gem. § 840 BGB zur Folge haben können.⁶⁶

So können Verstöße gegen das Urheberrecht zu einem erhöhten Haftungs- und Prozessrisiko führen. Ein Beispiel stellt der Fall dar, in dem ein Arbeitnehmer urheberrechtswidrig Software vervielfältigt und nutzt, indem er sie über das Torrent-Netzwerk auf den Arbeitsplatz-Computer lädt und dort einsetzt.⁶⁷ Eine Mittäterschaft bzw. Beihilfe liegt u. U. vor, wenn der Arbeitgeber diese Vorgänge duldet, weil ihm dadurch ökonomische Vorteile erwachsen⁶⁸.

3.1.5 Verhinderung einer Systemüberlastung

Zu einer Überlastung des Computersystems bzw. des Unternehmensnetzwerks kann es insbesondere dann kommen, wenn keine Breitbandanbindung zum Internet besteht und Arbeitnehmer zu ihrem privaten Vergnügen auf aufwändige Web-Inhalte, die bspw. zahlreiche Multimedia-Anwendungen beinhalten, am Arbeitsplatz-Computer zugreifen oder sich große Dateien, z. B. ganze Kinofilme, auf den Rechner laden.⁶⁹

Der Arbeitgeber kann nicht akzeptieren, dass im Extremfall Belange des Unternehmens hinter die Privatinteressen einzelner Mitarbeiter zurücktreten müssen.

⁶⁶ Vgl. *Barton*, K&R 2004, 305 (307).

⁶⁷ Vgl. *Elschner* (o. Fußn. 3), S. 8.

⁶⁸ Vgl. *Barton* (o. Fußn. 66), 305 (307).

⁶⁹ Vgl. *Zilkens* (o. Fußn. 57), 253 (256 f); vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 218.

3.1.6 Vermeidung eines Imageschadens

Wird in der Öffentlichkeit bekannt, dass sich Mitarbeiter eines bestimmten Unternehmens auf einschlägigen Webseiten aufhalten, kann dies zu einem erheblichen Imageverlust führen⁷⁰, da jegliche Aktivität im Internet nachvollziehbare Datenspuren hinterlässt⁷¹. Jedem Arbeitgeber wird daran gelegen sein, ein solches rufschädigendes Verhalten zu unterbinden.

3.1.7 Unterbinden strafbarer Handlungen

Gerade vor dem Hintergrund einer potenziellen (Mit-)Haftung des Arbeitgebers wird er zu verhindern versuchen, dass die betriebliche Computeranlage zur Begehung strafbarer Handlungen bzw. zum Aufruf von Internet-Seiten, welche strafbare oder sittenwidrige Inhalte darstellen, verwendet wird⁷². Der Aufruf pornografischer Web-Inhalte fällt zwar nicht zwangsläufig in einen strafbaren Bereich, dennoch wird das Unternehmen dies untersagen wollen, da andernfalls u. U. eine Störung des Betriebsfriedens entsteht⁷³.

Hinzu treten spezifische Computerstraftatbestände, wie das Ausspähen von Daten gem. § 202a StGB, die Datenveränderung gem. § 303a StGB oder sogar die Computersabotage nach § 303b StGB. Das Vorliegen dieser Straftatbestände kann unter bestimmten Bedingungen zusätzlich einen zivilrechtlichen Schadenersatzanspruch gegen das Unternehmen auslösen.⁷⁴

⁷⁰ Vgl. Besgen/Prinz, in: Besgen/Prinz (o. Fußn. 56), § 1 Rdnr. 121.

⁷¹ Vgl. Altenburg/v. Reinersdorff/Leister, MMR 2005, 135 (136); vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 213.

⁷² Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 219; vgl. Mattl (o. Fußn. 21), S. 19; vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1492).

⁷³ Vgl. Mattl (o. Fußn. 21), S. 19 f.

⁷⁴ Vgl. Barton (o. Fußn. 66), 305 (307).

Als ein Argument für die Rechtfertigung der Überwachung speziell des E-Mail-Verkehrs kann die Vorbeugung von Beleidigungen und abfälligen Bemerkungen über Vorgesetzte und Kollegen genannt werden⁷⁵. Denkbar ist darüber hinaus auch, dass durch missverständliche Äußerungen, die möglicherweise nur durch die sprachlichen Eigenheiten der Online-Sprache begründet sind, der Betriebsfrieden nachteilig beeinträchtigt wird, da in kürzester Zeit nahezu beliebig viele Personen die E-Mail erhalten können⁷⁶.

3.1.8 Schutz vor Wirtschaftsspionage

Die Kontrolle der Internet-Aktivitäten durch den Arbeitgeber, insbesondere jedoch der E-Mail-Kommunikation, stellt weiterhin ein brauchbares Mittel gegen Wirtschaftsspionage dar: Durch die Überprüfung der E-Mail-Inhalte ist es für den Arbeitgeber ein Leichtes, sich ein Bild darüber zu verschaffen, welcher Mitarbeiter „aus dem Nähkästchen plaudert“ und Geschäftsgeheimnisse verrät.⁷⁷

Zutreffend dürfte diesbezüglich der Einwand sein, dass Mitarbeiter, die sich systematisch Geschäftsgeheimnisse aneignen wollen, wohl kaum den leicht nachvollziehbaren Weg über den E-Mail-Dienst wählen, sondern eher auf eine andere Art und Weise versuchen werden, die geheimen Daten nach außen zu tragen⁷⁸.

⁷⁵ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 218.

⁷⁶ Vgl. *Elschner* (o. Fußn. 3), S. 10 f.

⁷⁷ Vgl. *Mester*, in: *Hammermeister/Reich/Rose* (o. Fußn. 62), S. 36 f; vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 218.

⁷⁸ Vgl. *Mattl* (o. Fußn. 21), S. 20; vgl. *Koeppen* (o. Fußn. 7), S. 31.

3.2 Schutzinteressen des Arbeitnehmers

Aus den vorangegangenen Ausführungen zu den Arbeitgeberinteressen lässt sich ein grundsätzliches Überwachungsinteresse anerkennen. Die Frage ist, wieweit eine solche Überwachung gehen und welcher technischen Mittel sich der Arbeitgeber dazu bedienen darf. Es steht außer Zweifel, dass eine lückenlose Kontrolle der Online-Aktivitäten zu einer systematischen Überwachung des Arbeits-, Leistungs- und Sozialverhaltens führt⁷⁹. Arbeitnehmer haben die berechtigte Erwartung, dass ein gewisser Schutz ihrer Privatsphäre auch am Arbeitsplatz gewährleistet wird – der Arbeitsplatz ist nämlich der Ort, an dem sich Arbeitnehmer i. d. R. zu einem wesentlichen Teil ihrer Lebenszeit aufhalten und an dem sie Beziehungen zu anderen Personen knüpfen.⁸⁰

Die Erforderlichkeit des Schutzes der Arbeitnehmer resultiert aus den nachfolgend aufgezeigten Risiken, welche mit der Internet- und E-Mail-Überwachung einhergehen.

Vorweg wird darauf hingewiesen, dass die nachstehenden Risiken umso höher einzustufen sind, je mehr die Arbeitnehmer auf den virtuellen Arbeitsplatz angewiesen sind und die elektronischen IuK-Mittel nutzen⁸¹. Im Gegensatz zu anderen Überwachungsmaßnahmen, bspw. der Video- oder Telefonüberwachung, kann in diesem Fall auch kontrolliert werden, wie sich der Arbeitnehmer - losgelöst von seinem Arbeitskontext - im Internet bewegt, mit wem er kommuniziert und für welche Informationen er sich interessiert. So können seine persönlichen Interessen, Neigungen, Charaktereigenschaften, sein Verhalten gegenüber Kollegen, Kunden und Dritten sowie sein sonstiges

⁷⁹ Vgl. Zilkens (o. Fußn. 57), 253 (257).

⁸⁰ Vgl. Koeppen (o. Fußn. 7), S. 30 f.

⁸¹ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 220; vgl. Elschner (o. Fußn. 3), S. 14 f.

Verhalten am Arbeitsplatz detailliert festgestellt, archiviert und ausgewertet werden.⁸²

3.2.1 Vermeidung der Schaffung eines gläsernen Mitarbeiters

Die Analyse der Online-Aktivitäten von Mitarbeitern eröffnet dem Arbeitgeber die Möglichkeit, sich ein umfassendes Bild über persönliche Vorlieben etc. seiner Belegschaftsmitglieder zu verschaffen. Informiert sich ein Beschäftigter in der Mittagspause im Internet etwa über medizinische, politische oder religiöse Themen, dann erregt er durch sein Verhalten genauso die Aufmerksamkeit des Arbeitgebers, wie wenn er z. B. mittels E-Mail Kontakt zu einer Selbsthilfegruppe oder Personalabteilung eines anderen Unternehmens aufnimmt.⁸³

Neben die Gefahr der Ausforschung persönlicher Interessen durch den Arbeitgeber tritt das Risiko der Kenntniserlangung über das Sozialverhalten der Arbeitnehmer; so kann die Überwachung der E-Mail-Kommunikation aussagekräftige Erkenntnisse über zwischenmenschliche Sympathien und Antipathien sowie über private Beziehungen zu Kollegen und Dritten liefern. Darüber hinaus lassen sich sämtliche positive wie negative Meinungsäußerungen über den Arbeitgeber in Erfahrung bringen.⁸⁴

Die aus dieser „Spionagetätigkeit“ gewonnenen Informationen über persönliche Interessen und Sozialverhalten können insbesondere im Hinblick auf personelle Entscheidungen für den Arbeitgeber von Interesse sein⁸⁵. Im Übrigen entsteht durch die Informationssammlung und -auswertung ein Kräfteungleichgewicht: Der Arbeitgeber gewinnt gegenüber seinen Beschäftigten einen erheblichen Informa-

⁸² Vgl. *Elschner* (o. Fußn. 3), S. 15.

⁸³ Vgl. *Elschner* (o. Fußn. 3), S. 16; vgl. *Tinnefeld*, MMR 2001, 797 (798).

⁸⁴ Vgl. *Koeppen* (o. Fußn. 7), S. 32 f; vgl. *Elschner* (o. Fußn. 3), S. 16 f.

⁸⁵ Vgl. *Koeppen* (o. Fußn. 7), S. 33.

tionsvorsprung⁸⁶. Die Informationsübermacht des Arbeitgebers betrifft jedoch nicht nur den Arbeitnehmer als Individuum, sondern auch die Beschäftigten in ihrer Gesamtheit. Durch zielgerichtete Auswertung der E-Mail-Kommunikation zwischen Arbeitnehmern, Betriebsrat und Gewerkschaftsvertretern erlangt der Arbeitgeber i. d. R. Informationsvorteile, welche er in Kollektivverhandlungen zu seinen Gunsten nutzen kann⁸⁷.

3.2.2 Schutz vor technikimmanenten Gefahren

Die technisierte Kontrolle birgt zusätzliche Risiken im Hinblick auf die Objektivität der gewonnenen Ergebnisse⁸⁸. Ein mögliches Problem stellt der Kontextverlust dar. Gerät ein Arbeitnehmer im Rahmen einer Internet-Recherche, die im Zusammenhang mit der Erfüllung seiner Arbeitsaufgaben steht, zufällig oder weil er in der Suchmaschine nicht erkennen kann, dass es sich bei der vermeintlich seriösen Seite um ein Angebot mit dubiosen Inhalt handelt, auf eine Seite mit bspw. pornografischen Inhalten, so sieht der Arbeitgeber später in der Log-Datei nur, dass der Arbeitnehmer ein pornografisches Angebot aufgerufen hat. Jedoch sind die näheren Umstände des Einzelfalls nicht mehr nachvollziehbar.⁸⁹

Eine weitere, damit eng verbundene Schwierigkeit ergibt sich aus der vermeintlichen Objektivität des Computers. Im Allgemeinen besteht eine Richtigkeitsvermutung für automatisiert verarbeitete Daten, weil die Daten im Verarbeitungsprozess keinen subjektiven Beeinträchtigungen unterliegen. Für den Arbeitgeber entsteht beim Lesen des Computerausdrucks einer Log-Datei der Eindruck, dass objektive und unangreifbare Tatsachen vorlägen. Die Konsequenz für den „ertapp-

⁸⁶ Vgl. Zilkens (o. Fußn. 57), 253 (257); vgl. Elschner (o. Fußn. 3), S. 17.

⁸⁷ Vgl. Elschner (o. Fußn. 3), S. 17.

⁸⁸ Vgl. Koeppen (o. Fußn. 7), S. 34.

⁸⁹ Vgl. Elschner (o. Fußn. 3), S. 18.

ten“ Arbeitnehmer ist, dass er kaum eine Chance hat, die genauen Umstände für z. B. den Besuch einer bestimmten Webseite glaubhaft darzulegen und somit die „Aussage“ des Computers zu widerlegen.⁹⁰

Darüber hinaus eröffnet die Verknüpfung der angefallenen Daten aus dem Kommunikationsverhalten und aus anderen Verhaltensbereichen die Möglichkeit, ein umfassendes Persönlichkeitsprofil über den Arbeitnehmer zu erstellen. Je mehr Einzeldaten dabei erfasst werden, desto größer wird die Problematik hinsichtlich des Kontextverlusts sowie der Scheinobjektivität.⁹¹ Deutlich wird dies, wenn man folgendes Beispiel betrachtet: Ein Mitarbeiter, der im Rahmen einer Internet-Recherche versehentlich auf Seiten mit pornografischen Inhalten gelangt ist, bekommt regelmäßig, unbestellt und ungewollt Spam-Mails mit entsprechenden Inhalten in sein betriebliches E-Mail-Postfach zugestellt. Werden jetzt die kontextverkürzten Daten aus beiden Bereichen zu einem Gesamtergebnis zusammengefasst, ergibt sich folgendes Bild: Arbeitnehmer X besucht Internet-Seiten, die pornografischen Inhalt haben und lässt sich E-Mails mit ebensolchen Inhalten zusenden.⁹²

Ein weiteres technikspezifisches Risiko bildet der Verewigungseffekt der einmal erhobenen Daten über Arbeitnehmer, die faktisch ohne zeitliche Begrenzung archiviert werden können. Einerseits entsteht dabei ein zusätzlicher Kontextverlust, der allein durch die zeitliche Distanz zum zurückliegenden Verhalten zustande kommt; andererseits werden oftmals nur solche Daten zeitlich beschränkt oder sogar fortwährend aufbewahrt, die eine Auffälligkeit widerspiegeln. Die dauerhafte Verfügbarkeit und Abrufbarkeit gesammelter Negativdaten führt geradezu zu einer Stigmatisierung eines betroffenen Ar-

⁹⁰ Vgl. Koeppen (o. Fußn. 7), S. 35 f.; vgl. Elschner (o. Fußn. 3), S. 19 f.

⁹¹ Vgl. Koeppen (o. Fußn. 7), S. 36 f.

⁹² Vgl. Elschner (o. Fußn. 3), S. 21.

beitnehmers, die eine unvoreingenommene Beurteilung seiner Person zumindest erschwert.⁹³

⁹³ Vgl. *Elschner* (o. Fußn. 3), S. 22 f.

4 RECHTLICHER RAHMEN

Dieses Kapitel beinhaltet eine Darstellung der verschiedenen Rechtsquellen, die im Zusammenhang mit der Internet- und E-Mail-Überwachung von Arbeitnehmern stehen.

4.1 Europäische Vorschriften

Europarecht beeinflusst zunehmend die nationale Gesetzgebung der EU-Mitgliedsstaaten, so auch beim Datenschutz. Ein nicht zu unterschätzendes Problem stellt hierbei die Umgehung nationaler Datenschutzvorschriften dadurch dar, dass sich der Unternehmenssitz in einem anderen Land befindet, als jenem, in dem die Datenspeicherung erfolgt⁹⁴.

In Bezug auf die Überwachung der Internet- und E-Mail-Aktivitäten von Arbeitnehmern werden nachfolgend kurz die einschlägigen Vorschriften auf Gemeinschaftsebene aufgezeigt.

Die Europäische Menschenrechtskonvention (EMRK) und die Charta der Grundrechte der EU sind als Regelwerke der allgemeinen europäischen Vorschriften anzuführen. Art. 8 der EMRK befasst sich mit dem Recht auf Achtung des Privat- und Familienlebens, wobei sich sein Schutzbereich auch auf den Arbeitsplatz, die Kommunikation am Arbeitsplatz und den Datenschutz erstreckt. Die Charta der Grundrechte der EU enthält durch Art. II-67 eine Vorschrift zur Achtung des Privat- und Familienlebens und durch Art. II-68 eine Regelung zum Schutz personenbezogener Daten.⁹⁵

⁹⁴ Vgl. *Schönfeld/Strese/Flemming*, MMR 2001, 8 (10).

⁹⁵ Vgl. *Koeppen* (o. Fußn. 7), S. 99 f.

Weiterhin sind die beiden EG-Richtlinien 95/46/EG (Datenschutzrichtlinie) und 2002/58/EG⁹⁶ (Datenschutzrichtlinie für elektronische Kommunikation) zu nennen. EG-Richtlinien verpflichten die Mitgliedsstaaten, die Vorschriften der Richtlinie in nationales Recht umzusetzen.⁹⁷ Die EG-Datenschutzrichtlinie wurde durch die Novellierung des Bundesdatenschutzgesetzes im Jahre 2001 im deutschen Recht implementiert⁹⁸. Gem. Art. 1 Abs. 1 der Datenschutzrichtlinie soll der Schutz der Grundrechte und Grundfreiheiten sowie insbesondere der Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten gewährleistet sein. Art. 1 Abs. 2 der Richtlinie soll Beschränkungen des freien Verkehrs personenbezogener Daten zwischen den Mitgliedsstaaten verhindern. Darüber hinaus sieht Art. 29 der Datenschutzrichtlinie vor, dass die Mitgliedsstaaten eine unabhängige Datenschutzgruppe einrichten, die eine beratende Funktion einnimmt. Ihre Aufgaben wurden in Art. 30 Datenschutzrichtlinie und in Artikel 15 Datenschutzrichtlinie für elektronische Kommunikation manifestiert. Die Datenschutzgruppe leistet Beiträge in Form von Beratungen, Stellungnahmen, Empfehlungen sowie offiziellen Vorgaben, die die Datenschutzrichtlinie bezüglich elektronischer Überwachung auslegen sollen. Gerichtet sind die Beiträge der Datenschutzgruppe an die einzelnen Mitgliedsstaaten der EU, nicht jedoch an die Arbeitgeber selbst. Die Richtlinie 2002/58/EG regelt den Umgang mit und die Verarbeitung von personenbezogenen Daten sowie den Schutz der Privatsphäre auf dem Gebiet elektronischer Kommunikation.⁹⁹ Die Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation wurde in Deutschland durch entsprechende Änderung des Telekommunikationsgesetzes im Jahr 2004 vollzogen¹⁰⁰.

⁹⁶ Sie löste die Richtlinie 97/66/EG ab.

⁹⁷ Vgl. *Koeppen* (o. Fußn. 7), S. 101-105.

⁹⁸ Vgl. *Weißgerber*, Arbeitsrechtliche Fragen bei der Einführung und Nutzung vernetzter Computerarbeitsplätze, 2003, S. 124.

⁹⁹ Vgl. *Koeppen* (o. Fußn. 7), S. 101-106.

¹⁰⁰ Vgl. *Hoeren*, Internetrecht (Stand: März 2008), S. 394 Rdnr. 600, http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz2008.pdf (30.4.08).

4.2 Deutsche Vorschriften

Spezielle Arbeitnehmerdatenschutzvorschriften, die den Umgang mit Internet und E-Mail am Arbeitsplatz regeln, existieren bislang nicht, obwohl deren Notwendigkeit unzweifelhaft angezeigt ist, und sie auch von der Politik gefordert werden. Vorschriften, anhand derer sich die Zulässigkeit von Überwachungsmaßnahmen durch den Arbeitgeber beurteilen lassen, finden sich derzeit in Form allgemeiner gesetzlicher Vorgaben.¹⁰¹

4.2.1 Verfassungsrechtliche Ebene

Auch Grundrechte finden Eingang in das Arbeitsverhältnis. Dies geschieht nicht unmittelbar, sondern mittelbar durch zivilrechtliche Generalklauseln. Die mittelbare Drittwirkung stützt sich auf die Theorie der objektiven Werteordnung.¹⁰² Im Arbeitsverhältnis besteht ein Kräfteungleichgewicht zu Lasten der Arbeitnehmer, die deshalb besonders schutzwürdig sind. Jedoch verfügt auch der Arbeitgeber über grundrechtlich geschützte Interessen, was zur Folge hat, dass ein Ausgleich zwischen den Grundrechten der Arbeitnehmer einerseits und den Grundrechten des Arbeitgebers andererseits geschaffen werden muss.¹⁰³ Die im Zusammenhang mit der Internet- und E-Mail-Überwachung stehenden Grundrechte des Arbeitgebers werden im Folgenden den Grundrechten der Arbeitnehmer gegenübergestellt.

¹⁰¹ Vgl. *Mattl* (o. Fußn. 21), S. 51.

¹⁰² Vgl. *Mengel*, BB 2004, 2014 (2015).

¹⁰³ Vgl. *Panzer*, Mitarbeiterkontrolle und neue Medien, 2004, S. 117.

4.2.1.1 Tangierte Grundrechte auf Arbeitgeberseite

4.2.1.1.1 Allgemeine Handlungsfreiheit aus Art. 2 Abs. 1 GG

Art. 2 Abs. 1 GG verkörpert ein allgemeines Freiheitsgrundrecht, das durch spezielle Freiheitsgrundrechte verdrängt wird; der allgemeinen Handlungsfreiheit kommt insofern eine Auffangfunktion zu.¹⁰⁴ Das bedeutet konkret, wenn ein bestimmtes Verhalten nicht in den Schutzbereich spezieller Freiheitsgrundrechte (hier: Berufsfreiheit, Art. 12 Abs. 1 GG und Eigentumsrecht, Art. 14 GG) fällt, wird es durch den Schutz des Art. 2 Abs. 1 GG gedeckt. Die allgemeine Handlungsfreiheit gewährt dem Grundrechtsträger, unter Einhaltung der im zweiten Halbsatz des Abs. 1 enthaltenen Schrankentrias, das subjektive Recht zur freien Persönlichkeitsentfaltung.¹⁰⁵

4.2.1.1.2 Berufsfreiheit aus Art. 12 Abs. 1 GG

Art. 12 Abs. 1 GG dient ganz allgemein auch dem Schutz der unternehmerischen Berufsausübungsfreiheit. Aus der Berufsfreiheit ergibt sich für den Arbeitgeber eine Handlungs- und Entscheidungssouveränität in allen unternehmensrelevanten Feldern.¹⁰⁶ Erfasst sind dadurch im Wesentlichen die Entscheidung über die Verwendung des Kapitaleinsatzes, die Organisation der betrieblichen Abläufe und die Festlegung der individuellen Arbeitsinhalte sowie die Bestimmung der zu nutzenden Arbeits- und Kommunikationsmittel.¹⁰⁷

¹⁰⁴ Vgl. *Lang*, in: Beck'scher Online-Kommentar GG, (Ed. 1, Stand: 1.2.2008), Art. 2 Rdnr. 30.

¹⁰⁵ Vgl. *Steidle*, Multimedia-Assistenten im Betrieb, 2005, S. 83.

¹⁰⁶ Vgl. *Panzer* (o. Fußn. 103), S. 140.

¹⁰⁷ Vgl. *Steidle* (o. Fußn. 105), S. 85.

4.2.1.1.3 Eigentumsrecht aus Art. 14 GG

Dem Arbeitgeber werden die freie wirtschaftliche Betätigung, der Erwerb von Eigentum und dessen ökonomische Nutzung gewährleistet. Nicht vom Eigentumsrecht erfasst sind potenzielle Gewinnchancen und eventuelle Erwerbsaussichten, weil sie (noch) nicht zum Vermögensbestand des Unternehmens gerechnet werden können. Jedoch zählen auch Inhalte der geschäftlichen Kommunikation, sofern sie Geschäftsgeheimnisse enthalten, zu den vermögenswerten Rechtspositionen, welche vom Eigentumsrecht erfasst sind.¹⁰⁸

Ferner steht im Zusammenhang mit dem Eigentumsrecht das Recht am eingerichteten und ausgeübten Gewerbebetrieb aus Art. 14 Abs. 1 GG in Rede. Die Frage, ob der eingerichtete und ausgeübte Gewerbebetrieb die Merkmale des verfassungsrechtlichen Eigentumsbegriffs aufweist, blieb bislang vom BVerfG unbeantwortet. Ein weiter gehender Schutz des Gewerbebetriebs als der Schutz seiner Grundlagen soll nicht in Betracht kommen, da das Unternehmen zwar die tatsächliche, jedoch nicht die rechtliche Zusammenfassung der zum Vermögen zählenden Rechte und Sachen, welche ohnehin schon unter dem Schutz vor verfassungswidrigen Eingriffen stehen, sei.¹⁰⁹

4.2.1.2 Tangierte Grundrechte auf Arbeitnehmerseite

4.2.1.2.1 Allgemeines Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG

Das allgemeine Persönlichkeitsrecht ist die zentrale Schutznorm für Arbeitnehmer, wenn Überwachungsmaßnahmen des Arbeitgebers in Rede stehen. Es enthält das Recht eines jeden Einzelnen auf Achtung

¹⁰⁸ Vgl. *Steidle* (o. Fußn. 105), S. 88 f.

¹⁰⁹ Vgl. *Axer*, in: Beck'scher Online-Kommentar GG, (Ed. 1, Stand: 1.2.2008), Art. 14 Rdnrn. 51 f.; vgl. *Steidle* (o. Fußn. 105), S. 89 f.

seiner Menschenwürde und auf individuelle Persönlichkeitsentfaltung.¹¹⁰ Dieses Grundrecht gilt allerdings nicht schrankenlos; von vornherein kann seine Reichweite nicht abschließend ausgemacht werden. Vielmehr muss in jedem Einzelfall anhand einer Güter- und Interessenabwägung für sich festgestellt werden, welche von den miteinander kollidierenden Interessen zurückzutreten haben.¹¹¹ Generell wird eine Kontrolle durch den Arbeitgeber dann zulässig sein, wenn sie nach Inhalt, Form und sämtlichen Begleitumständen geboten und zudem das schonendste Mittel zur Erreichung des angestrebten Zwecks ist¹¹².

Seinen Niederschlag im Arbeitsrecht findet das Grundrecht insbesondere in § 75 Abs. 2 BetrVG, wonach Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb Beschäftigten zu schützen und zu fördern haben, sowie in arbeitsrechtlichen Generalklauseln¹¹³.

Von besonderer Relevanz für die Themenstellung dieser Arbeit ist das Recht auf informationelle Selbstbestimmung als *eine* besondere Ausprägung des allgemeinen Persönlichkeitsrechts¹¹⁴. Dieses Recht entstand als Ausfluss aus dem Persönlichkeitsrecht durch Rechtsprechung des BVerfG im „Volkszählungsurteil“¹¹⁵ vom 15.12.1983¹¹⁶. Danach soll grundsätzlich jeder selbst über die Erhebung, Verwendung und Weitergabe seiner Daten bestimmen können¹¹⁷. Die Recht-

¹¹⁰ Vgl. Panzer (o. Fußn. 103), S. 136.

¹¹¹ Vgl. Erler (o. Fußn. 18), S. 123; vgl. Koeppen (o. Fußn. 7), S. 150 f.

¹¹² Vgl. Hanau/Hoeren (o. Fußn. 12), S. 60.

¹¹³ Vgl. Hanau/Hoeren (o. Fußn. 12), S. 60; vgl. Erler (o. Fußn. 18), S. 121-123; vgl. Besgen/Prinz, in: Besgen/Prinz (o. Fußn. 56), § 1 Rdnr. 36.

¹¹⁴ Vgl. Hanau/Hoeren (o. Fußn. 12), S. 59 f.; vgl. Erler (o. Fußn. 18), S. 122; vgl. Busse, in: Besgen/Prinz (Hrsg.), Neue Medien und Arbeitsrecht, § 10 Rdnr. 7.

¹¹⁵ BVerfGE 65,1 = NJW 1984, 419.

¹¹⁶ Vgl. Tuchbreiter, Beteiligungsrechte des Betriebsrats bei der Einführung und Anwendung moderner Kommunikationsmittel, 2007, S. 161; Elschner betrachtet das Recht auf informationelle Selbstbestimmung unzutreffend als eigenständiges Grundrecht (vgl. Elschner, (o. Fußn. 3), S. 109).

¹¹⁷ Vgl. Höld (o. Fußn. 55), S. 119.

fertigung eines Eingriffs in das informationelle Selbstbestimmungsrecht muss dieselben Voraussetzungen erfüllen wie ein Eingriff in das allgemeine Persönlichkeitsrecht¹¹⁸; so wird das Recht auf informationelle Selbstbestimmung immer dann eingeschränkt werden können, wenn überwiegende Interessen der Allgemeinheit vorliegen¹¹⁹.

4.2.1.2.2 Fernmeldegeheimnis aus Art. 10 GG

Art. 10 Abs. 1 GG erklärt das Brief-, Post- und Fernmeldegeheimnis als unverletzlich¹²⁰. Das allgemeine Persönlichkeitsrecht im Hinblick auf bestimmte Kommunikationsarten wird durch Art. 10 GG konkretisiert. Was die Kontrolle des Internet- und E-Mail-Verkehrs anbelangt, ist nur das Fernmeldegeheimnis von Bedeutung.¹²¹ Es schützt den Inhalt und die näheren Umstände der Kommunikation¹²². Den Eingang in einfachgesetzliche Vorschriften fand das durch Art. 10 GG zugesicherte Fernmeldegeheimnis – insbesondere vor dem Hintergrund der Privatisierung des früheren staatlichen Kommunikationsunternehmens – durch § 88 TKG¹²³. Darüber hinaus ist die Einhaltung des Fernmeldegeheimnisses nunmehr durch § 206 StGB strafrechtlich abgesichert¹²⁴.

¹¹⁸ Vgl. *Koeppen* (o. Fußn. 7), S. 152.

¹¹⁹ Vgl. *Weißgerber* (o. Fußn. 98), S. 100.

¹²⁰ Vgl. *Koeppen* (o. Fußn. 7), S. 153.

¹²¹ Vgl. *Elschner* (o. Fußn. 3), S. 127-132.

¹²² Vgl. *Rofsnagel*, Datenschutz in einem informatisierten Alltag, 2007, S. 113; vgl. *Weißgerber* (o. Fußn. 98), S. 109.

¹²³ Vgl. *Steidle* (o. Fußn. 105), S. 105; vgl. *Gola*, Datenschutz und Multimedia am Arbeitsplatz, 2006, S. 35 Rdnrn. 81 f.

¹²⁴ Vgl. *Steidle* (o. Fußn. 105), S. 105; vgl. *Gola* (o. Fußn. 123), S. 38-50.

4.2.2 Ebene der einfachen Gesetze und Rechtsverordnungen

4.2.2.1 Datenschutz-, Telekommunikations- und Telemedienrecht

Die Abgrenzung der unterschiedlichen Regelungsbereiche des allgemeinen Datenschutzrechts, des Telekommunikationsrechts und des Telemedienrechts gilt als zwingende Notwendigkeit zur Beurteilung, welches Gesetz im konkreten Fall einschlägig ist bzw. welche Gesetze einschlägig sind. Nachfolgende Abbildung veranschaulicht die Zusammensetzung des Telekommunikationsvorgangs¹²⁵, auf dessen drei Ebenen jeweils spezifische Datenschutzvorschriften gelten¹²⁶.

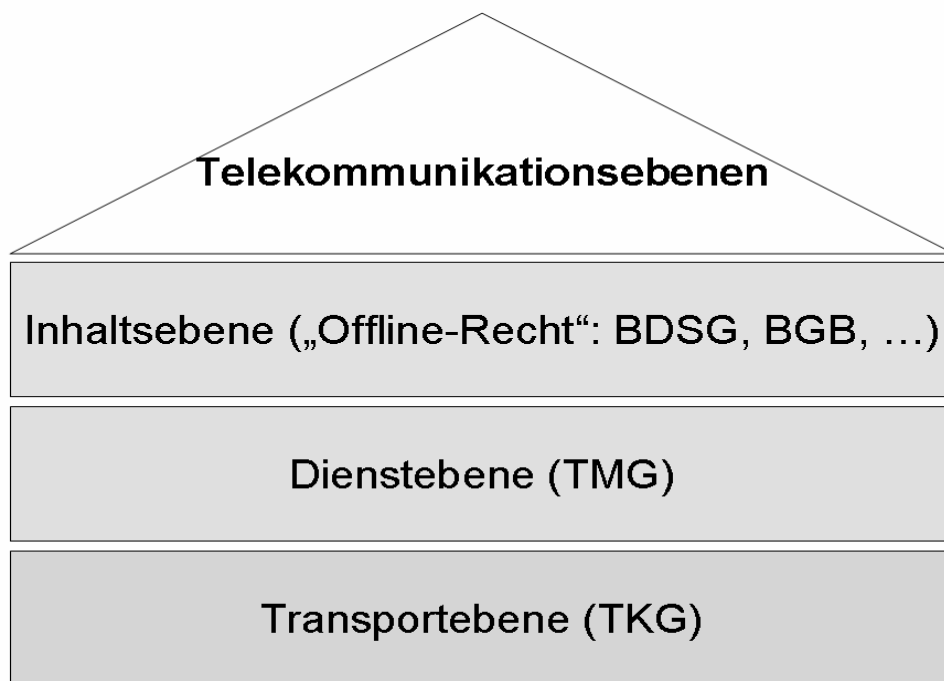


Abb. 1: Drei Ebenen der Telekommunikation.

Quelle: Der Verfasser.

¹²⁵ Vgl. *Mattl* (o. Fußn. 21), S. 57.

¹²⁶ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 230.

Die unterste Ebene der im Schaubild dargestellten Telekommunikationsebenen erfasst die Technik zur Informationsübermittlung¹²⁷; betroffen hiervon sind etwa Fragen über die Bereitstellung von Netzknoten oder unter welchen Voraussetzungen öffentliche Wege zur Verlegung von Verbindungsleitungen genutzt werden dürfen¹²⁸. In § 3 Nr. 22 TKG wird der Begriff der Telekommunikation als „...der technische Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen“ definiert. Telekommunikationsdienste nach dem klassischen Verständnis stellen die Sprachtelefonie oder der Datentransfer im Internet dar.¹²⁹ Unter bestimmten Voraussetzungen können jedoch auch höherwertige Dienste, wie E-Mail, unter einen Telekommunikationsdienst subsumiert werden¹³⁰: Dies ist der Fall, wenn die E-Mail auf dem Computer des Nutzers verfasst und schließlich über den Anbieter lediglich versandt wird. Findet hingegen irgendwo dazwischen eine weitere Bearbeitung der E-Mail - etwa durch die Überprüfung auf Viren - statt, ist der Dienst auf einer höheren Ebene einzustufen, was folglich den Anwendungsbereich des Telemediengesetzes eröffnet.¹³¹ Unter diesen Voraussetzungen kommen das Telekommunikationsgesetz und das Telemediengesetz, ausgenommen bestimmter Datenschutzvorschriften des Telemediengesetzes, gleichzeitig zur Anwendung. Die Begründung hierzu findet sich im Europarecht: Einerseits fallen solche Dienste als Dienste der Informationsgesellschaft unter die E-Commerce-Richtlinie und andererseits zugleich als TK-Dienste unter die Telekommunikationsrahmenrichtlinie.¹³²

Auf der – im Vergleich zur Transportebene – höher angesiedelten Dienstebene befinden sich Angebote zur Nutzung bestimmter Inhalte. Obwohl auf dieser Stufe des Telekommunikationsvorgangs der

¹²⁷ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 225; vgl. Panzer (o. Fußn. 103), S. 172.

¹²⁸ Vgl. Mattl (o. Fußn. 21), S. 58 f.; vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 225.

¹²⁹ Vgl. Steidle (o. Fußn. 105), S. 143.

¹³⁰ Vgl. Mattl (o. Fußn. 21), S. 59; vgl. Steidle (o. Fußn. 105), S. 143.

¹³¹ Vgl. Steidle (o. Fußn. 105), S. 143.

¹³² Vgl. Roßnagel, NVwZ 2007, 743 (745).

Information als solcher zentrale Bedeutung zukommt, ist zur Übertragung einer solchen zwangsläufig ein Transport vorausgesetzt.¹³³ Eine Unterscheidung zwischen Tele- und Mediendiensten wurde mit Inkrafttreten des Telemediengesetzes hinfällig; insofern besteht nunmehr größere Rechtssicherheit, da eine Abgrenzung in Einzelfällen nicht immer trennscharf vollzogen werden konnte. Es spielt inzwischen keine Rolle mehr, ob es sich um eine reine Dienstleistung im Sinne einer Beschaffung von faktischen Informationen (etwa durch ein Online-Telefonverzeichnis) oder um redaktionell gestaltete Texte zur öffentlichen Meinungsbildung (bspw. durch einen Nachrichtendienst) handelt.¹³⁴

Für die oberste Ebene, welche den Inhalt der übermittelten Information betrifft, gelten die allgemeinen Rechtsnormen des „Offline-Rechts“¹³⁵. Ein eindringliches Beispiel liefert die folgende Situation: Ein Online-Börseninformationsdienst bezeichnet in seinem Internet-Auftritt ein Unternehmen als schrottreif, obgleich diese Aussage nicht der Wahrheit entspricht. Etwaige Schadenersatzansprüche dieses Unternehmens richten sich dann nach § 823 Abs. 1 BGB.¹³⁶ Was den Umgang mit personenbezogenen Daten anbelangt, gelten die allgemeinen Regelungen des Bundesdatenschutzgesetzes und bereichsspezifische Vorschriften des Sozialgesetzbuches, des Bürgerlichen Gesetzbuches sowie von Betriebsvereinbarungen¹³⁷.

Im Übrigen ist darauf hinzuweisen, dass sich die Grenzziehung zwischen den drei aufgezeigten Ebenen oftmals nicht exakt vornehmen lässt, was in der Folge zur Konkurrenz der anzuwendenden

¹³³ Vgl. *Mattl* (o. Fußn. 21), S. 60 f.

¹³⁴ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnrn. 226-228.

¹³⁵ Vgl. *Mattl* (o. Fußn. 21), S. 61.

¹³⁶ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 229.

¹³⁷ Vgl. *Steidle* (o. Fußn. 105), S. 146 f.; vgl. *Mattl* (o. Fußn. 21), S. 61 f; vgl. *Gola*, MMR 1999, 322 (323).

Normen führen kann. Dieser Umstand deutet auf die Schwierigkeit der gesamten Materie hin.¹³⁸

4.2.2.1.1 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz¹³⁹ enthält allgemeine datenschutzrechtliche Verpflichtungen, die sich mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche und nichtöffentliche Stellen auseinandersetzen¹⁴⁰. Das Bundesdatenschutzgesetz kommt gem. § 1 Abs. 3 BDSG im Verhältnis zu anderen Datenschutzgesetzen nur subsidiär zur Anwendung (*lex generalis*); d. h. wenn ein spezielleres Gesetz den Sachverhalt erfasst, sind die Vorschriften des speziellen Gesetzes einschlägig¹⁴¹. Als zentrale Rechtsvorschrift in Bezug auf die Überwachung der elektronischen Kommunikationsmittel der Arbeitnehmer gilt § 4 BDSG. Er regelt die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung. § 4 Abs. 1 BDSG verwirklicht ein Verbot mit Erlaubnisvorbehalt – ein dem gesamten Datenschutzrecht innewohnender Grundsatz.¹⁴² Das Bundesdatenschutzgesetz erlaubt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur, soweit es diese Vorgänge selbst oder eine andere Rechtsvorschrift zulässt. Im Übrigen benötigt man für eine zulässige Durchführung der genannten Zwecke stets die Einwilligung des betroffenen Arbeitnehmers.¹⁴³

¹³⁸ Vgl. *Mattl* (o. Fußn. 21), S. 62.

¹³⁹ Siehe dazu bspw. *Tinnefeld*, NJW 2001, 3078-3083.

¹⁴⁰ Vgl. *Elschner* (o. Fußn. 3), S. 272.

¹⁴¹ Vgl. *Panzer* (o. Fußn. 103), S. 152; vgl. *Gola* (o. Fußn. 123), S. 51 Rdnr. 120; vgl. *Henke*, IT und Datenschutz im Unternehmen, 2006, S. 31; vgl. *Lelley*, in: *Worzalla*, S. 23 Rdnr. 56; vgl. *Weißgerber* (o. Fußn. 98), S. 121.

¹⁴² Vgl. *Tuchbreiter* (o. Fußn. 116), S. 154; vgl. *Panzer* (o. Fußn. 103), S. 156.

¹⁴³ Vgl. *Klasen*, Unternehmensinterne Datennetze im Lichte der Betriebsverfassung, 2005, S. 123.

4.2.2.1.2 Telekommunikationsgesetz

Durch die Normen des Telekommunikationsgesetzes wird grundsätzlich die Technik der Informationsübermittlung erfasst¹⁴⁴. Der Gesetzeszweck ist in § 1 TKG verankert: Das Telekommunikationsgesetz soll den Wettbewerb im Bereich Telekommunikation und die Telekommunikationsinfrastrukturen durch Regulierung fördern und flächendeckend angemessene und ausreichende Dienstleistungen gewährleisten. Überdies regelt das Telekommunikationsgesetz die grundsätzliche Möglichkeit der Erbringung von Telekommunikationsleistungen – z. B. durch das Zurverfügungstellen öffentlicher Wege – und beinhaltet die für die Arbeitnehmerüberwachung wichtigen Bestimmungen des Fernmeldegeheimnisses in § 88 TKG sowie des bereichsspezifischen Datenschutzes in §§ 91 ff. TKG.¹⁴⁵ Die Regelungen des Telekommunikationsgesetzes gehen als *lex specialis* den Normen des Bundesdatenschutzgesetzes vor¹⁴⁶.

4.2.2.1.3 Telemediengesetz

Das Telemediengesetz trat am 1.3.2007 in Kraft und vereint die ehemaligen Vorschriften des Teledienstegesetzes, des Telediensteschutzgesetzes und des Mediendienste-Staatsvertrags, die damit allesamt außer Kraft gesetzt wurden, in einem einzigen Gesetz¹⁴⁷. Der Gesetzgeber hatte zum Ziel, das einstmalige Regelungschaos zwischen Telediensten und Mediendiensten aus der Welt zu schaffen¹⁴⁸. Das Telemediengesetz umfasst im Wesentlichen Regelungen zur Haftung

¹⁴⁴ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 255.

¹⁴⁵ Vgl. *Henke* (o. Fußn. 141), S. 35 f.; vgl. *Höld* (o. Fußn. 55), S. 128 f; vgl. *Lelley*, in: *Worzalla*, S. 23 Rdnr. 57.

¹⁴⁶ Vgl. *Koeppen* (o. Fußn. 7), S. 167.

¹⁴⁷ Vgl. *Mattl* (o. Fußn. 21), S. 116; vgl. *Rofßnagel* (o. Fußn. 132), 743 (748).

¹⁴⁸ Vgl. *Hoeren*, NJW 2007, 801 (806), der gleichzeitig zu bedenken gibt, ob durch die Vereinheitlichung zum Telemediengesetz ein nicht noch größeres Regelungschaos als vorher entstanden sei, das nunmehr die Abgrenzung von Telemedien zu Rundfunk und Telekommunikation betreffe.

von Internet-Providern, generelle Informationspflichten im E-Commerce und datenschutzrechtliche Bestimmungen im Internet, welchen ein besonderer Stellenwert für die Beurteilung der Zulässigkeit der Überwachung zukommen kann¹⁴⁹. Auch die Normen des Telemediengesetzes verdrängen als speziellere Vorschriften das Bundesdatenschutzgesetz.

4.2.2.2 Arbeitsrecht

4.2.2.2.1 Betriebsverfassungsgesetz

Auch kollektivarbeitsrechtliche Normen gilt es im Zusammenhang mit der Internet- und E-Mail-Überwachung von Mitarbeitern zu beachten. Sofern ein Betriebsrat im Unternehmen eingerichtet ist, kann hier insbesondere eine Betriebsvereinbarung, in der die Nutzungsbedingungen der elektronischen Kommunikationssysteme geregelt sind, eine wichtige Rolle einnehmen.¹⁵⁰ Für die Mitarbeiterkontrolle im Hinblick auf die Nutzung der betrieblichen IuK-Anlage ist § 87 Abs. 1 Nr. 6 BetrVG von Bedeutung. Nach diesem steht dem Betriebsrat ein Mitbestimmungsrecht zu, wenn es im Unternehmen um die Einführung und Anwendung technischer Einrichtungen geht, die dazu bestimmt sind, Verhaltens- oder Leistungskontrollen durchzuführen.¹⁵¹

4.2.2.2.2 Bildschirmarbeitsverordnung

Die Bildschirmarbeitsverordnung setzt i. V. m. dem Arbeitsschutzgesetz die Richtlinie 90/270/EWG über die Mindestvorschriften bezüglich der Sicherheit und des Gesundheitsschutzes bei der Arbeit

¹⁴⁹ Vgl. Hoeren (o. Fußn. 148), 801.

¹⁵⁰ Vgl. Lelley, in: Worzalla, S. 25 Rdnr. 63.

¹⁵¹ Vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1500).

an Bildschirmgeräten um. Ein Arbeitsplatz mit Online-Zugang eröffnet den sachlichen Anwendungsbereich der Verordnung¹⁵². Wenn Überwachungsmaßnahmen in Rede stehen, ist Nr. 22 des Anhangs, der an Bildschirmarbeitsplätze zu stellende Anforderungen aufführt, zu beachten¹⁵³. Nr. 22 des Anhangs lautet: „Ohne Wissen der Benutzer darf keine Vorrichtung zur qualitativen oder quantitativen Kontrolle verwendet werden“.

Die Verordnung gibt jedoch Anlass zur Kritik: § 1 Abs. 1 BildscharbV sieht vor, dass die Verordnung für die „Arbeit“ an Bildschirmgeräten gilt; somit reduziert sich das Kontrollverbot auf lediglich die dienstliche Nutzung. Überdies kann an Nr. 22 des Anhangs moniert werden, dass Kontrollen durchgeführt werden dürfen, sofern die Benutzer davon wissen. Dieses Wissen über die Kontrolle ist weit auszulegen: Dafür genügt es, wenn sich Mitarbeiter allgemein bewusst sind, dass ihre Leistung technisch überwacht wird oder überwacht werden kann. Der Arbeitgeber muss auch nicht auf Überwachungsaktivitäten hinweisen, sondern es reicht aus, dass dieses Wissen bspw. aus allgemeinen Erfahrungssätzen hergeleitet werden kann.¹⁵⁴

¹⁵² Vgl. *Elschner* (o. Fußn. 3), S. 29.

¹⁵³ Vgl. *Kiper* in: *Schulzki-Haddouti* (o. Fußn. 36), S. 104; vgl. *Steidle* (o. Fußn. 105), S. 121.

¹⁵⁴ Vgl. *Erlner* (o. Fußn. 18), S. 142 f.

5 ÜBERWACHUNG DER INTERNET- UND E-MAIL-KOMMUNIKATION NACH AKTUELLER RECHTSLAGE

5.1 Abgrenzung zwischen betrieblicher und privater Nutzung

Zunächst ist zu klären, wann es sich um eine dienstliche und wann um eine private Nutzung der Medien handelt, da diese Unterscheidung für die rechtliche Beurteilung der Zulässigkeit einer Überwachung durch den Arbeitgeber zwingend erforderlich ist¹⁵⁵. Der Umstand, dass eine erlaubte Privatnutzung vorliegt, eröffnet – wie noch zu zeigen sein wird – den Anwendungsbereich des Telekommunikationsrechts und des Telemedienrechts¹⁵⁶.

Nach h. M. liegt eine dienstliche Nutzung vor, sobald die Nutzung dazu bestimmt ist, die Arbeit zu fördern. Der eingetretene Erfolg ist dafür allerdings nicht ausschlaggebend, sodass auf die Absicht, die Arbeit voranzutreiben, abzustellen ist.¹⁵⁷ Bestehen Zweifel im Hinblick auf die Abgrenzung, kann auf die diesbezüglichen Grundsätze des Unfallversicherungsrechts und der Arbeitnehmerhaftung zurückgegriffen werden; in beiden Regelungsmaterien wird ein Ereignis vorausgesetzt, das im „ursächlichen und inneren Zusammenhang mit einer betrieblichen Tätigkeit“ steht.¹⁵⁸

Telefonisch abgewickelte Privatgespräche aus dienstlichem Anlass werden als Dienstgespräche behandelt. Um einen solchen Fall handelt es sich z. B. dann, wenn ein Mitarbeiter seine Ehefrau anruft, um ihr

¹⁵⁵ Vgl. *Mengel* (o. Fußn. 102), 2014; vgl. *Kömpf/Kunz*, NZA 2007, 1341 (1343).

¹⁵⁶ Vgl. *Steidle* (o. Fußn. 105), S. 162.

¹⁵⁷ Vgl. *Ernst* (o. Fußn. 53), 585 (588); vgl. *Steidle* (o. Fußn. 105), S. 162; vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 177; vgl. *Weißnicht*, MMR 2003, 448; vgl. *Däubler* (o. Fußn. 64), 323 (324); vgl. *Rath/Karner* (o. Fußn. 35), 446 (449).

¹⁵⁸ Vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 177; vgl. *Steidle* (o. Fußn. 105), S. 162.

mitzuteilen, dass er länger als geplant im Betrieb arbeiten müsse und demzufolge später nach Hause komme.¹⁵⁹ Die Zulässigkeit dienstlich motivierter Privatanrufe ergibt sich aus der Fürsorgepflicht des Arbeitgebers¹⁶⁰. Dieser für das Sprachtelefon entwickelte Grundsatz ist auch auf andere Formen von Kommunikationsmedien anzuwenden – also auch auf E-Mail –, da sich dieselbe Interessenlage ergibt, und die Bedeutung anderer Kommunikationsmedien im Arbeitsumfeld der des Telefons grundsätzlich entspricht¹⁶¹.

Ferner muss es dem Arbeitnehmer in besonderen Notfällen gestattet sein, die Kommunikationseinrichtungen des Unternehmens zu nutzen¹⁶². Ein Notfall liegt bspw. dann vor, wenn sich ein Beschäftigter nach dem Wohlbefinden eines verunfallten Angehörigen erkundigen und deshalb im Krankenhaus anrufen will. Dazu kann er alle ihm zur Verfügung stehenden Kommunikationsmedien, selbstredend einschließlich Internet und E-Mail, verwenden.¹⁶³

Darüber hinaus darf Privates am Arbeitsplatz kommuniziert werden. Hierbei handelt es sich um einen mäßigen privaten Austausch unter Kollegen, die sich dabei z. B. nach ihrem gegenseitigen Wohlergehen erkundigen dürfen. Diese Kommunikation kann auch mit einer E-Mail erfolgen.¹⁶⁴

Für die Bestimmung der Privatnutzung ist eine Negativabgrenzung vorzunehmen; eine reine Privatnutzung ist immer dann gegeben, wenn keine betriebliche Nutzung bzw. Privatnutzung aus betrieblichem Anlass vorliegt¹⁶⁵.

¹⁵⁹ Vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 178.

¹⁶⁰ Vgl. *Ernst* (o. Fußn. 53), 585 (588).

¹⁶¹ Vgl. *Steidle* (o. Fußn. 105), S. 163; vgl. *Ernst* (o. Fußn. 53), 585 (588); vgl. *Weißgerber* (o. Fußn. 98), S. 70.

¹⁶² Vgl. *Mengel* (o. Fußn. 102), 2014; vgl. *Weißgerber* (o. Fußn. 98), S. 69.

¹⁶³ Vgl. *Weißgerber* (o. Fußn. 98), S. 69 f.

¹⁶⁴ Vgl. *Ernst* (o. Fußn. 53), 585 (588).

¹⁶⁵ Vgl. *Steidle* (o. Fußn. 105), S. 163.

5.1.1 Erlaubnis zur privaten Nutzung

Die Entscheidung darüber, ob und in welchem Umfang Mitarbeiter die betrieblichen IuK-Anlagen nutzen dürfen, trifft allein der Arbeitgeber¹⁶⁶. Ihm steht es darüber hinaus frei, insbesondere auch die Nutzung der betrieblichen Kommunikationsmittel zu privaten Zwecken zu erlauben¹⁶⁷. Ein Recht auf Privatnutzung existiert nicht¹⁶⁸. Das Recht auf freie Nutzungsbestimmung ergibt sich aus dem Eigentums- und Direktionsrecht des Arbeitgebers¹⁶⁹.

5.1.1.1 Ausdrückliche Erlaubnis

Eine Gestattung zum Gebrauch der elektronischen Kommunikationstechnik zu privaten Zwecken kommt zunächst durch eine ausdrückliche Erlaubnis in Betracht¹⁷⁰. Diese kann in Form einer Klausel im Arbeitsvertrag oder, was häufiger anzutreffen ist, in einer Zusatzvereinbarung zum Arbeitsvertrag¹⁷¹ verankert oder durch eine Betriebsvereinbarung geregelt sein¹⁷². Ein Muster einer Zusatzvereinbarung zum Arbeitsvertrag und ein Muster einer Betriebsvereinbarung sind im Anhang der vorliegenden Arbeit enthalten (Anlage 4 und Anlage 5).

Entscheidet sich der Arbeitgeber für die Option Erlaubnis zur Privatnutzung mittels Arbeitsvertrag bzw. Zusatzvereinbarung zum Arbeitsvertrag, und will er die Internet-Nutzung im Laufe der Zeit neu reglementieren, z. B. neue Festlegung der erlaubten privaten Nut-

¹⁶⁶ Vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135; vgl. *Rath/Karner* (o. Fußn. 35), 446 (448); vgl. *Nägele/Meyer* (o. Fußn. 34), 312.

¹⁶⁷ Vgl. *Nägele/Meyer* (o. Fußn. 34), 312; vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 180; vgl. *Ernst* (o. Fußn. 53), 585; vgl. *Weißnicht* (o. Fußn. 157), 448; vgl. *Kramer*, NZA 2004, 457 (458).

¹⁶⁸ Vgl. *Ernst* (o. Fußn. 53), 585; vgl. *Kömpf/Kunz* (o. Fußn. 155), 1341 (1344).

¹⁶⁹ Vgl. *Steidle* (o. Fußn. 105), 163; vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 180.

¹⁷⁰ Vgl. *Zilkens* (o. Fußn. 57), 253 (256).

¹⁷¹ Vgl. *Mattl* (o. Fußn. 21), S. 37 f.

¹⁷² Vgl. *Weißnicht* (o. Fußn. 157), 448.

zungsdauer, dann muss mit jedem einzelnen Arbeitnehmer eine neue Regelung getroffen werden. Falls sich Mitarbeiter einer einvernehmlichen Abänderung widersetzen, kann nur noch das Mittel der Änderungskündigung herangezogen werden, sofern die ursprüngliche Vereinbarung keine Freiwilligkeitsklausel enthält.¹⁷³ In der betrieblichen Praxis wird häufig auf eine Betriebsvereinbarung zurückgegriffen, da sie einen gravierenden Vorteil gegenüber der Alternative des Arbeitsvertrags mit sich bringt: Die Betriebsvereinbarung erlaubt eine einfache Homogenisierung der Arbeitsbedingungen bei geringem bürokratischen Aufwand. Bei Bedarf wird sie gekündigt, und der Arbeitgeber schließt mit dem Betriebsrat eine neue Regelung ab. Durch die große Flexibilität des Instruments Betriebsvereinbarung wird auch Anpassungserfordernissen aufgrund des technischen Fortschritts Rechnung getragen.¹⁷⁴ Daneben besteht die Möglichkeit der Bekanntmachung innerhalb des Unternehmens durch eine Internet-Policy o. ä.¹⁷⁵ Im Anhang ist ein Muster einer Internet-Policy abgedruckt (Anlage 6). Ein praktikabler Weg kann auch die Vergabe sowohl einer dienstlichen als auch einer privaten E-Mail-Adresse an den Arbeitnehmer sein¹⁷⁶.

5.1.1.2 Konkludente Erlaubnis

Schwieriger zu beurteilen ist die Frage, ob eine konkludente Erlaubnis vorliegt. Sie wäre bspw. dann problemlos anzunehmen, wenn der Arbeitgeber von sich aus bei der Installation der Browser-Software auf den Arbeitsplatz-PCs Favoriten wie etwa „Auto und Motor“, „Spiele“, „Gesundheit“ oder „Reisen“ festlegt.¹⁷⁷ Der Umfang einer konkludenten Erlaubnis ergibt sich durch Auslegung nach §§ 133 und 157

¹⁷³ Vgl. *Mattl* (o. Fußn. 21), S. 38.

¹⁷⁴ Vgl. *Mattl* (o. Fußn. 21), S. 37.

¹⁷⁵ Vgl. *Steidle* (o. Fußn. 105), S. 164; vgl. *Mattl* (o. Fußn. 21), S. 38.

¹⁷⁶ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 6; vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 183.

¹⁷⁷ Vgl. *Däubler* (o. Fußn. 64), 323 (325).

BGB¹⁷⁸. Falls privates Telefonieren erlaubt ist, wird der Beschäftigte davon ausgehen können, dass etwa im selben Umfang die Nutzung des Internets und des E-Mail-Dienstes gestattet ist¹⁷⁹. Auch wird man von einer konkludenten Erlaubnis ausgehen können, wenn in Aufenthaltsräumen Computer mit Internet-Zugang zur freien Benutzung aufgestellt sind oder die Inanspruchnahme des Internet-Anschlusses am Arbeitsplatz zu privaten Belangen mit dem einzelnen Arbeitnehmer abgerechnet wird.¹⁸⁰

5.1.1.3 Betriebliche Übung

Durch eine entsprechende betriebliche Übung kann ebenfalls eine Erlaubnis zur Privatnutzung der betrieblichen Kommunikationseinrichtung entstehen¹⁸¹. Eine dahingehende Betriebsübung stellt sich allerdings nur ein, wenn die praktizierte Privatnutzung für den Arbeitgeber erkennbar war, von ihm geduldet wird, und die Arbeitnehmer darauf vertrauen durften, dass auch zukünftig dieser Zustand herrschen wird¹⁸². Da eine höchstrichterliche Rechtsprechung zur Frage, ab welchem Zeitraum eine betriebliche Übung im Zusammenhang mit der privaten Nutzung der elektronischen Kommunikationssysteme noch nicht existiert, wird grundsätzlich angenommen, dass sechs bis zwölf Monate hierfür ausreichen¹⁸³. Im Streitfall hat der Arbeitnehmer zu beweisen, dass eine betriebliche Übung vorliegt¹⁸⁴.

¹⁷⁸ Vgl. *Weißnicht* (o. Fußn. 157), 448.

¹⁷⁹ Vgl. *Däubler* (o. Fußn. 64), 323 (325); vgl. *Zilkens* (o. Fußn. 57), 253 (256); vgl. *Hoeren* (o. Fußn. 10), S. 249; im Gegensatz dazu *Lelley*, in: *Worzalla*, S. 14 Rdnr. 30.

¹⁸⁰ Vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 184.

¹⁸¹ Vgl. *Weißnicht* (o. Fußn. 157), 448; vgl. *Beckschulze/Henkel* (o. Fußn. 61), 1491 (1492).

¹⁸² Vgl. *Steidle* (o. Fußn. 105), S. 164; vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 185; vgl. *Beckschulze/Henkel* (o. Fußn. 61), 1491 (1492).

¹⁸³ Vgl. *Barton*, NZA 2006, 460 (461); vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 185; vgl. *Steidle* (o. Fußn. 105), S. 164; im Gegensatz dazu *Waltermann*, NZA 2007, 529-533, der das Entstehen einer betrieblichen Übung zur Nutzung von Internet und E-Mail aufgrund der Anwendung von Rechtsprechungsgrundsätzen zur betrieblichen Übung ablehnt.

¹⁸⁴ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 9.

5.1.1.4 Einschränkung der Erlaubnis

Die genehmigte Privatnutzung kann sowohl zeitlich als auch inhaltlich eingeschränkt werden. Denkbar ist etwa die Beschränkung auf Pausen, das Verbot des Aufrufs von Webseiten mit bestimmten Inhalten, die Untersagung der Verwendung des E-Mail-Dienstes für private Zwecke, die Festlegung von Obergrenzen hinsichtlich übertragener Datenmenge oder das Verbot des Öffnens von Attachments.¹⁸⁵ Ferner kommt das sog. Übermaßverbot zum Tragen, welches dem Beschäftigten untersagt, exzessiv zu Privatzwecken von der IuK-Technik Gebrauch zu machen und dabei seine arbeitsvertraglichen Pflichten massiv zu beeinträchtigen¹⁸⁶.

5.1.1.5 Rücknahme der Erlaubnis

Da die Erlaubnis zur privaten Nutzung der Dienste eine freiwillige Leistung des Arbeitgebers darstellt, kann er diese auch wieder zurücknehmen¹⁸⁷. Wurde die Leistung jedoch ausdrücklich zugesichert, steht dem zukünftigen Verbot i. d. R. der Arbeitsvertrag, die Zusatzvereinbarung zum Arbeitsvertrag bzw. eine Betriebsvereinbarung entgegen. Will der Arbeitgeber die Erlaubnis entziehen, muss er – außer bei einer Betriebsvereinbarung – mit jedem einzelnen Beschäftigten eine Vereinbarung treffen. Falls keine einvernehmliche Vereinbarung zustande kommt, bleibt als Alternative die Änderungskündigung - vergleichbar dem oben dargestellten Vorgehen bei Nutzungsänderungen.¹⁸⁸ Der Arbeitgeber hat überdies schon im Vorfeld die Möglichkeit, die Weichen für eine potenzielle Erlaubnisrücknahme zu stellen: Er kann seine Einwilligung an einen Widerrufsvorbehalt knüpfen. Dies setzt

¹⁸⁵ Vgl. *Nägele/Mayer* (o. Fußn. 34), 312; vgl. *Ernst* (o. Fußn. 53), 585 (586).

¹⁸⁶ Vgl. *Weißnicht* (o. Fußn. 157), 448.

¹⁸⁷ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 27; vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 186.

¹⁸⁸ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 27; vgl. *Nägele/Mayer* (o. Fußn. 34), 312 (313).

jedoch einen sachlichen Grund, bspw. eine Systemüberlastung, voraus, da der Arbeitgeber nach „billigem Ermessen“ (§ 315 BGB) zu entscheiden hat.¹⁸⁹ Der Widerrufsvorbehalt stellt insofern hohe Ansprüche an den Arbeitgeber, denn seine Ausübung muss einer gerichtlichen Überprüfung standhalten. Deshalb ist Arbeitgebern unbedingt zu raten, die Gestattung unter einen Freiwilligkeitsvorbehalt zu stellen¹⁹⁰; aufgrund dessen entsteht erst gar kein Anspruch auf die Leistung. Der Freiwilligkeitsvorbehalt erlaubt die Einstellung oder Modifikation der Leistung ohne vorhergehende Ankündigung oder Bindung an § 315 BGB. Die einzige Einschränkung stellt der Gleichbehandlungsgrundsatz dar.¹⁹¹ Zwingende Voraussetzungen für einen wirksamen Freiwilligkeitsvorbehalt sind erstens ein ausdrücklicher Hinweis auf die Freiwilligkeit und zweitens ein deutliches Signal, dass ein Anspruch auf die Leistung für die Zukunft nicht besteht¹⁹². Die Beendigung der betrieblichen Übung kann durch eine gegenläufige betriebliche Übung, d. h. durch ein Verhalten, bei dem das Gegenteil praktiziert wird, erreicht werden¹⁹³. In der Praxis gestaltet sich die Etablierung einer gegenläufigen betrieblichen Übung jedoch äußerst schwierig¹⁹⁴.

5.1.2 Konsequenzen der erlaubten Privatnutzung

Die Unterscheidung zwischen ausschließlich dienstlicher Nutzung und privater Nutzung der elektronischen Kommunikationseinrichtungen hat gravierende Auswirkungen auf die vom Arbeitgeber einzuhaltenden Datenschutzvorschriften und mithin auf die Zulässigkeit

¹⁸⁹ Vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 188.

¹⁹⁰ Vgl. *Mattl* (o. Fußn. 21), S. 38; vgl. *Barton* (o. Fußn. 183), 460 (463); vgl. *Waltermann* (o. Fußn. 183), 529 (532 f.).

¹⁹¹ Vgl. *Barton* (o. Fußn. 183), 460 (463).

¹⁹² Vgl. *Kramer* (o. Fußn. 167), 457 (459).

¹⁹³ Vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 188.

¹⁹⁴ Siehe dazu ausführlich *Barton*, NZA 2006, 460-466, der verschiedene Möglichkeiten zur Beendigung der betrieblichen Übung darstellt, dabei jedoch auch auf Maßnahmen eingeht, die nur bei einer ausdrücklichen Vereinbarung wirken können.

von Überwachungsmaßnahmen. Es ist vorab jeweils festzustellen, welche Gesetze für die ausschließlich betriebliche Nutzung und für die erlaubte Privatnutzung Geltung erlangen.

Betrachtet man zunächst den Fall der ausschließlich dienstlichen Nutzung - und somit der unerlaubten Privatnutzung -, muss festgestellt werden, anhand welcher gesetzlichen Bestimmungen die Kontrollmaßnahmen des Arbeitgebers zu beurteilen sind. Da jeder Inanspruchnahme des Internet- und E-Mail-Anschlusses eine Telekommunikation zu Grunde liegt, ist zu prüfen, ob das Telekommunikationsgesetz auch im Verhältnis zwischen dem Arbeitgeber und seinen Beschäftigten Anwendung findet¹⁹⁵. Gem. § 91 Abs. 1 TKG finden die datenschutzrechtlichen Vorschriften des Telekommunikationsgesetzes nur dann Beachtung, wenn das Unternehmen Telekommunikationsdienste nach § 3 Nr. 24 TKG geschäftsmäßig erbringt oder an deren Erbringung mitwirkt. Unter geschäftsmäßigem Erbringen von Telekommunikationsdiensten ist nach der Legaldefinition aus § 3 Nr. 10 TKG „...das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht“ zu verstehen. Bei der Erbringung ist nicht auf eine Gewerblichkeit, sondern lediglich auf eine Geschäftsmäßigkeit abzustellen; diese ist regelmäßig gegeben, wenn der Dienst nachhaltig, also dauerhaft angeboten wird.¹⁹⁶ Weiterhin gilt es zu beachten, dass von der Bestimmung des § 3 Nr. 10 TKG nicht nur spezielle Telekommunikationsunternehmen erfasst sind, sondern sämtliche „gewöhnliche“ Unternehmen, die durch die Bereitstellung und den Gebrauch von bspw. Internet-Zugang, E-Mail-Anschluss und Telefonanlagen einen Telekommunikationsdienst erbringen.¹⁹⁷ Der Arbeitnehmer, der im Rahmen der Erfüllung seiner Arbeitsaufgaben auf die Inanspruchnahme von Internet und/oder E-Mail angewiesen ist, nimmt allerdings die Stellung eines Besitzdieners

¹⁹⁵ Vgl. *Steidle* (o. Fußn. 105), S. 158.

¹⁹⁶ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnrn. 18-20.

¹⁹⁷ Vgl. *Gola* (o. Fußn. 137), 322 (323); vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 20.

gem. § 855 BGB ein; er ist insoweit Teil des Unternehmens und nicht „Dritter“¹⁹⁸. Darüber hinaus liegt auch kein „Angebot“ vor, bei dem die Arbeitnehmer nach Belieben entscheiden können, ob sie die betrieblichen Kommunikationsmittel einsetzen wollen oder nicht – im Rahmen des Arbeitsverhältnisses obliegt ihnen die Pflicht, die Techniken zu benutzen¹⁹⁹. Die Anwendung des Telekommunikationsgesetzes und damit das Beachtungserfordernis insbesondere des Fernmeldegeheimnisses aus § 88 TKG und der bereichsspezifischen Datenschutzbestimmungen der §§ 91 ff. TKG scheidet bei der betrieblichen Kommunikation aus²⁰⁰.

Da Web-Dienste und i. d. R. auch der E-Mail-Dienst elektronische Informations- und Kommunikationsdienste i. S. d. § 1 Abs. 1 S. 1 TMG darstellen²⁰¹, ist zunächst fraglich, inwieweit das Telemediengesetz im Verhältnis zwischen Arbeitgeber und Arbeitnehmern bei der rein dienstlichen Nutzung zur Anwendung gelangt. Die Antwort darauf findet sich in § 11 Abs. 1 S. 1 Nr. 1 TMG: Bei einer rein dienstlichen Nutzung sind die Datenschutzbestimmungen des Telemediengesetzes in Ermangelung eines Anbieter-Nutzer-Verhältnisses ausdrücklich nicht im Arbeitsverhältnis einschlägig²⁰².

Anwendbar jedoch ist das Bundesdatenschutzgesetz als subsidiäres „Auffanggesetz“ gem. § 1 Abs. 3 BDSG, das bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten einschlägig ist, wenn keine Spezialgesetze greifen²⁰³. Der Gesetzeszweck ist in § 1 Abs. 1 BDSG manifestiert. Das Gesetz soll den Schutz des Persönlichkeitsrechts des Einzelnen beim Umgang mit seinen personenbezoge-

¹⁹⁸ Vgl. Steidle (o. Fußn. 105), S. 159; vgl. Schönfeld/Strese/Flemming (o. Fußn. 94), 8 (11); vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 23.

¹⁹⁹ Vgl. Höld (o. Fußn. 55), S. 130; vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 23.

²⁰⁰ Vgl. Tinnefeld (o. Fußn. 83), 797 (799); vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 23.

²⁰¹ Vgl. Roßnagel (o. Fußn. 132), 743 (745).

²⁰² Vgl. Kömpf/Kunz (o. Fußn. 155), 1341 (1344); vgl. Mattl (o. Fußn. 21), S. 126 f.

²⁰³ Vgl. Lelley, in: Worzalla, S. 26 Rdnr. 67.

nen Daten gewährleisten. § 3a BDSG normiert einen wichtigen Grundsatz des Bundesdatenschutzgesetzes, namentlich die Datenvermeidung und Datensparsamkeit. Die Datenverarbeitungssysteme sollen hiernach so gestaltet und ausgewählt sein, dass keine oder so wenig wie möglich personenbezogene Daten erhoben, verarbeitet und genutzt werden. Außerdem soll die Möglichkeit der Anonymisierung gem. § 3 Abs. 6 BDSG und Pseudonymisierung gem. § 3 Abs. 6a BDSG wahrgenommen werden, soweit dies machbar ist und im angemessenen Verhältnis zum angestrebten Schutzzweck steht.²⁰⁴ Neben den datenschutzrechtlichen Erlaubnistatbeständen des Bundesdatenschutzgesetzes im Hinblick auf die Überwachung sind bei der untersagten Privatnutzung von Internet und E-Mail ferner die mittelbar geltenden Grundrechte der Arbeitnehmer zu berücksichtigen²⁰⁵. Der Vollständigkeit halber wird darauf hingewiesen, dass Unternehmen, die in den Anwendungsbereich des Bundesdatenschutzgesetzes fallen, gem. § 9 BDSG und der Anlage zum § 9 S. 1 BDSG geeignete technische und organisatorische Maßnahmen zu treffen haben, die Datensicherheit und Schutz personenbezogener Daten gewährleisten²⁰⁶.

Erlaubt oder duldet zumindest der Arbeitgeber dagegen die Privatnutzung der elektronischen Kommunikationsmittel, ergibt sich eine völlig andere rechtliche Situation. Unter dieser Voraussetzung kommen das bereichsspezifische Telekommunikationsgesetz und das Telemediengesetz zur Anwendung. Bei der erlaubten Privatnutzung tritt das Bundesdatenschutzgesetz als *lex generalis* hinter die speziellen Normen des Telekommunikationsgesetzes und Telemediengesetzes zurück.

Das Telekommunikationsgesetz erlangt Gültigkeit im Verhältnis zwischen Arbeitgeber und Arbeitnehmern, da die Mitarbeiter durch die Erlaubnis zur Privatnutzung die Stellung von „Dritten“ gem. § 3 Nr.

²⁰⁴ Vgl. Panzer (o. Fußn. 103), S. 153.

²⁰⁵ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 28; vgl. Mattl (o. Fußn. 21), S. 129; vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (136).

²⁰⁶ Vgl. Steidle (o. Fußn. 105), S. 177 f.

10 TKG einnehmen. Ungeachtet dessen, ob die Mitarbeiter das betriebliche Kommunikationssystem entgeltlich oder unentgeltlich zu privaten Zwecken nutzen dürfen, agieren sie in beiden Fällen nicht mehr als Teil des Unternehmens und ebenso wenig in Erfüllung ihrer arbeitsvertraglich geschuldeten Pflichten. Vielmehr bleibt es jedem Arbeitnehmer selbst überlassen, ob er vom Telekommunikationsnutzungsangebot des Arbeitgebers Gebrauch machen oder dies ablehnen will.²⁰⁷ Das telekommunikationsrechtliche Pendant zu § 9 BDSG verkörpert § 109 TKG. Bei erlaubter Privatnutzung obliegt dem Arbeitgeber nach § 109 Abs. 1 Nr. 1 und Nr. 2 TKG die Pflicht, technische und sonstige Maßnahmen zu treffen, welche das Fernmeldegeheimnis, die personenbezogenen Daten, die Telekommunikations- und Datenverarbeitungssysteme schützen sollen.²⁰⁸

Gem. § 2 Nr. 1 TMG „...ist Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“. Da schon die bloße Vermittlung eines Nutzungszugangs dazu führt, dass der Arbeitgeber die Stellung eines Diensteanbieters einnimmt, wird er zu einem solchen, wenn er die private Internet- und E-Mail-Nutzung zulässt und somit zumindest den Zugang zu fremden Telemediendiensten vermittelt.²⁰⁹ Im Übrigen liegt ein Anbieter-Nutzer-Verhältnis gem. § 11 TMG vor; die Bereitstellung der Dienste erfolgt gerade nicht zu ausschließlich dienstlichen Zwecken.

Das Bundesdatenschutzgesetz kommt bei der gestatteten Privatnutzung nur noch insoweit zur Anwendung, als es durch die spezialgesetzlichen Regelungen nicht verdrängt wird²¹⁰.

²⁰⁷ Vgl. *Steidle* (o. Fußn. 105), S. 161; vgl. *Däubler* (o. Fußn. 26), § 4 Rdnrn. 235 f.; vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 82.

²⁰⁸ Vgl. *Rath/Karner* (o. Fußn. 35), 446 (450).

²⁰⁹ Vgl. *Mattl* (o. Fußn. 21), S. 122-124.

²¹⁰ Vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (136 f.).

Es bleibt im Ergebnis festzuhalten, dass bei der ausschließlich betrieblichen Inanspruchnahme des Internets und des E-Mail-Anschlusses durch Mitarbeiter lediglich die Vorschriften des Bundesdatenschutzgesetzes und die Grundrechte der Arbeitnehmer Beachtung finden müssen. Liegt eine wie auch immer gestaltete Gestattung zur privaten Internet- und E-Mail-Nutzung vor, sind die Regelungen des Telekommunikationsgesetzes und des Telemediengesetzes einschlägig. Welche Konsequenzen sich daraus im Einzelnen für die Kontrollmöglichkeiten des Arbeitgebers bei der verbotenen privaten Inanspruchnahme einerseits und der gestatteten Privatnutzung andererseits ergeben, wird im Folgenden ausführlich erörtert.

5.2 Überwachung des Internets

5.2.1 Überwachung bei unerlaubter Privatnutzung bzw. bei betrieblicher Nutzung

Eine unerlaubte Privatnutzung des Internets kann sich entweder aus der Überschreitung der vom Arbeitgeber gebilligten Grenzen einer zulässigen Privatnutzung oder aus der Privatnutzung an sich ergeben, falls eine solche verboten ist²¹¹. Die rechtliche Beurteilung der verbotenen Privatnutzung und der betrieblichen Nutzung elektronischer Kommunikationsmittel ist identisch.

Wie in den vorangegangenen Ausführungen bereits aufgezeigt wurde, sind für Kontrollmaßnahmen bei der untersagten Privatnutzung das Bundesdatenschutzgesetz und die mittelbar wirkenden Grundrechte heranzuziehen.

Die arbeitgeberseitige Kontrolle der IuK-Architektur bedeutet eine Erhebung und Verarbeitung personenbezogener Daten i. S. d. § 3

²¹¹ Vgl. Steidle (o. Fußn. 105), S. 315.

BDSG²¹². Die Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung ist in § 4 BDSG geregelt. § 4 Abs. 1 BDSG sieht die Erhebung, Verarbeitung und Nutzung personenbezogener Daten als zulässig an, soweit dies das Bundesdatenschutzgesetz selbst oder eine andere Rechtsvorschrift erlaubt oder anordnet, oder der Betroffene seine Einwilligung dazu erteilt hat.

5.2.1.1 Gesetzliche Ermächtigung

Die für Internet- und E-Mail-Überwachungsmaßnahmen in Frage kommenden gesetzlichen Ermächtigungsgrundlagen i. S. d. § 4 Abs. 1 BDSG ergeben sich aus § 28 Abs. 1 S. 1 Nr. 1 und Nr. 2 BDSG²¹³. Die Zwecke, für die die personenbezogenen Daten verarbeitet oder genutzt werden sollen, sind gem. § 28 Abs. 1 S. 2 BDSG bei ihrer Erhebung konkret festzulegen. Das bedeutet, der Arbeitgeber hat seine Mitarbeiter vorab in Kenntnis zu setzen, wozu die Daten erhoben werden. Diese Information sollte schriftlich erfolgen und die konkreten Zwecke benennen (bspw. als präventive Schutzmaßnahme vor Virenbefall, zur Sicherstellung der Funktionsfähigkeit der Systeme, zur Kontrolle der Verwendung der geschuldeten Arbeitszeit)²¹⁴. Die Rechtsgrundlage zu dieser Verpflichtung ergibt sich aus den §§ 33 Abs. 1 i. V. m. 4 Abs. 3 BDSG und Nr. 22 des Anhangs der BildscharbV²¹⁵.

§ 28 Abs. 1 S. 1 Nr. 1 BDSG erlaubt das Erheben, Speichern, Verändern oder Übermitteln von Daten mit Personenbezug oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, wenn es der Zweckbestimmung des Arbeitsvertrags dient. Der unbestimmte

²¹² Vgl. Barton (o. Fußn. 183), 460 (462); vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 29.

²¹³ Vgl. Panzer (o. Fußn. 103), S. 156.

²¹⁴ Vgl. Mattl (o. Fußn. 21), S. 131; vgl. Elschner (o. Fußn. 3), S. 286.

²¹⁵ Vgl. Elschner (o. Fußn. 3), 286.

Rechtsbegriff der „Zweckbestimmung des Vertragsverhältnisses“ erfordert, dass eine umfassende Interessenabwägung zwischen den Arbeitgeberinteressen und dem allgemeinen Persönlichkeitsrecht der Arbeitnehmer vorgenommen wird²¹⁶. Diese Interessenabwägung muss dem Grundsatz der Verhältnismäßigkeit genügen, da andernfalls ein unangemessener Eingriff in das Arbeitnehmerpersönlichkeitsrecht vorläge, was wiederum das Ausscheiden einer Zweckbestimmung zur Folge hätte²¹⁷. Die Zweckbestimmung des Arbeitsverhältnisses besteht darin, dass der Arbeitnehmer eine adäquate Arbeitsleistung erbringt, die im synallagmatischen Verhältnis zur vertraglich vereinbarten Entlohnung steht. Als Gläubiger der Arbeitsleistung muss es dem Arbeitgeber zustehen, die Erbringung der Arbeit durch Kontrollen zu überprüfen. Erst die Überwachung der Nutzungsgewohnheiten ermöglicht es zu erkennen, ob die Mitarbeiter sich an ausgesprochene Nutzungsverbote halten, oder sie durch die Hingabe zu einer unerlaubten Inanspruchnahme des Internet- und E-Mail-Anschlusses einen Teil der Arbeitszeit vergeuden und sich mithin vertragswidrig verhalten. Der Arbeitgeber ist also grundsätzlich befugt, die dienstliche Kommunikation im Hinblick auf die Aufdeckung von Missbrauch und potenziell entstehenden Kosten zu überwachen.²¹⁸

Die Zulässigkeit für den Umgang mit personenbezogenen Daten nach § 28 Abs. 1 S. 1 Nr. 2 BDSG ist unter Abwägung der berechtigten Interessen der verantwortlichen Stelle und der schutzwürdigen Interessen des Betroffenen zu ermitteln²¹⁹. Zu dieser Vorschrift existieren unterschiedliche Meinungen: Eine davon schließt die Anwendung der Nr. 2 im Arbeitsverhältnis aus, da der Umgang mit personenbezogenen Daten ausschließlich für die Zweckbestimmung

²¹⁶ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 32; vgl. Panzer (o. Fußn. 103), S. 157.

²¹⁷ Vgl. Koeppen (o. Fußn. 7), S. 180.

²¹⁸ Vgl. Mattl (o. Fußn. 21), S. 132; vgl. Hanau/Hoeren (o. Fußn. 12), S. 52; vgl. Tinnefeld/Viethen, NZA 2000, 977 (982); vgl. Gola (o. Fußn. 123), S. 114 Rdnr. 258; vgl. Weißnicht (o. Fußn. 157), 448 (450); vgl. Elschner (o. Fußn. 3), S. 277.

²¹⁹ Vgl. Gliss/Kramer, Arbeitnehmerdatenschutz, 2006, S. 38.

des Arbeitsverhältnisses erlaubt sei; die andere vertritt die Auffassung, die beiden Zulässigkeitsalternativen (Nr. 1 und Nr. 2) bestünden im Arbeitsverhältnis nebeneinander.²²⁰ § 28 Abs. 1 S. 1 Nr. 2 BDSG sei immer dann heranzuziehen, wenn die Zweckbestimmung des Arbeitsverhältnisses nach Nr. 1 allein keine hinreichende Rechtsgrundlage für den Umgang mit den Daten biete²²¹. Von praktischer Relevanz ist dieser Meinungsstreit jedoch nicht, da die Interessenabwägung nach § 28 Abs. 1 S. 1 Nr. 2 BDSG regelmäßig dieselbe ist, wie sie auch bei Nr. 1 vorgenommen werden muss. Beide Alternativen erfordern die Abwägung zwischen dem allgemeinen Persönlichkeitsrecht der Arbeitnehmer- und den berechtigten Interessen der Arbeitgeberseite.²²²

Für beide Erlaubnistatbestände gilt also zu beachten, dass der Eingriff in die Privatsphäre der Arbeitnehmer nur insoweit gestattet ist, als es für den Zweck des Arbeitsverhältnisses unbedingt notwendig erscheint²²³. Beim Gebrauch von Internet und E-Mail zu betrieblichen Zwecken wird die Interessenabwägung im Ergebnis regelmäßig dazu führen, dass der Arbeitnehmer weitreichende Einschnitte in sein Persönlichkeitsrecht akzeptieren muss²²⁴.

²²⁰ Vgl. *Panzer* (o. Fußn. 103), S. 158 m. w. N.

²²¹ Vgl. *Barton* (o. Fußn. 183), 460 (463).

²²² Vgl. *Panzer* (o. Fußn. 103), S. 158 f.

²²³ Vgl. *ErfK/Wank* § 28 BDSG Rdnr. 4; vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), §10 Rdnr. 33.

²²⁴ Vgl. *Nägele/Meyer* (o. Fußn. 34), 312 (314).

5.2.1.1.1 Äußere Umstände

Unter die äußeren Umstände der Internet-Telekommunikation sind insbesondere Daten wie Zugriffsdatum, Uhrzeit, Dauer der Verbindung, übertragenes Datenvolumen und aufgerufene Internet-Adresse zu subsumieren²²⁵.

Ist die Nutzung des Internets zu ausschließlich betrieblichen Zwecken erlaubt, besteht im Hinblick auf die somit unerlaubte Privatnutzung kein schützenswertes Persönlichkeitsinteresse der Arbeitnehmer. Nutzen Mitarbeiter trotz bestehenden Verbots den Internet-Zugang zu privaten Angelegenheiten, verhalten sie sich arbeitsvertrags- und mithin rechtswidrig.²²⁶ Der Arbeitgeber muss die Möglichkeit haben zu überprüfen, ob sich seine Beschäftigten an das bestehende Nutzungsverbot halten. Dieses Arbeitgeberinteresse überwiegt nach h. M. bei der Verhältnismäßigkeitsprüfung im Rahmen des § 28 Abs. 1 S.1 Nr. 1 bzw. Nr. 2 BDSG. Wesentliche Argumente, auf die sich dieses überwiegende Interesse stützt, sind die Verhinderung eines übermäßigen Arbeitszeitverbrauchs, die Minimierung des Risikos, dass Viren und Trojaner ins betriebliche Netzwerk eingeschleust werden, und das Unterbinden der Strafbarkeit durch Handlungen der Belegschaft.²²⁷ Sofern also ein konkreter Zweck gegeben ist und der Grundsatz der Verhältnismäßigkeit eingehalten wird, dürfen die äußeren Daten kontrolliert werden²²⁸. Dazu zählt auch die angesurfte Internet-Adresse, da der Arbeitgeber nur so erkennen kann, ob es sich um eine dienstlich veranlasste Nutzung oder um eine Privatnutzung handelt²²⁹. Diesbezüglich muss jedoch angemerkt werden, dass eine Klassifi-

²²⁵ Vgl. Busse, in: Besen/Prinz (o. Fußn. 114), § 10 Rdnr. 51.

²²⁶ Vgl. Besen/Prinz, in: Besen/Prinz (o. Fußn. 56), § 1 Rdnr. 53; vgl. Däubler (o. Fußn. 64), 323 (327).

²²⁷ Vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (136); vgl. Elschner (o. Fußn. 3), S. 283 f.; vgl. Mengel (o. Fußn. 102), 2014 (2020); vgl. Gola (o. Fußn. 123), S. 114 Rdnrn. 258 f.; vgl. Matzl (o. Fußn. 21), S. 146; vgl. Bernhardt/Barthel, AuA 2008, 150 (152).

²²⁸ Vgl. Kömpf/Kunz (o. Fußn. 155), 1341 (1345); vgl. Elschner (o. Fußn. 3), S. 284; vgl. Weißnicht (o. Fußn. 157), 448 (450).

²²⁹ Vgl. Mengel (o. Fußn. 102), 2014 (2020); vgl. Tuchbreiter (o. Fußn. 116), S. 185.

zierung des Benutzungsvorgangs nach dienstlich oder privat in vielen Fällen anhand der Internet-Adresse schwierig oder sogar unmöglich ist²³⁰. So kann praktisch nicht festgestellt werden, ob der Mitarbeiter das Nachrichtenportal „sueddeutsche.de“ im Rahmen einer arbeitsbezogenen Recherche oder aus privatem Interesse in Anspruch genommen hat. Anders wäre es beim Aufruf der Webseiten „unternehmen-x.de“ im Vergleich zu „erotik.de“.²³¹

Allerdings darf die Protokollierung der bei der Internet-Nutzung anfallenden äußeren Daten nicht soweit führen, dass ein vollumfängliches Persönlichkeitsprofil der Mitarbeiter entsteht²³². Daher sind im Zusammenhang mit einer Missbrauchskontrolle anlassbezogene, stichprobenartige Überprüfungen als ausreichend anzusehen²³³. Die Gefahr der Schaffung des gläsernen Arbeitnehmers ist umso höher einzustufen, je mehr die Beschäftigten auf die virtuellen Arbeitsmittel angewiesen sind²³⁴. Eine solche unzulässige Vollkontrolle lässt sich aber dadurch verhindern, dass sämtliche Nutzungsaktivitäten anonymisiert aufgezeichnet werden, die Kontrolle jedoch nur stichprobenartig und bei Missbrauchsverdacht eine einzelfallbezogene Überwachung durchgeführt wird²³⁵.

Es kann festgehalten werden, dass im Rahmen der dienstlichen Inanspruchnahme des Internet-Anschlusses sämtliche äußeren Verbindungsdaten des Kommunikationsvorgangs durch den Arbeitgeber kontrolliert werden dürfen; diese Kontrolle ist unter Berücksichtigung des allgemeinen Persönlichkeitsrechts der Arbeitnehmer verhältnismäßig²³⁶.

²³⁰ Vgl. *Tuchbreiter* (o. Fußn. 116), S. 185; vgl. *Steidle* (o. Fußn. 105), S. 294.

²³¹ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 258; vgl. *Weißnicht* (o. Fußn. 157), 448 (451).

²³² Vgl. *Elschner* (o. Fußn. 3), S. 285.

²³³ Vgl. *Gola* (o. Fußn. 123), S. 117 Rdnr. 262; vgl. *Elschner* (o. Fußn. 3), S. 286.

²³⁴ Vgl. *Elschner* (o. Fußn. 3), S. 285.

²³⁵ Vgl. *Gola* (o. Fußn. 123), S. 117 Rdnr. 264; vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 53.

²³⁶ Vgl. *Mattl* (o. Fußn. 21), S. 146.

5.2.1.1.2 Inhaltsdaten

Ist die Inanspruchnahme des Internets zu ausschließlich dienstlichen Zwecken gestattet, fallen grundsätzlich nur personenbezogene Daten an, die im direkten Zusammenhang mit der Erfüllung der Arbeitsaufgabe stehen; insofern sind keine personenbezogenen Daten betroffen, die in die Privatsphäre der Mitarbeiter reichen.²³⁷ Dem Arbeitgeber ist schon bei der Überprüfung der äußeren Umstände der Internet-Kommunikation erlaubt, auch die angewählte Internet-Adresse zu protokollieren und einzusehen. Aus diesem Grund kann der Arbeitnehmer auch kein schützenswertes Interesse mehr im Hinblick auf die Inhalte der aufgerufenen Webseiten geltend machen.²³⁸

Aber auch bei der Kontrolle der Inhaltsdaten muss auf ein Problem hingewiesen werden, das dem Internet immanent ist, namentlich die Schnelllebigkeit. Es liegt in der Natur der Sache, dass Inhalte, die bspw. in der Online-Zeitung „sueddeutsche.de“ dargestellt sind, am folgenden Tag durch aktuelle Artikel ersetzt werden. Somit ist es grundsätzlich denkbar, dass eine Webseite kurze Zeit nach Aufruf völlig andere Inhalte wiedergibt als die ursprünglichen.²³⁹ Eine valide Inhaltskontrolle ließe sich nur anhand der auf dem Proxy-Server gespeicherten Dateien, welche die Webseite genau so darstellen, wie sie tatsächlich auf dem Dienst-Computer erschien, realisieren.

Im Übrigen gilt auch für die Überwachung der Inhaltsdaten, dass eine Vollkontrolle ausscheiden muss; als verhältnismäßig im Zusammenhang mit betrieblichen Kontrollzwecken gelten jedoch Stichproben²⁴⁰.

²³⁷ Vgl. Steidle (o. Fußn. 105), S. 292.

²³⁸ Vgl. Bernhardt/Barthel (o. Fußn. 227), 150 (152); vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 52; vgl. Mattl (o. Fußn. 21), S. 146.

²³⁹ Vgl. Mengel (o. Fußn. 102), 2014 (2019); vgl. Steidle (o. Fußn. 105), S. 294.

²⁴⁰ Vgl. Steidle (o. Fußn. 105), S. 296.

5.2.1.2 Prüfung von Erweiterungsmöglichkeiten der Überwachungsbefugnis

Das Bundesdatenschutzgesetz hält neben den dargestellten gesetzlichen Erlaubnistatbeständen des § 28 Abs. 1 S. 1 Nr. 1 und Nr. 2 BDSG weitere Möglichkeiten offen, die Internet- und E-Mail-Überwachung in zulässiger Weise zu gestalten. Gelangen diese Alternativen zum Einsatz, stehen dem Arbeitgeber u. U. sogar weiter gehende Eingriffsbefugnisse zu als über die gesetzlichen Erlaubnistatbestände.

5.2.1.2.1 Einwilligung der Arbeitnehmer

Der Arbeitnehmer kann durch seine Einwilligung die Befugnisse des Arbeitgebers, mit den personenbezogenen Daten umzugehen, über die gesetzlichen Erlaubnistatbestände hinaus erweitern. Mittels einer diesbezüglichen Einwilligung lässt sich eine Beschränkung des informationellen Selbstbestimmungsrechts der Mitarbeiter vornehmen.²⁴¹ Normiert ist der Erlaubnistatbestand der Einwilligung i. S. d. § 4 Abs. 1 BDSG in § 4a BDSG. Die Einwilligung entspricht einer vorherigen Zustimmung gem. § 183 BGB, sodass die Zulässigkeit des Umgangs mit den Daten auch nicht durch ein nachträgliches Einverständnis erreicht werden kann²⁴². Die Einwilligung nach § 4a BDSG ist in der Praxis problematisch, da ihre geforderte Förmlichkeit leicht zu juristischen Fehlern führt²⁴³.

Gem. § 4a Abs. 1 S. 1 BDSG erlangt die Einwilligung nur dann Wirksamkeit, wenn sie auf dem freien Willen des Betroffenen beruht. Die Feststellung, inwieweit überhaupt Freiwilligkeit bei der Erteilung der Einwilligung vorgelegen hat, muss unter strengen Vorausset-

²⁴¹ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 57.

²⁴² Vgl. Panzer (o. Fußn. 103), S. 161; vgl. Zscherpe, MMR 2004, 723 (724).

²⁴³ Vgl. Gliss/Kramer (o. Fußn. 219), S. 35.

zungen vollzogen werden²⁴⁴. Von tatsächlicher Freiwilligkeit kann nur die Rede sein, wenn der Mitarbeiter bei Versagen der Einwilligung keine negativen Konsequenzen befürchten muss²⁴⁵. Der Arbeitnehmer ist deshalb gem. § 4a Abs. 1 S. 2 BDSG über die Folgen einer verweigerten Einwilligung aufzuklären. Der Mitarbeiter befindet sich im Arbeitsverhältnis unter der wirtschaftlichen Machtposition des Arbeitgebers. Diese Tatsache kann dazu führen, dass sich der Arbeitnehmer unter Druck gesetzt fühlt und sich in einer Zwangslage befindet.²⁴⁶ Man stelle sich das anschauliche Beispiel eines Arbeitsvertragsabschlusses vor: Unterschreibt der Arbeitnehmer hier nicht eine diesbezügliche Einwilligungserklärung, wird der Arbeitsvertrag wohl erst gar nicht zustande kommen.²⁴⁷ In solchen Fällen und selbstredend in jenen, in denen die Einverständniserklärung aufgrund einer arglistigen Täuschung erteilt wurde, kann von Freiwilligkeit keine Rede sein²⁴⁸. Ein weiteres notwendiges Merkmal einer freiwilligen Erklärung ist die Möglichkeit, die Einwilligung für die Zukunft widerrufen zu können²⁴⁹.

Darüber hinaus muss dem Arbeitnehmer klar sein, welche Tragweite seine Einwilligung hat²⁵⁰. Demzufolge unterliegt der Arbeitgeber der Pflicht, von vornherein genau darzulegen, für welche Zwecke die Daten benötigt werden²⁵¹. Überdies sind ggf. weitere Übermittlungsempfänger der personenbezogenen Daten zu nennen und abschließend zu beschreiben²⁵².

²⁴⁴ Vgl. Koeppen (o. Fußn. 7), S. 182.

²⁴⁵ Vgl. Panzer (o. Fußn. 103), S. 161; vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 59.

²⁴⁶ Vgl. Gola (o. Fußn. 123), S. 132 Rdnr. 291; vgl. Koeppen (o. Fußn. 7), S. 182; vgl. Gliss/Kramer (o. Fußn. 219), S. 35.

²⁴⁷ Vgl. Erler (o. Fußn. 18), S. 97; vgl. Koeppen (o. Fußn. 7), S. 182.

²⁴⁸ Vgl. Zscherpe (o. Fußn. 242), 723 (726); vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 59.

²⁴⁹ Vgl. Gliss/Kramer (o. Fußn. 219), S. 36; vgl. Panzer (o. Fußn. 103), S. 162.

²⁵⁰ Vgl. Panzer (o. Fußn. 103), S. 161.

²⁵¹ Vgl. Koeppen (o. Fußn. 7), S. 182.

²⁵² Vgl. Gliss/Kramer (o. Fußn. 219), S. 35.

Die Einwilligung ist ferner gem. § 4a Abs. 1 S. 3 BDSG schriftlich zu erteilen, soweit nicht eine andere Form aufgrund besonderer Umstände angemessen ist. Ein besonderer Umstand liegt bspw. i. d. R. vor, wenn eine außerordentliche Eilbedürftigkeit angezeigt ist.²⁵³ Falls die Einverständniserklärung zusammen mit anderen Dokumenten, z. B. mit einem Arbeitsvertrag, abgegeben wird, ist sie in ihrer äußerlichen Erscheinungsform deutlich hervorzuheben²⁵⁴. Die intendierte Warnfunktion der Schriftform erfüllt nur solange ihren Zweck, wie die Arbeitnehmer auch erkennen können, was mit ihren Daten geschieht²⁵⁵.

Die Beweislast, dass die Einwilligung tatsächlich auf der freien Entscheidung des einzelnen Arbeitnehmers beruhte, trägt allein der Arbeitgeber. Kann er diesen Nachweis nicht erbringen, ist die Einverständniserklärung unwirksam und somit der Umgang mit den personenbezogenen Daten unzulässig.²⁵⁶ Wurden solche Daten bereits verarbeitet, sind sie gem. §§ 20 Abs. 2 Nr. 1, 35 Abs. 2 Nr. 1 BDSG unverzüglich zu löschen. Je nach Einzelfall muss der Arbeitgeber Schadenersatzzahlungen gem. § 7 BDSG, eine Geldbuße gem. § 43 Abs. 2 Nr. 1 BDSG oder eine Strafe gem. §§ 44 Abs. 1 i. V. m. 43 Abs. 2 Nr. 1 BDSG befürchten.²⁵⁷

²⁵³ Vgl. Panzer (o. Fußn. 103), S. 161; vgl. Hoeren (o. Fußn. 10), S. 247.

²⁵⁴ Vgl. Panzer (o. Fußn. 103), S. 161.

²⁵⁵ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 65.

²⁵⁶ Vgl. Koeppen (o. Fußn. 7), S. 183; vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 68.

²⁵⁷ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 68.

5.2.1.2.2 Regelung durch Betriebsvereinbarung oder Tarifvertrag

Auch kollektivrechtliche Regelungsinstrumente, wie ein Tarifvertrag als überbetrieblicher Rahmen oder eine betriebsspezifische Betriebsvereinbarung zur Reglementierung der Nutzung von Internet und E-Mail, können als „andere Rechtsvorschrift“ i. S. d. § 4 Abs. 1 BDSG Anwendung finden²⁵⁸. In einem solchen Fall gehen die Vorschriften des Tarifvertrags bzw. der Betriebsvereinbarung denen des Bundesdatenschutzgesetzes vor²⁵⁹.

Besonders für große Unternehmen bietet der Weg über eine Betriebsvereinbarung gem. § 77 BetrVG – sofern ein Betriebsrat existiert – einen entscheidenden Vorteil gegenüber der oben dargestellten Einwilligung jedes einzelnen Mitarbeiters: Der Verwaltungsaufwand reduziert sich durch die Reglementierung der Internet- und E-Mail-Nutzung sowie deren Kontrolle in einer Betriebsvereinbarung auf ein Minimum. Die Beteiligung des Betriebsrats stellt gem. § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG ohnehin eine notwendige Voraussetzung zur Einholung individueller Einwilligungserklärungen dar.²⁶⁰

Die Frage, ob durch eine Betriebsvereinbarung auch zu Ungunsten der Belegschaft abgewichen werden darf, wird in der Literatur unterschiedlich beantwortet²⁶¹. Die Rechtsprechung des BAG zur Telefondatenüberwachung²⁶² gelangte zum Ergebnis, dass Betriebsvereinbarungen auch dann als eine „andere Rechtsvorschrift“ anzusehen sind, wenn sie vom Schutzniveau des Bundesdatenschutzgesetzes zu Lasten der Arbeitnehmer abweichen²⁶³. Die in § 4 Abs. 1 BDSG manifestierte Abdingbarkeit des Bundesdatenschutzgesetzes ist an keine Einschrän-

²⁵⁸ Vgl. Erler (o. Fußn. 18), S. 93; vgl. Koeppen (o. Fußn. 7), S. 181 f.; siehe hierzu ausführlich Sassenberg/Bamberg, DuD 2006, 226-229.

²⁵⁹ Vgl. Lelley, in: Worzalla, S. 25 Rdnr. 63.

²⁶⁰ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnrn. 75 f.

²⁶¹ Vgl. Panzer (o. Fußn. 103), S. 160; vgl. Elschner (o. Fußn. 3), S. 307 f. m. w. N.

²⁶² BAG, Beschl. v. 27.5.1986 = NJW 1987, 674 = NZA 1986, 643.

²⁶³ Vgl. Höld (o. Fußn. 55), S. 125; vgl. Hoeren (o. Fußn. 10), S. 248.

kungen gebunden. Es ist daher nicht nachvollziehbar, warum nicht auch unter das Schutzniveau des Bundesdatenschutzgesetzes abgewichen werden kann. Außerdem muss berücksichtigt werden, dass auch durch eine individuelle Einwilligung der Arbeitnehmer eine weiter reichende Datenverarbeitung zulässig ist.²⁶⁴ Die Öffnungsklausel des § 4 Abs. 1 BDSG wäre überflüssig, bestünde nur die Möglichkeit, zu Gunsten der Mitarbeiter vom Bundesdatenschutzgesetz abzuweichen²⁶⁵.

Im Ergebnis kann durch den Abschluss einer diesbezüglichen Betriebsvereinbarung im Hinblick auf den Schutzstandard des Bundesdatenschutzgesetzes auch zu Lasten der Arbeitnehmer abgewichen werden²⁶⁶. Die Grenze der Gestaltungsmöglichkeit ist allerdings erreicht, wenn gegen grundgesetzliche Wertungen, zwingende Gesetznormen oder arbeitsrechtliche Grundsätze, insbesondere gegen § 75 Abs. 2 BetrVG, verstoßen wird²⁶⁷. Ob sich der Betriebsrat, der die Interessen der Belegschaft zu vertreten hat, überhaupt zu einer Verschlechterung des allgemeinen Datenschutzes „hinreißen lässt“, ist äußerst fraglich. Die Vorschrift des § 75 BetrVG soll jedenfalls die Wahrung des Persönlichkeitsrechts der Arbeitnehmer sicherstellen.²⁶⁸

Die Möglichkeit, die Internet- und E-Mail-Nutzung und insbesondere deren Kontrollmöglichkeit durch Arbeitgeber auf tarifvertraglicher Ebene zu regeln, kommt praktisch nur selten in Frage. Hauptgrund dafür ist die Verschiedenartigkeit der IuK-Systeme, die in den mit dem Tarifvertrag erfassten Unternehmen zum Einsatz gelangen. Es lassen sich kaum auf sämtliche Unternehmen gleichermaßen anwendbare Vereinbarungen treffen.²⁶⁹

²⁶⁴ Vgl. *Tuchbreiter* (o. Fußn. 116), S. 159; vgl. *Höld* (o. Fußn. 55), S. 126 f.

²⁶⁵ Vgl. *Erler* (o. Fußn. 18), S. 95; vgl. *Höld* (o. Fußn. 55), S. 126.

²⁶⁶ Vgl. *Hanau/Hoeren* (o. Fußn. 12), S. 59; vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 301; vgl. *Erler* (o. Fußn. 18), S. 95; im Gegensatz dazu *Steidle* (o. Fußn. 105), S. 191.

²⁶⁷ Vgl. *Panzer* (o. Fußn. 103), S. 160; vgl. *Tuchbreiter* (o. Fußn. 116), S. 159.

²⁶⁸ Vgl. *Höld* (o. Fußn. 55), S. 127.

²⁶⁹ Vgl. *Hanau/Hoeren* (o. Fußn. 12), S. 59.

5.2.2 Überwachung bei erlaubter Privatnutzung

Wie bereits in Kapitelunterpunkt 5.1.2 dargelegt wurde, führt die Erlaubnis der Privatnutzung von Internet und E-Mail zur Anwendbarkeit des Telekommunikations- und des Telemediengesetzes, da ein Anbieter-Nutzer-Verhältnis zwischen dem Unternehmen und den Arbeitnehmern vorliegt.

Die zentrale Vorschrift der telekommunikationsrechtlichen Regelungen verkörpert das Fernmeldegeheimnis nach § 88 TKG. Es stellt die einfachgesetzliche Ausprägung des in Art. 10 Abs. 1 GG manifestierten Fernmeldegeheimnisses dar. Seine Schutzfunktion gilt gem. § 88 Abs. 2 S. 1 TKG gegenüber dem Diensteanbieter, problembezogen gegenüber dem Arbeitgeber und seinen Erfüllungsgehilfen.²⁷⁰ Die in § 88 Abs. 3 TKG vorgesehenen Kontrollmöglichkeiten sind als Grundrechtsbeschränkung i. S. v. Art. 10 Abs. 2 GG zu verstehen²⁷¹.

Gem. § 88 Abs. 1 TKG erstreckt sich das Fernmeldegeheimnis auf den Inhalt der Kommunikation und ihre näheren Umstände, also auch darauf, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Darüber hinaus erfasst es ebenso die näheren Umstände erfolgloser Verbindungsversuche; so fällt z. B. die Meldung des Internet-Browsers „Die Webseite kann nicht angezeigt werden“ unter das Fernmeldegeheimnis²⁷².

In § 88 Abs. 3 S. 1 TKG ist geregelt, dass die in den Telekommunikationsvorgang involvierten Personen nur soweit Kenntnis vom Inhalt oder den näheren Umständen der Kommunikation nehmen dürfen, als es für die geschäftsmäßige Erbringung und den Schutz der technischen Systeme erforderlich ist. Nach der hier bezeichneten Erforder-

²⁷⁰ Vgl. Steidle (o. Fußn. 105), S. 171 f.

²⁷¹ Vgl. Erler (o. Fußn. 18), S. 47 f.

²⁷² Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 273.

lichkeit richtet sich die Zulässigkeit von Überwachungsmaßnahmen.²⁷³ Weiterhin lässt die Beschränkung auf das erforderliche Maß den Grundsatz der Datensparsamkeit aus § 3a BDSG erkennen²⁷⁴. § 88 Abs. 3 S. 2 TKG enthält ferner einen Zweckbindungsgrundsatz: So dürfen auch Kenntnisse über Tatsachen, die unter das Fernmeldegeheimnis fallen, nur zu den in S. 1 genannten Zwecken verwendet werden. Welche Daten zur Erbringung der Dienste und zum Schutz der Systeme erforderlich sind, ist den §§ 95 ff. TKG zu entnehmen.²⁷⁵ Inwieweit die Zweckbindung konkrete Auswirkungen auf die Internet- und E-Mail-Überwachung am Arbeitsplatz hat, gilt es noch zu untersuchen.

Damit sich der Arbeitgeber überhaupt auf die Beachtung der Vorschriften des Telekommunikationsgesetzes und des Telemediengesetzes einstellen kann, muss ihm klar sein, ob eine dienstliche oder private Nutzung vorliegt. Beim E-Mail-Account lässt sich diese Unterscheidung einfach vornehmen, indem bspw. Privatnachrichten mit einem entsprechenden Vermerk in der Betreffzeile gekennzeichnet werden, oder indem den Beschäftigten eine zweite E-Mail-Adresse zur Verfügung gestellt wird, die sie zu ausschließlich privater Korrespondenz gebrauchen dürfen.²⁷⁶

Ungleich schwieriger ist diese Unterscheidung bei der Inanspruchnahme des Internet-Dienstes. Da das Auseinanderhalten beider Nutzungsarten nur mit einem unverhältnismäßig hohen technischen Aufwand²⁷⁷ möglich ist, kommen in der Praxis nur die Vereinbarung fester Zeiten zur privaten Inanspruchnahme und das Aufstellen spezieller Computer-Terminals, die eigens der Erledigung außerbetrieb-

²⁷³ Vgl. Koeppen (o. Fußn. 7), S. 170.

²⁷⁴ Vgl. Panzer (o. Fußn. 103), S. 175.

²⁷⁵ Vgl. Steidle (o. Fußn. 105), S. 260.

²⁷⁶ Vgl. Steidle (o. Fußn. 105), S. 173.

²⁷⁷ Denkbar wäre die Einrichtung eines separaten Benutzerkontos im Betriebssystem, unter dem man sich anmelden muss, wenn man eine private Nutzung vornehmen will.

licher Belange dienen sollen, in Betracht. Andernfalls liegt eine Mischnutzung vor, die besonders behandelt werden muss²⁷⁸.

5.2.2.1 Beurteilung nach dem Telekommunikationsgesetz

Explizit unterscheidet das Telekommunikationsgesetz drei verschiedene Datenarten. Zu diesen zählen:

- „...Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden“, namentlich Bestandsdaten gem. § 3 Nr. 3 TKG;
- „...Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben“, sog. Standortdaten gem. § 3 Nr. 19 TKG;
- „...Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet und genutzt werden“, also Verkehrsdaten gem. § 3 Nr. 30 TKG.

Eine Definition für die mittels Telekommunikation übertragenen Inhalte ist im Gesetz nicht enthalten, da diese Art von Daten nicht von der Regelungsebene des Telekommunikationsgesetzes erfasst ist²⁷⁹. Unter dem nachfolgend verwendeten Begriff „Inhaltsdaten“ sind die verschickten und empfangenen Informationen zu verstehen²⁸⁰.

²⁷⁸ Zur Mischnutzung des Internets siehe Kapitelunterpunkt 5.2.3.

²⁷⁹ Vgl. Steidle (o. Fußn. 105), S. 251.

²⁸⁰ Vgl. Holenstein (o. Fußn. 13), S. 99.

Für die rechtliche Beurteilung der Überwachung des Internet- und E-Mail-Verkehrs der Mitarbeiter sind Standortdaten im Normalfall nicht relevant²⁸¹.

Die Benachrichtigungspflicht aus § 33 BDSG, wonach der Arbeitgeber seine Beschäftigten über die Speicherung ihrer Daten, über deren Art und über die Zwecke ihrer Erhebung, Verarbeitung oder Nutzung zu benachrichtigen hat, findet ihren Niederschlag in § 93 TKG. Die Verpflichtung zur Benachrichtigung aus § 33 BDSG wird im Bereich der Telekommunikation durch die bereichsspezifische Vorschrift verdrängt.²⁸²

5.2.2.1.1 Bestandsdaten

Bestandsdaten gem. § 3 Nr. 3 TKG dürfen nach § 95 TKG durch den Diensteanbieter erhoben und verwendet werden. Einschränkend ist zu berücksichtigen, dass die Daten zur Erfüllung der Zwecke des § 3 Nr. 3 TKG erforderlich sein müssen. Bestandsdaten sind dauerhaft gespeichert und ermöglichen die Telekommunikation im Rahmen der vertraglichen Beziehung. Namentlich handelt es sich um persönliche Angaben wie Anschrift, (Benutzer-)Name und Kontonummer sowie feste IP-Adressen. Zwischen dem Arbeitgeber und seinen Beschäftigten liegt jedoch kein spezielles Vertragsverhältnis in Bezug auf die Inanspruchnahme der elektronischen Kommunikationsmittel zu Grunde; deshalb sind die Daten aus dem Arbeitsvertrag den Bestandsdaten der Telekommunikation gleichzusetzen.²⁸³

Das Erheben und Verwenden von Bestands- und Verkehrsdaten ist gem. § 100 Abs. 1 TKG zulässig, um Störungen oder Fehler an den Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu

²⁸¹ Anders wäre die Situation z. B. beim Einsatz mobiler Endgeräte.

²⁸² Vgl. Büttgen, in: Beck'scher TKG-Kommentar, 3. Aufl. (2006), § 93 Rdnr. 7.

²⁸³ Vgl. Steidle (o. Fußn. 105), S. 251 f.

beseitigen²⁸⁴. Zu solchen ungeplanten Abläufen zählen eine fehlerhafte Entgeltabrechnung, Störungen durch Virenbefall oder andere technisch bedingte Störungen²⁸⁵. Die strikte Zweckbindung führt dazu, dass die Kontrolle der Bestands- und Verkehrsdaten mit dem Ziel der Arbeitsüberprüfung unzulässig ist²⁸⁶.

Im Hinblick auf den Verdacht auf Leistungerschleichungen und sonstige rechtswidrige Nutzungen regelt § 100 Abs. 3 S. 1 TKG, dass bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte Bestands- und Verkehrsdaten erhoben und verwendet werden dürfen, um o. g. Fehlverhalten aufzudecken und zu unterbinden²⁸⁷. Der Verdacht solcher missbräuchlichen Nutzungen kann sich z. B. aus einem erhöhten Datenvolumen ergeben. Dem Arbeitgeber ist es gestattet, sich nicht personenbezogen über die Auslastung des betriebseigenen Internet- und E-Mail-Servers zu informieren. Soweit kein Personenbezug vorliegt, fallen die Daten nicht unter den telekommunikationsrechtlichen Erlaubnisvorbehalt.²⁸⁸ Jede Nutzung, die von den Bestimmungen des Diensteanbieters abweicht, ist rechtswidrig; somit ist auch die private Inanspruchnahme des Internets durch Mitarbeiter, wenn sie verboten wurde, rechtswidrig. Dazu zählen weiterhin Fälle, in denen zeitliche oder inhaltliche Nutzungsgrenzen überschritten wurden.²⁸⁹ Das Dokumentationserfordernis ermöglicht eine detaillierte Nachvollziehbarkeit und erhöht zugleich die Rechtssicherheit aller Beteiligten²⁹⁰. Die Vorschrift des § 100 Abs. 3 S. 5 TKG verpflichtet den Arbeitgeber, der Maßnahmen nach § 100 Abs. 3 S. 1 TKG vornimmt, unverzüglich die Regulierungsbehörde und den Bundesbeauftragten

²⁸⁴ Vgl. Ohlenburg, MMR 2004, 431 (437).

²⁸⁵ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnrn. 99-101.

²⁸⁶ Vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (137); vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 101.

²⁸⁷ Vgl. Ohlenburg (o. Fußn. 284), 431 (437); vgl. Steidle (o. Fußn. 105), S. 261.

²⁸⁸ Vgl. Elschner (o. Fußn. 3), S. 213.

²⁸⁹ Vgl. Elschner (o. Fußn. 3), S. 212; vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 102.

²⁹⁰ Vgl. Ohlenburg (o. Fußn. 284), 431 (437).

oder die Bundesbeauftragte für Datenschutz darüber zu informieren; dies soll eine Kontrolle der eingeleiteten Maßnahmen sicherstellen²⁹¹.

Die Möglichkeit der zulässigen Erhebung und Verwendung von Bestands- und Verkehrsdaten nach § 100 Abs. 3 S. 1 TKG dient allerdings nicht dem Schutz des Arbeitgebers als Gläubiger der Arbeitsleistung. Die gewonnenen Daten dürfen nicht zur arbeitsrechtlichen Sanktion von Mitarbeitern herangezogen werden, sondern ausschließlich zur Aufdeckung missbräuchlicher Nutzungen der betrieblichen Kommunikationssysteme.²⁹²

5.2.2.1.2 Verkehrsdaten

Die bereits im Zusammenhang mit den Bestandsdaten dargelegten Vorschriften des § 100 Abs. 1, Abs. 3 S. 1 TKG gelten für Verkehrsdaten entsprechend.

Der Diensteanbieter ist gem. § 100 Abs. 3 S. 2 TKG befugt, aus allen Verkehrsdaten, die höchstens sechs Monate alt sind, diejenigen Verbindungsdaten zu ermitteln, die tatsächliche Anhaltspunkte für rechtswidrige Nutzungen begründen. Überdies erlaubt § 100 Abs. 3 S. 3 TKG die Bildung eines pseudonymisierten Gesamtdatenbestands zur Aufdeckung von Leistungerschleichungen.²⁹³

Die in § 96 Abs. 1 TKG aufgezählten Verkehrsdaten dürfen darüber hinaus zur Entgeltermittlung gem. § 97 Abs. 1 TKG verwendet werden. Zu den genannten Verkehrsdaten zählen bspw. das Datum und die Uhrzeit der Verbindung, das übermittelte Datenvolumen und der beanspruchte Telekommunikationsdienst.²⁹⁴ Die Nutzung der Ver-

²⁹¹ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 103.

²⁹² Vgl. Elschner (o. Fußn. 3), S. 215 f.

²⁹³ Vgl. Ohlenburg (o. Fußn. 284), 431 (437).

²⁹⁴ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 89.

kehrsdaten setzt die vorherige Vereinbarung mit den Beschäftigten voraus, dass eine nutzungsabhängige Abrechnung durchgeführt wird²⁹⁵.

Auch die Kontrolle der Verkehrsdaten unterliegt der strengen Zweckbindung der Störungsbeseitigung und Missbrauchsaufdeckung. Erfolgt ferner keine Entgeltabrechnung für die private Internet-Nutzung gegenüber Arbeitnehmern, etwa weil das Unternehmen über eine Flatrate verfügt, dürfen die Verkehrsdaten grundsätzlich weder erfasst, noch - vor dem Hintergrund einer Kontrolle - gespeichert werden²⁹⁶. Lediglich die Möglichkeit zur anonymen Überprüfung der Kapazitätsauslastung, um bspw. einen Erweiterungsbedarf der technischen Voraussetzungen zu identifizieren, steht dem Arbeitgeber zu²⁹⁷. Die Überwachung der Verkehrsdaten im Hinblick auf das Verhalten der Arbeitnehmer ist nicht zulässig.

5.2.2.1.3 Inhaltsdaten

Sofern eine Erlaubnis zur Privatnutzung des Internets erteilt wurde, muss die Überwachung der Telekommunikationsinhalte durch den Arbeitgeber grundsätzlich ausscheiden²⁹⁸.

Einzelne Autoren vertreten allerdings in der Literatur die Meinung, dass in Ausnahmefällen die Kommunikationsinhalte eingesehen werden dürfen²⁹⁹. Zu solchen Ausnahmen zählten z. B. Verrat von Geschäftsgeheimnissen, begründeter Verdacht auf Straftaten und schwe-

²⁹⁵ Vgl. Steidle (o. Fußn. 105), S. 262 f.; vgl. Elschner (o. Fußn. 3), S. 204.

²⁹⁶ Vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1496); im Zusammenhang mit E-Mail: vgl. Mengel (o. Fußn. 102), 2014 (2018).

²⁹⁷ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 92.

²⁹⁸ Vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (137); vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 106.

²⁹⁹ So Steidle (o. Fußn. 105), S. 261; Weißnicht (o. Fußn. 157), 448 (450); in Bezug auf E-Mail-Inhalte: Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (137); Beckschulze/Henkel (o. Fußn. 61), 1491 (1494).

re Vertragsverletzungen, Mobbing sowie unberechtigte Nutzung von Software³⁰⁰.

Angesichts der Tatsache, dass § 88 Abs. 3 S. 3 TKG eine Verwendung der Daten für andere Zwecke als die geschäftsmäßige Erbringung der Dienste und des Schutzes der technischen Systeme nur soweit als zulässig einstuft, als das Telekommunikationsgesetz oder eine andere gesetzliche Vorschrift diese Verwendung vorsieht und sich ausdrücklich auf Telekommunikationsvorgänge bezieht, fehlt es an einem Erlaubnistatbestand, der eine Überwachung der inhaltsbezogenen Internet-Kommunikation zulässt. Weder wegen einer vermuteten Straftat, noch wegen betrieblicher Interessen im Hinblick auf die Aufdeckung unerlaubter Privatnutzungen darf der Inhalt eingesehen werden. Selbst § 100 Abs. 3 TKG erlaubt lediglich die Erhebung und Verwendung von Bestands- und Verkehrsdaten zur Aufdeckung von Leistungerschleichungen und rechtswidrigem Gebrauchmachen von Telekommunikationsnetzen und -diensten.³⁰¹

Die einzige Ausnahmesituation, in der das Fernmeldegeheimnis in Bezug auf die Telekommunikationsinhalte durchbrochen werden darf, ist nach § 88 Abs. 3 S. 4 TKG diejenige, in der eine Katalogstraftat nach § 138 StGB vorliegt. Erfährt bspw. der Arbeitgeber durch einen Zufall, dass ein Mitarbeiter einen Mord plant, ist er sogar verpflichtet, die Strafverfolgungsbehörden davon zu unterrichten.³⁰²

5.2.2.2 Beurteilung nach dem Telemediengesetz

Das Telemediengesetz findet nach § 1 Abs. 1 S. 1 TMG Anwendung auf alle elektronischen IuK-Dienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Signalübertragung

³⁰⁰ Vgl. *Beckschulze/Henkel* (o. Fußn. 61), 1491 (1494).

³⁰¹ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnrn. 107-109.

³⁰² Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 111.

über Telekommunikationsnetze bestehen, oder telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 RStV sind. Konkret bedeutet dies: Besteht der Telekommunikationsvorgang aus einer reinen Signalübertragung, so sind die Vorschriften des Telemediengesetzes nicht einschlägig; der Sachverhalt ist dann anhand des Telekommunikationsgesetzes zu beurteilen. Völlig anders verhält es sich bei Telekommunikationsdiensten, die *überwiegend* in der Übertragung von Signalen über Telekommunikationsnetze bestehen und – neben der Übertragungsdienstleistung – eine inhaltliche Leistung bieten, wie der Internet-Zugang und die E-Mail-Übermittlung. Für diese Dienste gelten sowohl das Telekommunikationsgesetz als auch das Telemediengesetz, je nachdem, ob die Dienstebene oder die Telekommunikationsebene betroffen ist.³⁰³ Beim Internet- und E-Mail-Providing bedarf es folglich einer genauen Betrachtung, welche Dienstleistung im Vordergrund steht – die Transportleistung oder die transportierten Inhalte³⁰⁴.

Als „echte“ Telemediendienste bezeichnet die Gesetzesbegründung bspw. Suchmaschinen, Angebote zu Wetter-, Umwelt- und Verkehrsdaten, Teleshopping und elektronische Presse³⁰⁵. In der betrieblichen Praxis dürfte es nur in absoluten Ausnahmefällen vorkommen, dass ein Unternehmen seinen Mitarbeitern solche Online-Dienstleistungen anbietet³⁰⁶. Mithin kommt ein Bereithalten eigener bzw. fremder Telemedien i. S. v. § 2 Abs. 1 TMG für den gewöhnlichen Arbeitgeber nicht in Betracht. Da er jedoch durch den Vorgang des Internet- wie auch des E-Mail-Providings i. S. v. § 2 Abs. 1 TMG Zugang zur Nutzung vermittelt, nimmt er bei der erlaubten Privatnutzung gegenüber seinen Beschäftigten dennoch die Stellung eines Diensteanbieters ein³⁰⁷.

³⁰³ Vgl. BR-Drs. 556/06, S. 17; vgl. Mattl (o. Fußn. 21), S. 125 f.; vgl. Bender/Kahlen, MMR 2006, 590 (591).

³⁰⁴ Vgl. Hoeren (o. Fußn. 148), 801 (802); vgl. Roßnagel (o. Fußn. 132), 743 (745).

³⁰⁵ Vgl. BR-Drs. 556/06, S. 18.

³⁰⁶ Vgl. Mattl (o. Fußn. 21), S. 122.

³⁰⁷ Vgl. Mattl (o. Fußn. 21), S. 124.

Wenn aber der Arbeitgeber in der Funktion als Access-Provider lediglich den Zugang zu fremden Internet-Angeboten vermittelt, gilt die Sonderregelung des § 11 Abs. 3 TMG, die sich auf Telemedien bezieht, welche überwiegend in der Signalübertragung über Telekommunikationsnetze bestehen. Der Dienst als Zugangsvermittler unterliegt sowohl dem Telemedienrecht als auch dem Telekommunikationsrecht – und damit den Datenschutzbestimmungen des Telekommunikationsgesetzes.³⁰⁸ Für Telemedien, die gleichzeitig unter die Datenschutzvorschriften des Telekommunikationsgesetzes fallen, sollen nur noch bestimmte Datenschutzregelungen des Telemediengesetzes gelten³⁰⁹. Diese sind namentlich das Koppelungsverbot nach § 12 Abs. 3 TMG, die Datenverarbeitung zur Missbrauchsbekämpfung nach § 15 Abs. 8 TMG und die dazugehörigen Sanktionen nach § 16 Abs. 2 Nr. 2 und Nr. 5 TMG³¹⁰. Aufgrund der Tatsache, dass die Inanspruchnahme des Internets zu Privatzwecken im Regelfall nicht gegen ein Nutzungsentgelt erfolgt, und auch die Bereitstellung des Internet-Zugangs nicht von der Einwilligung des Arbeitnehmers in eine zweckentfremdete Verwendung seiner Daten abhängig gemacht wird, verbleibt ein nur sehr geringer Anwendungsbereich des Telemediengesetzes³¹¹.

Als Ergebnis ist festzuhalten, dass die datenschutzrechtlichen Vorschriften des Telemediengesetzes bei der erlaubten Privatnutzung des Internet-Anschlusses nur sehr eingeschränkt zur Anwendung gelangen. In der Folge ergibt sich die Zulässigkeit der Internet-Überwachung bei der erlaubten Privatnutzung ganz wesentlich aus den Bestimmungen des Telekommunikationsgesetzes und aus denen des subsidiär anwendbaren Bundesdatenschutzgesetzes.

³⁰⁸ Vgl. *Rath/Karner* (o. Fußn. 35), 446 (450).

³⁰⁹ Vgl. *BR-Drs.* 556/06, S. 22.

³¹⁰ Vgl. *Spindler*, CR 2007, 239 (242).

³¹¹ Vgl. *Rath/Karner* (o. Fußn. 35), 446 (451).

5.2.2.3 Prüfung von Erweiterungsmöglichkeiten der Überwachungsbefugnis

Wie gezeigt wurde, sind bei der zulässigen Privatnutzung des Internet-Anschlusses aufgrund der strengen Maßstäbe des Fernmeldegeheimnisses kaum Spielräume vorhanden, die eine Überwachung durch den Arbeitgeber erlauben. Lediglich zur Störungsbeseitigung, Entgeltabrechnung – falls überhaupt ein Nutzungsentgelt erhoben wird – und zur Aufklärung missbräuchlicher Inanspruchnahmen der Telekommunikationsanlagen darf eine Kontrolle der äußeren Umstände stattfinden. Es gilt deshalb zu prüfen, ob nicht, wie auch bei der zu ausschließlich betrieblichen Zwecken erlaubten Nutzung, eine Ausdehnung der Überwachungsbefugnis realisiert werden kann. Aufgrund der Sonderregelung des § 11 Abs. 3 TMG ist im Hinblick auf eine Erweiterung der Kontrollbefugnis im Rahmen des Telemediengesetzes auf die Vorschriften des Telekommunikationsgesetzes zurückzugreifen.

5.2.2.3.1 Einwilligung der Arbeitnehmer

Nach § 88 Abs. 3 S. 3 TKG dürfen Kenntnisse, die dem Fernmeldegeheimnis unterliegen, nur dann zweckentfremdet verwendet werden, wenn das Telekommunikationsgesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich ausdrücklich auf Telekommunikationsvorgänge bezieht. Zwar ist von einer Öffnungsklausel durch eine Einwilligung, wie sie ausdrücklich in § 4 Abs. 1 BDSG und in § 12 Abs. 1 TMG enthalten ist, keine Rede; jedoch wird die Einwilligung auch nicht explizit ausgeschlossen. Da schon die Möglichkeit besteht, auf das in Art. 10 GG verankerte Fernmeldegeheimnis zu verzichten, muss dies erst recht für die einfachgesetzliche Regelung gelten.³¹²

³¹² Vgl. *Mattl* (o. Fußn. 21), S. 87 f.

Das Telekommunikationsgesetz enthält in § 94 TKG eine Vorschrift zur Einwilligung im elektronischen Verfahren. Nach dieser kann die Einwilligungserklärung auch elektronisch erfolgen. Eine Voraussetzung dazu ist, dass die Einwilligung bewusst und eindeutig erklärt wurde. Dies kann bspw. durch eine qualifizierte elektronische Signatur nach § 2 Nr. 3 SigG sichergestellt werden³¹³. Das Protokollierungserfordernis stellt eine weitere Anforderung an die Einwilligung dar. Außerdem muss der Inhalt jederzeit abrufbar und die Einwilligung an sich für die Zukunft widerrufbar sein.

Ferner ist das in § 95 Abs. 5 TKG manifestierte Koppelungsverbot zu berücksichtigen. Hiernach darf die Erbringung von Telekommunikationsdiensten nicht davon abhängen, ob der Teilnehmer in die Verwendung seiner Daten für andere Zwecke einwilligt, wenn er einen anderen Zugang zu diesen Diensten nicht oder in nicht zumutbarer Weise erhalten kann. Zumindest im Arbeitsverhältnis wird diese Regelung nicht zum Tragen kommen, da inzwischen die Mehrheit aller Haushalte über einen Internet-Anschluss verfügt oder zumindest theoretisch darüber verfügen könnte, sodass eine diesbezügliche Unzumutbarkeit auszuschließen ist. An dieser Norm lässt sich unschwer erkennen, dass das Telekommunikationsgesetz nicht für die Anwendung im Arbeitsverhältnis vorgesehen ist.³¹⁴ Das Koppelungsverbot aus § 95 Abs. 5 TKG gilt in diesem Zusammenhang mithin nicht im Arbeitsverhältnis.

Aufgrund der Tatsache, dass das Telekommunikationsgesetz neben der elektronischen Einwilligung keine weiteren Vorschriften zur datenschutzkonformen Einwilligung beinhaltet, ist auf § 4a Abs. 1 BDSG³¹⁵ zurückzugreifen³¹⁶. Die Aspekte Freiwilligkeit und Hinweis

³¹³ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 113.

³¹⁴ Vgl. Mattl (o. Fußn. 21), S. 93 f.

³¹⁵ Siehe zur Einwilligung nach dem Bundesdatenschutzgesetz Kapitelunterpunkt 5.2.1.2.1.

³¹⁶ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 117.

auf Zweck der Einwilligung gelten als zwingende Voraussetzungen für eine wirksame Einwilligung i. S. d. § 4a Abs. 1 BDSG; darüber hinaus stellen i. d. R. Schriftform und - einzelfallbezogen - Hinweis auf Folgen einer Verweigerung sowie besondere Hervorhebung der Einwilligung weitere Bedingungen dar³¹⁷. Ein Muster einer diesbezüglichen Einwilligung ist im Anhang abgedruckt (Anlage 7).

Im Ergebnis kann der Arbeitnehmer durch Einwilligung wirksam auf den Schutz durch das Fernmeldegeheimnis verzichten. In diesem Zusammenhang ist auf ein Problem hinzuweisen: Es geht um die Frage, ob eine solche Einwilligung auch das gegenüber den Kommunikationspartnern zu beachtende Fernmeldegeheimnis erfasst.³¹⁸ Im Grunde genommen müssten sämtliche am Telekommunikationsvorgang Beteiligten den Verzicht auf das Fernmeldegeheimnis erklären, was in der Praxis nicht möglich ist³¹⁹. Bei der Nutzung des Internets im Rahmen des WWW ist der Verzicht auf das Fernmeldegeheimnis im Normalfall unproblematisch, da kein anderer Kommunikationspartner betroffen ist. Eine Ausnahme stellt bspw. die Kommunikation in einem webbasierten Chatroom dar, bei dessen Nutzung durchaus Grundrechte Dritter berührt sind.³²⁰ Die angesprochene Schwierigkeit ist ganz besonders bei der Nutzung des E-Mail-Dienstes von hoher Brisanz³²¹.

³¹⁷ Vgl. Zscherpe (o. Fußn. 242), 723 (724-727).

³¹⁸ Vgl. Erler (o. Fußn. 18), S. 54.

³¹⁹ Vgl. Beckschulze, DB 2003, 2777 (2780).

³²⁰ Vgl. Erler (o. Fußn. 18), S. 54.

³²¹ In der Literatur (so bspw. Beckschulze (o. Fußn. 319), 2777 (2780); im Ergebnis auch Mattl (o. Fußn. 21), S. 98-102) wird vertreten, dass eine Verletzung des Fernmeldegeheimnisses des Kommunikationspartners abzulehnen sei, wenn der Mitarbeiter eine Einwilligung erteilt hat. Beckschulze argumentiert, wer E-Mails – ohne sie als privat zu deklarieren – an eine betriebliche E-Mail-Adresse schicke, begeben sich damit selbst aus dem Anwendungsbereich des Fernmeldegeheimnisses.

5.2.2.3.2 Regelung durch Betriebsvereinbarung oder Tarifvertrag

Kollektivvereinbarungen könnten für den Arbeitgeber eine einfache und zugleich praktikable Möglichkeit darstellen, den Verzicht auf das Fernmeldegeheimnis zu reglementieren, da sich auf diesem Weg ein erheblicher Verwaltungsaufwand umgehen ließe. Im Übrigen müsste der Betriebsrat – falls ein solcher existiert – ohnehin bei der Ausgestaltung einer individuellen Einwilligung herangezogen werden, da er diesbezügliche Mitbestimmungsrechte besitzt³²².

Teilweise wird die Meinung vertreten, Betriebsvereinbarungen könnten ohne weiteres das Fernmeldegeheimnis der Mitarbeiter beschränken³²³. Gestützt wird diese Aussage auf einen Beschluss des BAG³²⁴ zur Mitbestimmung bei der Telefondatenerfassung, demgemäß durch eine Betriebsvereinbarung auch zu Ungunsten der Arbeitnehmer von den Vorschriften des Bundesdatenschutzgesetzes abgewichen werden könne. § 75 Abs. 2 BetrVG biete ausreichenden Persönlichkeitsschutz. Bei Übertragung des vom BAG aufgestellten Grundsatzes zur Frage der Abdingbarkeit des Fernmeldegeheimnisses aus § 88 TKG durch eine Betriebsvereinbarung bleibt allerdings unberücksichtigt, dass sich der Beschluss lediglich an den Maßstäben des Bundesdatenschutzgesetzes orientiert hatte, da das Telekommunikationsgesetz zu diesem Zeitpunkt noch gar nicht in Kraft war.³²⁵

Die Einschränkung des Fernmeldegeheimnisses nach § 88 Abs. 3 S. 3 TKG ist nur dann zulässig, wenn das Telekommunikationsgesetz selbst oder eine „andere gesetzliche Vorschrift“ dies vorsieht, welche sich darüber hinaus gleichzeitig auf Telekommunikationsvorgänge beziehen muss. Im Vergleich dazu sind Betriebsvereinbarungen „andere Rechtsvorschriften“ i. S. d. § 4 Abs. 1 BDSG und können

³²² Vgl. *Mattl* (o. Fußn. 21), S. 102.

³²³ Vgl. *Mattl* (o. Fußn. 21), S. 103 m. w. N.

³²⁴ BAG, Beschl. v. 27.05.1986 = NJW 1987, 674 = NZA 1986, 643.

³²⁵ Vgl. *Mattl* (o. Fußn. 21), S. 103 f.

mithin die Einwilligung unproblematisch ersetzen³²⁶. Zwar entfalten Betriebsvereinbarungen ihre Wirkung unmittelbar und normativ zwischen den Betriebsparteien, dessen ungeachtet stellen sie keine gesetzlichen Vorschriften i. S. v. § 88 Abs. 3 S. 3 TKG dar³²⁷. Beschränkungen des Fernmeldegeheimnisses sind jedoch nur auf Grundlage eines Parlamentsgesetzes gerechtfertigt³²⁸.

Die Regelung eines Verzichts auf das Fernmeldegeheimnis kann im Ergebnis nicht durch eine Betriebsvereinbarung oder einen Tarifvertrag getroffen werden³²⁹. Denkbar und zulässig wäre jedoch bspw. eine Vorgehensweise, bei der die Kollektivvereinbarung eine entsprechende Klausel enthielte, in welche die Arbeitnehmer aber trotzdem individuell einwilligen müssten, um der Klausel Wirksamkeit zu verleihen³³⁰.

5.2.3 Überwachung bei Mischnutzung

Bei einer Mischnutzung des Internet-Anschlusses ist die Privatnutzung des Internets erlaubt, jedoch kann technisch nicht unterschieden werden, ob die Inanspruchnahme dienstlichen oder privaten Charakter besitzt. Liegt eine solche Situation vor, schützt das Fernmeldegeheimnis aus § 88 TKG die gesamte über den Anschluss abgewickelte Telekommunikation. Dies hat zur Folge, dass auch die Kontrolle betrieblicher Nutzungsvorgänge grundsätzlich ausscheiden muss. Liegt von Seiten der Belegschaft keine Verzichtserklärung im Hinblick auf das Fernmeldegeheimnis vor, dann sind die Inhaltsdaten des Nutzungsvorgangs für den Arbeitgeber grundsätzlich tabu. Sollte ferner

³²⁶ Vgl. *Elschner* (o. Fußn. 3), S. 198 f.

³²⁷ Vgl. *Mattl* (o. Fußn. 21), S. 105; vgl. *Elschner* (o. Fußn. 3), S. 199.

³²⁸ Vgl. *Erlner* (o. Fußn. 18), S. 55.

³²⁹ Vgl. *Weißnicht* (o. Fußn. 157), 448 (449); vgl. *Hanau/Hoeren* (o. Fußn. 12), S. 51; vgl. *Gola* (o. Fußn. 137), 322 (327); vgl. *Hilber/Frik*, RdA 2002, 89 (94); vgl. *Haufsmann/Krets*, NZA 2005, 259 (263).

³³⁰ Vgl. *Mattl* (o. Fußn. 21), S. 109 f.

kein konkreter Missbrauchsverdacht vorliegen, dürfen die äußeren Umstände des Telekommunikationsvorgangs nur gespeichert werden, wenn und soweit es zur Erbringung des Dienstes oder zur Entgeltabrechnung unbedingt erforderlich ist.³³¹ Ebenso erlangen einzelne Datenschutzvorschriften des Telemediengesetzes gleichermaßen für die privat wie dienstlich motivierte Inanspruchnahme des Internets Geltung³³².

5.3 Überwachung von E-Mail

5.3.1 Überwachung bei unerlaubter Privatnutzung bzw. betrieblicher Nutzung

Das Arbeitgeberinteresse, den betrieblichen E-Mail-Verkehr zu kontrollieren, ergibt sich insbesondere aus dem Wunsch, unerlaubte Nutzungen aufzudecken, um sie zukünftig zu unterbinden. Ganz elementare Anliegen können dieses Interesse rechtfertigen. Zu nennen sind in diesem Zusammenhang der Schutz von Geschäftsgeheimnissen, die Sicherheit vor Schadsoftware und das Unterbinden strafrechtlich relevanter Handlungen durch Mitarbeiter, die das Unternehmen selbst gefährden könnten.³³³

Auch bei der Beurteilung der Zulässigkeit von Überwachungsmaßnahmen bei der unerlaubten Privatnutzung des E-Mail-Accounts muss – wie bei der Internet-Nutzung zu ausschließlich betrieblichen Zwecken – gem. § 28 Abs. 1 S. 1 Nr. 1 und Nr. 2 BDSG eine Interessenabwägung vollzogen werden. Die bereits bei der unerlaubten Inanspruchnahme des Internets aufgezeigten Möglichkeiten, die Überwachungsbefugnis durch eine Einwilligung oder eine Kollektivver-

³³¹ Vgl. *Steidle* (o. Fußn. 105), S. 312-314.

³³² Vgl. *Mattl* (o. Fußn. 21), S. 127.

³³³ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 34.

einbarung auszuweiten, gelten für die verbotene Privatnutzung des E-Mail-Accounts analog.

Es gilt jedoch zu prüfen, ob die bereits von der Rechtsprechung entwickelten Grundsätze zur Telefonüberwachung auch auf den E-Mail-Dienst übertragbar sind, da in diesem Fall ein konkreter rechtlicher Rahmen schon besteht³³⁴. Fraglich ist also, ob die E-Mail mit dem Telefonat vergleichbar ist; hierzu gehen die Meinungen in der Literatur auseinander.

Ein Teil der Autoren³³⁵ sieht den Austausch mittels E-Mail als eine mit dem Telefonat vergleichbare Kommunikation; deshalb soll die E-Mail-Kommunikation unter denselben Schutz gestellt sein wie das Telefonat³³⁶. Das grundrechtlich geschützte Recht am eigenen Wort als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts dient als Grundlage zum Schutz dienstlicher Telefongespräche³³⁷. Die entwickelten Grundsätze des BVerfG und des BAG zum Persönlichkeitschutz beschränken sich jedoch nicht auf bestimmte Situationen und Techniken³³⁸. Argumentiert wird, die E-Mail-Kommunikation ermögliche den Dialog, wenngleich nicht in verbaler Form, innerhalb kürzester Zeit; es komme nicht darauf an, ob zum Telefonhörer oder zur Tastatur gegriffen werde³³⁹. Darüber hinaus sei eine E-Mail unformell und von hoher Spontaneität geprägt, insofern könne nicht ausgeschlossen werden, dass z. B. flapsige Bemerkungen über einen Vorgesetzten auch in einer dienstlichen E-Mail enthalten seien³⁴⁰. Wie auch das heimliche Mithören eines Telefonats unerlaubt sei, dürfe auch der Inhalt von E-Mail-Nachrichten grundsätzlich nicht kontrolliert wer-

³³⁴ Vgl. Steidle (o. Fußn. 105), S. 273.

³³⁵ So bspw. Däubler (o. Fußn. 26), § 4 Rdnrn. 248 f.; Raffler/Hellich, NZA 1997, 862 (863); Weißgerber (o. Fußn. 98), S. 141 f.; Däubler (o. Fußn. 64), 323 (327).; Mester, in: Hammermeister/Reich/Rose (o. Fußn. 62), S. 53; Ernst (o. Fußn. 53), 585 (589).

³³⁶ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 248.

³³⁷ Vgl. Mattl (o. Fußn. 21), S. 140.

³³⁸ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 248.

³³⁹ Vgl. Weißgerber (o. Fußn. 98), S. 141 f.; vgl. Tuchbreiter (o. Fußn. 116), S. 175.

³⁴⁰ Vgl. Steidle (o. Fußn. 105), S. 277; vgl. Mattl (o. Fußn. 21), S. 140.

den. Eine Ausnahme liege aber vor, wenn bspw. ein begründeter Verdacht auf Straftaten bestehe.³⁴¹ Seine Grenze finde das Überwachungsverbot der Telefonate allerdings dann, wenn es lediglich um die äußeren Daten gehe, also um Datum, Dauer und Ziel³⁴². Die bloße Erfassung der äußeren Begleitumstände von Telefonaten bedeute einen weit weniger intensiven Eingriff in das Arbeitnehmerpersönlichkeitsrecht als die Überwachung der Gesprächsinhalte³⁴³.

Dieser Grundsatz lässt sich unproblematisch auf die Kontrolle der äußeren Daten von E-Mails übertragen³⁴⁴. Damit eng verbunden steht die Frage, ob auch die vollständige E-Mail-Adresse des externen Kommunikationspartners gespeichert und eingesehen werden darf, da auch dessen Recht auf informationelle Selbstbestimmung betroffen ist, oder ob eine Verkürzung der E-Mail-Adresse – im Sinne einer Unkenntlichmachung – des Kommunikationspartners zu erfolgen hat³⁴⁵. Die ungekürzte Speicherung ist nach überwiegender Ansicht zulässig, da der Arbeitgeber auch bei der dienstlichen Briefpost die Adressaten einsehen darf³⁴⁶. Im Übrigen kann eine Missbrauchskontrolle ohne Kenntnis der gesamten E-Mail-Adresse in vielen Fällen praktisch nicht stattfinden³⁴⁷.

³⁴¹ Vgl. *Däubler* (o. Fußn. 64), 323 (327); vgl. *Tuchbreiter* (o. Fußn. 116), S. 175.

³⁴² Vgl. *Mester*, in: *Hammermeister/Reich/Rose* (o. Fußn. 62), S. 53 f.; vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 35.

³⁴³ Vgl. *Tuchbreiter* (o. Fußn. 116), S. 167.

³⁴⁴ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 38.

³⁴⁵ Vgl. *Ernst* (o. Fußn. 53), 585 (589); vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 39.

³⁴⁶ Vgl. *Mengel* (o. Fußn. 102), 2014 (2016); *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 39; vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (136); ohne Ergebnis *Ernst* (o. Fußn. 53), 585 (590).

³⁴⁷ Vgl. *Barton* (o. Fußn. 183), 460 (462).

Nach h. M. wird davon ausgegangen, dass die E-Mail eher mit einem Brief als mit einem Telefonat zu vergleichen ist³⁴⁸. Die E-Mail-Nachricht muss schriftlich abgefasst und niedergelegt werden. Zum Absenden ist ein weiteres Tätigwerden erforderlich. Erfolgt zusätzlich eine Rechtschreibprüfung, kommt es zu einer weiteren Zeitverzögerung, die ebenfalls zu einer stärkeren Distanzierung zum Telefonat beiträgt. Die E-Mail erfüllt weiterhin die Textform nach § 126b BGB, insofern wäre die Gleichstellung mit dem flüchtig gesprochenen Wort verfehlt.³⁴⁹ Insbesondere die Flüchtigkeit des gesprochenen Wortes bei der mündlichen Kommunikation begründet die besondere Schutzbedürftigkeit der Gesprächspartner³⁵⁰. Beim Telefonat findet die Kommunikation quasi „unter vier Augen“ statt. Die Gesprächspartner haben zwar die Möglichkeit, das Gesprochene jederzeit zu korrigieren, sie äußern sich aber in vielen Fällen mit weit geringerer Vorüberlegung und Überprüfung des Gesprochenen als sie es beim Verfassen einer E-Mail tun würden.³⁵¹ Auch tritt im betrieblichen Alltag die E-Mail zunehmend an die Stelle des Geschäftsbriefs³⁵². Darüber hinaus ist der zivilrechtlichen Literatur zu entnehmen, dass die E-Mail nicht als Willenserklärung unter Anwesenden i. S. d. § 147 BGB, sondern als Willenserklärung unter Abwesenden betrachtet wird³⁵³.

Entsprechend zur Überwachung der dienstlichen Internet-Nutzung sind auch bei der dienstlichen Inanspruchnahme des E-Mail-Accounts die Mitarbeiter darüber zu unterrichten, dass der E-Mail-Anschluss kontrolliert wird³⁵⁴.

³⁴⁸ Vgl. Mengel (o. Fußn. 102), 2014 (2017); vgl. Gola (o. Fußn. 137), 322 (326); vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1494); vgl. Hanau/Hoeren (o. Fußn. 12), S. 53 f.; vgl. Steidle (o. Fußn. 105), S. 279; vgl. Tuchbreiter (o. Fußn. 116), S. 177; vgl. Hilber/Frik (o. Fußn. 329), 89 (95); vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (136); vgl. Kömpf/Kunz (o. Fußn. 155), 1341 (1344); vgl. Rath/Karner (o. Fußn. 35), 446 (450); vgl. Beckschulze (o. Fußn. 319), 2777 (2779); vgl. Mattl (o. Fußn. 21), S. 46; vgl. Zilkens (o. Fußn. 57), 253 (260).

³⁴⁹ Vgl. Besgen/Prinz, in: Besgen/Prinz (o. Fußn. 56), § 1 Rdnr. 41.

³⁵⁰ Vgl. Mengel (o. Fußn. 102), 2014 (2017).

³⁵¹ Vgl. Höld (o. Fußn. 55), S. 197.

³⁵² Vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1492).

³⁵³ Ebda.

³⁵⁴ Vgl. Mattl (o. Fußn. 21), S. 142; vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1494 f.).

5.3.1.1 Äußere Umstände

Die äußeren Daten einer E-Mail, bspw. der Zeitpunkt des Versands, der Betreff und die ungekürzte E-Mail-Adresse des Kommunikationspartners, können genauso wie die äußeren Umstände bei der betrieblichen Post zu vorher festgelegten Zwecken bzw. zur Wahrung berechtigter Arbeitgeberinteressen eingesehen werden³⁵⁵.

Der Umgang mit den äußeren Rahmendaten wird jedoch dann unzulässig, wenn eine anlassunabhängige und lückenlose Überwachung über die gesamte Arbeitszeit hinweg vorgenommen wird. Dies gilt auch bei ausschließlich dienstlichen E-Mails. Liegt eine solche Vollkontrolle vor, ist ein unverhältnismäßiger Eingriff in das Arbeitnehmerpersönlichkeitsrecht zu bejahen.³⁵⁶ Die lediglich abstrakte Gefahr, der betriebliche E-Mail-Anschluss könnte missbraucht werden, reicht nicht aus, eine lückenlose Auswertung des Netzverkehrs zu vollziehen. Deshalb stellen - wie bei der Überwachung des Internets - stichprobenartige und verdachtsbezogene Kontrollen das mildere Mittel gegenüber einer vollständigen Auswertung der anfallenden Daten dar.³⁵⁷

5.3.1.2 Inhaltsdaten

Da betriebliche E-Mails der geschäftlichen Briefpost gleichstehen, gehören sie als Arbeitsmittel zum Unternehmen³⁵⁸. Ist die private Inanspruchnahme des E-Mail-Anschlusses untersagt, kann eine Inhaltskontrolle der dienstlichen E-Mails zur Zweckbestimmung des Arbeitsverhältnisses und zur Wahrung berechtigter Arbeitgeber-

³⁵⁵ Vgl. *Steidle* (o. Fußn. 105), S. 284.

³⁵⁶ Vgl. *Elschner* (o. Fußn. 3), 279; vgl. *Barton* (o. Fußn. 183), 460 (463); vgl. *Rath/Karner* (o. Fußn. 35), 446 (450).

³⁵⁷ Vgl. *Elschner* (o. Fußn. 3), S. 286.

³⁵⁸ Vgl. *Steidle* (o. Fußn. 105), S. 282.

interessen im Rahmen von § 28 Abs. 1 S. 1 Nr. 1 und Nr. 2 BDSG vorgenommen werden³⁵⁹. Der Arbeitgeber ist somit befugt, vom Inhalt der E-Mails Kenntnis zu nehmen oder sich die E-Mails ausdrucken zu lassen³⁶⁰. Wenn augenscheinlich kein Hinweis besteht, dass die E-Mail privater Natur ist, kann der Arbeitgeber davon ausgehen, dass es sich um eine betriebliche Nachricht handelt, die er wie die Dienstpost einsehen und kontrollieren darf. Der Absender einer E-Mail kann sich nicht darauf verlassen, dass der Inhalt nicht auch noch weiteren Personen neben dem eigentlichen Empfänger bekannt wird, bedenkt man die Tatsache, dass die elektronische Nachricht jederzeit ausgedruckt und zu den Akten genommen werden kann.³⁶¹

An anderer Stelle wird argumentiert, die Kontrollbefugnis des Arbeitgebers sei abhängig von der Form der betrieblichen E-Mail-Adresse. Laute diese etwa „vertrieb@unternehmen-x.de“, gestalte es sich völlig unproblematisch, den Inhalt einzusehen, da die E-Mail in jedem Fall als dienstlich zu qualifizieren sei. Anders zu beurteilen sei die Situation, in der der jeweilige Mitarbeiter über eine persönliche E-Mail-Adresse, bspw. „gerd.mueller@unternehmen-x.de“, verfüge. In diesem Fall solle dem Arbeitgeber kein Kontrollrecht zustehen, da die Adresse nicht generell als betriebsbezogen eingeordnet werden könne.³⁶² Dem muss entgegengehalten werden, dass es sich auch bei einer E-Mail-Adresse, die den Namen des Arbeitnehmers enthält, noch immer um einen dienstlichen E-Mail-Account handelt, bei dem die Nachricht dem bestimmten Mitarbeiter zugestellt wird³⁶³. Es ist also wieder die Parallele zur dienstlichen Briefpost zu ziehen, die der Arbeitgeber auch dann öffnen und einsehen darf, wenn der Brief an einen speziellen Mitarbeiter adressiert ist. Diese Befugnis ist nur dann

³⁵⁹ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 41; vgl. *Elschner* (o. Fußn. 3), S. 277-280.

³⁶⁰ Vgl. *Beckschulze* (o. Fußn. 319), 2777 (2779).

³⁶¹ Vgl. *Höld* (o. Fußn. 55), S. 198; vgl. *Mengel* (o. Fußn. 102), 2014 (2017); vgl. *Beckschulze* (o. Fußn. 319), 2777 (2779 f.); vgl. *Barton* (o. Fußn. 183), 460 (463).

³⁶² Vgl. *Ernst* (o. Fußn. 53), 585 (589 f.).

³⁶³ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 43.

nicht gegeben, wenn auf dem Brief bzw. in der E-Mail-Betreffzeile der Zusatz „persönlich“ oder „vertraulich“ vermerkt wurde.³⁶⁴

Einen Sonderfall im Hinblick auf die Frage nach der Zulässigkeit der Einsichtnahme von E-Mails stellen private Nachrichten dar, die trotz des Verbots der Privatnutzung versandt und/oder empfangen wurden. Das Kontrollrecht umfasst in einem solchen Fall auch die äußeren Daten von Privatnachrichten; dies ergibt sich bereits daraus, dass ohne diese Möglichkeit ein Missbrauch des E-Mail-Anschlusses gar nicht erst aufgedeckt werden kann.³⁶⁵ Deuten Anhaltspunkte darauf hin, dass es sich um Privatkorrespondenz handelt, ist die Untersuchung des Inhalts grundsätzlich unzulässig. Die Einsichtnahme versandter und anschließend abgespeicherter privater E-Mails - trotz eines diesbezüglichen Verbots - ist nur bis zu dem Punkt zulässig, an dem erkannt wird, dass es sich um private Inhalte handelt. Dasselbe gilt für eingehende E-Mails.³⁶⁶ Eine Inhaltskontrolle solcher Mails kommt allenfalls dann in Betracht, wenn anhand der äußeren Umstände die Zuordnung zu betrieblicher bzw. privater Kommunikation nicht möglich ist. Die Entscheidung darüber, ob eine Inhaltskontrolle gerechtfertigt ist, muss einzelfallbezogen und unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes getroffen werden.³⁶⁷

Da bereits die Vollkontrolle der äußeren Daten der betrieblichen E-Mails unzulässig ist, muss erst recht die vollumfängliche Einsichtnahme der Inhalte betrieblicher E-Mail-Nachrichten ausscheiden. Bei Vorliegen eines hinreichend konkreten Missbrauchsverdachts können die Überwachungsmaßnahmen gezielt ausgeweitet werden.³⁶⁸

³⁶⁴ Vgl. Barton (o. Fußn. 183), 460 (463); vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 46; vgl. Beckschulze (o. Fußn. 319), 2777 (2779).

³⁶⁵ Vgl. Mattl (o. Fußn. 21), S. 137; vgl. Raffler/Hellich (o. Fußn. 335), 862 (863).

³⁶⁶ Vgl. Steidle (o. Fußn. 105), S. 290.

³⁶⁷ Vgl. Mattl (o. Fußn. 21), S. 144.

³⁶⁸ Vgl. Elschner (o. Fußn. 3), S. 285 f.

5.3.2 Überwachung bei erlaubter Privatnutzung

Wie bereits darauf hingewiesen, muss eine Trennung zwischen der betrieblichen und privaten E-Mail-Kommunikation möglich sein, da ansonsten eine Mischnutzung des E-Mail-Accounts vorliegt. Die Unterscheidung zwischen betrieblichen und privaten E-Mails lässt sich entweder durch bspw. den Vermerk „PRIVAT“ in der Betreffzeile oder – einfacher – durch Bereitstellung einer zweiten E-Mail-Adresse zur ausschließlich privaten Nutzung realisieren.³⁶⁹

Bei der Beurteilung der Zulässigkeit von Überwachungsmaßnahmen im Rahmen der gestatteten Privatnutzung des E-Mail-Dienstes kann auf die bereits bei der zulässigen privaten Inanspruchnahme des Internet-Anschlusses aufgestellten Grundsätze verwiesen werden.

5.3.2.1 Beurteilung nach dem Telekommunikationsgesetz

Außer zur eigentlichen Erbringung des E-Mail-Dienstes, zur Störungs- und Fehlerbeseitigung, zur Entgeltabrechnung sowie zum Aufdecken und Unterbinden rechtswidriger Nutzungen erlaubt das Fernmeldegeheimnis keine andere Verwendung der Daten. Die enge Zweckbindung dieser Erlaubnistatbestände verbietet Kontrollen etwa zur Überprüfung der Arbeitsleistung. Die Überwachung der Inhalte privater E-Mails muss grundsätzlich ausscheiden.

5.3.2.2 Beurteilung nach dem Telemediengesetz

Da für den Arbeitgeber bereits durch das Bereitstellen eines E-Mail-Zugangs die Datenschutzvorschriften des Telekommunikationsgesetzes gelten, sind nach § 11 Abs. 3 TMG nur noch vereinzelte Daten-

³⁶⁹ Vgl. Panzer (o. Fußn. 103), S. 272.

schutzbestimmungen des Telemediengesetzes anzuwenden³⁷⁰. Die verbleibenden Datenschutznormen spielen bei der E-Mail-Überwachung praktisch keine Rolle; deshalb richtet sich die Zulässigkeit von Kontrollmaßnahmen nach dem im Telekommunikationsgesetz vorgesehenen Datenschutz.

Was die Erweiterung der Überwachungsbefugnis anbelangt, so kann – analog zur erlaubten privaten Internet-Nutzung – nur eine wirksame Einwilligung der Arbeitnehmer in weiter gehende Datenverarbeitungsprozesse und insbesondere in den Verzicht auf das Fernmeldegeheimnis als zulässiges Mittel betrachtet werden.

5.3.3 Überwachung bei Mischnutzung

Die Mischnutzung beim E-Mail-Account ist dann gegeben, wenn es dem Arbeitnehmer erlaubt ist, über die betriebliche E-Mail-Adresse auch private Nachrichten zu versenden und zu empfangen. Analog zur Überwachung bei Mischnutzung des Internet-Anschlusses kommt es zu einer Ausstrahlungswirkung des Fernmeldegeheimnisses gem. § 88 TKG auf sämtliche E-Mails – sowohl auf private als auch auf dienstliche.³⁷¹ Auch die zumindest eingeschränkte Geltung des Telemediengesetzes bei der Privatnutzung ist auf den dienstlichen Gebrauch vollständig zu übertragen³⁷².

Teilweise wird vertreten, dass dem Arbeitgeber bei der Mischnutzung ein Recht zur Kontrolle solcher E-Mails zustehe, die betriebsbezogene Inhalte vermuten ließen³⁷³. Bei der Mischnutzung ist von vornherein nicht ersichtlich, ob die E-Mails betrieblicher oder privater Natur sind.

³⁷⁰ Vgl. *BR-Drs.* 556/06, S. 22.

³⁷¹ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 97.

³⁷² Vgl. *Mattl* (o. Fußn. 21), S. 127.

³⁷³ So *Höld* (o. Fußn. 55), S. 199; *Hanau/Hoeren* (o. Fußn. 12), S. 54; vgl. *Steidle* (o. Fußn. 105), S. 312 f.

Der Einblick in die E-Mails würde deshalb zu einer Aushebelung des durch das Fernmeldegeheimnis gewährleisteten Schutzes führen.³⁷⁴ Lediglich die Einwilligung der Arbeitnehmer, dass sie bei einer Mischnutzung des Systems auf den Schutz des Fernmeldegeheimnisses verzichten, vermag das Überwachungsverbot zu heilen³⁷⁵.

5.4 Überwachung bei besonderen Berufsgruppen

Die aufgezeigten Grundsätze zur Internet- und E-Mail-Überwachung am Arbeitsplatz sind nicht uneingeschränkt auf sämtliche Arbeitnehmer anwendbar. Besonders zu behandeln sind Beschäftigte, die ihr Wissen, das sie im Rahmen der dienstlichen Tätigkeit erworben haben, nicht an Dritte weitergeben dürfen.³⁷⁶ Als „Dritter“ ist auch der Arbeitgeber zu qualifizieren, wenn er solche Personen als Arbeitnehmer in seinem Unternehmen beschäftigt³⁷⁷. Für die Berufsgruppen mit Sonderstatus enthält § 203 StGB eine eigene Strafvorschrift³⁷⁸. Zu den Arbeitnehmern, die einen solchen Sonderstatus genießen, zählen gem. § 203 Abs. 1 StGB Träger von Berufsgeheimnissen, wie Rechtsanwälte, Angehörige von Heilberufen und Psychologen. Nach einem Urteil des BAG³⁷⁹ zur Telefondatenüberwachung ist es unzulässig, die Zielrufnummer eines angestellten Psychologen zu erfassen, da dies Rückschlüsse auf die betreute Person zuließe.³⁸⁰ Dieser Grundsatz ist auf sämtliche durch § 203 Abs. 1 StGB erfassten Berufsgruppen zu übertragen. Auch muss sich das, was für Telefongespräche gilt, auf den Bereich Internet und E-Mail erstrecken³⁸¹. Nicht zulässig ist daher die Überwachung der dienstlichen E-Mail-Kommunikation sowie der

³⁷⁴ Vgl. Mengel (o. Fußn. 102), 2014 (2018).

³⁷⁵ Vgl. Steidle (o. Fußn. 105), S. 313 f.

³⁷⁶ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 263.

³⁷⁷ Vgl. Raffler/Hellich (o. Fußn. 335), 862 (866).

³⁷⁸ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 263.

³⁷⁹ BAG, Urt. v. 13.1.1987 = NZA 1987, 515.

³⁸⁰ Vgl. Steidle (o. Fußn. 105), S. 309.

³⁸¹ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 264.

aufgerufenen Webseiten aufgrund vorrangiger Interessen sowohl dieser Berufsgruppen als auch deren Kommunikationspartner. Das Verbot umfasst dabei die äußeren Verbindungsdaten und erst recht die inhaltliche Komponente.³⁸² Ausnahmen sind nur aufgrund richterlicher Anordnung möglich³⁸³.

Als weitere besonders zu behandelnde Arbeitnehmer gelten solche, die über ein Zeugnisverweigerungsrecht verfügen. Dieses Recht auf Zeugnisverweigerung ergibt sich aus § 53 Abs. 1 Nr. 5 StPO und § 383 Abs. 1 Nr. 5 ZPO und betrifft Journalisten.³⁸⁴ Der weitreichende Schutz, der für Personen, die Beiträge für Presse, Rundfunk und Fernsehen ausarbeiten, gilt, wird durch § 41 Abs. 3 S. 2 BDSG gestärkt: Selbst bei Persönlichkeitsrechtsverletzungen durch Berichterstattung in den Medien dürfen die Namen der Informanten nicht preisgegeben werden.³⁸⁵ Für Geistliche muss dasselbe gelten³⁸⁶. In diesem Zusammenhang ist jedoch die sog. innere Pressefreiheit zu beachten. Danach bestehen keine vollumfängliche Weisungsungebundenheit der Journalisten einerseits und kein vorbehaltloser Geheimnisschutz gegenüber dem Arbeitgeber andererseits. Im Einzelfall mag das Arbeitgeberinteresse an einer Überprüfung der Informationen überwiegen, sodass die Kontrolle des E-Mail-Verkehrs als gerechtfertigt angesehen werden kann.³⁸⁷

Ebenso genießen Beschäftigte mit fachlicher Unabhängigkeit, bspw. Richter, betriebliche Datenschutzbeauftragte, Immissionsschutz- und Störfallbeauftragte, einen besonderen Schutz³⁸⁸. Ein Richter etwa ist

³⁸² Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 54; vgl. Weißnicht (o. Fußn. 157), 448 (451).

³⁸³ Vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1495).

³⁸⁴ Vgl. Elschner (o. Fußn. 3), S. 288; vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1495); vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 265.

³⁸⁵ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 265; vgl. Elscher (o. Fußn. 3), S. 288 f.; vgl. Raffler/Hellich (o. Fußn. 335), 862 (866).

³⁸⁶ Vgl. Däubler (o. Fußn. 26), § 4 Rdnr. 266.

³⁸⁷ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 55.

³⁸⁸ Vgl. Steidle (o. Fußn. 105), S. 310.

niemandem Rechenschaft schuldig, weshalb er im Verfahren einen Prozessvertreter über E-Mail konsultiert hat³⁸⁹. Die Personengruppe der fachlich Unabhängigen unterliegt in Ausübung ihrer Tätigkeit keiner fachlichen Weisungsgebundenheit und darf nicht in ihrem Kommunikationsverhalten beschränkt werden³⁹⁰.

Im Bereich der Wissenschaft tätige Arbeitnehmer fallen unter den besonderen Schutz der Wissenschaftsfreiheit aus Art. 5 Abs. 3 GG³⁹¹. Die Konkretisierung des Grundrechts auf Wissenschaftsfreiheit ergibt sich aus der Zweckbindung des § 40 Abs. 1 BDSG, der die Datenverarbeitung und -nutzung von zur wissenschaftlichen Forschung erhobenen und gespeicherten personenbezogenen Daten zu ausschließlich wissenschaftlichen Zwecken erlaubt³⁹². Der Arbeitgeber darf diese Daten also nicht in Kontrollabsicht zur Kenntnis nehmen³⁹³. Es scheidet schon die Erfassung der Daten über die Online-Nutzung zur Entgeltabrechnung aus, falls dadurch in irgendeiner Weise Rückschlüsse auf z. B. Testpersonen, die an einem Online-Interview teilgenommen haben, gezogen werden könnten³⁹⁴.

Der Betriebsrat darf gem. § 78 S. 1 BetrVG nicht in seiner Aufgabenerfüllung behindert werden; insofern genießt auch er einen Sonderstatus. Bezogen auf seine Tätigkeit ist er unabhängig vom Arbeitgeber und unterliegt auch nicht der Kontrolle durch den Arbeitgeber.³⁹⁵ Der E-Mail- und Internet-Verkehr darf nicht protokolliert und ausgewertet werden, da hierin eine Einschränkung der Handlungs- und Entscheidungsfreiheit des Betriebsrats und mithin eine Störung zu sehen ist. Darüber hinaus steht einer Überwachung der Betriebsratkommunikation das Persönlichkeitsrecht der Arbeitnehmer, auf die geschlossen

³⁸⁹ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 267.

³⁹⁰ Vgl. *Elschner* (o. Fußn. 3), S. 289.

³⁹¹ Vgl. *Elschner* (o. Fußn. 3), S. 290.

³⁹² Vgl. *Steidle* (o. Fußn. 105), S. 310.

³⁹³ Vgl. *Raffler/Hellich* (o. Fußn. 335), 862 (866).

³⁹⁴ Vgl. *Elschner* (o. Fußn. 3), S. 289.

³⁹⁵ Vgl. *Steidle* (o. Fußn. 105), S. 310.

werden könnte, entgegen. Eine Überwachung führte zu einem dazu, dass sich die Mitarbeitervertretung in ihrer Funktion als Vertrauensorgan beeinträchtigt sähe, zum anderen würde das Vertrauen der Mitarbeiter in eine vertrauliche Kommunikation erschüttert.³⁹⁶

Da das Überwachungsverbot für Beschäftigte mit Sonderstatus nur für die Kommunikation, bei der ihre Verschwiegenheitspflicht berührt ist, Gültigkeit hat, ansonsten die allgemeinen Grundsätze der Überwachung der betrieblichen Nutzung anzuwenden sind, ist durch eine entsprechende Systemkonfiguration dafür Sorge zu tragen, dass diese Telekommunikationsvorgänge nicht von der automatischen Protokollierung erfasst werden.³⁹⁷

Es empfiehlt sich demzufolge ausdrücklich, eine zweite E-Mail-Adresse einzurichten, auf der die gewöhnliche betriebliche Korrespondenz abgewickelt wird. Durch ein eigenes Zugangsprofil im Internet-Browser ließe sich eine technische Trennung zur Unterscheidung zwischen Tätigkeit im Rahmen des Sonderstatus und Ausübung der gewöhnlichen Arbeitsaufgabe realisieren. Andernfalls gilt es, die Sonderregelungen für das Berufsgeheimnis auf alle Kommunikationsvorgänge anzuwenden.³⁹⁸

5.5 Folgen einer unerlaubten Privatnutzung

Arbeitnehmer begehen durch die unerlaubte Inanspruchnahme des Internets und des E-Mail-Accounts eine arbeitsvertragliche Pflichtverletzung³⁹⁹. Die grundsätzliche Nutzung der IuK-Technik bei nicht vorhandener Nutzungsregelung, die Nichteinhaltung eines bestehenden

³⁹⁶ Vgl. *Elschner* (o. Fußn. 3), S. 298 f.

³⁹⁷ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 264; vgl. *Steidle* (o. Fußn. 105), S. 311; vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 54; vgl. *Elschner* (o. Fußn. 3), S. 288.

³⁹⁸ Vgl. *Steidle* (o. Fußn. 105), S. 311.

³⁹⁹ Vgl. *Däubler* (o. Fußn. 64), 323 (327); vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 53.

Verbots, die Überschreitung der zeitlichen und inhaltlichen Vorgaben, der unsachgemäße Umgang mit den elektronischen Kommunikationsmitteln oder die Vornahme strafbarer Handlungen stellen missbräuchliche und somit unerlaubte Nutzungsformen dar⁴⁰⁰. Der Arbeitgeber kann in Abhängigkeit der Schwere der Pflichtverletzung Sanktionen verhängen⁴⁰¹.

5.5.1 Ermahnung

Ganz allgemein stellt die Ermahnung eine durch den Gläubiger an den Schuldner gerichtete eindeutige und bestimmte Aufforderung zur Erbringung der geschuldeten Leistung dar⁴⁰². Insbesondere für die Fälle, in denen der Nachweis einer Pflichtverletzung des Beschäftigten nicht eindeutig gelingt, ist die Ermahnung ein geeignetes Sanktionsinstrument, das dem Arbeitnehmer gleichzeitig zu erkennen gibt, dass entsprechende Verhaltensweisen auch zukünftig nicht geduldet werden⁴⁰³. Die Ermahnung kommt ebenfalls dann in Betracht, wenn der Mitarbeiter keine Kenntnis von dem Verbot der Privatnutzung hatte⁴⁰⁴. Sie erfordert keine bestimmte Fristsetzung und keine Androhung negativer arbeitsrechtlicher Konsequenzen⁴⁰⁵.

5.5.2 Sperrung des Internet-Zugangs

Die vollständige Sperrung des Internet-Accounts für verhaltensauffällige Mitarbeiter ist als probates Mittel zur Verhinderung zukünftiger Verstöße anzusehen⁴⁰⁶. Weniger einschneidend ist eine Zugriffs-

⁴⁰⁰ Vgl. *Lelley*, in: *Worzalla*, S. 17 Rdnr. 38; vgl. *Däubler* (o. Fußn. 26), § 3 Rdnr. 194.

⁴⁰¹ Vgl. *Holenstein* (o. Fußn. 13), S. 147.

⁴⁰² Vgl. *v. Hase*, NJW 2002, 2278 (2280).

⁴⁰³ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 128.

⁴⁰⁴ Vgl. *Däubler* (o. Fußn. 64), 323 (327).

⁴⁰⁵ Vgl. *v. Hase* (o. Fußn. 402), 2278 (2280).

⁴⁰⁶ Vgl. *Holenstein* (o. Fußn. 13), S. 148.

einschränkung, bei der bspw. spezifische Inhalte anhand vordefinierter Listen (Black Lists) nicht mehr aufrufbar sind. Auch der umgekehrte Fall ist möglich: Hier werden von vornherein die Internet-Adressen bestimmt, die ausschließlich anwählbar sind (White Lists).⁴⁰⁷ Diese Filterverfahren können analog auf den E-Mail-Dienst übertragen werden. Jedoch sind sowohl die Beschränkung des Internet- als auch des E-Mail-Anschlusses problembehaftet. Die sich potenziell daraus ergebenden Schwierigkeiten wurden bereits in Kapitel 3 aufgezeigt.

5.5.3 Abmahnung

Eine Legaldefinition für den Begriff der Abmahnung existiert nicht⁴⁰⁸. Ihr kommt jedoch im Arbeitsrecht eine besondere Bedeutung zu: Einerseits gilt sie als grundsätzliche Voraussetzung für den Ausspruch einer späteren verhaltensbedingten Kündigung, andererseits ist sie gleichzeitig auf den Fortbestand des Arbeitsverhältnisses gerichtet – sie erfüllt insofern eine Doppelfunktion.⁴⁰⁹ Da die Abmahnung regelmäßig einer Kündigung aus verhaltensbedingten Gründen voraus gehen muss, sind insbesondere ihre notwendigen formellen Voraussetzungen zu berücksichtigen. Die rechtswirksame Abmahnung muss mindestens enthalten:

- Darlegung des konkret zu bezeichnenden Fehlverhaltens;
- Rüge des Fehlverhaltens;
- Aufforderung zu künftigem vertragskonformen Verhalten;
- unmissverständliche Androhung arbeitsrechtlicher Konsequenzen für den Wiederholungsfall.⁴¹⁰

⁴⁰⁷ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 132.

⁴⁰⁸ Vgl. *v. Hase*, (o. Fußn. 402), 2278 (2280).

⁴⁰⁹ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 65.

⁴¹⁰ Vgl. *Hunold*, NZA-RR 2000, 169 (170-173).

Generell besteht für den Ausspruch einer Abmahnung Formfreiheit, sie kann folglich auch mündlich erteilt werden. Davon ist jedoch dringend abzuraten; zur ausreichenden Beweissicherung ist die schriftliche Ausfertigung notwendig.⁴¹¹ Für den Ausspruch der Abmahnung existiert darüber hinaus keine Ausschlussfrist, innerhalb derer der Mitarbeiter abzumahnern ist⁴¹². Es ist dennoch empfehlenswert, die Abmahnung innerhalb von zwei Wochen nach Kenntnisnahme der Pflichtverletzung zu erteilen, nicht zuletzt um der ihr innewohnenden Warnfunktion Nachdruck zu verleihen⁴¹³.

5.5.4 Kürzung der Vergütung

Dem Arbeitgeber steht das Recht zu, die Gegenleistung – namentlich die Vergütung – für die geschuldete Arbeit entsprechend zu kürzen, sollten Arbeitnehmer ihrer Arbeitspflicht in nicht genügendem Maße nachkommen. Da das Arbeitsverhältnis nach § 611 BGB ein synallagmatisches Austauschverhältnis beinhaltet, können Arbeitnehmer, die ihre Privatangelegenheiten im Unternehmen während der Arbeitszeit verrichten, auch nicht den vollen Vergütungsanspruch geltend machen.⁴¹⁴ Dabei ist es im Ergebnis gleich, ob die Arbeitnehmer durch Betrug bei der Zeiterfassung den Betrieb vorzeitig verlassen, oder der Arbeitszeitdiebstahl durch die Privatnutzung von Internet und E-Mail vollzogen wird⁴¹⁵.

⁴¹¹ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 67.

⁴¹² Vgl. *Hunold* (o. Fußn. 410), 169 (173).

⁴¹³ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 56), § 1 Rdnr. 71.

⁴¹⁴ Vgl. *Gola* (o. Fußn. 123), S. 158 Rdnr. 346.

⁴¹⁵ Vgl. *Beckschulze* (o. Fußn. 319), 2777 (2781).

5.5.5 Ordentliche Kündigung

Die ordentliche Kündigung des Arbeitsverhältnisses bestimmt sich nach den Vorschriften der §§ 620 bis 625 BGB. Wichtig ist in diesem Zusammenhang, dass gem. § 23 Abs. 1 S. 3 KSchG in Betrieben mit regelmäßig mehr als zehn Arbeitnehmern weitere Vorschriften des Kündigungsschutzgesetzes zu beachten sind. Sonderregelungen bestehen für Arbeitsverhältnisse, die vor dem 31. Dezember 2003 bestanden haben. Der Grund für diese zusätzlichen Kündigungsschutzvorschriften ist, die Arbeitnehmer vor sozial ungerechtfertigten Kündigungen zu schützen⁴¹⁶. Falls der erweiterte Anwendungsbereich des Kündigungsschutzgesetzes eröffnet ist, so gilt – problembezogen – nach § 1 Abs. 2 S. 1 KSchG die Kündigung als sozial gerechtfertigt, wenn sie durch Gründe, die im Verhalten des Arbeitnehmers liegen, bedingt ist. Der ordentlichen, fristgerechten Kündigung muss im Regelfall eine einschlägige Abmahnung vorausgehen. Der betroffene Mitarbeiter soll die Möglichkeit haben, sein Verhalten zu korrigieren. Die Rechtfertigung der Kündigung besteht in einer negativen Zukunftsprognose. Für den Fall, dass der Kündigung keine einschlägige und darüber hinaus auch nicht wirksame Abmahnung vorausging, fehlt es am Kündigungserfordernis. Im Ergebnis bleibt eine solche Kündigung unwirksam.⁴¹⁷ Existiert ein Betriebsrat, so ist dieser hinzuzuziehen. Die Anhörung gilt als zwingende Wirksamkeitsvoraussetzung für die Kündigung.⁴¹⁸

Selbst nur geringfügige Pflichtverletzungen können in ihrer Summe dazu führen, dass sie erheblich ins Gewicht fallen⁴¹⁹. Es empfiehlt sich daher für den Arbeitgeber unbedingt, jedes pflichtwidrige abmahnungsrechtfertigende Verhalten seiner Mitarbeiter abzumahnern, um

⁴¹⁶ Vgl. Freund/Knoblach/Eisele, Praxisorientierte Personalwirtschaftslehre, 6. Aufl. (2003), S. 54.

⁴¹⁷ Vgl. Besgen/Prinz, in: Besgen/Prinz (o. Fußn. 56), § 1 Rdnr. 101.

⁴¹⁸ Vgl. Bernhardt/Barthel (o. Fußn. 227), 150 (152).

⁴¹⁹ Vgl. Däubler (o. Fußn. 26), § 3 Rdnr. 196.

eine eventuelle spätere ordentliche Kündigung auf eine substantiierte Grundlage stellen zu können.

Für ein so gravierendes Fehlverhalten, für das eine Abmahnung ausnahmsweise entbehrlich ist, kommt regelmäßig die außerordentliche, fristlose Kündigung in Betracht⁴²⁰.

5.5.6 Außerordentliche Kündigung

Eine außerordentliche Kündigung gem. § 626 BGB erlaubt dem Arbeitgeber die sofortige Trennung vom Mitarbeiter, ohne eine Frist einhalten zu müssen⁴²¹. Sie ist gem. § 626 Abs. 1 BGB aus wichtigem Grund zulässig, wenn Tatsachen vorliegen, bei denen dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und beiderseitiger Interessenabwägung der Fortbestand des Arbeitsverhältnisses bis zum Ende der Kündigungsfrist bzw. bis zur Beendigung eines befristeten Arbeitsvertrags nicht zugemutet werden kann. Die außerordentliche Kündigung verkörpert das schärfste arbeitsrechtliche Reaktionsmittel des Arbeitgebers auf Pflichtverletzungen durch Arbeitnehmer.

Die in § 626 BGB geregelte außerordentliche Kündigung kann nur bei Vorliegen eines wichtigen Grundes ausgesprochen werden. Ob ein solcher gegeben ist, wird anhand einer zweistufigen Prüfung ermittelt:

1. Auf der ersten Stufe erfolgt eine Untersuchung des Sachverhalts dahingehend, ob die begangene Pflichtverletzung einen wichtigen Grund an sich darstellen kann. Die besonderen Umstände des Einzelfalls werden auf dieser Stufe vollständig außer Acht gelassen.

⁴²⁰ Vgl. Besgen/Prinz, in: Besgen/Prinz (o. Fußn. 56), § 1 Rdnr. 101.

⁴²¹ Vgl. Freund/Knoblach/Eisele (o. Fußn. 416), S. 56.

2. Die konkreten Umstände des Einzelfalls und die Interessen beider Vertragsparteien bilden die zweite Stufe der Beurteilung, ob eine außerordentliche Kündigung gerechtfertigt erscheint. Dabei gilt es zu beachten, dass der Kündigungszweck nicht in der Sanktion der Pflichtverletzung besteht, sondern in der Vermeidung künftiger potenzieller Pflichtverletzungen.⁴²²

Ferner ist die zweiwöchige Ausschlussfrist gem. § 626 Abs. 2 S. 1 BGB zu wahren. Diese Frist beginnt erst zu laufen, wenn der Kündigungsberechtigte die kündigungsrechtfertigenden Tatsachen möglichst abschließend aufgeklärt hat. Dazu soll auch der zu Kündigende selbst angehört werden.⁴²³ Darüber hinaus ist der Betriebsrat – sofern ein solcher besteht – gem. § 102 Abs. 1 BetrVG anzuhören⁴²⁴.

Es ist auf eine weitere Kündigungsform hinzuweisen, namentlich die (außerordentliche) Verdachtskündigung⁴²⁵. Sie kommt schon beim bloßen Verdacht auf eine schwere Pflichtverletzung oder eine Straftat in Betracht. Die im Arbeitsverhältnis erforderliche Vertrauensgrundlage muss durch den Verdacht so erschüttert sein, dass eine weitere Zusammenarbeit nicht mehr zumutbar ist.⁴²⁶ Dem Verdacht müssen objektive Tatsachen zu Grunde liegen, die den Ausspruch einer außerordentlichen Kündigung rechtfertigen⁴²⁷.

⁴²² Vgl. Bernhardt/Barthel (o. Fußn. 227), 150.

⁴²³ Vgl. Besgen/Prinz, in: Besgen/Prinz (o. Fußn. 56), § 1 Rdnr. 115; vgl. Bernhardt/Barthel (o. Fußn. 227), 150 (151 f.).

⁴²⁴ Vgl. Bernhardt/Barthel (o. Fußn. 227), 150 (152).

⁴²⁵ Siehe dazu ausführlich Langner/Witt, DStR 2008, 825-830.

⁴²⁶ Vgl. Langner/Witt (o. Fußn. 425), 825.

⁴²⁷ Vgl. Bernhardt/Barthel (o. Fußn. 227), 150 (153).

5.5.7 Schadenersatzansprüche

Potenzielle Schadenersatzansprüche des Arbeitgebers gegenüber seinen Mitarbeitern können sich aus der vertraglichen oder deliktischen Haftung ergeben. Die Regelung des vertraglichen Anspruchs enthält § 280 Abs. 1 BGB. Diese Vorschrift muss im Zusammenhang mit der verbotenen Privatnutzung von Internet und E-Mail am Arbeitsplatz jedoch i. V. m. § 619a BGB gesehen werden, wonach die Darlegungs- und Beweislast für die Vertragsverletzung vom Arbeitgeber zu tragen sind. Der Anspruch des Arbeitgebers erstreckt sich auf den kausal durch die schuldhafte Handlung verursachten Schaden und auf die evtl. entstandenen Mehrkosten durch die unerlaubte Nutzung der IuK-Technik.⁴²⁸

Ein deliktischer Schadenersatzanspruch kann aus einer unerlaubten Handlung gem. § 823 Abs. 1 BGB resultieren. Etwa ein Schaden durch Virenbefall der betriebseigenen Rechnernetze aufgrund der unerlaubten Internet-Nutzung kann einen Schadenersatzanspruch gegenüber dem Mitarbeiter begründen.⁴²⁹ Ein Datenverlust stellt eine Eigentumsverletzung i. S. d. § 823 Abs. 1 BGB dar. Da jedoch ein reiner Vermögensschaden kein absolutes Recht verkörpert, ist eine deliktische Arbeitnehmerhaftung in Bezug auf solche Schäden ausgeschlossen.⁴³⁰ Grobe Fahrlässigkeit ist jedenfalls dann anzunehmen, wenn die gesamte Belegschaft bspw. mittels einer E-Mail darauf hingewiesen wurde, eine bestimmte Datei nicht zu öffnen, weil diese als Schadprogramm einzustufen ist, aber ein Arbeitnehmer die Malware trotzdem ausführt⁴³¹. Eine vorsätzliche Schadenverursachung durch einen Mitarbeiter begründet sogar einen uneingeschränkten Haftungsanspruch⁴³².

⁴²⁸ Vgl. *Elschner* (o. Fußn. 3), S. 93-95.

⁴²⁹ Vgl. *Beckschulze/Henkel* (o. Fußn. 61), 1491 (1498).

⁴³⁰ Vgl. *Elschner* (o. Fußn. 3), S. 94.

⁴³¹ Vgl. *Lelley*, in: *Worzalla*, S. 33 Rdnr. 83; vgl. *Beckschulze/Henkel* (o. Fußn. 61), 1491 (1498).

⁴³² Vgl. *Lelley*, in: *Worzalla*, S. 33 Rdnr. 82.

5.5.8 Strafanzeige

Führen die arbeitgeberseitigen Kontrollmaßnahmen zur Aufdeckung strafbarer Handlungen, die mittels der betrieblichen IuK-Anlage durch Mitarbeiter verübt wurden, ist dem Arbeitgeber dringend zu raten, dies bei den zuständigen Strafverfolgungsbehörden anzuzeigen. Zu den in Rede stehenden strafbaren Handlungen zählen insbesondere der Download gewaltverherrlichender oder kinderpornografischer Inhalte, Verstöße gegen das Urheberrecht und die Verbreitung ehrverletzender, wahrheitswidriger und beleidigender Behauptungen über andere Personen⁴³³. Besonders vor dem Hintergrund einer drohenden Durchsuchung durch die Strafverfolgungsbehörden und einer Beschlagnahme von Rechnern und Datenspeichern und des damit einhergehenden Imageverlusts und finanziellen Schadens führt an einer Anzeigenerstattung praktisch kein Weg vorbei⁴³⁴.

Liegt ein Fall einer schweren, in § 138 StGB aufgezählten Straftat vor, hat der Arbeitgeber sogar die Strafverfolgungsbehörden unverzüglich zu benachrichtigen. Das den Arbeitnehmer bei der zulässigen Privatsnutzung schützende Fernmeldegeheimnis muss in einer solchen Situation sogar zwingend durchbrochen werden.⁴³⁵

Erfüllen Mitarbeiter Straftatbestände, bleibt es dem Arbeitgeber unbenommen, neben der Strafanzeige auch arbeitsrechtliche Maßnahmen zu ergreifen. Je nach Schwere der Tat stellen die ordentliche oder die außerordentliche Kündigung geeignete Sanktionsmittel dar.

⁴³³ Vgl. Besgen/Prinz, in: Besgen/Prinz (o. Fußn. 56), § 1 Rdnrn. 95-97.

⁴³⁴ Zum empfohlenen Verhalten bei Durchsuchungsmaßnahmen siehe Michalke, NJW 2008, 1490-1494.

⁴³⁵ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 111.

5.6 Folgen einer rechtswidrigen Überwachung

Eine unzulässige Überwachung der betrieblichen IuK-Mittel kann empfindliche zivil- und sogar strafrechtliche Konsequenzen für den Arbeitgeber nach sich ziehen⁴³⁶. Diese negativen Folgen werden nachfolgend dargestellt.

5.6.1 Unterlassungsanspruch

Dem Arbeitnehmer steht im Falle einer drohenden erstmaligen oder wiederholten Verletzung seines Persönlichkeitsrechts ein verschuldensunabhängiger Unterlassungsanspruch aus § 823 Abs. 1 i. V. m. § 1004 Abs. 1 S. 2 BGB analog zu⁴³⁷. Das Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts stellt ein „sonstiges Recht“ i. S. d. § 823 Abs. 1 BGB dar⁴³⁸.

Da die allgemeinen und bereichsspezifischen Datenschutzvorschriften Schutzgesetze i. S. d. § 823 Abs. 2 BGB sind, führt ein Verstoß gegen sie gem. §§ 823 Abs. 2, 1004 Abs. 1 S. 2 BGB i. V. m. den verletzten Datenschutznormen ebenfalls zum Anspruch auf Unterlassung⁴³⁹.

Auch dem Betriebsrat steht ein Unterlassungsanspruch zu, wenn der Arbeitgeber gegen das Mitbestimmungsrecht aus § 87 Abs. 1 BetrVG verstoßen hat⁴⁴⁰. Ein solcher Verstoß führt zur individualrechtlichen Unwirksamkeit der Maßnahme; die Arbeitnehmer besitzen in diesem Fall ein Leistungsverweigerungsrecht⁴⁴¹. Darüber hinaus existiert ein

⁴³⁶ Vgl. Mengel (o. Fußn. 102), 2014 (2021).

⁴³⁷ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 152; vgl. Weißnicht (o. Fußn. 157), 448 (451); vgl. Zilkens (o. Fußn. 57), 253 (258).

⁴³⁸ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 152.

⁴³⁹ Vgl. Elschner (o. Fußn. 3), S. 309; vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (137).

⁴⁴⁰ Vgl. Panzer (o. Fußn. 103), S. 299-301.

⁴⁴¹ Vgl. Panzer (o. Fußn. 103), S. 317.

weiterer, jedoch an strengere Voraussetzungen geknüpfter Unterlassungsanspruch des Betriebsrats aus § 23 Abs. 3 BetrVG⁴⁴².

5.6.2 Beseitigungsanspruch

Wurde bereits eine rechtswidrige Überwachung durchgeführt, hat der Arbeitnehmer einen verschuldensunabhängigen Beseitigungsanspruch. Dieser ergibt sich aus § 823 Abs. 1 bzw. 2 i. V. m. § 1004 Abs. 1 S. 1 BGB und erstreckt sich auf die Löschung der erhobenen oder verwendeten Daten bei allen Stellen, die die Daten gespeichert haben.⁴⁴³

Analog dazu hat auch der Betriebsrat einen Beseitigungsanspruch, wenn der Arbeitgeber ein mitbestimmungswidriges Handeln bereits ausgeführt hat⁴⁴⁴.

5.6.3 Löschungsanspruch

Neben den eben aufgezeigten deliktischen Ansprüchen steht dem Arbeitnehmer darüber hinaus ein Anspruch auf Löschung gem. § 35 Abs. 2 Nr. 1 und Nr. 3 BDSG zu, falls eine unzulässige Speicherung der personenbezogenen Daten vorliegt (Nr. 1) oder die Speicherung dadurch unzulässig geworden ist, dass die Daten zur Erfüllung des Zwecks, wofür sie ursprünglich erhoben wurden, nicht mehr erforderlich sind (Nr. 3)⁴⁴⁵.

⁴⁴² Vgl. Panzer (o. Fußn. 103), S. 316 f.

⁴⁴³ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 153; vgl. Weißnicht (o. Fußn. 157), 448 (451); vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (137).

⁴⁴⁴ Vgl. Panzer (o. Fußn. 103), S. 301.

⁴⁴⁵ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 153; vgl. Elschner (o. Fußn. 3), S. 309.

5.6.4 Verwertungsverbot

Hat der Arbeitgeber unzulässige Überwachungsmaßnahmen durchgeführt, gilt nach h. M. für die gewonnenen arbeitnehmerbezogenen Daten ein Verwertungsverbot. Im Ergebnis dürfen keine Beurteilungen, Abmahnungen, Kündigungen oder sonstige personelle Maßnahmen auf Tatsachen gestützt werden, die auf unzulässige Weise erhoben wurden.⁴⁴⁶ Die auf der Grundlage dieser Daten bereits vollzogenen Maßnahmen sind im Rahmen des Beseitigungsanspruchs wieder rückgängig zu machen⁴⁴⁷. Informationen, die jedoch zufällig bei einer rechtmäßigen Datenverwendung durch den Arbeitgeber entdeckt werden, unterliegen nicht dem Verwertungsverbot⁴⁴⁸.

Für Daten, die rechtswidrig ermittelt wurden, besteht darüber hinaus ein prozessuales Beweisverwertungsverbot, sodass sie als Beweismittel z. B. in einem Kündigungsprozess ausscheiden müssen⁴⁴⁹. Eine Berücksichtigung solcher Beweise kommt jedoch möglicherweise dann in Betracht, wenn besondere Umstände – bspw. eine notwehrähnliche Situation – den Eingriff rechtfertigen⁴⁵⁰.

5.6.5 Zurückbehaltungsrecht

Gem. § 273 Abs. 1 i. V. m. § 618 Abs. 1 BGB kann dem Arbeitnehmer ein Leistungsverweigerungsrecht zustehen, wenn seine dienstliche Internet-Nutzung rechtswidrig überwacht wird. Dieses Zurückbehaltungsrecht ergibt sich aus einer unverhältnismäßigen Beeinträchtigung

⁴⁴⁶ Vgl. *Elschner* (o. Fußn. 3), S. 311; vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 271; vgl. *Rath/Karner* (o. Fußn. 35), 446 (449). vgl. *Ernst* (o. Fußn. 53), 585 (587); vgl. *Schönfeld/Strese/Flemming* (o. Fußn. 94), 8 (11).

⁴⁴⁷ Vgl. *Elschner* (o. Fußn. 3), S. 311 f.

⁴⁴⁸ Vgl. *Steidle* (o. Fußn. 105), S. 311.

⁴⁴⁹ Vgl. *Weißnicht* (o. Fußn. 157) 448 (451); vgl. *Elschner* (o. Fußn. 3), S. 312; vgl. *Zilkens* (o. Fußn. 57), 253 (259); vgl. *Barton* (o. Fußn. 66), 305 (312).

⁴⁵⁰ Vgl. *Kömpf/Kunz* (o. Fußn. 155), 1341 (1345).

gung des allgemeinen Persönlichkeitsrechts.⁴⁵¹ Nach überwiegender Ansicht besteht auch dann das Recht auf Arbeitsverweigerung, wenn der Betriebsrat keine Zustimmung nach § 87 Abs. 1 Nr. 6 BetrVG zum Betreiben des Internet-Arbeitsplatzes bzw. des Unternehmensnetzwerkes erteilt hat⁴⁵². Nimmt ein Arbeitnehmer sein Zurückbehaltungsrecht wahr, bleibt der Anspruch auf Zahlung des Arbeitsentgelts gem. § 615 BGB unberührt⁴⁵³.

Nach h. M. resultiert aus einer unzulässigen Überwachung, die nur die Privatnutzung des Internets erfasst, kein Leistungsverweigerungsrecht, da das Erbringen der geschuldeten Arbeitsleistung hiervon nicht betroffen ist⁴⁵⁴.

5.6.6 Schadenersatzansprüche

Arbeitnehmern kann Anspruch auf Schadenersatz aus § 823 Abs. 1, 2 BGB sowie § 280 Abs. 1 BGB wegen einer Verletzung der Schutzpflichten des Arbeitgebers aus § 618 Abs. 1 BGB zustehen⁴⁵⁵. Als weitere Anspruchsgrundlagen sind § 7 BDSG und § 44 TKG zu benennen⁴⁵⁶. Der Anspruch kommt nur in Betracht, sofern der Arbeitgeber schuldhaft gehandelt hat und dem Arbeitnehmer ein materieller Schaden entstanden ist⁴⁵⁷.

Ein Anspruch auf Ersatz eines immateriellen Schadens aus § 253 Abs. 2 BGB analog kann sich ergeben, wenn die unzulässige Datenverar-

⁴⁵¹ Vgl. *Elschner* (o. Fußn. 3), S. 310 f.

⁴⁵² Vgl. *Elschner* (o. Fußn. 3), S. 311; vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (138).

⁴⁵³ Vgl. *Elschner* (o. Fußn. 3), S. 311.

⁴⁵⁴ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 156; vgl. *Elschner* (o. Fußn. 3), S. 311; vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (137 f).

⁴⁵⁵ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 154; vgl. *Elschner* (o. Fußn. 3), S. 310.

⁴⁵⁶ Vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (137).

⁴⁵⁷ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 154.

beitung eine schwerwiegende Beeinträchtigung des Persönlichkeitsrechts darstellt. Weitere Voraussetzung ist, dass die Wiedergutmachung nicht durch Unterlassung, Löschung oder Rückgängigmachung von Maßnahmen, die auf die aus der Überwachung gewonnenen Erkenntnisse gestützt wurden, erreicht werden kann. Man wird davon ausgehen können, dass bei einer systematischen und vollständigen Überwachung und Auswertung des Internet-Verkehrs sowie bei der Einsichtnahme in private E-Mails die Voraussetzungen für den Anspruch erfüllt sind.⁴⁵⁸

5.6.7 Strafbarkeit

Die Strafbarkeit des Arbeitgebers kann sich aus verschiedenen Tatbeständen ergeben: Es könnte zunächst die Verletzung des Briefgeheimnisses, § 202 StGB, in Frage stehen. Dazu müsste allerdings das Öffnen eines verschlossenen Schriftstücks vorliegen. Die Vorschrift dient dem Schutz verkörperter Schriftstücke. Sie kann auch aufgrund des dem Strafrecht immanenten Analogieverbots nicht auf E-Mails erweitert werden, weshalb die Tatbestandsvoraussetzungen nicht erfüllt sind. Selbst wenn die E-Mail-Nachricht ausgedruckt wird, also eine Verkörperung stattfindet, fehlt es am Merkmal des Verschlössenseins, da nun jeder Dritte von der ausgedruckten Nachricht Kenntnis nehmen kann.⁴⁵⁹

Im Folgenden werden einschlägige Straftatbestände dargestellt.

⁴⁵⁸ Vgl. *Elschner* (o. Fußn. 3), S. 310.

⁴⁵⁹ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 158; vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (138); vgl. *Nägele/Meyer* (o. Fußn. 34), 312 (315); vgl. *Panzer* (o. Fußn. 103), S. 311 f.; vgl. *Mattl* (o. Fußn. 21), S. 160.

5.6.7.1 Ausspähen von Daten

Aufgrund dieser Lücke im Gesetz wurde nachträglich § 202a ins StGB eingefügt, der sich auf den Begriff der nicht unmittelbar wahrnehmbaren Daten bezieht. Nach § 202a StGB macht sich strafbar, wer unbefugt sich oder einem anderen Daten verschafft, die nicht für ihn bestimmt und die gegen einen unberechtigten Zugang besonders gesichert sind. Das Vorliegen privater Korrespondenz und mithin die fehlende Bestimmung für den Arbeitgeber kann bspw. durch den Betreff einer E-Mail, die angehängten Dateien oder über den Absender erkennbar sein. Eine ausreichende Sicherung vor unberechtigtem Zugang kann angenommen werden, wenn Vorkehrungen getroffen wurden, welche objektiv geeignet und subjektiv - nach dem Willen des Berechtigten - dazu bestimmt sind, den Zugang zu den Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Dies ist z. B. dann der Fall, wenn dem Arbeitnehmer ein separater passwortgeschützter E-Mail-Account für die Privatnutzung zur Verfügung gestellt wird.⁴⁶⁰ Vor der Einfügung des § 202c StGB galt es als umstritten, ob sich der Arbeitgeber nach § 202a StGB strafbar macht, wenn er durch Passwort geschützte Privatdateien eines Arbeitnehmers auf dem betrieblichen Computer in Augenschein nimmt⁴⁶¹. Eine Klarstellung enthält § 202c StGB: Nach diesem ist bereits das Vorbereiten einer Straftat nach § 202a StGB strafbar, wenn sich Personen dazu Passwörter oder andere Sicherungscodes, die den Zugang zu den Daten ermöglichen, verschaffen.

⁴⁶⁰ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 159 f.; vgl. *Nägele/Meyer* (o. Fußn. 34), 312 (315); vgl. *Mattl* (o. Fußn. 21), S. 161-163.

⁴⁶¹ Damals zweifelnd *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (138); bejahend *Weißgerber*, NZA 2003, 1005 (1007-1009); verneinend *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 160.

5.6.7.2 Abfangen von Daten

Gem. § 202b StGB macht sich strafbar, wer sich unbefugt mithilfe technischer Mittel nicht für ihn bestimmte Daten aus einer nicht-öffentlichen Datenübertragung verschafft. Als Tatobjekt kommen nur Daten in Frage, die sich in einem Übermittlungsvorgang befinden. Beim Tatbestandsmerkmal „Nichtöffentlichkeit“ ist auf die Art des Übertragungsvorgangs abzustellen. Auch ansonsten öffentlich zugängliche Informationen können durch eine Internet-Übertragung nicht-öffentlich sein. Zur Tatbestandsverwirklichung ist es außerdem nicht notwendig, dass die Daten gespeichert bzw. aufgezeichnet werden. Bei der E-Mail-Kommunikation bspw. reicht die bloße Kenntnisnahme aus. Technische Mittel i. S. d. Vorschrift stellen u. a. Passwörter und Software dar.⁴⁶² In § 202c StGB ist das Vorbereiten einer Straftat nach § 202b StGB geregelt.

5.6.7.3 Verletzung des Fernmeldegeheimnisses

Erlaubt der Arbeitgeber eine Privatnutzung der betrieblichen IuK-Architektur, so unterliegt sie nach § 88 TKG und § 206 StGB dem Fernmeldegeheimnis. Das Fernmeldegeheimnis schützt durch § 206 Abs. 5 S. 2, 3 StGB den Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an dem Telekommunikationsvorgang beteiligt war oder ist. Aber auch erfolglose Verbindungsversuche werden vom Fernmeldegeheimnis erfasst.⁴⁶³

§ 206 Abs. 1 StGB bietet Schutz gegen die unbefugte Mitteilung von Tatsachen an andere Personen. Da es an einer Mitteilung an andere Personen mangelt, falls der Arbeitgeber lediglich eine Inhaltskontrolle der E-Mails seiner Mitarbeiter vornimmt, drohen strafrechtliche Sank-

⁴⁶² Vgl. *BT-Drs.* 16/3656, S. 11.

⁴⁶³ Vgl. *Mattl* (o. Fußn. 21), S. 163 f.; vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 161.

tionen erst, sobald der Arbeitgeber andere Personen über dem Fernmeldegeheimnis unterliegende Informationen in Kenntnis setzt. Der Strafbarkeit entgeht der Arbeitgeber nur dann, wenn die Mitarbeiter vorab eine entsprechende Einwilligung erteilt haben oder der Arbeitgeber sich durch Nichtanzeige geplanter Straftaten nach § 138 StGB selbst strafbar machte.⁴⁶⁴ Notwehr nach § 32 StGB oder rechtfertigender Notstand nach § 34 StGB können als Rechtfertigungsgründe für einen Eingriff in das Fernmeldegeheimnis nicht dienen⁴⁶⁵. Es existieren lediglich zwei Möglichkeiten, Kontrollmaßnahmen in Bezug auf Telekommunikationsaktivitäten der Arbeitnehmer auszuführen, ohne dabei das strafrechtlich geschützte Fernmeldegeheimnis zu verletzen: Entweder der Arbeitgeber selbst überwacht seine Mitarbeiter und gibt keine Informationen darüber an Dritte weiter, oder aber er verbietet generell die Privatnutzung der elektronischen Medien, denn in diesem Fall ist er zur Wahrung des Fernmeldegeheimnisses erst gar nicht verpflichtet⁴⁶⁶.

In der betrieblichen Praxis werden häufig spezielle Filterprogramme eingesetzt, durch die der unternehmenseigene Server ankommende E-Mails auf potenzielle Viren untersucht und ferner prüft, ob es sich bei den Nachrichten um Spam-Mails handelt, um sie in beiden Fällen sofort zu löschen, die Verbindung zu unterbrechen oder die Nachricht auszufiltern⁴⁶⁷. Ein solches Vorgehen ist regelmäßig strafbar nach § 206 Abs. 2 Nr. 2 StGB und nach § 303a StGB.

Wer als Inhaber oder Beschäftigter eines geschäftsmäßig Telekommunikationsdienste erbringenden Unternehmens eine dem Unternehmen anvertraute Sendung unbefugt unterdrückt, macht sich gem. § 206 Abs. 2 Nr. 2 StGB strafbar. Das Filtern und Blockieren von E-Mails,

⁴⁶⁴ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 161 f.; vgl. Mattl (o. Fußn. 21), S. 163-167; vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 71), 135 (138).

⁴⁶⁵ Vgl. Busse, in: Besgen/Prinz (o. Fußn. 114), § 10 Rdnr. 162.

⁴⁶⁶ Vgl. Mattl (o. Fußn. 21), S. 167.

⁴⁶⁷ Vgl. Lelley, in: Worzalla, S. 35 Rdnr. 84.

die sich nach ihrem Empfang auf dem Unternehmensserver befinden, erfüllt die Voraussetzungen der Norm, falls das Unternehmen eine Privatnutzung des E-Mail-Anschlusses gestattet.⁴⁶⁸ Das Tatbestandsmerkmal des unbefugten Handelns kann durch eine Einwilligung der Mitarbeiter ausgeschlossen werden⁴⁶⁹. Ein Muster einer solchen Einwilligung ist im Anhang enthalten (Anlage 8). Nur bei der Löschung von virenbehafteten E-Mails kann – ohne vorab erteilte Einwilligung der Mitarbeiter – evtl. davon ausgegangen werden, dass die Arbeitnehmer ihr Einverständnis zur Entfernung erteilt hätten⁴⁷⁰. Die Mitarbeiter müssen bei einer solchen Vorgehensweise vorab informiert werden. Auch der unterbundene Zustellungsversuch von virenverseuchten E-Mails muss ihnen mitgeteilt werden.⁴⁷¹ Als weiteren Rechtfertigungsgrund zur Löschung von E-Mails, die Viren, Trojaner oder sonstige Schadprogramme enthalten, zählt § 109 Abs. 1 TKG, nach dem der Arbeitgeber, der die Privatnutzung zumindest duldet, geeignete technische Schutzmaßnahmen zu treffen hat, welche Störungen und Schäden an der TK-Anlage verhindern sollen. Dies gilt jedoch nicht für Spam-Mails. Unerwünschte Werbe-Mails greifen nicht in den Betrieb des TK-Systems selbst ein, wie es bei Viren der Fall ist. Ferner besteht die Möglichkeit, dass der Arbeitnehmer Interesse am Inhalt von Spam-Mails hat.⁴⁷²

5.6.7.4 Datenveränderung

Besonders brisant ist die Vorschrift des § 303a Abs. 1 StGB, bei der die Verwirklichung der Tatbestandsvoraussetzungen auch dann zur Strafbarkeit führt, wenn die Privatnutzung ausdrücklich untersagt wurde; die Unterdrückung bzw. Löschung von E-Mails erfüllt die Tatbe-

⁴⁶⁸ Vgl. *Heidrich/Tschoepe*, MMR 2004, 75 (76-78).

⁴⁶⁹ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 166.

⁴⁷⁰ Vgl. *Schmidl*, DuD 2005, 267-271.

⁴⁷¹ Vgl. *Hoeren*, NJW 2004, 3513 (3516 f.).

⁴⁷² Vgl. *Schmidl*, MMR 2005, 343 (344); vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 168.

standsmerkmale. Die Strafbarkeit lässt sich, wie bereits in den Ausführungen zu § 206 Abs. 2 Nr. 2 StGB aufgezeigt, durch besondere Rechtfertigungsgründe oder die Einwilligung der Arbeitnehmer ausschließen.⁴⁷³ Schutzgut in §303a StGB ist die Verfügungsbefugnis des Empfängers⁴⁷⁴.

5.6.7.5 Sonstige Straftatbestände

Im Übrigen kommt eine Strafbarkeit des Arbeitgebers aus §§ 44 i. V. m. 43 Abs. 2 BDSG in Betracht⁴⁷⁵. Diese setzt eine vorsätzliche Handlung gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht gegen das Bundesdatenschutzgesetz voraus⁴⁷⁶. Für den Bereich der Internet- und E-Mail-Überwachung dürfte diese Strafvorschrift jedoch kaum einschlägig sein⁴⁷⁷.

5.6.8 Ordnungswidrigkeit

Ordnungswidrigkeiten im Bereich des Bundesdatenschutzgesetzes ergeben sich durch Verstöße gegen Verfahrensregeln aus § 43 Abs. 1 BDSG und durch die unzulässige Erhebung oder Verarbeitung personenbezogener Daten aus § 43 Abs. 2 BDSG⁴⁷⁸. Die Höhe des Bußgeldes beträgt gem. § 43 Abs. 3 BDSG für Verstöße, die in Abs. 1 aufgeführt sind, bis zu 25.000 Euro, für Verstöße aus Abs. 2 bis zu 250.000 Euro.

Das Telekommunikationsgesetz enthält in § 149 TKG Bußgeldvorschriften; auf die Themenstellung bezogen sind § 149 Abs. 1 Nr. 16

⁴⁷³ Vgl. *Lelley*, in: *Worzalla*, S. 38 Rdnrn. 91-94; vgl. *Schmidl* (o. Fußn. 472), 343 (346).

⁴⁷⁴ Vgl. *Schmidl* (o. Fußn. 472), 343 (346).

⁴⁷⁵ Vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (138).

⁴⁷⁶ Vgl. *Busse*, in: *Besgen/Prinz* (o. Fußn. 114), § 10 Rdnr. 171.

⁴⁷⁷ Vgl. *Panzer* (o. Fußn. 103), S. 296.

⁴⁷⁸ Vgl. *Panzer* (o. Fußn. 103), S. 294 f.; vgl. *Altenburg/v. Reinersdorff/Leister* (o. Fußn. 71), 135 (138).

und Nr. 17 TKG von Relevanz. Eine Ordnungswidrigkeit liegt demnach vor, wenn entgegen § 95 Abs. 2 oder § 96 Abs. 2 S. 1 oder Abs. 3 S. 1 TKG Daten verwendet oder entgegen § 96 Abs. 2 S. 2 oder § 97 Abs. 3 S. 2 TKG Daten nicht oder nicht rechtzeitig gelöscht werden. Gem. § 149 Abs. 2 TKG droht hierbei eine Geldbuße mit bis zu 300.000 Euro.⁴⁷⁹

Auch im Telemediengesetz sind mit § 16 TMG Bußgeldvorschriften verankert. Die durch § 16 Abs. 2 Nr. 2 und Nr. 5 TMG erfassten Ordnungswidrigkeitstatbestände können für die Kontrolle der Internet- und E-Mail-Aktivitäten der Arbeitnehmer von Belang sein. § 16 Abs. 3 TMG bestimmt die Höhe des Bußgeldes mit bis zu 50.000 Euro.

5.7 Rechte der Arbeitnehmer bei Verwendung personenbezogener Daten durch den Arbeitgeber

Mitarbeiter besitzen gegenüber ihrem Arbeitgeber Benachrichtigungs- und Auskunftsansprüche sowie ggf. einen Anspruch auf Berichtigung, Löschung und Sperrung von Daten, falls ihre personenbezogenen Daten verwendet werden. Diese Rechte ergeben sich aus den §§ 33 bis 35 BDSG und sollen dem Betroffenen adäquate Informationen über seine Daten bereitstellen und ihm, falls erforderlich, Rechte zu deren Korrektur einräumen⁴⁸⁰.

Nach § 33 Abs. 1 S. 1 BDSG sind die Mitarbeiter über die Internet- und E-Mail-Kontrollen zu benachrichtigen⁴⁸¹. Diese Benachrichtigung hat grundsätzlich vor jeder erstmaligen Speicherung personenbezogener Daten zu erfolgen. Dies gilt nicht bei Vorliegen eines der in § 33 Abs. 2 BDSG aufgeführten Ausnahmetatbestände. Eine Benachrichtigung ist

⁴⁷⁹ Vgl. *Mattl* (o. Fußn. 21), S. 168.

⁴⁸⁰ Vgl. *Däubler*, NZA 2001, 874 (880); vgl. *Schönfeld/Strese/Flemming* (o. Fußn. 94), 8 (10).

⁴⁸¹ Vgl. *Ernst* (o. Fußn. 53), 585 (591); vgl. *Nägele/Meyer* (o. Fußn. 34), 312 (315).

gem. § 33 Abs. 2 Nr. 7b BDSG nicht notwendig, wenn die Daten für eigene Zwecke gespeichert sind, und die Benachrichtigung die Geschäftszwecke erheblich gefährden würde. Ein solcher Fall ist anzunehmen, wenn der Arbeitgeber Überwachungsmaßnahmen durchführen will, um einen erwiesenen Geheimnisverrat durch Mitarbeiter aufzudecken. Die Bekanntgabe, dass entsprechende Kontrollen durchgeführt werden, würde höchstwahrscheinlich dazu führen, dass die betreffenden Mitarbeiter wichtiges Beweismaterial vernichteten.⁴⁸² Für telekommunikationsbezogene Dienste verdrängt die Informationspflicht des § 93 TKG die Benachrichtigungspflicht des § 33 BDSG⁴⁸³.

§ 34 BDSG enthält Regelungen über die Auskunftsrechte der Betroffenen. Durch § 34 Abs. 1 BDSG ist festgelegt, dass der Mitarbeiter im Grundsatz einen Anspruch darauf hat, u. a. zu erfahren, welche Daten der Arbeitgeber über ihn gespeichert hat und zu welchem Zweck die Speicherung erfolgte. Wichtig in diesem Zusammenhang ist ferner, dass § 34 BDSG ein unabdingbares Recht i. S. v. § 6 Abs. 1 BDSG darstellt, das nicht durch ein Rechtsgeschäft oder gar eine Betriebsvereinbarung beschränkt oder ausgeschlossen werden kann.⁴⁸⁴

Die Berichtigung unrichtiger personenbezogener Daten schreibt § 35 Abs. 1 BDSG vor. Als notwendig erweist sich der Berichtigungsanspruch deshalb, weil die Speicherung falscher personenbezogener Daten das informationelle Selbstbestimmungsrecht der Arbeitnehmer verletzen kann. § 35 Abs. 2 BDSG enthält einen Anspruch auf Löschung der Daten, falls einer der enumerativ aufgezählten Sachverhalte vorliegt. Gem. § 35 Abs. 3 BDSG sind die Daten zu sperren anstatt zu löschen, wenn bestimmte Aufbewahrungsfristen der Löschung entgegenstehen oder eine Beeinträchtigung schutzwürdiger Interessen zu befürchten oder eine Löschung aufgrund der besonderen Art der Speicherung nicht oder nur mit einem unverhältnis-

⁴⁸² Vgl. Erler (o. Fußn. 18), S. 102.

⁴⁸³ Vgl. Büttgen, in: Beck'scher TKG-Kommentar (o. Fußn. 282), § 93 Rdnr. 7.

⁴⁸⁴ Vgl. Erler (o. Fußn. 18), S. 101 f.

mäßigen Aufwand zu bewerkstelligen wäre.⁴⁸⁵ Auch § 35 BDSG verkörpert ein unabdingbares Recht i. S. v. § 6 Abs. 1 BDSG.

Weiterhin besteht das Recht des Arbeitnehmers auf Einsicht in die Personalakte gem. § 83 Abs. 1 BetrVG⁴⁸⁶. Somit ist es dem Arbeitnehmer möglich, die über ihn durch Überwachungsmaßnahmen gesammelten und festgehaltenen Daten zur Kenntnis zu nehmen.

⁴⁸⁵ Vgl. Steidle (o. Fußn. 105), S. 326 f.

⁴⁸⁶ Vgl. Steidle (o. Fußn. 105), S. 326; vgl. Tinnefeld/Viethen (o. Fußn. 218), 977 (982); vgl. Schönfeld/Strese/Flemming (o. Fußn. 94), 8 (10).

6 BETRIEBSVERFASSUNGSRECHTLICHE ASPEKTE

Der Gültigkeitsbereich des Betriebsverfassungsgesetzes erstreckt sich grundsätzlich auf alle privatwirtschaftlichen Betriebe⁴⁸⁷. Die Intention des Gesetzes besteht darin, eine vertrauensvolle Zusammenarbeit zwischen Arbeitgeber und Arbeitnehmervertretung, einschließlich ihrer jeweiligen Verbände, zu ermöglichen und zu fördern. Darüber hinaus soll eine Entschärfung des dem Arbeitsverhältnis innewohnenden Kräfteungleichgewichts dadurch erfolgen, dass Arbeitgeber in ihren Rechten insoweit beschränkt werden, als es für den Persönlichkeits- und sozialen Schutz der Arbeitnehmer notwendig erscheint.⁴⁸⁸

Gem. § 1 Abs. 1 BetrVG werden in Betrieben mit in der Regel wenigstens fünf ständig wahlberechtigten Arbeitnehmern – von denen drei wählbar sind – Betriebsräte gewählt. Die Wahl des Betriebsrats liegt im freien Ermessen der Arbeitnehmer, obgleich der Wortlaut dieser Vorschrift nahe legt, es handle sich um eine betriebsverfassungsrechtliche Pflicht⁴⁸⁹. Aufgabe des Betriebsrats ist, die Interessen der Arbeitnehmer gegenüber dem Arbeitgeber zu vertreten und durchzusetzen.

Ganz allgemein stehen dem Kollektivorgan folgende Beteiligungsrechte in betrieblichen Angelegenheiten zu:

- Unterrichtsrechte (z. B. §§ 80 Abs. 2 S. 1, 99, 102, 111 BetrVG),
- Anhörungs- und Vorschlagsrechte (z. B. §§ 92 Abs. 2, 102 BetrVG),

⁴⁸⁷ Vgl. ErfK/*Eisemann* § 1 BetrVG Rdnr. 6.

⁴⁸⁸ Vgl. *Scholz*, Personalmanagement, 5. Aufl. (2000), S. 176.

⁴⁸⁹ Vgl. *Besgen*, in: Beck'scher Online-Kommentar Arbeitsrecht, BetrVG, (Ed. 7, Stand: 1.3.2008), § 1 Rdnr. 2.

- Beratungsrechte (z. B. §§ 90 Abs. 2, 111 BetrVG) und
- Mitbestimmungsrechte (z. B. Zustimmungsverweigerungsrechte § 99 BetrVG, Zustimmungserfordernisse bzw. Initiativrechte §§ 87 Abs. 1, 103 BetrVG)⁴⁹⁰.

Wie bereits in Kapitel 5 aufgezeigt wurde, bewegen sich Kontrollmaßnahmen in einem engen gesetzlichen Rahmen. Existiert ein Betriebsrat, so hat der Arbeitgeber – neben den bereits aufgezeigten verfassungs- und datenschutzrechtlichen Grenzen – zusätzlich Beteiligungsrechte des Betriebsrats zu beachten⁴⁹¹.

Im Hinblick auf die Überwachung des Internet- und E-Mail-Verkehrs des Betriebsrats als Institution mit Sonderstatus konnte bereits in Kapitelunterpunkt 5.4 dargelegt werden, dass der Betriebsrat durch den Arbeitgeber nicht kontrolliert werden darf. Aufgrund dessen, dass die Überwachung als eine unzulässige Behinderung i. S. d. § 78 S. 1 BetrVG zu qualifizieren und überdies als eine Störung des Vertrauensverhältnisses zwischen Belegschaft und Mitarbeitervertretung anzusehen ist, darf eine Protokollierung und Auswertung der Betriebsratkommunikation nicht vollzogen werden⁴⁹².

Die wichtigsten betriebsverfassungsrechtlichen Aspekte, die im Kontext der Internet- und E-Mail-Überwachung stehen, werden nachfolgend beleuchtet.

6.1 Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG

Im Zusammenhang mit der Einführung und Anwendung von elektronischen Informations- und Kommunikationsmitteln im Betrieb

⁴⁹⁰ Vgl. ErfK/*Eisemann* § 1 BetrVG Rdnr. 18.

⁴⁹¹ Vgl. *Panzer* (o. Fußn. 103), S. 193.

⁴⁹² Vgl. *Elschner* (o. Fußn. 3), S. 297.

nimmt § 87 Abs. 1 Nr. 6 BetrVG die bedeutsamste Stellung ein⁴⁹³. Dieses Mitbestimmungsrecht dient dem Persönlichkeitsschutz der Arbeitnehmer. Es stellt insoweit eine konkrete Ausgestaltung des in § 75 Abs. 2 BetrVG verankerten allgemeinen Arbeitnehmerpersönlichkeitsrechts dar, wonach Arbeitgeber und Betriebsrat die freie Persönlichkeitsentfaltung der Arbeitnehmer zu schützen und zu fördern haben⁴⁹⁴.

Gem. § 87 Abs. 1 Nr. 6 BetrVG verfügt der Betriebsrat bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, ein Mitbestimmungsrecht. Dieses Mitbestimmungsrecht kommt allerdings nur dann zum Tragen, wenn keine gesetzliche und tarifliche Regelung besteht. Die Öffnungsklausel des § 4 Abs. 1 BDSG erlaubt eine vom Bundesdatenschutzgesetz abweichende Reglementierung durch eine Betriebsvereinbarung.⁴⁹⁵ Nur für die erlaubte Privatnutzung der elektronischen Kommunikationsmedien muss – selbst für den Fall, dass eine diesbezügliche Betriebsvereinbarung vorliegt – eine Einwilligung der Arbeitnehmer in Kontrollmaßnahmen eingeholt werden, da das Telekommunikationsgesetz keine entsprechende Öffnungsklausel enthält⁴⁹⁶. § 87 Abs. 1 Nr. 6 BetrVG greift auch dann, wenn eine schon bestehende technische Einrichtung geändert, erweitert oder ergänzt wird und sich somit ihre Anwendung anders gestaltet⁴⁹⁷.

Der Begriff „technische Einrichtung“ ist nach dem BAG und der h. M. weit zu fassen: Zu verstehen sind darunter optische, mechanische, elektronische, akustische und sonstige Geräte, die ein bestimmtes Maß

⁴⁹³ Vgl. *Weißgerber* (o. Fußn. 98), S. 39; vgl. *Weißnicht* (o. Fußn. 157), 448 (452).

⁴⁹⁴ Vgl. *Panzer* (o. Fußn. 103), S. 194.

⁴⁹⁵ Vgl. *Altenburg/v. Reinersdorff/Leister*, MMR 2005, 222 (223).

⁴⁹⁶ Vgl. *Elschner* (o. Fußn. 3), S. 307; vgl. *Altenburg/v. Reinersdorff/Leister*, (o. Fußn. 495), 222 (223).

⁴⁹⁷ Vgl. *Däubler* (o. Fußn. 26), § 4 Rdnr. 292; vgl. *Böker/Kamp*, Betriebliche Nutzung von Internet, Intranet und E-Mail, 2003, S. 79.

an Vergegenständlichung aufweisen. Internet-Arbeitsplätze weisen die geforderte Vergegenständlichung auf, da neben der erforderlichen Software – welche zweifelsohne keine ausreichende Vergegenständlichung realisiert – verschiedene Hardwarekomponenten benötigt werden. Insofern ist auf das Gesamtsystem abzustellen.⁴⁹⁸

Dem Überwachungsbegriff lassen sich Vorgänge unterordnen, die der Gewinnung von Informationen über Verhalten und Leistung von Mitarbeitern dienen und regelmäßig aufgezeichnet werden, um sie letztendlich der menschlichen Wahrnehmung zugänglich zu machen und/oder auszuwerten⁴⁹⁹. Anhand der anfallenden Internet- und E-Mail-Protokolle ist unstrittig eine Überwachung möglich⁵⁰⁰.

Der Wortlaut der Vorschrift legt nahe, dass sie darauf abstellt, dass die Überwachung tatsächlich vollzogen oder mindestens beabsichtigt wird. Der Begriff des Bestimmtheits ist jedoch sehr weit auszulegen: Es genügt, wenn durch das System allein objektiv die Möglichkeit besteht, die Arbeitnehmer zu überwachen.⁵⁰¹ Diese Möglichkeit ist schon beim Einsatz herkömmlicher Programme zur Nutzung des Internet- oder E-Mail-Dienstes gegeben; dazu bedarf es keiner speziellen Überwachungssoftware⁵⁰². Das Mitbestimmungsrecht besteht jedoch nicht, falls der Arbeitgeber technische Anlagen einführt oder anwendet, die ausschließlich anonyme Daten erheben⁵⁰³.

Der Überwachungsgegenstand muss weiterhin das Verhalten oder die Leistung der Arbeitnehmer sein. Unter Verhalten versteht man jedes

⁴⁹⁸ Vgl. Besgen/Prinz, in: Besgen/Prinz, Neue Medien und Arbeitsrecht, § 2 Rdnr. 3; vgl. Hanau/Hoeren (o. Fußn. 12), S. 78.

⁴⁹⁹ Vgl. Hanau/Hoeren (o. Fußn. 12), S. 78 f.; vgl. Altenburg/v. Reinersdorff/Leister (o. Fußn. 495), 222 (223); vgl. Elschner (o. Fußn. 3), S. 305.

⁵⁰⁰ Vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1500).

⁵⁰¹ Vgl. Schönfeld/Strese/Flemming (o. Fußn. 94), 8 (12); vgl. Nägele/Meyer (o. Fußn. 34), 312 (315); vgl. Hanau/Hoeren (o. Fußn. 12), S. 85.

⁵⁰² Vgl. Besgen/Prinz, in: Besgen/Prinz (o. Fußn. 498), § 2 Rdnrn. 4-7; vgl. Beckschulze/Henkel (o. Fußn. 61), 1491 (1500); vgl. Weißnicht (o. Fußn. 157), 448 (452).

⁵⁰³ Vgl. Weißnicht (o. Fußn. 157), 448 (452).

Tun und Unterlassen mit Relevanz zur Erfüllung der Arbeitsaufgabe. Insoweit wird die Leistung bereits vom Verhalten erfasst. Notwendig ist in diesem Zusammenhang nur, dass sich einzelne Verhaltensweisen bestimmten Mitarbeitern zuordnen lassen. Unmöglich ist dies etwa bei einem Internet-Terminal, den zehn verschiedene Mitarbeiter unter derselben Nutzerkennung bedienen können.⁵⁰⁴

Im Ergebnis erfüllt die Einführung und Anwendung des Internet- und E-Mail-Dienstes die Voraussetzungen des § 87 Abs. 1 Nr. 6 BetrVG, sodass ein Mitbestimmungsrecht besteht. Wie die Wahrnehmung dieses Rechts konkret aussehen kann, wird im nachfolgenden Kapitelunterpunkt behandelt.

6.2 Ausübung der Mitbestimmung

Der Betriebsrat hat im Rahmen der Mitbestimmung die Persönlichkeitssphäre der Arbeitnehmer durch präventive Maßnahmen zu schützen⁵⁰⁵. Das Mitbestimmungsrecht wird in den meisten Fällen durch den Abschluss einer Betriebsvereinbarung wahrgenommen⁵⁰⁶. Die Betriebsvereinbarung ist ein privatrechtlicher kollektiver Normenvertrag zwischen Arbeitgeber und Betriebsrat, der unmittelbar und zwingend auf die Arbeitsverhältnisse einwirkt⁵⁰⁷. Gem. § 77 Abs. 2 BetrVG sind Betriebsvereinbarungen gemeinsam zu beschließen, schriftlich niederzulegen, von beiden Parteien zu unterzeichnen und im Betrieb an geeigneter Stelle auszulegen.

Eine Betriebsvereinbarung zur Internet- und E-Mail-Nutzung im Unternehmen dient dazu, konkrete Vorschriften für den Umfang und die

⁵⁰⁴ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 498), § 2 Rdnr. 8; vgl. *Hanau/Hoeren* (o. Fußn. 12), S. 81.

⁵⁰⁵ Vgl. *Sassenberg/Bamberg* (o. Fußn. 258), 226.

⁵⁰⁶ Vgl. *Nägele/Meyer* (o. Fußn. 34), 312 (315).

⁵⁰⁷ Vgl. *Lelley*, in: *Worzalla*, S. 64 Rdnr. 159.

Grenzen der Inanspruchnahme aufzustellen. Überdies sollten unbedingt klare Regelungen im Hinblick auf die Erfassung und Auswertung von Protokollen durch den Arbeitgeber enthalten sein.⁵⁰⁸ Darüber hinaus ist anzuraten, auch Fragen zur Sicherheit des betrieblichen Netzwerks zu klären, Abwesenheitsregelungen festzulegen, den Umgang mit Verschlüsselungstechnik zu regeln und – falls bspw. eine gelegentliche Privatnutzung toleriert wird – auf einen maßvollen Umgang mit den Medien hinzuweisen.⁵⁰⁹

Über weitgehende Rechte verfügt der Betriebsrat, falls die Einführung der Internet- und E-Mail-Technik im Betrieb ohne bzw. gegen seine Zustimmung erfolgt: In diesem Fall steht ihm ein Unterlassungsanspruch zu, mit dem sich die rechtswidrige Installation unterbinden lässt. Wurden bereits entsprechende Techniken eingerichtet, steht der Mitarbeitervertretung ein Beseitigungsanspruch zu, mit dem sie sogar den Abbau der Anlage zu erzwingen vermag. Kann in Bezug auf die Einführung und Anwendung der technischen Anlagen keine Einigung erzielt werden, ist nach § 87 Abs. 2 BetrVG die Einigungsstelle anzurufen.⁵¹⁰

Das Mitbestimmungsrecht des Betriebsrats gilt jedoch nicht schrankenlos. Die zulässige Grenze ist erreicht, sobald in Persönlichkeitsrechte der Arbeitnehmer eingegriffen wird.⁵¹¹ So wäre es z. B. nicht mit § 75 Abs. 2 BetrVG zu vereinbaren, eine Betriebsvereinbarung abzuschließen, die eine Vollkontrolle des Internet- und E-Mail-Verkehrs der Belegschaft vorsähe.

⁵⁰⁸ Vgl. *Elschner* (o. Fußn. 3), S. 306 f.

⁵⁰⁹ Vgl. *Schönfeld/Strese/Flemming* (o. Fußn. 94), 8 (12).

⁵¹⁰ Vgl. *Besgen/Prinz*, in: *Besgen/Prinz* (o. Fußn. 498), § 2 Rdnrn. 23-25; vgl. *Weißnicht* (o. Fußn. 157), 448 (452).

⁵¹¹ Vgl. *Beckschulze/Henkel* (o. Fußn. 61), 1491 (1501); vgl. *Ernst* (o. Fußn. 53), 585 (591).

7 RECHTSPRECHUNG

Im jüngsten Urteil vom 31.5.2007⁵¹² zu einer verhaltensbedingten Kündigung wegen privater Internet-Nutzung stützt sich das BAG auf drei frühere Entscheidungen⁵¹³, bei denen es Grundsätze zur privaten Internet-Nutzung aufgestellt und diese mit dem aktuellen Urteil bekräftigt hat. Die in den Entscheidungen wiederholten kündigungsrelevanten Pflichtverletzungen, welche durch die Privatnutzung des Internets in Betracht kommen, sind insbesondere:

- Die Nichteinhaltung eines bestehenden ausdrücklichen Verbots zur privaten Inanspruchnahme des Internet-Anschlusses bzw. der IT-Architektur;
- die Privatnutzung des Internets während der Arbeitszeit.⁵¹⁴ Die Verletzung der arbeitsvertraglich geschuldeten Arbeitspflicht des Arbeitnehmers ist umso gravierender, je mehr er zeitlich und inhaltlich seine Arbeit vernachlässigt⁵¹⁵;
- das unbefugte Herunterladen erheblicher Datenmengen aus dem Internet auf den Dienst-Computer⁵¹⁶;
- der Gebrauch des Internet-Anschlusses zu privaten Zwecken an sich. Wenn diesbezüglich keine ausdrückliche Gestattung oder zumindest Duldung vorliegt, ist die private Inanspruchnahme grundsätzlich unzulässig und stellt demzufolge eine Verletzung der arbeitvertraglichen Pflichten dar.⁵¹⁷

Im in Rede stehenden Urteil geht es im Sachverhalt um einen verheirateten und zwei Kindern zum Unterhalt verpflichteten Baulei-

⁵¹² BAG, Urt. v. 31.5.2007 = NZA 2007, 922 = NJW 2007, 2653.

⁵¹³ BAG, Urt. v. 7.7.2005 = NZA 2006, 98 = NJW 2006, 540; BAG, Urt. v. 12.1.2006 = NZA 2006, 980 = NJW 2006, 2510; BAG, Urt. v. 27.4.2006 = NZA 2006, 977 = NJW 2006, 2939.

⁵¹⁴ Vgl. *Kramer*, NZA 2007, 1338.

⁵¹⁵ Vgl. *Ernst*, DuD 2006, 223 (224 f.); vgl. *Bernhardt/Barthel* (o. Fußn. 227), 150 f.

⁵¹⁶ Vgl. *Fischer*, AuR 2006, 206.

⁵¹⁷ Vgl. *Kramer*, NZA 2006, 194 (196).

ter (Kläger), der bei der Beklagten bzw. bei deren Rechtsvorgängerin seit dem 1.1.1999 angestellt war. Als die Beklagte routinemäßig den Dienst-PC - auf den unzweifelhaft auch andere Arbeitnehmer Zugriff nehmen konnten - kontrollierte, wurde festgestellt, dass zahlreiche Bild- und Videodateien mit erotischen Inhalten abgespeichert waren und mit dem Dienst-PC auch Erotikseiten im Internet besucht wurden. Eine Nutzungsregelung für den privaten Umgang mit dem PC existierte nicht. Der Kläger hat überdies an einigen Tagen, an denen die bezeichneten Dateien aufgerufen wurden, Überstunden abgerechnet. Daraufhin wurde dem Kläger mit Schreiben vom 6.12.2004 außerordentlich, hilfsweise ordentlich gekündigt.

Der Kläger erhob beim ArbG Kaiserslautern⁵¹⁸ Kündigungsschutzklage, welche er auf folgende Aussagen stützte: Zu einer Privatnutzung des Dienst-PCs, bei der er DVDs und andere Videodateien mit erotischem Inhalt angesehen habe, sei es nie gekommen. Auch der Aufruf von Erotikseiten im Internet habe nie stattgefunden. Weiterhin habe er an manchen Tagen, an denen die betriebsfremde Nutzung vollzogen wurde, überhaupt keinen Zugang zum Dienst-PC gehabt, wie etwa am 21.2.2004, an dem er auf einer Baustelle gewesen sei. Das ArbG hat der Klage stattgegeben. Durch das Berufungsurteil des LAG⁵¹⁹ wurde die Entscheidung teilweise abgeändert: Das LAG hat festgestellt, dass das Arbeitsverhältnis nicht durch die außerordentliche Kündigung aufgelöst worden ist, da es an einer Abmahnung fehlte. Über die hilfsweise ordentliche Kündigung entschied das LAG, dass diese auch ohne Abmahnung wirksam sei. Mit der zugelassenen Revision verfolgt der Kläger die Wiederherstellung der erstinstanzlichen Entscheidung.

Das BAG hatte sich mit der Frage der Wirksamkeit der ordentlichen Kündigung und deren Rechtfertigung durch § 1 Abs. 2 KSchG zu befassen. Eine solche liegt vor, wenn der Arbeitnehmer eine Vertrags-

⁵¹⁸ ArbG Kaiserslautern, Urt. v. 10.3.2005 - 7 Ca 2183/04.

⁵¹⁹ LAG Rheinland-Pfalz, Urt. v. 8.9.2005 = BeckRS 2006, 41314.

pflicht – i. d. R. schuldhaft – erheblich verletzt hat, das Arbeitsverhältnis dadurch beeinträchtigt wird, eine zumutbare Möglichkeit einer anderen Beschäftigung nicht besteht und die Beendigung des Arbeitsverhältnisses unter Abwägung der Interessen beider Parteien billigenswert und angemessen erscheint. Im Rahmen einer verhaltensbedingten Kündigung ist das Prognoseprinzip heranzuziehen. Die verhaltensbedingte Kündigung soll damit keine Sanktion für begangenes Fehlverhalten darstellen, sondern die Vermeidung des Risikos weiterer erheblicher Pflichtverletzungen bezwecken. Die Kündigung aufgrund einer Vertragsverletzung setzt regelmäßig eine Abmahnung voraus. Erst wenn der Arbeitnehmer nach Vorliegen einer einschlägigen Abmahnung erneut seine arbeitsvertraglichen Pflichten verletzt, kann regelmäßig davon ausgegangen werden, dass es auch zukünftig zu Vertragsstörungen kommen wird. Ferner muss bei einem identischen Kündigungssachverhalt eine einheitliche Beurteilung des Abmahnungserfordernisses für die außerordentliche wie für die ordentliche Kündigung erfolgen. Es ist widersprüchlich, warum die außerordentliche Kündigung mangels vorausgegangener Abmahnung ausscheiden muss, aber die ordentliche Kündigung trotz fehlender Abmahnung vollzogen werden kann.⁵²⁰

In dem BAG-Urteil wurden Grundsätze darüber aufgestellt, welche Beweise der Arbeitgeber vorzutragen hat, damit das Gericht eine sozial gerechtfertigte verhaltensbedingte Kündigung annehmen kann. Demnach muss der Arbeitgeber darlegen,

- in welchem konkreten zeitlichen Ausmaß sich die Privatnutzung innerhalb der Arbeitszeit abgespielt hat;
- welches Datenvolumen vom Internet oder anderen Medien auf dem betrieblichen IuK-System gespeichert wurde;

⁵²⁰ Vgl. *Kramer* (o. Fußn. 514), 1338 (1339 f.).

- inwiefern es konkret zu Störungen bzw. Belastungen der EDV-Anlage gekommen ist oder welche diesbezügliche Gefahr vom Fehlverhalten des Mitarbeiters ausging;
- in welcher Höhe Kosten durch die private Internet-Nutzung entstanden sind;
- wie groß die konkrete Gefahr einer Rufschädigung des Arbeitgebers war und ferner, inwieweit Dritte und Betriebsangehörige von den erotischen Inhalten Kenntnis nehmen konnten.⁵²¹

Die von der Berufungsinstanz getroffenen Feststellungen zu den möglichen Pflichtverletzungen seien fehlerhaft, bemerkte das BAG. Darüber hinaus hat das LAG – selbst wenn eine erhebliche Pflichtverletzung vorgelegen hätte – eine notwendige Interessenabwägung nicht vorgenommen.⁵²² Die Rechtssache wurde an das LAG⁵²³ zur Weiterverhandlung zurückverwiesen; dieses entschied zu Gunsten des Klägers. Demnach ist das Arbeitsverhältnis durch die Kündigung nicht aufgehoben worden, und der Kläger muss weiter beschäftigt werden. Die Kündigung ist gem. § 1 Abs. 2 KSchG nicht aus verhaltensbedingten Gründen sozial gerechtfertigt. Es kann dahingestellt bleiben, ob der Kläger tatsächlich im dargelegten Umfang Erotikbilder betrachtet und Internet-Seiten mit erotischem Inhalt aufgerufen hat. Die Unwirksamkeit der Kündigung ergibt sich schon allein daraus, dass es einer vorhergehenden Abmahnung bedurft habe.⁵²⁴

Das BAG hat mit seinem Urteil vom 31.5.2007 festgestellt, dass eine unerlaubte Privatnutzung durchaus zu einer Kündigung führen kann; um allerdings eine Kündigung ohne vorhergehende einschlägige Ab-

⁵²¹ Vgl. *Kramer* (o. Fußn. 514), 1338 (1340).

⁵²² Vgl. *Kramer* (o. Fußn. 514), 1338 (1340).

⁵²³ LAG Rheinland-Pfalz, Urt. v. 13.12.2007 = BeckRS 2008, 50972.

⁵²⁴ Vgl. o. V., http://www.arbeitsrecht.de/arbeitsrecht/RechtKompakt/Rechtsprechung/2008/2008_04_10_kuendigung_wegen_privater_nutzung_eines_dienst-pcs_erfordert_abmahnung.php?navid=1 (13.5.08).

mahnung als gerechtfertigt ansehen zu können, muss eine ausschweifende, exzessive Nutzung vorgelegen haben⁵²⁵.

⁵²⁵ Vgl. o. V., http://www.arbeitsrecht.de/arbeitsrecht/RechtKompakt/Rechtsprechung/2008/2008_04_10_kuendigung_wegen_privater_nutzung_eines_dienst-pcs_erfordert_abmahnung.php?navid=1 (13.5.08).

8 FAZIT UND AUSBLICK

Die vorstehenden Ausführungen machen deutlich, dass auf Seiten der Arbeitgeber zahlreiche berechnigte Interessen existieren, die Benutzung des Internet- und E-Mail-Anschlusses der Mitarbeiter zu kontrollieren. Hierzu steht eine Vielzahl von technischen Möglichkeiten zur Verfügung - angefangen von der relativ simplen Analyse des Browsers und des E-Mail-Clients am Arbeitsplatzrechner, über die Auswertung der im Server bzw. in der Firewall anfallenden Zugriffsprotokolle bis hin zum Einsatz spezieller Überwachungssoftware, die eine praktisch lückenlose Aufzeichnung des gesamten Surfverhaltens erlaubt. Selbst wenn die Arbeitgeberinteressen noch so einleuchtend sind, kann dem Arbeitgeber die nahezu grenzenlose Überwachung nicht zugestanden werden. Den Belangen des Unternehmens stehen die Schutzinteressen der Mitarbeiter entgegen. Die gewonnenen Ergebnisse aus den Überwachungsmaßnahmen bergen erhebliche Risiken für die Arbeitnehmer. Im Extremfall ließe sich durch gezieltes Ausspionieren ein umfassendes Persönlichkeitsprofil der gesamten Belegschaft erstellen, auf dessen Grundlage sich personelle Maßnahmen stützen ließen. Um diesen Gefahren zu begegnen, existieren einfachgesetzliche allgemeine Datenschutzbestimmungen sowie bereichsspezifische Telekommunikations- und Telemedienschutzbestimmungen. Überdies sind stets mittelbar geltende verfassungsrechtliche Vorgaben - darunter insbesondere das allgemeine Persönlichkeitsrecht der Mitarbeiter - zu beachten, die auch im Arbeitsverhältnis ihre Wirkung entfalten. Existiert darüber hinaus ein Betriebsrat im Unternehmen, sind zusätzlich dessen Beteiligungsrechte zu berücksichtigen. Für die Anwendbarkeit und somit für die Strenge der vom Arbeitgeber einzuhaltenden Vorschriften der jeweiligen Gesetze ist entscheidend, ob der Arbeitgeber die Privatnutzung der elektronischen Kommunikationsmittel gestattet bzw. duldet, oder ob er eine solche Nutzungsmöglichkeit untersagt. Die zentrale „Weichenstellung“, inwiefern strikte Datenschutznormen die Überwachungsmöglichkeiten be-

schränken, nimmt letztendlich der Arbeitgeber durch seine Entscheidung für die Zulässigkeit bzw. für das Verbot der Privatnutzung von Internet und E-Mail am Arbeitsplatz selbst vor.

Fällt die Entscheidung dahingehend aus, dass die Internet- und E-Mail-Nutzung nur zu betrieblichen Zwecken erlaubt wird, steht dem Arbeitgeber ein umfassendes Kontrollrecht zu, sofern eine diesbezügliche Benachrichtigung der Mitarbeiter erfolgt ist. Sowohl auf die äußeren Daten des Internet- und E-Mail-Verkehrs als auch auf die jeweiligen Inhalte darf bspw. zum Zweck der Kontrolle des Nutzungsverbots zugegriffen werden. Dienstliche E-Mails sind sogar wie herkömmliche Geschäftspost zu behandeln und somit dem Arbeitgeber für Einblicke uneingeschränkt zugänglich. Eine Ausnahme gilt allerdings dann, wenn z. B. der Nachrichtenbetreff erkennen lässt, dass die Nachricht privater Natur ist. Im Übrigen sind die Kontrollmaßnahmen so zu gestalten, dass sie stichprobenartig und/oder anlassbezogen durchgeführt werden. Eine Vollkontrolle, bei der das gesamte Verhalten und die Leistung über die ganze Arbeitszeit hinweg erfasst werden, darf keinesfalls stattfinden. Die Überwachungsbefugnis lässt sich durch individuelle Einwilligungen oder eine Kollektivvereinbarung erweitern.

Gestattet der Arbeitgeber hingegen die Privatnutzung des Internet- und E-Mail-Anschlusses, so müssen für diese Nutzungsform die Vorschriften des Telekommunikations- und – wenn auch sehr eingeschränkt – des Telemediengesetzes Beachtung finden. Im Vordergrund der Datenschutzregelungen steht dabei das Fernmeldegeheimnis, das Kontrollen nur zu festgelegten Zwecken zulässt. Um weiter gehende Kontrollen zulässig zu vollziehen, ist eine Einwilligung in die Beschränkung des Fernmeldegeheimnisses oder in den Verzicht auf das Fernmeldegeheimnis der Beschäftigten unumgänglich. Bei einer sog. Mischnutzung erfasst das Fernmeldegeheimnis sämtliche Kommuni-

kationsvorgänge – ungeachtet dessen, ob es sich um dienstliche oder private handelt.

Im Anhang verdeutlicht ein Schaubild den Zusammenhang zwischen den zu beachtenden Rechtsvorschriften bei der arbeitsplatzbezogenen Internet- und E-Mail-Überwachung (Anlage 9).

Eine Möglichkeit, Überwachungsmaßnahmen datenschutzkonform zu gestalten, besteht darin, die anfallenden Kommunikationsdaten durch ein technisches System zu anonymisieren. Da es sich bei diesen Daten nicht um personenbezogene Daten handelt, ist dem Arbeitgeber ein vollumfängliches Kontrollrecht zuzubilligen. Falls die anonyme Überwachung zur Aufdeckung von Missbräuchen führt, kann anschließend – unter Beachtung der in der vorliegenden Abhandlung aufgezeigten Grundsätze – anhand personenbezogener Kontrollen die Identifizierung der verantwortlichen Mitarbeiter stattfinden. Ob sich ein solches Anonymisierungssystem für die betriebliche Praxis wirklich eignet, ist vorrangig abhängig von Wirtschaftlichkeitsaspekten.

Sowohl für Arbeitgeber als auch für Arbeitnehmer ist es in der gegenwärtigen Situation äußerst schwierig zu beurteilen, wie die vorhandenen datenschutzrechtlichen Vorschriften in Bezug auf die Telekommunikation am Arbeitsplatz anzuwenden sind – zugeschnitten sind die Regelungen nämlich auf herkömmliche Telekommunikations- und Telemedienanbieter. Mehr Transparenz bei den Rechtsvorschriften hinsichtlich der Überwachung der Anwendung der IuK-Technik am Arbeitsplatz diene der Rechtssicherheit auf Arbeitgeber- und Arbeitnehmerseite. Einzige Orientierung gibt die Rechtsprechung. Diese ist jedoch auf diesem Gebiet sehr lückenhaft und wird im Einzelfall das spezifische Problem nicht zu lösen vermögen.

Rechtsklarheit für Arbeitgeber und Arbeitnehmer dürfte das von verschiedenen Seiten schon seit Jahren geforderte Arbeitnehmerdaten-

schutzgesetz schaffen. Ziel sollte sein, ein spezifisches Datenschutzrecht für Arbeitnehmer zu entwickeln, das den Gesamtkomplex des Datenschutzes am Arbeitsplatz umfasst. Diesbezügliche gesetzgeberische Initiativen blieben indes aus. Selbst europarechtlich konnte bislang noch kein verbindlicher Rahmen geschaffen werden, der die einzelnen europäischen Mitgliedsstaaten zu einem Tätigwerden veranlasste.⁵²⁶ Es bleibt insofern abzuwarten, wann der deutsche Gesetzgeber ein speziell auf Arbeitsverhältnisse zugeschnittenes Datenschutzgesetz auf den Weg bringt und wie dieses konkret ausgestaltet sein wird.

⁵²⁶ Vgl. o. V., http://www.bfdi.bund.de/cln_027/nn_530440/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/Arbeitnehmerdatenschutzgesetz.html (19.6.08).

Anlagenverzeichnis

Anlage 1	Leitfaden für Arbeitgeber zur Überwachung der Internet- und E-Mail-Aktivitäten der Mitarbeiter	S. 128
Anlage 2	Struktureller Zusammenhang zwischen Internet, Firewall bzw. Server und Intranet	S. 139
Anlage 3	Exemplarischer Auszug aus einem Logfile	S. 140
Anlage 4	Muster einer Zusatzvereinbarung zum Arbeitsvertrag in Bezug auf die Nutzung von Internet und E-Mail am Arbeitsplatz	S. 141
Anlage 5	Muster einer Betriebsvereinbarung	S. 142
Anlage 6	Muster einer Internet-Policy	S. 151
Anlage 7	Muster einer Einwilligung in den Verzicht auf das Fernmeldegeheimnis	S. 154
Anlage 8	Muster einer Einwilligung in die Löschung virenverseuchter E-Mails und Spam	S. 155
Anlage 9	Zusammenhang zwischen den zu beachtenden Rechtsvorschriften bei der Internet- und E-Mail-Überwachung am Arbeitsplatz	S. 156

Anlage 1: Leitfaden für Arbeitgeber zur Überwachung der Internet- und E-Mail-Aktivitäten der Mitarbeiter

Mit den nachfolgenden Ausführungen erhalten Arbeitgeber, die eine rechtskonforme Überwachung der Internet- und E-Mail-Aktivitäten ihrer Mitarbeiter durchführen wollen, eine Orientierung für das Vorgehen.

Der hier dargestellte Leitfaden für Arbeitgeber bildet eine kurze Zusammenfassung der essentiellen Inhalte der vorliegenden Arbeit im Hinblick auf die Zulässigkeit der Internet- und E-Mail-Überwachung am Arbeitsplatz; gleichzeitig bietet er einen empfohlenen Handlungsrahmen für die Ausgestaltung zulässiger Kontrollen. Die Darstellung des Leitfadens in Form sequentiell abzuarbeitender Schritte kann nicht erfolgen, da die unternehmensspezifischen Gegebenheiten zu unterschiedlich sind, um allgemeingültiges Vorgehen aufzeigen zu können.

1. Grundsätzliches

- **Entscheidung über Zulassung der Privatnutzung**

Zunächst muss der Arbeitgeber entscheiden, ob er die Privatnutzung des Internets und/oder des E-Mail-Dienstes überhaupt gestattet. Diese Entscheidung hat weitreichende Auswirkungen auf die Zulässigkeit von Überwachungsmaßnahmen. Es bedarf demzufolge einer gründlichen Überlegung, inwieweit der Arbeitgeber seinen Mitarbeitern Vertrauen schenken kann und sich dadurch in seinem Kontrollrecht beschränken lassen will. In das Entscheidungskalkül müssen auch wichtige Gesichtspunkte wie Motivation der Mitar-

beiter⁵²⁷ und Verbesserung der Kompetenz durch die Bereitstellung des Internet- und E-Mail-Anschlusses zu privaten Zwecken mit einbezogen werden.

- **Verbot der Privatnutzung**

Sehr weit geht allein das gesetzliche Kontrollrecht, wenn der Arbeitgeber den Mitarbeitern untersagt, das Internet und/oder den E-Mail-Anschluss für private Zwecke zu verwenden. In diesem Fall bestimmt sich die Zulässigkeit der Überwachung nach den Vorschriften des Bundesdatenschutzgesetzes sowie nach den mittelbar wirkenden Grundrechten der Arbeitnehmer. Zur einfachen Beweisbarkeit sollte das ausdrückliche Verbot schriftlich festgehalten werden. Dazu eignen sich Zusatzvereinbarungen zum Arbeitsvertrag, oder falls ein Betriebsrat im Unternehmen vorhanden ist, die Regelung durch eine Betriebsvereinbarung.

- **Erlaubnis der Privatnutzung**

Wenn die Inanspruchnahme der elektronischen Telekommunikationsmedien auch zu privaten Zwecken genehmigt werden soll, gilt es - zumindest in Bezug auf die Privatkommunikation - strikte Datenschutzbestimmungen, insbesondere des Telekommunikationsgesetzes und auch des Telemediengesetzes, einzuhalten, welche die Möglichkeit der zulässigen Überwachung gravierend einschränken. Die Erlaubnis zur Privatnutzung der Telekommunikationsmedien sollte hinsichtlich des vom Unternehmen gebilligten Nutzungsumfangs möglichst klar und eindeutig formuliert werden. Dies betrifft im Wesentlichen potenzielle zeitliche und inhaltliche Restriktionen. Überaus rat-

⁵²⁷ Eine Studie des Computerspieleherstellers PopCap ergab, dass durch das vollständige Verbot der Internet-Nutzung nicht nur Motivations- und Konzentrationsverluste zu beklagen waren, sondern dass diese Verluste vielmehr die Ursache enormer Produktivitätseinbußen darstellten. Allein in Großbritannien gingen durch eine solche Nutzungseinschränkung des Internets fünf Milliarden Euro jährlich an Produktivität verloren. (vgl. o. V., <http://www.heise.de/newsticker/meldung/109190> (9.6.08)).

sam ist es, einen sog. Freiwilligkeitsvorbehalt mit aufzunehmen; dieser Vorbehalt ermöglicht die unproblematische Rücknahme der freiwilligen Leistung für die Zukunft. Zur Erlaubniserteilung eignen sich insbesondere Internet-Policies, Zusatzvereinbarungen zum Arbeitsvertrag oder Betriebsvereinbarungen, falls ein Betriebsrat im Unternehmen vorhanden ist.

- **Betriebsrat**

Existiert im Unternehmen ein Betriebsrat, ist dieser ohnehin bei der Frage über die Ausgestaltung von Kontrollmaßnahmen in Bezug auf die Nutzung der betrieblichen IuK-Anlage hinzuzuziehen. Deshalb sollte die Möglichkeit des Abschlusses einer Betriebsvereinbarung, in welcher die Nutzungsbedingungen von Internet und E-Mail klar geregelt sind, wahrgenommen werden. In der Vereinbarung lassen sich die konkreten Überwachungsmechanismen und der Zweck der Überwachung benennen. Um ferner bspw. einer in der Betriebsvereinbarung enthaltenen Warnung vor missbräuchlicher Anwendung Nachdruck zu verleihen, können drohende arbeits- und strafrechtliche Konsequenzen verankert werden. Der einfache Weg der Nutzungsreglementierung über die Kollektivvereinbarung erspart dem Arbeitgeber nicht zuletzt Kosten, Arbeit und Zeit. Zwar ist zumindest bei der betrieblichen Inanspruchnahme die Ausweitung der Überwachungsbefugnis durch eine Betriebsvereinbarung möglich, jedoch dürfte diese Option für die Praxis nicht von Relevanz sein. Der Betriebsrat wird sich kaum auf eine Regelung, die zu Ungunsten der Belegschaft wirkt, mit dem Arbeitgeber einigen.

- **Keine Vollkontrolle**

Die Überwachung ist stets so zu gestalten, dass keine vollumfängliche Auswertung des Verhaltens und der Leistung der Belegschaft über die gesamte Arbeitszeit hinweg vorgenommen werden kann. Sie gilt es

daher auf stichprobenartige und anlassbezogene Kontrollen zu beschränken. Führen diese Kontrollen zu einem Verdacht auf missbräuchliche Nutzungen, kann die Überwachung gezielt intensiviert werden. Selbst bei Vorliegen einer Einwilligung der Arbeitnehmer in weiter gehende Kontrollen, als es die gesetzlich vorgesehenen Erlaubnistatbestände gestatten, ist der Grundsatz zu beachten, dass keine Vollkontrolle stattfinden darf.

- **Erweiterung der Kontrollbefugnis durch Einwilligung**

Sowohl bei der dienstlichen als auch bei der privaten Nutzung von Internet und E-Mail lässt sich die Befugnis zu weiter reichenden Kontrollen, als sie gesetzlich durch Erlaubnistatbestände vorgesehen sind, ausdehnen. Hierzu ist eine schriftliche Einwilligung der Arbeitnehmer notwendig. Diese ermöglicht im Extremfall auch die Überwachung zum Zwecke der Auswertung von Verhalten und Leistung der Arbeitnehmer. Da die Überwachungsbefugnis bei der dienstlichen Telekommunikation jedoch ohnehin schon sehr weit reicht, bietet sich die Erweiterung der Kontrollberechtigung insbesondere für den Fall an, in dem der Arbeitgeber die Privatnutzung von Internet und E-Mail erlauben will. Die Erlaubnis zur Privatnutzung kann an die Bedingung geknüpft werden, dass die Arbeitnehmer auf das Fernmeldegeheimnis verzichten, welches die Privatkommunikation ansonsten unter besonderen Schutz stellt. Somit besteht zwar die Erlaubnis zur Privatnutzung der Medien, jedoch wird diese davon abhängig gemacht, ob eine solche Einwilligung erteilt wird oder nicht.

Das Mittel der Einwilligung stellt mithin die einzige Möglichkeit dar, die Überwachung der Internet- und E-Mail-Kommunikation der Mitarbeiter auf ein Höchstmaß zu erweitern. Aus praktischen Gründen bedarf es aber der Überlegung, ob ein solch einschneidender Eingriff in die Persönlichkeitssphäre der Arbeitnehmer nicht ein zu großes Empfinden von Misstrauen vermittelt. Das Recht auf informationelle

Selbstbestimmung lässt sich zwar ohne weiteres durch eine Einwilligung einschränken, jedoch wird die Beschränkung zu Lasten des Vertrauensverhältnisses zwischen Arbeitgeber und Arbeitnehmer wirken und schließlich das Betriebsklima negativ beeinflussen.

Als starkes Argument für die Arbeitgeberseite spricht gleichwohl die Tatsache, dass Mitarbeiter, die keine missbräuchlichen Nutzungen durchführen, auch keinerlei Sanktionen zu befürchten haben. Überdies kann der Mitarbeiter selbst entscheiden, ob er überhaupt Nutzungsvorgänge zu privaten Zwecken vornehmen will oder nicht. In Unternehmen mit ausgeprägter positiver Unternehmenskultur wird sich ein restriktiver Umgang mit der IuK-Technik kaum durchsetzen lassen. Falls es darüber hinaus einen Betriebsrat im Unternehmen gibt, ist es ohnehin nahezu ausgeschlossen, dass sich dieser auf weitreichende Kontrollbefugnisse des Arbeitgebers einlässt.

Die nachfolgend in Teil 2, Überwachung der Internet-Kommunikation, und in Teil 3, Überwachung der E-Mail-Kommunikation, dargestellten Informationen und Hinweise beziehen sich auf die gesetzlichen Regelungen, die zum Tragen kommen, falls die Arbeitnehmer keine Einwilligung in weiter gehende Überwachungsbefugnisse erteilen.

- **Vermeidung der Mischnutzung**

Soll die Privatnutzung der elektronischen Kommunikationsmedien gestattet werden, die Arbeitnehmer aber keine Einwilligung in umfangreichere als in die gesetzlich vorgesehenen Datenverarbeitungsvorgänge erteilt haben, ist unbedingt darauf zu achten, dass eine Mischnutzung der Techniken vermieden wird. Bei der Mischnutzung kann nicht unterschieden werden, ob im konkreten Fall eine dienstliche oder private Inanspruchnahme des Internets bzw. des E-Mail-Dienstes vorliegt. Die Folge einer Vermischung betrieblicher und privater Nutzungsvorgänge ist, dass dem Überwachungsvorhaben

strenge Datenschutzvorschriften im Wege stehen. Konkrete Maßnahmen, welche die Mischnutzung zu unterbinden vermögen, sind nachfolgend in Teil 2 und Teil 3 dienstspezifisch dargestellt.

- **Benachrichtigung bzw. Information der Beschäftigten über Kontrollmaßnahmen und deren Zweck**

Ungeachtet dessen, ob die Inanspruchnahme der Medien auch zu privaten Zwecken erlaubt wird oder nicht, obliegt dem Arbeitgeber die Verpflichtung, seine Beschäftigten vorab über die Überwachungsmaßnahmen und den Zweck der Verwendung der erhobenen Daten in Kenntnis zu setzen.

- **Zweckbindung der Daten**

Werden personenbezogene Daten bspw. nur zum Zweck der Erbringung des Dienstes oder der Entgeltabrechnung erhoben, dürfen diese lediglich zu diesen Zwecken verwendet werden. Die Verwendung solcher Daten etwa für eine Leistungskontrolle der Mitarbeiter darf nicht stattfinden.

- **Datenvermeidung und Datensparsamkeit**

Es ist darauf zu achten, dass so wenig wie möglich personenbezogene Daten durch die Kontrollmaßnahmen erfasst werden. Besteht ferner die Möglichkeit, die Daten unter verhältnismäßigen Bedingungen zu anonymisieren bzw. zu pseudonymisieren, soll davon Gebrauch gemacht werden.

2. Überwachung der Internet-Kommunikation

2.1 Überwachung bei unerlaubter Privatnutzung bzw. bei betrieblicher Nutzung

- **Weitgehende Überwachungsbefugnis**

Schon die gesetzlichen Erlaubnistatbestände lassen eine umfassende Überwachung der Internet-Kommunikation zu, sodass eine Ausweitung der Überwachungsmöglichkeit durch Einwilligung praktisch nicht notwendig erscheint. Der Arbeitgeber darf sowohl die äußeren Daten der Kommunikation als auch die Inhalte einsehen. Um dies in zulässiger Weise realisieren zu können, benötigt der Arbeitgeber lediglich einen konkreten legitimen Zweck, wofür er die personenbezogenen Daten verarbeiten und nutzen will. Ein denkbarer Zweck in diesem Zusammenhang stellt die Kontrolle der Einhaltung des Privatnutzungsverbots des Internet-Anschlusses dar. Die Zweckbestimmung der Überwachung ist den Arbeitnehmern mitzuteilen. Im Übrigen gelten die bereits oben, im Punkt „Zweckbindung der Daten“, aufgezeigten Grundsätze.

2.2 Überwachung bei erlaubter Privatnutzung

- **Feste Nutzungszeiten**

Die Festlegung bestimmter Zeiten, in denen die Internet-Nutzung zu privaten Zwecken erlaubt ist, bietet sich an, um einer Mischnutzung entgegenzuwirken. Idealerweise kommen Pausenzeiten für die zulässige Privatnutzung in Betracht. Durch eine solche Regelung ist die unproduktive Verwendung der Arbeitszeit durch die Inanspruchnahme des Internet-Dienstes untersagt. Die Kontrolle der Internet-Kommunikation während der Arbeitszeit richtet sich dann nach den Grundsätzen der betrieblichen Nutzung. Für Kommunikationsvorgänge inner-

halb der Pausenzeiten gelten die im nachfolgenden Punkt „Strikte Zweckbindung“ dargestellten Prinzipien.

Die Alternative der „Auslagerung“ privater Nutzungsvorgänge auf separate Internet-Terminals lässt zwar die eindeutige Unterscheidung zwischen betrieblicher und privater Nutzung zu, jedoch ist diese Alternative mit einem erheblichen finanziellen sowie technischen Aufwand verbunden: Es darf nicht unberücksichtigt bleiben, dass Mitarbeiter – sofern sie solche Terminals tatsächlich in Anspruch nehmen – eindeutig identifiziert werden sollen (z. B. durch eine individuelle Nutzerkennung), damit potenzielle Gesetzesverstöße aufgeklärt und den entsprechenden Mitarbeitern zugeordnet werden können.

- **Strikte Zweckbindung**

Das Fernmeldegeheimnis setzt arbeitgeberseitigen Kontrollen enge Grenzen. Die äußeren Rahmendaten, wie Uhrzeit, IP-Adressen und Dauer der Verbindung, dürfen ausschließlich zu Zwecken der Erbringung des Dienstes inklusive Systemschutz, der Entgeltabrechnung – falls eine solche überhaupt gegenüber den Mitarbeitern erfolgt –, der Störungs- und Fehlerbeseitigung sowie bei einem Verdacht auf Leistungserschleichungen verwendet werden. Andere Absichten, etwa die Überwachung zur Überprüfung der Arbeitsleistung, können nicht als Rechtfertigungsgrund dienen. Das Überwachen der Kommunikationsinhalte bei der privaten Internet-Nutzung ist verboten.

3. Überwachung der E-Mail-Kommunikation

3.1 Überwachung bei unerlaubter Privatnutzung bzw. bei betrieblicher Nutzung

- **Weitgehende Überwachungsbefugnis**

Durch das Verbot der Privatnutzung des E-Mail-Dienstes sind regelmäßig nur solche Nachrichten im E-Mail-Postfach zu erwarten, die von geschäftlicher Relevanz sind. Deshalb darf der E-Mail-Account der Mitarbeiter zu festgelegten Zwecken überwacht werden. Die betriebliche E-Mail-Kommunikation ist der geschäftlichen Briefkorrespondenz gleichzusetzen, welche der Arbeitgeber ohne weiteres einsehen darf. Das Einsichtsrecht betrifft sowohl die äußeren Umstände der E-Mails, als auch deren Inhalte.

Eine Ausnahme ergibt sich allerdings dann, wenn der Arbeitnehmer trotz eines diesbezüglichen Verbots private E-Mails versendet und/oder empfängt. In diesem Fall dürfen grundsätzlich nur die äußeren Daten solcher E-Mails kontrolliert werden – ohne diese Befugnis bestünde keine Möglichkeit, überhaupt missbräuchliche Nutzungen aufzudecken. Nur wenn die äußeren Umstände keine eindeutige Zuordnung zur dienstlichen bzw. zur privaten Kommunikation zulassen, besteht das Recht, auch die Inhalte einzusehen – dies jedoch nur bis zu dem Moment, in dem festgestellt wird, dass eine Privatnachricht vorliegt.

- **Einwilligung in die Löschung virenverseuchter E-Mails und Spam**

Eine zumindest indirekte Überwachung der E-Mail-Kommunikation ergibt sich aus der automatischen „Durchleuchtung“ eingehender Nachrichten. Um das betriebliche Netzwerk vor Schäden und Überbelastung zu schützen, sollte von sämtlichen Arbeitnehmern die Einwil-

ligung in die Löschung virenverseuchter E-Mails und Spam eingeholt werden. Diese Vorgehensweise ist unabhängig davon, ob die private Nutzung erlaubt ist oder nicht, zu empfehlen. Eine diesbezügliche Einwilligung stellt die einzig sichere Möglichkeit dar, unerwünschte E-Mail-Nachrichten zu eliminieren, ohne sich dabei strafbar zu machen. Der unterbundene Zustellungsversuch vireninfizierter E-Mails ist den jeweiligen Arbeitnehmern mitzuteilen.

3.2 Überwachung bei erlaubter Privatnutzung

- **Verschiedene E-Mail-Adressen**

Um eine zweifelsfreie Unterscheidung zwischen betrieblicher und privater E-Mail-Kommunikation zu ermöglichen, empfiehlt es sich stets, die Arbeitnehmer anzuweisen, die betriebliche E-Mail-Adresse nicht für private Kommunikationsvorgänge zu verwenden, sondern für solche Zwecke eine separate E-Mail-Adresse zu nutzen. Dabei muss der Arbeitgeber selbst keinen zweiten E-Mail-Account, der für die Privatkommunikation vorgesehen ist, zur Verfügung stellen. Vielmehr bietet es sich an, dass sich Mitarbeiter, die private E-Mails auch am Arbeitsplatz versenden und empfangen wollen, selbst eine E-Mail-Adresse bei einem Web-Mail-Dienst einrichten bzw. ihren ggf. bereits bestehenden Account dafür nutzen.

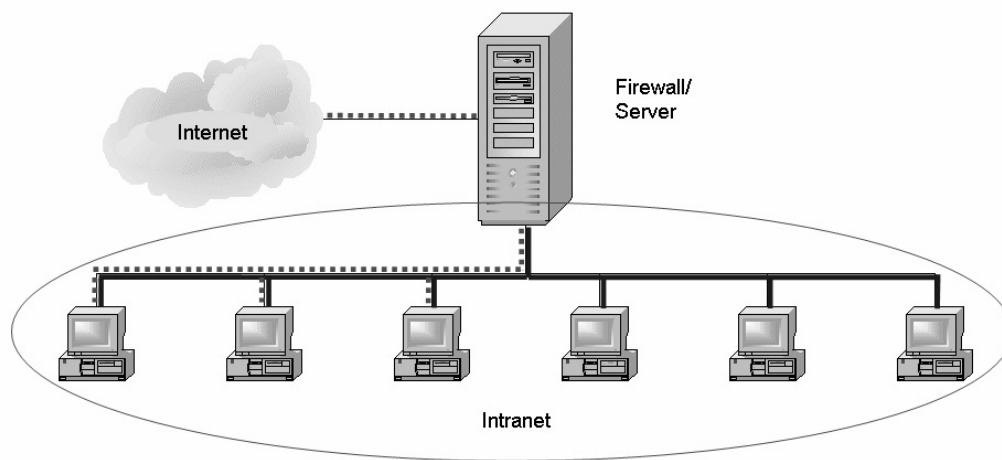
Durch diese Regelung kann die betriebliche E-Mail-Adresse, auf der nunmehr nur noch geschäftliche Korrespondenz zu erwarten ist, unproblematisch nach den in Punkt 3.1 aufgezeigten Grundsätzen kontrolliert werden.

Die private E-Mail-Kommunikation der Beschäftigten unterliegt dem Fernmeldegeheimnis. Stellt der Arbeitgeber eine separate E-Mail-Adresse zur privaten Nutzung bereit, so dürfen die äußeren Umstände der Kommunikation nur zu Zwecken der Dienstleistung inklusive

Systemschutz, evtl. der Entgeltabrechnung, der Störungs- und Fehlerbeseitigung sowie bei einem Verdacht auf Leistungerschleichungen verwendet werden. Eine Überwachung der Inhalte ist verboten. Falls der Arbeitgeber die Verwendung eines Web-Mail-Kontos zulässt, beurteilt sich die Zulässigkeit von Kontrollen nach der erlaubten Privatnutzung des Internet-Anschlusses.

Quelle: Der Verfasser.

Anlage 2: Struktureller Zusammenhang zwischen Internet, Firewall bzw. Server und Intranet



Quelle: in Anlehnung an o. V., <http://www.linux-hamburg.de/thintelligent/compnetz2.gif> (5.4.08).

Anlage 3: Exemplarischer Auszug aus einem Logfile

Rechnername	User	[Datum:Uhrzeit Zeitzone]	„Request“	Status	Dateigröße
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:19 +0200]	„GET /~rainer HTTP/1.0“	404	160
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:24 +0200]	„GET /~rainer/ HTTP/1.0“	404	161
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:33 +0200]	„GET / HTTP/1.0“	200	897
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:34 +0200]	„GET /gif/gl.gif HTTP/1.0“	200	427
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:34 +0200]	„GET /gif/awlogo.gif HTTP/1.0“	200	12706
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:34 +0200]	„GET /gif/apache_logo.gif HTTP/1.0“	200	23439
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:34 +0200]	„GET /git/suse_150.gif HTTP/1.0“	200	811
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:35 +0200]	„GET /gif/apache_pb.gif HTTP/1.0“	200	2326
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:46 +0200]	„GET /manual/ HTTP/1.0“	200	2207
192.168.17.23	Ulf Mack	[15/Mai/2008:18:57:47 +0200]	„GET /manual/images/sub.gif HTTP/1.0“	200	6083

Quelle: in Anlehnung an *Gerling*, IT-Sicherheit 3/2001, 18 (19).

Anlage 4: Muster einer Zusatzvereinbarung zum Arbeitsvertrag in Bezug auf die Nutzung von Internet und E-Mail am Arbeitsplatz

In Ergänzung zum Arbeitsvertrag vom _____ wird hinsichtlich der Nutzung der von der X GmbH zur Verfügung gestellten Kommunikationsmittel Internet und E-Mail folgendes festgelegt:

- (1) Die Nutzung der Kommunikationsmittel Internet und E-Mail wird auch zu privaten Zwecken gestattet. Der zur Privatnutzung vorgesehene Zeitraum beschränkt sich auf die regulären Pausenzeiten.
- (2) Das Abrufen, Anbieten oder Verbreiten von rechtswidrigen Inhalten, insbesondere solchen, die gegen strafrechtliche, datenschutzrechtliche, persönlichkeitsrechtliche, lizenz- oder urheberrechtliche Bestimmungen verstoßen sowie von politischen, diskriminierenden, diffamierenden oder verfassungsfeindlichen Inhalten ist unzulässig.
- (3) Die X GmbH weist darauf hin, dass die Einhaltung dieser Grundsätze durch Einsatz elektronischer Abfragen überprüft wird. Verstöße gegen die vorstehenden Regeln werden rechtlich verfolgt.
- (4) Die Bereitstellung der betrieblichen Kommunikationssysteme zur privaten Nutzung des Internet- und E-Mail-Dienstes für Arbeitnehmer stellt eine freiwillige Leistung dar. Ein Anspruch auf zukünftige Erbringung dieser Leistung wird ausgeschlossen.

Ort, Datum

Arbeitgeber

Arbeitnehmer

Quelle: in Anlehnung an o. V., <http://www.internetrecht-rostock.de/betriebsvereinbarung.pdf> (29.3.08).

Anlage 5: Muster einer Betriebsvereinbarung

Die X GmbH, vertreten durch den Geschäftsführer, Herrn N.N., und der Betriebsrat der X GmbH, vertreten durch den Vorsitzenden, Herrn N.N., schließen folgende Betriebsvereinbarung (BV):

§ 1 Gegenstand

Gegenstand dieser BV ist die Nutzung von E-Mail- und Internet-Diensten durch die Beschäftigten der X GmbH.

§ 2 Geltungsbereich

- (1) Diese BV gilt für alle Beschäftigten der X GmbH.
- (2) Die X GmbH vereinbart bei Verträgen mit Dritten, dass diese BV auch im Rahmen der Dienstleistung des Dritten für die X GmbH eingehalten wird.

§ 3 Zweckbestimmung

- (1) E-Mail dient der Kommunikation der Beschäftigten untereinander sowie mit externen Stellen.
- (2) Die Nutzung der Internet-Dienste dient dem Zugriff auf weltweit verfügbare Informationen und Daten und dem Angebot firmenbezogener Informationen.
- (3) Eine private Nutzung von E-Mail- und Internet-Diensten während der Dienstzeiten ist untersagt. Nutzungsvorgänge zu privaten Zwecken dürfen nur innerhalb der regulären Pausenzeiten vollzogen werden.
- (4) Die bei der Nutzung der E-Mail- und der Internet-Dienste anfallenden personenbezogenen Daten (Protokoll- oder Verbindungsdaten) dürfen nicht zu einer Leistungs- und Verhaltenskontrolle verwendet werden. Personenbezogene Daten, die zur Sicherstellung eines ordnungsgemäßen Betriebs der E-Mail- und Internet-Dienste erhoben und

gespeichert werden, unterliegen der besonderen Zweckbindung nach § 31 Bundesdatenschutzgesetz (BDSG).

§ 4 Begriffe

(1) Personenbezogene Daten (Personaldaten) sind Einzelangaben über persönliche und sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Beschäftigte der X GmbH).

(2) Im Übrigen gelten die Begriffsbestimmungen des BDSG.

§ 5 Netze

(1) Als Netz werden alle technischen Einrichtungen bezeichnet, die es ermöglichen, Daten zwischen zwei oder mehr Computern in Form von elektromagnetischen oder optischen Signalen zu senden, zu übertragen, zu vermitteln, zu empfangen, zu steuern oder zu kontrollieren.

(2) Die Einrichtungen des Netzes sind angemessen zu sichern, insbesondere Server, Router und ähnliche Netzeinrichtungen sind in Räumen aufzustellen, zu denen nur besonders Berechtigte Zugang haben. Die Verkabelung ist vor unberechtigten Zugriffen zu schützen. Angemessen ist die Sicherung (Satz 2), wenn der für die Schutzmaßnahmen zu erbringende technische und wirtschaftliche Aufwand im Verhältnis zur Bedeutung der zu schützenden Daten und der zu sichernden Anlagen und dem Risiko ihrer Verletzlichkeit verhältnismäßig ist.

§ 6 E-Mail

(1) E-Mail-Server sind zentral aufgestellte Computer, die der Verteilung, Zwischenspeicherung und gegebenenfalls auch der Speicherung von E-Mails dienen. Klienten sind die Arbeitsplatzrechner der Beschäftigten, auf denen E-Mails erstellt, empfangen, gelesen und verarbeitet werden.

(2) E-Mail-Server sind so aufzustellen, dass Unberechtigte keinen Zugang haben. Auf den Servern sind E-Mails gegen unberechtigte Zugriffe besonders zu sichern.

(3) E-Mails dürfen nur auf den dafür vorgesehenen E-Mail-Servern zwischengespeichert und an die Empfänger verteilt und zugestellt werden.

(4) Eingehende E-Mails können auf dem Arbeitsplatzcomputer des Empfängers, ausgehende auf dem des Absenders gespeichert werden.

(5) Die E-Mail-Server sind in Anlage 1 aufgeführt. Anlage 2 enthält die in der X GmbH eingesetzte E-Mail-Software für E-Mail-Server und -Klienten.

§ 7 Verwendung von E-Mail

(1) E-Mail wird zum Empfang und zur Versendung von elektronischer Post genutzt. Der E-Mail-Dienst kann zur Weitergabe von Dateien und Vorgängen benutzt werden. Eine automatisierte Vorgangssteuerung mittels E-Mail wird hiermit nicht eingeführt. Eine derartige Vorgangssteuerung bedarf zur Einführung einer gesonderten Betriebsvereinbarung.

(2) Die X GmbH kann zur Information der Beschäftigten ein „Schwarzes Brett“ im E-Mail-System einrichten oder E-Mails an alle Beschäftigten versenden. E-Mails mit identischem Inhalt an alle Beschäftigten müssen nicht verschlüsselt werden. Solange nicht alle Beschäftigten einen Arbeitsplatzrechner mit Zugriff auf E-Mail haben, werden sie auf herkömmliche Art (z. B. durch Aushänge oder Rundschreiben) informiert.

(3) Der Betriebsrat der X GmbH erhält auf Wunsch die gleichen E-Mail-Möglichkeiten zur Information der Beschäftigten wie die Geschäftsleitung.

(4) Das Löschen von unerwünschten E-Mails (Spam) geschieht nach vom Arbeitgeber zur Verfügung gestellten Regeln. Die Aktivierung dieser Regeln erfolgt durch den Beschäftigten.

§ 8 Verschlüsselung

(1) E-Mails mit vertraulichem Inhalt oder mit personenbezogenen Daten Dritter dürfen innerhalb der X GmbH sowie an externe Stellen nur

verschlüsselt versendet werden. Nachrichten mit Inhalten nach Satz 1 dürfen an externe Stellen nicht per E-Mail übermittelt werden, soweit diese nicht in der Lage sind, verschlüsselte E-Mails zu lesen.

(2) Das E-Mail-System muss ermöglichen, ausgehende E-Mails mit dem öffentlichen Schlüssel des Empfängers zu verschlüsseln. Das Format der ausgehenden verschlüsselten E-Mails soll einem offenen Standard für verschlüsselte E-Mails genügen.

(3) Zur Verschlüsselung der E-Mails stellt der Arbeitgeber ein Public-Key-Verschlüsselungsschema zur Verfügung. Jeder Beschäftigte erhält einen öffentlichen und einen privaten Schlüssel. Öffentliche Schlüssel werden allgemein zugänglich gemacht und in geeigneter Weise vor Manipulationen gesichert. Der private Schlüssel eines Beschäftigten wird ihm geschützt übergeben, so dass Dritte von ihm keine Kenntnis erlangen können. Private Schlüssel dürfen nicht dupliziert und an keiner zentralen Stelle innerhalb der X GmbH gespeichert werden.

(4) Schlüsselpaare nach Abs. 3 werden nach allgemein anerkannten Regeln generiert. Die zur Generierung der Schlüssel erforderlichen Daten werden nach der Schlüsselgenerierung unverzüglich gelöscht. Die privaten Schlüssel werden bevorzugt in Chipkarten gespeichert.

(5) Die X GmbH ist berechtigt, die E-Mail-Adressen und die öffentlichen Schlüssel der Beschäftigten Dritten zugänglich zu machen. Die erforderliche Einwilligung im Sinne des BDSG wird auf den Anträgen zur Einrichtung eines E-Mail-Accounts eingeholt.

§ 9 Vertretungsregelung

(1) Das E-Mail-System muss über die Funktionen Auto-Forward und Auto-Reply verfügen.

(2) Jeder Beschäftigte erhält zwei E-Mail-Adressen: eine funktionsbezogene (dienstliche) und eine namensbezogene (persönliche) Adresse. Eine funktionsbezogene E-Mail-Adresse kann sich auch auf eine Gruppe von Beschäftigten beziehen (z. B. auf eine Abteilung oder ein Referat). Die E-Mails an beide Adressen landen in derselben Mailbox. Für

normale Dienstgeschäfte wird die funktionsbezogene E-Mail-Adresse benutzt.

- a) Eine E-Mail an die funktionsbezogene Adresse wird bei Abwesenheit automatisch an den Stellvertreter weitergeleitet (Auto-Forward) oder der Absender wird automatisch über die Abwesenheit informiert (Auto-Reply). Vor vorhersehbarer Abwesenheit (z. B. Urlaub, Dienstreise) wird dieser Automatismus durch den Beschäftigten in Absprache mit dem Stellvertreter aktiviert. Bei unvorhersehbarer Abwesenheit (z. B. Krankheit) kann das Verfahren für diese funktionsbezogene Adresse durch den Postmaster (§ 11) auf Veranlassung des Vorgesetzten und in Absprache mit dem Stellvertreter aktiviert werden. Der Zeitpunkt ist schriftlich festzuhalten und dem Beschäftigten nach Rückkehr mitzuteilen.
- b) Eine E-Mail an die namensbezogene Adresse wird grundsätzlich nicht weitergeleitet. Jeder Beschäftigte kann die Absender automatisch über seine Abwesenheit informieren (Auto-Reply).

§ 10 Posteingangsbuch

(1) Die X GmbH führt ein elektronisches Posteingangsbuch. Dabei werden alle von außen eingehenden E-Mails an funktionsbezogene Adressen gemäß § 9 Abs. 2 mit Absender, Empfänger, E-Mail-ID, Datum und Uhrzeit in einer Log-Datei gespeichert.

(2) In E-Mail-Systemen kann man sich mittels der Optionen „Die E-Mail ist auf dem Zielrechner angekommen.“ (Zustellungsbestätigung) oder „Der Empfänger hat die E-Mail gelesen.“ (Lesebestätigung) davon überzeugen, ob eine Nachricht angekommen ist. Diese Optionen dürfen nicht zu Verhaltens- und Leistungskontrollen von Beschäftigten verwendet werden. Im E-Mail-System wird standardmäßig keine Lesebestätigung angegeben. Von Beschäftigten darf nicht verlangt werden, die Lesebestätigung zu aktivieren.

§ 11 Postmaster

Für die Verwaltung des E-Mail-Systems sind sog. Postmaster zuständig. Sie müssen mit den Bestimmungen des Fernmeldegeheimnisses im TKG und den Vorschriften des BDSG vertraut sein, und sie sind auf das Datengeheimnis gemäß § 5 BDSG zu verpflichten. Über alle Informationen, die sie durch ihre Tätigkeit erhalten, haben sie Stillschweigen zu bewahren. Dies gilt insbesondere auch für die unbeabsichtigte Kenntnisaufnahme von E-Mails mit dienstlichem oder persönlichem Inhalt.

§ 12 Zugriffsrechte und Passworte

- (1) Jeder Benutzer des E-Mail-Systems erhält eine Zugriffsberechtigung (Passwort) und einen eigenen Datenbereich (Mailbox).
- (2) Passworte bestehen aus mindestens sechs Zeichen, davon mindestens ein Sonderzeichen; damit sind alle Wörter ausgeschlossen, die im Duden stehen. Benutzer müssen ihre Passworte sorgfältig auswählen und geheim halten. Es ist untersagt, Passworte an andere weiterzugeben.
- (3) Ohne Kenntnis und Zustimmung der Beschäftigten dürfen Dritte keine Einsicht in die E-Mails eines Beschäftigten nehmen. Kenntnis und Zustimmung werden unterstellt, wenn E-Mails in Bereiche weitergeleitet werden, die für Dritte zugänglich sind.
- (4) Soweit die E-Mails dienstliche Inhalte betreffen, kann der Vorgesetzte verlangen, dass der Beschäftigte die E-Mails für ihn ausdruckt.

§ 13 Archivierung

- (1) Soweit zu Dokumentationszwecken erforderlich, werden ein- und ausgehende E-Mails ausgedruckt und wie Schriftstücke aufbewahrt. Die zugrunde liegenden Dateien werden im Rahmen der normalen Datensicherung gesichert (Anlage zu § 9 BDSG) und nicht archiviert.
- (2) Dienstliche E-Mails, die verschlüsselt empfangen und zu Nachweiszwecken noch benötigt werden, sind auszudrucken und zu den Akten zu nehmen.

§ 14 Internet-Dienste

- (1) Alle Beschäftigten, die Zugang zum Internet haben, können die in der Anlage 3 dieser BV aufgeführten Internet-Dienste nutzen. Bei deren Nutzung sind die in Anlage 4 dieser BV enthaltenen Vorschriften und Regeln zu beachten.
- (2) Soweit zum effektiven Zugriff auf das Internet Proxy- oder Cache-Server installiert werden, werden die Log-Dateien nur anonymisiert geschrieben.
- (3) Eine personenbezogene Kontrolle der Internet-Nutzung findet nur beim konkreten Verdacht der missbräuchlichen Benutzung statt. Die anfallenden Protokolldaten werden nur zur Klärung des konkreten Verdachts ausgewertet. Der Betriebsrat ist zu beteiligen.
- (4) Eine Auswertung der Nutzungsinformationen des WWW-Browsers auf der lokalen Festplatte eines Benutzers ist nur unter sinngemäßer Anwendung des Abs. 3 zulässig.
- (5) Der Arbeitgeber ist berechtigt, den Zugriff auf offensichtlich dienstlich nicht erforderliche Inhalte zu sperren.

§ 15 Information der Beschäftigten

Die Beschäftigten sind über die besonderen Probleme der E-Mail- und der Internet-Dienste zu unterrichten. Insbesondere ist auf folgendes hinzuweisen:

- a) gesetzliche Regelungen zum Fernmeldegeheimnis,
- b) Anwendung der Datenschutzvorschriften (BDSG),
- c) Zugänglichkeit unverschlüsselter E-Mails bei Transport im Netz,
- d) Probleme der Archivierung,
- e) dienstliche (arbeitsrechtliche), gesetzliche und ethische Grundsätze und Vorschriften bei der Nutzung von Internet-Diensten.

§ 16 Kontrolle der BV

(1) Der Betriebsrat hat das Recht, die Einhaltung dieser BV zu überprüfen.

(2) Der Betriebsrat kann zur Durchführung seiner aus dieser BV resultierenden Aufgaben nach Abstimmung mit der X GmbH Sachverständige seiner Wahl hinzuziehen; die notwendigen Kosten trägt die X GmbH.

§ 17 Verstöße

(1) Der Datenschutzbeauftragte, der Arbeitgeber und der Betriebsrat sind unverzüglich über Missbrauch und Missbrauchsversuche des E-Mail-Systems zu informieren. Alle Beschäftigten haben das Recht, vermutete oder tatsächliche Verstöße den Genannten vorzutragen. Das Beschwerderecht der Beschäftigten gem. der §§ 84 und 85 BetrVG bleibt hiervon unberührt.

(2) Personenbezogene Daten, die entgegen dieser BV erfasst oder gespeichert werden, dürfen nicht verwendet werden. Personelle Maßnahmen, die auf Informationen beruhen, die unter Verstoß gegen die Zweckbestimmung gem. § 3 gewonnen wurden, sind unwirksam. Der unberechtigte Zugriff auf personenbezogene Daten hat arbeitsrechtliche Konsequenzen.

§ 18 Freiwilligkeitsvorbehalt

Die Bereitstellung der betrieblichen Kommunikationssysteme zur privaten Nutzung des Internet- und E-Mail-Dienstes für Arbeitnehmer stellt eine freiwillige Leistung dar. Ein Anspruch auf zukünftige Erbringung dieser Leistung wird ausgeschlossen.

§ 19 Inkrafttreten und Kündigung

Diese BV tritt mit ihrer Unterzeichnung in Kraft. Sie kann mit einer Frist von drei Monaten zum Ende eines Kalenderjahres gekündigt

werden. Bis zum Abschluss einer neuen BV gilt die vorliegende Vereinbarung weiter.

Anlagen 1-3

Auf den Abdruck der Anlagen 1 bis 3 wird hier verzichtet, da diese Anlagen individuell erstellt werden müssen. Sie enthalten ausschließlich technische Informationen über die eingesetzte Hard- und Software sowie die genutzten Internet-Dienste.

Anlage 4: Code of Conduct

Unzulässig ist jede Internetnutzung, die geeignet erscheint, den Interessen der X GmbH oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Gesetze oder Verordnungen verstößt. Z. B. das Abrufen oder Anbieten von Texten, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen, das Abrufen oder Anbieten von weltanschaulicher, politischer oder kommerzieller Werbung, das Abrufen oder Anbieten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen oder pornographischen Äußerungen oder Abbildungen. Anbieten heißt Verbreiten über das WWW oder das Einstellen in Newsgroups oder Diskussionsforen in einer Art, dass die Firmenzugehörigkeit erkennbar ist (z. B. durch die E-Mail-Adresse des Absenders) oder unter Verwendung von EDV-Anlagen der X GmbH. Abrufen heißt auf im Netz vorhandene Informationen mit EDV-Anlagen der X GmbH zugreifen.

Quelle: in Anlehnung an Gerling, DuD 1997, 703-708.

Anlage 6: Muster einer Internet-Policy

In einer Zeit, in der die elektronischen Kommunikationsmöglichkeiten (E-Mail, Intranet, Websites und Internet) immer häufiger und von immer mehr Menschen eingesetzt werden, möchten wir alle Mitarbeiter an ihre persönliche Verantwortung beim Gebrauch der elektronischen Kommunikationsmittel des Unternehmens erinnern.

Die elektronischen Kommunikationsmittel bieten ein großes Potenzial, das zur Erreichung unserer Unternehmensziele produktiv genutzt werden kann. Diese Mittel bieten viele und wichtige Informationen, durch die unser Verbraucherverständnis verbessert, die Kommunikation mit unseren Kunden und Lieferanten erleichtert und ein Weg geboten wird, auf dem die Forschung sowie das Benchmarking mit externem Fokus betrieben werden kann. Bei Missbrauch können diese Technologien zu einer Verringerung der Produktivität und einer Verschwendung von Ressourcen führen. Haftungsfragen für das Unternehmen und/oder den einzelnen Mitarbeiter sowie letztendlich das Nichterreichen der Unternehmensziele können die Folge sein. Entsprechend dem von uns praktizierten Miteigentümer-Verhalten erwarten wir, dass Ressourcen und Arbeitszeit zur Verfolgung der Unternehmensziele eingesetzt werden.

Uns ist bewusst, dass ein minimaler Gebrauch der elektronischen Kommunikation zu persönlichen Zwecken wohl unvermeidlich ist, aber er sollte innerhalb vernünftiger Grenzen bleiben. Jeder Gebrauch zu persönlichen Zwecken sollte geringfügig bleiben und nicht die Geschäftsinteressen des Unternehmens berühren, und es sollten keine zusätzlichen Kosten entstehen. Die Unternehmensstandards sind zu wahren und die eigene Produktivität oder die anderer Mitarbeiter sollte nicht beeinträchtigt werden. Es ist wichtig, die Haltung des

Unternehmens zum richtigen (und falschen) Gebrauch der elektronischen Kommunikationssysteme deutlich zu machen.

Sachgemäßer Gebrauch umfasst:

- Weitergabe von Informationen in Zusammenhang mit Projekten und Geschäftsinteressen;
- Mitteilungen des Unternehmens, z. B. Organisationsänderungen, die für die Allgemeinheit bestimmt sind;
- Senden und Empfangen von geschäftlich veranlassten E-Mails und Dokumenten;
- Gebrauch zu persönlichen Zwecken, soweit er begrenzt und nicht häufig erfolgt, nicht die Geschäftsinteressen des Unternehmens berührt, keine Kostensteigerungen verursacht und den Unternehmensstandards entspricht.

Dem gegenüber bedeutet unsachgemäßer Gebrauch:

- Aktivitäten, die einen Interessenkonflikt darstellen;
- Spendenanfragen oder Bitten um Unterstützung für Veranstaltungen (mit Ausnahme von Veranstaltungen oder Aktionen, die vom Unternehmen unterstützt werden);
- Angebote zum Kauf oder Verkauf privater Waren oder Leistungen, religiöse Aktivitäten, Kettenbriefe, politische oder persönliche Meinungen, die nichts mit dem Unternehmen zu tun haben, sowie finanzielle Transaktionen, die keinen Bezug zum Unternehmen haben;
- herabwürdigende Bemerkungen über andere, einschließlich Lieferanten oder andere Unternehmen;

- illegale Aktivitäten;
- beleidigende, pornographische oder verleumderische Darstellungen.

Aufgrund der Gegebenheiten dieser Technologie sollte kein Mitarbeiter erwarten, dass die auf elektronischem Wege übermittelten Informationen privat sind. Wenn der Verdacht besteht, dass ein Mitarbeiter unsachgemäße Aktivitäten ausübt, behält sich das Unternehmen vor, im Rahmen der gesetzlichen Möglichkeiten die Verwendung von E-Mail und Intranet/Internet zu kontrollieren. Wenn ein Mitarbeiter den Eindruck hat, dass sich ein Kollege unsachgemäß verhält und/oder ein kompromittierendes Arbeitsumfeld schafft, kann er sich mit seinen Bedenken an den zuständigen HR-Manager wenden. Die Verletzung dieser Policy sowie der Unternehmensstandards zu sachgemäßem Gebrauch elektronischer Kommunikationssysteme kann ernste Disziplinarmaßnahmen nach sich ziehen, bis zum Verlust des Arbeitsplatzes.

Die Bereitstellung der betrieblichen Kommunikationssysteme zur privaten Nutzung des Internet- und E-Mail-Dienstes für Arbeitnehmer stellt eine freiwillige Leistung dar. Ein Anspruch auf zukünftige Erbringung dieser Leistung wird ausgeschlossen.

Bitte nehmen Sie sich etwas Zeit, diese Ausführungen zu verstehen und sehen Sie diese als eine Möglichkeit, unsere Produktivität durch den sachgerechten Gebrauch dieser Technologie zu steigern.

Quelle: in Anlehnung an o. V.,

<http://www.tse.de/vereinbarungen/internet%20und%20netze/policy.html> (18.6.08).

Anlage 7: Muster einer Einwilligung in den Verzicht auf das Fernmeldegeheimnis

Einwilligungserklärung

Ich bin damit einverstanden, dass mein Arbeitgeber, die X GmbH, meine personenbezogenen Daten im Zusammenhang mit der Internet- und E-Mail-Nutzung stichprobenartig zum Zwecke der Missbrauchsaufklärung und zur Kontrolle meiner Leistung sowie meines Verhaltens erheben, verarbeiten und nutzen darf. Ich verzichte hiermit ausdrücklich auf den Schutz der Internet- und E-Mail-Kommunikation durch das Fernmeldegeheimnis aus § 88 TKG.

Der Arbeitgeber gestattet die Privatnutzung des Internet- und E-Mail-Dienstes aufgrund der Unterzeichnung der vorliegenden Erklärung.

Diese Einwilligung erteile ich freiwillig; sie ist für die Zukunft frei widerruflich. Über die Konsequenzen der Einwilligung wurde ich umfassend aufgeklärt.

Ort, Datum

Arbeitnehmer

Quelle: Der Verfasser.

Anlage 8: Muster einer Einwilligung in die Löschung virenverseuchter E-Mails und Spam

Einwilligungserklärung

Aufgrund der Tatsache, dass sich der unternehmenseigene E-Mail-Server mit einer täglichen Flut an E-Mails, die einerseits teilweise Schadcode enthalten und andererseits unerwünschte Werbe-E-Mails (Spam) darstellen, belastet wird, ist die automatische Aussortierung und Löschung solcher E-Mails für das Funktionieren des betrieblichen Netzwerks unabdingbar.

Ich erkläre mich damit einverstanden, dass mein Arbeitgeber, die X GmbH, die an meine E-Mail-Adresse gerichteten Nachrichten, welche Schadsoftware enthalten und/oder eindeutig als Spam zu qualifizieren sind, zum Zweck der Aufrechterhaltung der betrieblichen Telekommunikationseinrichtung löschen darf.

Diese Einwilligung erteile ich freiwillig; sie ist für die Zukunft frei widerruflich. Über die Konsequenzen der Einwilligung wurde ich umfassend aufgeklärt.

Ort, Datum

Arbeitnehmer

Quelle: Der Verfasser.

Anlage 9: Zusammenhang zwischen den zu beachtenden Rechtsvorschriften bei der Internet- und E-Mail-Überwachung am Arbeitsplatz

Quelle: Der Verfasser.

