UNIVERSITÄTSLEHRGANG FÜR INFORMATIONSRECHT UND RECHTSINFORMATION
AN DER RECHTSWISSENSCHAFTLICHEN FAKULTÄT DER UNIVERSITÄT WIEN

Internetnutzung am Arbeitsplatz: Anmerkungen zu einem ersten Gesetzesentwurf

Nutzungs- und Kontrollmöglichkeiten des betrieblichen Internetzugangs – Analyse der datenschutz-, arbeits- und telekommunikationsrechtlichen Situation in Österreich im Lichte eines neuen Gesetzesentwurfs für das Beamtendienstrecht

MASTER THESIS

zur Erlangung des akademischen Grades

„Master of Laws“(LL.M.)

INFORMATIONSRECHT UND RECHTSINFORMATION

an der Universität Wien

(Universitätslehrgang für Informationsrecht und Rechtsinformation der Universität Wien)

eingereicht von

Dipl.-Wirt.Jur.(FH) Thomas Hartmann

begutachtet von

MR Mag. Dr. Waltraut Kotschy,
Geschäftsführendes Mitglied der Datenschutzkommission

Wien, im Juni 2009

Ehrenwörtliche Erklärung

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Wien, im Juni 2009

Abkürzungs- und Zitierweise

Die Abkürzungen entstammen den „Abkürzungs- und Zitierregeln der österreichischen Rechtssprache und europarechtlicher Rechtsquellen“ (AZR), welche im Auftrag des Österreichischen Juristentages von *Friedl/Loebenstein* herausgegeben wurden (6. Auflage, 2008).

Die Zitate entsprechen in der Regel den Vorschlägen der AZR.

„According to the Court's case-law,
telephone calls from business premises are prima facie
covered by the notions of 'private life' and 'correspondence'
for the purposes of Art. 8 § 1 [...].
It follows logically that e-mails sent from work
should be similarly protected under Art. 8,
as should information
derived from the monitoring of personal internet usage." *

---

* EGMR, Urteil vom 03.04.2007, *Copland vs. Vereinigtes Königreich*, Nr 62617/00, Rz 41-44

Der Europäische Gerichtshof für Menschenrechte, EGMR, überträgt seine bisherige Rechtsprechung, dass Telefongespräche von Mitarbeitern am Arbeitsplatz „Privatleben" und „Korrespondenz" iSd Art 8 Abs 1 EMRK und entsprechend durch die Europäische Menschenrechtskonvention geschützt sind, mit der zitierten Entscheidung auf die Nutzung von E-Mail und Internet. Der Schutzbereich des Art 8 Abs 1 EMRK umfasst nach der Entscheidung des EGMR ausdrücklich auch die Verkehrsdaten (Zeitpunkt und Dauer einer Kommunikation sowie speziell auch die angewählten Nummern).

Inhaltsverzeichnis

1. Einführung

Die vorliegende Arbeit widmet sich der Frage, ob und inwieweit Arbeitgeber die Internet- und E-Mail-Nutzung ihrer Mitarbeiter kontrollieren dürfen. Das Thema erhält aktuell durch verschiedene Entwicklungen eine besondere Bedeutung:

- Im Jahr 2007 waren 95 Prozent der Arbeitsplätze in Deutschland mit einem Internetzugang ausgestattet.[1]
- Zugleich surften im Jahr 2007 rund 30 Prozent der deutschen Arbeitnehmer während der Arbeitszeit im Internet; dies ist fast eine Verdoppelung innerhalb von fünf Jahren.[2]

Abb. 1 (Quelle: BITKOM e.V., Presseinformation v 12.07.2007, S.1)[3]

- Zugleich gerieten in den letzten Monaten namhafte deutsche Konzerne in heftige (Presse-) Kritik, weil sie die E-Mail tausender Mitarbeiter „gescannt" haben sollen.[4]
- Ob private Internetnutzung durch den Arbeitgeber kontrolliert werden darf, richtet sich regelmäßig nach Arbeits-, Datenschutz- **und** Telekommunikationsrecht sowie nach grundrechtlichen Positionen. Die angesprochenen Rechtsbereiche haben sich der gegenständlichen Fragestellung vorwiegend jeweils pro domo angenommen; Schwierigkeiten an den Schnittstellen, die in der betrieblichen Rechtsanwendung sichtbar werden, wurde bislang jedoch eher wenig

[1] *BITKOM e.V.*, Presseinformation v 03.08.2008, S. 1ff
[2] *BITKOM e.V.*, Presseinformation v 03.08.2008, S. 1ff
[3] Die Schätzung für 2007 hat sich zwischenzeitlich bestätigt, vgl. vorangehende FN
[4] Angesichts der Skandale ua bei der Telekom und der Deutschen Bahn eine „Renaissance" der seit jeher diskutierten Frage nach der Zulässigkeit der Mitarbeiterüberwachung konstatierend *Steinkühler/Raif*, AuA 2009, 213 (214); *Haar*, iX Nr. 6/2009, 90ff

Aufmerksamkeit geschenkt.[5] Fast „ausschließlich aus Sicht des Arbeitsrechts diskutiert“ worden sei die Frage, ob die Internetnutzung der Arbeitnehmer kontrolliert werden dürfe, konstatiert *Jahnel*.[6]

- Mit dem rasanten Einzug des Internets in den betrieblichen Alltag konnte das Arbeits- und Datenschutzrecht de lege lata in den letzten Jahren nicht mithalten. „Unterdeterminiert“ ist nach *Brodil* die österreichische Rechtsordnung im Hinblick auf den Arbeitnehmerdatenschutz.[7] Insgesamt seien die Rechtsprobleme des betrieblichen Internetzugangs „mannigfaltig und de lege lata nicht einfach zu lösen“, wünschenswert wären deshalb und „aufgrund der enormen Bedeutung der IT in der modernen Arbeitswelt“ näher determinierte gesetzgeberische Vorgaben.[8]
- Seit Jahren werden auch in Deutschland eigene Regelungen für den Datenschutz von Arbeitnehmern gefordert.[9] Ob es noch vor der Bundestagswahl im September 2009 zu einer Novellierung des Datenschutzrechts kommt, ist nicht absehbar; mit spezifischen Gesetzesbestimmungen zum Arbeitnehmerdatenschutz ist aber wohl nicht zu rechnen.[10] In der deutschen Literatur wird weithin ein „klarer Regelungsbedarf für ein Arbeitnehmerdatenschutzgesetz“[11] attestiert.

---

[5] *Bundesbeauftragter für Datenschutz*, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, S. 1

[6] *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *IT-LAW.AT (Hrsg)*, e-Mail – elektronische Post im Recht, S. 97

[7] *Brodil*, ZAS 2009, 121 (126); vgl. dazu auch kursorischen Überblick bei *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 61ff

[8] *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 68

[9] Schon im Jahr 2001 hielt die *Artikel 29 Datenschutzgruppe* für Deutschland fest: „Das Parlament hat − einer Anregung des Bundesbeauftragten für Datenschutz entsprechend − die Regierung wiederholt aufgefordert, ein Gesetz über Datenschutz am Arbeitsplatz vorzulegen.“ (*Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 5); stellvertretend für viele *Schönfeld/Strese/Flemming*, MMR 2001, 8 (11)

[10] „Ich sehe zum Beispiel noch Verbesserungsmöglichkeiten beim Datenschutz von Arbeitnehmern. Hier gibt es veritable Lücken. Ich will da noch vor der Bundestagswahl Fortschritte. Wenn es in dieser Koalition nicht zu einem gemeinsamen Entwurf eines Arbeitnehmer-Datenschutzgesetzes reicht, werde ich einen vorlegen. Darüber können die Wähler dann mitabstimmen“, so Bundesarbeitsminister Olaf Scholz zuletzt in einem Interview des Magazins Focus am 25.05.2009 (Titel „Finger weg vom Arbeitsrecht“); vgl auch *Bundesministerium für Arbeit und Soziales (Hrsg)*, BMAS plant eigenständiges Arbeitnehmerdatenschutzgesetz (Pressemitteilung v 16.02.2009) sowie *Bundesministerium für Inneres (Hrsg)*, Bundeskabinett beschließt Grundsatzregelung zum Datenschutz der Arbeitnehmer (Pressemitteilung v 18.02.2009). Stellvertretend für die diese Gesetzesinitiative in Deutschland begleitenden Stimmen *GDD e.V.*, Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages am 11.05.2009, S. 1ff; *Steinkühler/Raif*, AuA 2009, 213ff

[11] Jüngst *Haar*, iX Nr. 6/2009, 90 (92). Der *GDD e.V.* möchte datenschutzrechtliche Lücken aus rechtssystematischen Gründen hingegen im dBDSG geschlossen sehen, *GDD e.V.*, Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages am 11.05.2009, S. 1ff. Auch *Gola/Klug* wenden sich gegen eine Minderung der „Rolle des BDSG als Grundgesetz des Datenschutzes“, *Gola/Klug*, NJW 2008, 2481 (2483).

Vor diesem Hintergrund ist es bemerkenswert, dass die österreichische Regierung am 24.03.2009 eine Regierungsvorlage betreffend Bundesgesetz, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz und das Bundes-Personalvertretungsgesetz geändert werden soll (im Folgenden stets als „Gesetzesentwurf" bezeichnet),[12] vorgelegt hat. Zwar sind die recht detaillierten Regelungen nur für Beschäftigungsverhältnisse im öffentlichen Dienst (zB Beamtendienstrecht) vorgesehen. Weil sich in Österreich erstmals ein Gesetzgeber an konkrete bereichsspezifische Regelungen herantraut, erscheint es lohnenswert, sich zumindest mit dem Gehalt des Gesetzesentwurfs näher zu befassen.

Die vorliegende Arbeit will bezüglich der Nutzung und Kontrolle von Internetdiensten am Arbeitsplatz

1.) einen Überblick über die geltende Rechtslage im Arbeits-, Datenschutz- und Telekommunikationsrecht liefern (Kapitel 2, 3, 4.1., 4.2., 5.1. und 5.2) und

2.) die rechtspolitischen Wertungen des österreichischen Gesetzesentwurfs einordnen und untersuchen, ob die eingebrachten Regelungen auch für den Arbeitnehmerdatenschutz im privatrechtlichen Bereich geeignet und insoweit richtungweisend für weitere Gesetzesinitiativen in Österreich und Deutschland sein können (Kapitel 4.3., 4.4. sowie ab Kapitel 5.3.).[13] Der (ablehnenden) Stellungnahme der *Wirtschaftskammer Österreich* zum Gesetzesentwurf zufolge sind „auch Auswirkungen im Bereich des privaten Arbeitsrechts zu erwarten (etwa über die Judikatur des OGH)."[14]

[12] 160 d.B. (XXIV. GP), abgedruckt mit Erläuterungen und den zitierten Stellungnahmen im Anhang; vorangegangener Ministerialentwurf: ME Beamten-Dienstrechtsgesetz 1979, Vertragsbedienstetengesetz 1948 u. a., Änderung, 17/ME [XXIV. GP])

[13] Beachte zum Modellcharakter, dass folgender Satz der Erläuterungen des Ministerialentwurfs (nach dem Anhörungsverfahren) aus dem eingebrachten Gesetzesentwurf gestrichen wurde: **„Nicht nur denkbar, sondern auch erwünscht ist, dass der vorliegende Entwurf Beispielcharakter sowohl im öffentlichen als auch im privaten Bereich entwickelt und somit zumindest indirekt die Unternehmenskultur in Österreich positiv beeinflusst."** (ME Beamten-Dienstrechtsgesetz 1979, Vertragsbedienstetengesetz 1948 u. a., Änderung, 17/ME [XXIV. GP] Erläuterungen S. 1)

[14] *Wirtschaftskammer Österreich*, Stellungnahme, S. 1 (siehe Anhang)

2. Relevante Terminologie

2.1. Personenbezogene Daten

In den Anwendungs- und Schutzbereich des DSG 2000 fallen ausschließlich personenbezogene Daten iSd § 4 Z 1 DSG. Es ist daher vorab zu prüfen, ob der Mitarbeiter bei der Nutzung insbesondere von Internetdiensten personenbezogene Daten hinterlässt.

In der betrieblichen Praxis ist regelmäßig davon auszugehen, dass dem einzelnen Mitarbeiter ein individueller Zugang (Account) zur Computernutzung am Arbeitsplatz vom Arbeitgeber vorgegeben wird. Innerhalb dieses − grundsätzlich mittels eines Benutzernamens und eines Passwortes ausschließlich für den jeweiligen Mitarbeiter zugänglichen − Accounts[15] richtet sich der Mitarbeiter einen individuellen E-Mail-Dienst ein, vergleichbar dem Briefpapier oder der Visitenkarte des Arbeitgebers, auf dem etwa auch Name, Funktion, Abteilung und die individuellen Kontaktmöglichkeiten des Mitarbeiters vermerkt sind.

Daneben bleibt für die Nutzung anderer Internetdienste wie etwa dem World Wide Web (www) festzuhalten, dass der Mitarbeiter mit der IP-Adresse des Computers auf die Webseiten zugreift.[16] Diese Zugriffe werden über sog log files vom System protokolliert und können anhand der IP-Adresse sowie des individuellen Accounts des Mitarbeiters diesem eindeutig zugeordnet werden.[17]

Im Ergebnis hinterlässt der Mitarbeiter bei der Nutzung von Internetdiensten am Arbeitsplatz – also zB beim Surfen im WWW – Spuren in Form von log-files, die personenbezogene Daten (Verkehrsdaten des Mitarbeiters) darstellen und damit den Anwendungsbereich des DSG eröffnen.

---

[15] Spezielle Sonderfragen wie Zugriffsrechte von Systemadministratoren, Help Desks und anderen besonders qualifizierten Stellen bleiben an dieser Stelle unbehandelt.

[16] Zu dynamisch vergebenen IP-Adressen als personenbezogene Daten (arg „bestimmbar“ iSd § 4 Z 1 DSG 2000): DSK v 11.10.06, GZ K213.000/0005-DKS/2006), dazu *Leitner*, lex:itec 2006, 23 (24)

[17] DSK Bescheid v 20.06.08, GZ K121.358/0009-DSK/2008 (Bescheid beim VfGH angefochten, VfGH-Zl. B 1440/08); DSK Bescheid v 20.07.07, GZ: K121.289/0006-DSK/2007 (arg. Verwendung von Daten über bestimmbare Personen, vgl § 4 Z 1 DSG 2000); *Kotschy/Reimer*, ZAS 2004, 167; *Gerhartl*, ASoK 2008, 147

Schon im Jahr 2001 stellte die *Artikel 29 Datenschutzgruppe* zur Verarbeitung personenbezogener Daten von Beschäftigten fest:

> *„Für die Überwachung des E-Mail-Verkehrs ist die Verarbeitung personenbezogener Daten unerlässlich."*[18]

Von der Lehre nur vereinzelt[19] beachtet wurde bisher, dass eine E-Mail nicht nur personenbezogene Daten des Mitarbeiters sondern auch personenbezogene Daten des Kommunikationspartners verursacht (vgl Abb. 2).

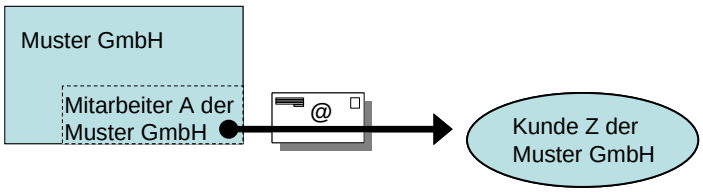

Abb. 2
Eine E-Mail – personenbezogene Daten von mind. zwei Personen
Quelle: eigene Darstellung

Will ein Arbeitgeber Einsicht in die personenbezogenen Daten des E-Mail-Verkehrs eines Mitarbeiters halten, so stellt dies grundsätzlich einen Eingriff in das Recht auf Datenschutz des Mitarbeiters und zugleich einen Eingriff in das Recht auf Datenschutz des Empfängers (zB Kunde Z in Abb. 2) bzw. Absenders der E-Mail dar.[20]

Mit einer Zustimmungserklärung nach § 1 Abs 2 DSG 2000, § 8 Abs 1 Z 2 DSG 2000 und ggf § 10 AVRAG kann der Mitarbeiter nur in die Verwendung seiner eigenen personenbezogenen Internetdaten einwilligen.[21] Ein Ausweg wird entlang des Gesetzeswortlauts insofern nur erblickt werden können, wenn der Arbeitgeber die Kontrolle von E-Mail-Daten auch gegenüber dem jeweiligen betriebsexternen (privaten) E-Mail-Empfänger bzw. -Absender mit überwiegenden berechtigten Interessen rechtfertigen kann.[22] Zu beachten ist

[18] *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 2
[19] *Kotschy/Reimer*, ZAS 2004, 167
[20] Die Kommunikationsdaten Dritter (zB von Bekannten und Familienangehörigen) seien „mit noch mehr Vorsicht" zu behandeln als bei den Mitarbeitern, fordert *Haar*, iX Nr. 6/2009, 90.
[21] *Kotschy/Reimer*, ZAS 2004, 167
[22] Interessant, aber leider ohne weitere Ausführungen, ist die Feststellung in der Stellungnahme des *Bundesministeriums für Justiz*, dass mit den nach § 79c Abs 2 Gesetzesentwurf vorgesehenen Kontrollmaßnahmen „jedenfalls auch Eingriffe in die Persönlichkeitsrechte Dritte möglich bzw. verbunden" seien, „weshalb den Bestimmungen des Datenschutzgesetzes auch außerhalb der Dienstverhältnisses besondere Bedeutung zukommt (§ 1 und §§ 17ff DSG)." (*Bundesministerium für Justiz*, Stellungnahme zu 17/ME [XXIV. GP], S. 1)

auch der insoweit vergleichbare Ansatz des telekommunikationsrechtlichen Vertraulichkeitsschutzes nach § 93 Abs 3 TKG 2003, welcher nur bei Zustimmung *aller* Benutzer zurücktritt.[23]

2.2. Kommunikationsdaten

Bei einer Betrachtung der E-Mail- und Internetnutzung ist nach Verkehrs- und Inhaltsdaten zu differenzieren. Die Begriffsbestimmung erfolgt im Wesentlichen unter Heranziehung des TKG.

2.2.1. Verkehrsdaten

Bei den Verkehrsdaten[24] einer E-Mail handelt es sich um die äußeren Verkehrs- und Zugangsdaten, wie insbesondere die E-Mail-Adresse des Empfängers, die Größe der versendeten elektronischen Nachricht, die Zeit der Versendung, die erfolgreiche Zustellung der elektronischen Nachricht.[25] In einem Vergleich mit der konventionellen Papierpost würden Verkehrsdaten all die Angaben umfassen, die auf dem Briefkuvert abzulesen sind, ohne dass dieses dazu geöffnet werden müsste.

2.2.2. Inhaltsdaten

Bei den Inhaltsdaten einer E-Mail handelt es sich um die inhaltliche Nachricht der elektronischen Post. Bei der konventionellen Papierpost müsste das Briefkuvert zuerst geöffnet werden, ehe der Inhalt einsehbar wäre.

Problematisch erscheint die Betreffzeile einer E-Mail, die in der klassischen Papierpost keine Probleme bereiten würde, da sie in der textlichen Umgebung eines Briefes eingebunden und insofern gleichermaßen von dem Briefumschlag geschützt ist. Bei einer E-Mail hingegen wird regelmäßig die Betreffzeile in dem Posteingangs- bzw. Postausgangsordnern zusammen mit den Verkehrsdaten angezeigt. *Brodil* anerkennt den „Betreff“ einer E-Mail

[23] Vgl dazu näher unten Kap 3.1.3. und Kap 5.1.
[24] Nach TKG 1997 „Vermittlungsdaten“
[25] EGMR, Urteil v 03.04.07, *Copland vs. Vereinigtes Königreich*, Nr 62617/00, Rz 41-44 (Unter Verweis auf seine Jud zu Telefongesprächen am Arbeitsplatz bestätigt der EGMR mit diesem Urteil erstmals, dass auch Verkehrsdaten von E-Mail- und Internetnutzung am Arbeitsplatz unter den Schutz des Art 8 Abs 1 EMRK fallen. Als Verkehrsdaten im Urteil genannt werden Dauer und Zeitpunkt der Kommunikation sowie die angewählte Nummer.)

zwar als Inhaltsdatum, zur Unterscheidung dienstlicher von privaten E-Mail sei die Kenntnis der (ggf privat gewidmeten) Betreffzeile für den Arbeitgeber aber „unerlässlich und im Rahmen der vorzunehmenden Interessenabwägung gedeckt“[26]

2.3. Sensible Daten

Sensible Daten sind nach § 4 Z 2 DSG 2000 Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben. Betrifft eine Datenverwendung sensible Daten, so folgen deutlich erhöhte Zulässigkeitsanforderungen. Unzweifelhaft und insofern beim gegenständlichen Thema ohne Besonderheit ist, dass Inhaltsdaten etwa einer E-Mail sensible Daten enthalten können.

Strittig hingegen ist bei der Internetnutzung die Einordnung der URL (wohl eher Verkehrsdatum)[27], die Arbeitnehmer anwählen, wie zB www.oegb.at, www.buddhatempel.org oder www.rheumaliga.at.[28] Auch bei dem Versenden einer E-Mail können die Verkehrsdaten grundsätzlich auf sensible Daten des Arbeitnehmers schließen lassen, etwa wenn dieser eine E-Mail an recht@akwien.at oder beratung@aidshilfe.at verschickt (vgl Abb. 3).[29]

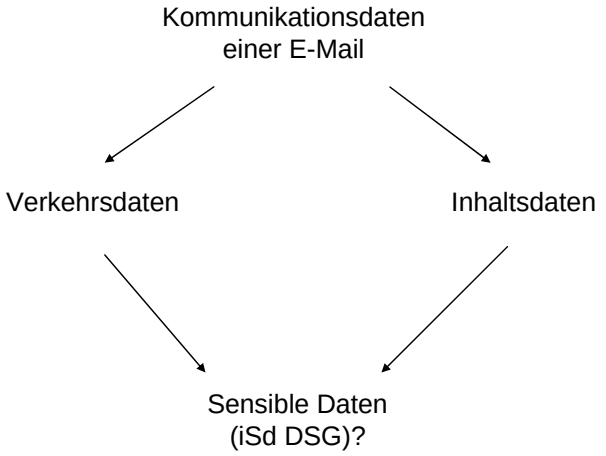

Abb. 3 Einordnung der Kommunikationsdaten einer E-Mail
Quelle: eigene Darstellung

[26] *Brodil*, ZAS 2009, 121 (125)

[27] „Zwitterstellung der URL“, beschreibt treffend *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 27, 43f

[28] Die URL sei geeignet, über Arbeitnehmer sensible Daten zu erheben, so *Brodil*, ZAS 2009, 121 (125); aA *Rotter*, ASok 1999, 118

[29] *Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in *Österreichische Juristenkommission (Hrsg)*, Grundrechte in der Informationsgesellschaft, S. 167; *Sacherer*, RdW 2005; 173; *Dellisch*, ASok 2001, 319 (Bsp xxxx@aknoe.at); solche E-Mail-Adressen als sensible Daten des Arbeitnehmers einzuordnen, gehe zu weit, meint hingegen *Brodil*, ZAS 2009, 121 (125)

Bei einer (zulässigen) Kontrolle der Internet-und E-Mail-Nutzung kann der Arbeitgeber ex ante nicht nach sensiblen und nichtsensiblen Daten differenzieren. Nach der herrschenden Lehre soll eine Einordnung als sensible Daten erfolgen, weil jedenfalls auch sensible Daten des Arbeitnehmers tangiert sein könnten.[30]

Sicherlich ist ein besonderer Schutz der sensiblen Daten iSd § 4 Z 2 DSG 2000 auch auf dem Gebiet des Arbeits- und Dienstrechts geboten. Zutreffend ist insoweit das Beispiel der Artikel 29 Datenschutzgruppe: Die Verarbeitung von genetischen Daten in einem Beschäftigungskontext ist eine Verarbeitung sensibler Daten.[31] Auch ist mit dem EuGH davon auszugehen, dass die Information, eine Person könne wegen einer Fußverletzung temporär nicht arbeiten, ein sensibles Datum ist.[32]

Gerade aber im Zusammenhang mit den Verkehrsdaten erscheint es überzogen, a priori sämtliche Verkehrsdaten als sensibel zu betrachten. Zu überlegen ist deshalb eine teleologische Interpretation: Sensible Daten bedürfen eines starken Schutzes, wenn sie zu einer Benachteiligung des Mitarbeiters führen könnten. Es ist deshalb anzuerkennen, dass ein Arbeitgeber die Religionszugehörigkeit der Mitarbeiter speichert, um mit der Personalplanung auf kirchliche Feiertage Rücksicht nehmen zu können.[33]

Bei einer (zulässigen) Kontrolle des betrieblichen Internetzugangs hat der Arbeitgeber regelmäßig nicht das Ziel, sensible (Nutzungs-)Daten des Mitarbeiters auszuforschen und zu dessen Nachteil zu verwenden. Der Arbeitgeber will vielmehr überprüfen, ob sich der Mitarbeiter an die

---

[30] „Potentiell sensible Daten" − *Brodil*, ZAS 2009, 121 (125); *Sacherer*, RdW 2005, 173; *Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in *Österreichische Juristenkommission (Hrsg)*, Grundrechte in der Informationsgesellschaft, S. 167; *Gerhartl*, ASoK 2008, 147 (148); *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in: *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 4267; aA *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg.)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 43f (Einmaliges Auffinden von sensiblen Daten gebiete noch keine Einordnung in sensible Daten.)

[31] *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 18; dazu auch *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 157

[32] EuGH 6.11.03, *Lindqvist*, C-101/01; vgl *Mayer-Schönberger/Brandl*, Datenschutzgesetz, S. 33, 315

[33] Regelmäßig darf der Arbeitgeber auch die Gewerkschaftsmitgliedschaft eines Beschäftigten speichern, um die Gewerkschaftsbeiträge vom Gehalt einzubehalten und an die Gewerkschaft abzuführen; weitere Beispiele für ein legitimes Interesse des Arbeitgebers am Vorhalten sensibler Beschäftigtendaten von der *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 18f

Nutzungsvereinbarungen des betrieblichen Internetzugangs hält. Soweit der Arbeitgeber nicht nach sensiblen Daten des Mitarbeiters sucht bzw. die Internetnutzung genau danach auswerten beabsichtigt, sind Verkehrsdaten nicht grundsätzlich als sensible Daten einzuordnen.[34]

[34] Vorsichtig *Ehmann/Helfrich*, EG-Datenschutzrichtlinie Kurzkommentar, Art. 8 Rz 9 (Verwendungszusammenhang sei maßgebend)

3. Exkurs zur Anwendbarkeit des TKG 2003[35]

Das Telekommunikationsrecht enthält in den §§ 92 ff TKG 2003 sektorspezifische Datenschutzbestimmungen, die gemäß § 92 Abs 1 TKG 2003 Anwendungsvorrang gegenüber dem DSG 2000 haben. Von entscheidender Bedeutung ist für die vorliegende Arbeit, ob der Arbeitgeber, indem er einen Internetzugang zur Verfügung stellt, gegenüber seinen Mitarbeitern zum Adressatenkreis des TKG 2003 gehört.

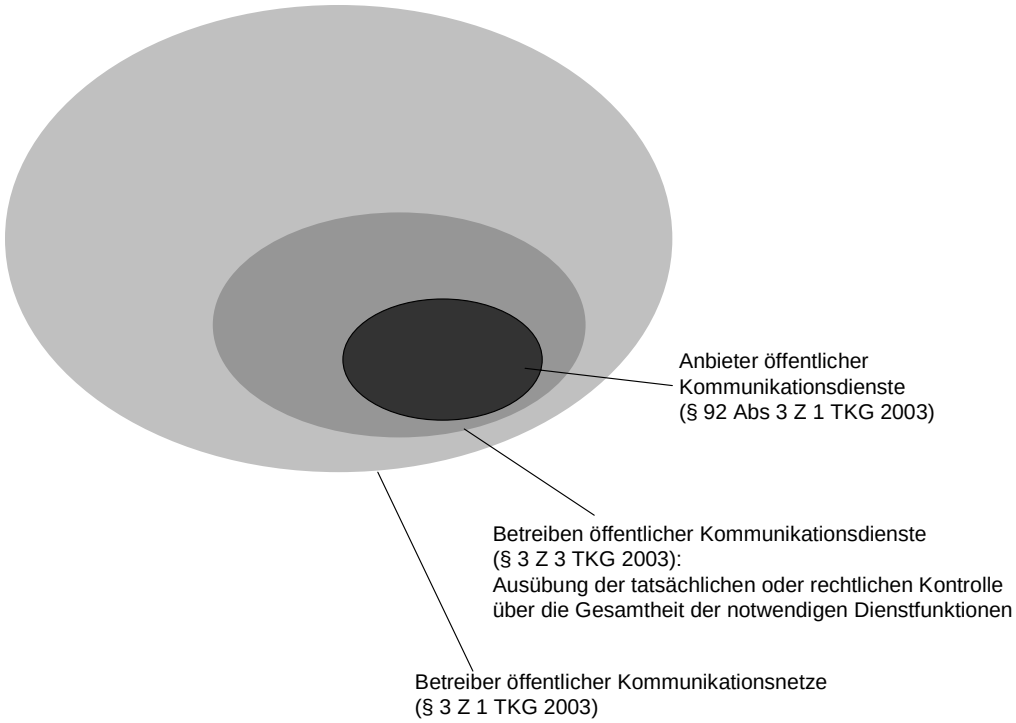

Abb. 4 Adressatenkreis im TKG 2003
Quelle: eigene Darstellung

3.1. Auslegung nach dem Wortlaut

Es ist zu prüfen, ob ein Arbeitgeber gegenüber einem Mitarbeiter insbesondere den datenschutzrechtlichen Spezialvorschriften des TKG 2003 unterliegt. Die Normadressaten des relevanten 12. Abschnittes des TKG 2003 sind unterschiedlich[36] (vgl Abb. 4) und determinieren die folgende Einteilung:

[35] Zur abweichenden Rechtslage diesbezüglich in Deutschland zB *Bundesbeauftragter für Datenschutz*, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, S. 2f; ausführlich auch *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S. 8ff (teils Subsidiarität des dBDSG zu dem deutschen Telekommunikationsrecht, insbesondere bei privater Internetnutzung der Mitarbeiter)

[36] Missglückt bzw. widersinnig seien die im TKG 2003 neuen Begriffsbestimmungen, meinen die Fachkommentare: In richtlinienkonformer Interpretation seien die §§ 92ff TKG 2003 auf die Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste

3.1.1. Diensteanbieter (§§ 94 Abs 1, 96, 101 TKG 2003)

Die Datenschutzbestimmungen der §§ 94 Abs 1, 96, 101 TKG 2003 richten sich an Anbieter iSd § 92 Abs. 3 Z 1 TKG 2003. Anbieter ist demnach ein „Betreiber von öffentlichen Kommunikationsdiensten".

Ein „Kommunikationsdienst" ist gemäß § 3 Z 9 TKG 2003 „eine gewerbliche Dienstleistung, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht (...)". Es ist strittig, ob ein Arbeitgeber eine gewerbliche Dienstleistung anbieten will, wenn er den Mitarbeitern einen Internetzugang zur (auch privaten) Verfügung stellt.[37]

Weiterhin müsste der Kommunikationsdienst öffentlich zugänglich sein. Dieses Kriterium wird nach herrschender Meinung regelmäßig nicht erfüllt sein, weil der Arbeitgeber den Internetzugang nur einem geschlossenen Benutzerkreis, nämlich den Mitarbeitern, zur Verfügung stellen will.[38] Dies gilt im Übrigen unabhängig davon, ob ein Arbeitgeber eine private Internetnutzung seiner Mitarbeiter toleriert oder diese sogar in einem eingeschränkten Umfang ausdrücklich gestattet.[39]

Die Datenschutzbestimmungen der §§ 94 Abs 1, 96, 101 TKG 2003 ist für den Arbeitgeber gegenüber seinen Mitarbeitern folglich nicht einschlägig.[40]

---

anzuwenden, fordern *Ruhle/Freund/Kronegger/Schwarz*, Das neue österreichische Telekommunikations- und Rundfunkrecht, S. 471f; abstellen auf den Anbieter iSd § 92 Abs 3 Z 1 TKG 2003 wollen *Parschalk/Otto/Weber/Zuser*, Telekommunikationsrecht, S. 208f (insb FN 669); keine konsequente Verwendung des Begriffs „Anbieter" in den §§ 92ff TKG 2003 feststellend und für eine richtlinienkonforme Klärung durch die Judikatur *Singer*, in *Stratil (Hrsg)*, TKG 2003, § 92 Anm 4.

[37] Ablehnend OGH 13.06.02, 8 Ob A 288/01p; *Parschalk/Otto/Weber/Zuser*, Telekommunikationsrecht, S. 209 (insb FN 671); *Zanger/Schöll*, Telekommunikationsgesetz, § 96 Rz 15; *Brodil*, ZAS 2004, 17 (18); vorsichtig *Sacherer*, RdW 2005, 627; aA *Thiele*, ecolex 2001, 613; *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 21ff; *Pracher*, Datenschutz in der Telekommunikation, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 353

[38] *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *IT-LAW.AT (Hrsg)*, E-Mail – elektronische Post im Recht, S. 91f; *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 21ff; *Brodil*, ZAS 2004, 17 (19); *Parschalk/Otto/Weber/Zuser*, Telekommunikationsrecht, S. 209 (insb FN 671); so im Ergebnis auch OGH 13.06.2002, 8 Ob A 288/01p

[39] *Zanger/Schöll* behaupten, der Arbeitgeber könne „die Anwendung der Verpflichtungen nach §§ 92ff TKG ausschließen", wenn er eine Privatnutzung des dienstlichen Internetzugangs verboten habe (*Zanger/Schöll*, Telekommunikationsgesetz, § 96 Rz14).

[40] Wohl veraltete Mindermeinung *Thiele*, ecolex 2001, 613, *Pracher*, Datenschutz in der Telekommunikation, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 353, jedenfalls falls der Arbeitgeber die private Mitbenutzung erlaubt habe

3.1.2. Netzbetreiber (§§ 93 Abs 2, 97, 99 TKG 2003)

Die Datenschutzbestimmungen der §§ 93 Abs 2, 97, 99 TKG 2003 richten sich an Betreiber iSd § 3 Z 1 iVm § 92 Abs 3 TKG 2003. Betreiber ist demnach „ein Unternehmen, das ein öffentliches Kommunikationsnetz oder eine zugehörige Einrichtung bereitstellt, oder zur Bereitstellung hiervon befugt ist".

Ein öffentliches Kommunikationsnetz ist gemäß § 3 Z 17 TKG 2003 „ein Kommunikationsnetz, das ganz oder überwiegend zur Bereitstellung öffentlich zugänglicher Kommunikationsdienste dient".

Der Arbeitgeber wird regelmäßig kein Übertragungssystem oder Vermittlungs- und Leitwegeeinrichtungen sowie anderweitige technische Infrastruktur iSd § 3 Z 11 TKG 2003 haben, allein indem er den Mitarbeitern den Anschluss an ein solches Kommunikationsnetz bereitstellt bzw. vermittelt. An die bereits oben (Kap 3.1.2.) dargestellte fehlende öffentliche Zugänglichkeit ist auch an dieser Stelle zu erinnern.

Die Datenschutzbestimmungen der §§ 93 Abs 2, 97, 99 TKG 2003 sind für den Arbeitgeber gegenüber seinen Mitarbeitern folglich nicht einschlägig.

3.1.3. Kommunikationsgeheimnis (§ 93 Abs 3 TKG 2003)

Nach § 93 Abs 3 S 1 TKG 2003 ist „das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer" unzulässig. Die Pflicht zur Einhaltung der Vertraulichkeit der Kommunikation ist von jedermann zu beachten, wenn die sonstigen Tatbestandsvoraussetzungen erfüllt sind.[41]

Im Unterschied zu den Fallgruppen der Kap 3.1.1. und 3.1.2. ist es für die Anwendbarkeit von § 93 Abs 3 S 1 TKG 2003 nicht erforderlich, dass der

[41] OGH 13.06.02, 8 Ob A 288/01p; *Parschalk/Otto/Weber/Zuser*, Telekommunikationsrecht, S. 209; *Ruhle/Freund/Kronegger/Schwarz*, Das neue österreichische Telekommunikations- und Rundfunkrecht, S. 473

Arbeitgeber selbst einen öffentlichen Kommunikationsdienst oder ein öffentliches Kommunikationsnetz vorhält. Maßgeblich ist insoweit lediglich, ob die E-Mail eines Mitarbeiters eine „Nachricht“ iSd § 92 Abs 3 Z 7 TKG 2003 vorliegt.[42]

Eine Nachricht ist nach § 92 Abs 3 Z 7 TKG 2003 jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird. Die E-Mail müsste über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet werden, wobei ein Kommunikationsdienst nach § 3 Z 9 TK 2003 eine gewerbliche Dienstleistung ist. Weiter zu prüfen ist, ob es sich um einen öffentlich zugänglichen Kommunikationsdienst handelt.

E-Mail der Mitarbeiter sind − unabhängig davon, ob sie dienstlichen oder privaten Charakter haben − dazu bestimmt, vom Anschluss des Arbeitgebers über ein öffentliches Kommunikationsnetz (Internet) und einen öffentlichen Kommunikationsdienst (Provider) an den Empfänger zu gelangen.[43] Damit sind sämtliche E-Mail durch das Kommunikationsgeheimnis nach § 93 Abs 3 TKG 2003 geschützt und zwar insbesondere vor einem Aufzeichnen oder sonstigen Überwachen des Arbeitgebers. Zu beachten ist, dass sich das Kommunikationsgeheimnis seit der Neufassung des TKG im Jahr 2003 ausdrücklich auch auf die Verkehrs- und Standortdaten der Nachrichten erstreckt.[44]

Der sehr hohe Schutz des Kommunikationsgeheimnisses kann grundsätzlich nur aufgehoben werden, wenn alle Benutzer eingewilligt haben. Zu beachten ist in diesem Zusammenhang, dass eine Einwilligung des Absenders einer E-w nicht ausreichend wäre; notwendig wäre zusätzlich auch eine Einwilligung des bzw. der Empfänger der E-Mail. [45]

---

[42] Siehe ausführlich Kap 3.4. und 5.4.

[43] Es sei denn, der Arbeitgeber erbringt einen Kommunikationsdienst nur für Mitarbeiter im Rahmen eigener Infrastruktur (zB Intranet, eigener Mailserver ohne Anbindung zum Internet); vgl ausführlich dazu weiter unten Kap 3.4. und 5.4.

[44] Bis zur Neufassung des TKG 2003 nicht; vgl § 88 Abs 3 TKG 1997 und OGH 13.06.02, 8 Ob A 288/01p; dazu auch *Brodil*, ZAS 2004, 17 (45)

[45] Beachte aber die neueste Judikatur des deutschen Bundesarbeitsgerichts: Hört ein Dritter zufällig und ohne Wissen der Gesprächspartner ein Telefonat von Arbeitgeber und Arbeitnehmer mit, so ist eine entsprechende Aussage des Dritten in einem Prozess zum Beweis zugelassen. BAG, Urteil v 23.4.09, Az 6 AZR 189/08

Die insoweit eindeutige Tatbestandsmäßigkeit des Kommunikationsgeheimnisses des § 93 Abs 3 TKG 2003 beantwortet indessen nicht abschließend die Relevanz für Arbeitgeber. Denn Rechtsfolgen bei einer Verletzung des § 93 Abs. 3 TKG 2003 sieht − zumindest im TKG 2003 selbst − nur § 108 TKG 2003 vor, der eine Strafbestimmung nur für Betreiber und dessen Personal vorsieht. Wie oben (Kap 3.1.2.) aufgezeigt, ist der Arbeitgeber in diesem Sinn kein Betreiber. Er würde sich demnach bei einer Überwachung von E-Mail zwar rechtswidrig verhalten, wäre nach TKG 2003 aber nach TKG 2003 deshalb nicht belangbar. Ob der Arbeitgeber diesfalls strafrechtlich zur Rechenschaft gezogen werden könnte, steht nicht „automatisch" fest. Insbesondere muss bei § 119 StGB Absicht nachgewiesen werden, der Schutzumfang des § 119 StGB dürfte zudem auf Inhaltsdaten begrenzt sein. Darüber hinaus werden Rechtfertigungsgründe zugunsten des Arbeitgebers in Betracht zu ziehen sein, wenn dieser den Mitarbeitern die private Internetnutzung ganz oder teilweise verboten hat.[46]

3.2. Zwischenergebnis

De lege lata sind die sektorspezifischen Datenschutzbestimmungen des TKG 2003 nicht im Rahmen eines Beschäftigungsverhältnisses anwendbar, auch ein Verstoß gegen § 93 Abs 3 TKG 2003 führt jedenfalls nicht zu Sanktionen des Arbeitgebers nach dem TKG 2003, den Schutz des Telekommunikationsgeheimnisses gewährleistet die Rechtsordnung über das Verfassungs- und Strafrecht.[47] Dies gilt unabhängig davon, ob bzw. inwieweit der Arbeitgeber seinen Mitarbeitern eine private Nutzung des Internetzuganges gestattet.

3.3. Teleologische, systematische, historische Auslegung

Das Telekommunikationsrecht hat drei Akteure vor Augen:

(1.) Zum einen den Netzbetreiber, der die notwendige technische Infrastruktur zur Verfügung stellt, um die Basis für Datenverkehr und somit Dienstleistungen im modernen Informationszeitalter abzusichern.

[46] Zu weiteren in Betracht zu ziehenden strafrechtlichen Tatbeständen (insb §§ 118, 118a, 119, 119a, 120 Abs 2a StGB) zB Reindl, Computerstrafrecht, S. 28ff, *Laimer/Mayr*, DRdA 2003, 410 (412)
[47] *Parschalk/Otto/Weber/Zuser*, Telekommunikationsrecht, S. 206ff

Die physischen Telekommunikationsnetze unterliegen aus historischen (Staatsbetriebe) und natürlichen (ein Netz) Gründen einer hohen Monopolneigung und bedürfen in Verfolgung grundlegender europarechtlicher Prinzipien einer sektorspezifischen Wettbewerbsregulierung, welche das TKG 2003 vorsieht.

(2.) Diese Kommunikationsnetze werden durch vielfältige Kommunikationsdienste mit Leben gefühlt. Zu den bekanntesten Dienstleistungen zählen die Internetdienste des World Wide Web sowie Dienste zum Versenden elektronischer Nachrichten. Die Distanzüberbrückung, die Postunternehmen in der Beförderung von Briefpost erbringen, übernehmen für elektronische Post Anbieter von Kommunikationsdiensten. Diese sind insbesondere Adressat von Verhaltensregeln zB im TKG 2003, im ECG oder im KSchG, welche das Auftreten gegenüber ihren Nutzern ein Stück weit vorgeben.

(3.) Die Nutzer, die aus welchen Motiven auch immer, die Infrastruktur und die Dienste in Anspruch nehmen.

Angesichts dieser Ausgangslage bezweckt das TKG 2003 zuvorderst die Förderung des Wettbewerbs im Bereich der elektronischen Kommunikation.[48] Mit Wirksamwerden im Jahr 2003 hat der österreichische Gesetzgeber die Datenschutzrichtlinie für elektronische Kommunikation in dem sektorspezifischen Wettbewerbsgesetz TKG umgesetzt.

Vorliegend ist regelmäßig davon auszugehen, dass sich ein Mitarbeiter der elektronischen Kommunikationsdienste im Namen seines Arbeitgebers bedient, um betriebliche Interessen wahrzunehmen. Der Arbeitgeber stellt dazu den Mitarbeitern die Betriebsmittel Computer und Internetanschluss zur Verfügung. Der Arbeitgeber erfüllt insoweit weder die unter (1.) aufgezeigte Rolle eines Netzbetreibers, noch will er iSv (2.) seinen Mitarbeitern (und anderen Dritten) einen Internetzugang anbieten, um diesen zu betriebsfremden

[48] So der zweifelsfreie europarechtliche Telos, meint zB *Brodil*, ZAS 2004, 17 (19)

Zwecken zu nutzen.[49] Der Arbeitgeber ist also selbst lediglich Anschlussinhaber und (einfacher) Nutzer der allgemein zugänglichen Kommunikationsnetze und -dienste eines Providers und unterliegt daher mitnichten den Schutzbestimmungen des TKG 2003, sondern ist durch diese den Netzbetreibern und Diensteanbietern gegenüber berechtigt. Dem Arbeitgeber ist sein Personal insoweit grundsätzlich zuzurechnen.

Eine Trennung, wie in Deutschland zu beobachten ist, in dienstliche und private Internetnutzung der Mitarbeiter ist mE unangemessen und überzogen. Zum einen erscheint eine Trennung in der betrieblichen Praxis für den Arbeitgeber nicht praktizierbar, so dass im Zweifel von privater Internetnutzung auszugehen wäre und damit eine umfassende Anwendung auch des TKG 2003 weithin eröffnet wäre, was aus den genannten Erwägungen nicht gewollt sein kann.[50] Vor allem aber ist darauf hinzuweisen, dass eine private Internetnutzung in Ansehung des Wesens einer Beschäftigung nur ein für den Arbeitnehmer erfreulicher Nebeneffekt in klar beschränktem Ausmaß sein kann. Die berechtigten Datenschutzinteressen der Beschäftigten werden − wie noch zu zeigen sein wird − hinreichend durch arbeits-, datenschutz-, verfassungs- und andere rechtliche Bestimmungen außerhalb des TKG 2003 gewahrt. Die hohen Schutzstandards für die Beziehung eines Nutzers gegenüber den Diensteanbietern und Netzbetreibern wären insoweit verfehlt. Zu beachten ist auch, dass eine solche Rechtsanwendung gewöhnlich nicht im Sinne der Arbeitnehmerschaft sein wird. Würde etwa allein aus einer geduldeten Privatnutzung folgen, dass der Arbeitgeber deshalb das TKG-Regime zu befolgen hat, so wäre ihm juristisch und ökonomisch zu raten, die private Nutzung des Internetzugangs jedenfalls ausdrücklich auszuschließen.

Hinzu kommt, dass mehrere zentrale Bestimmungen für die Beschäftigungssituation sachlich nicht zutreffen können. Hierzu folgende Beispiele:

[49] Anderes wäre nur dann anzunehmen, falls der Arbeitgeber das Internet Service Providing vollständig selbst übernimmt oder für seine Mitarbeiter nur ein rein unternehmensinternes Kommunikationsnetzwerk vorsieht.
[50] Vgl dazu unten eingehend Kap 5

- Würde man den Arbeitgeber als Betreiber iSd TKG 2003 qualifizieren, so würde er zu Zwangsabschlüssen (Zusammenschaltungen) verpflichtet werden.
- Weiter hätte der Arbeitgeber als Betreiber iSd TKG 2003 umfassende telekommunikationsspezifische Anzeige- und Konzessionspflichten zu erfüllen.
- Der Arbeitgeber muss in dienstliche Korrespondenz Einsicht nehmen können. Hätte er zB die Datenverarbeitungsverbote und Löschungspflichten des TKG 2003 zu beachten, so wäre er in seiner allgemeinen unternehmerischen Betätigungsfreiheit empfindlich gestört.

Generell ist aber festzuhalten, dass allgemeine Prinzipien und Verfassungsrechte von jedermann, also auch vom Arbeitgeber, zu beachten sind. Zuerst zu nennen ist hier das Kommunikationsgeheimnis nach Art. 10a StGG, das mit einer einfachgesetzlichen Ausformung in § 93 Abs 3 TKG 2003 zu finden ist.

3.4. Richtlinienkonforme Interpretation

Teilweise im Gegensatz zu den Bestimmungen des österreichischen TKG 2003 spricht die einschlägige EG-Datenschutzrichtlinie für elektronische Kommunikation[51] konsequent von „öffentlichen Kommunikationsnetzen“ und „öffentlich zugänglichen elektronischen Kommunikationsdiensten“. Es ist insoweit mE eindeutig, das im Unterschied zu geschlossenen Netzwerken (zB Intranet) europarechtlich nur öffentlich zugängliche Netze und Dienste Gegenstand der Datenschutzbestimmungen des TKG 2003 sein sollen.[52]

[51] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

[52] Dieses Ergebnis sei kurios, findet *Pracher*, Datenschutz in der Telekommunikation, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 353

3.5. Ergebnis

In Österreich ist das TKG 2003 regelmäßig nicht anwendbar auf Arbeitgeber, wenn diese ihren Mitarbeitern einen Internetzugang am Arbeitsplatz zur Verfügung stellen und evtl. auch eine Privatnutzung einräumen.[53] Arbeitgeber sind insoweit nicht mit typischen Internet-Providern vergleichbar, welche das TKG 2003 als sektorspezifisches Wettbewerbsrecht vor Augen hat. Für jedermann, also auch für den Arbeitgeber, zu beachten gilt es das Kommunikationsgeheimnis, dessen Verletzung allerdings keine Sanktionen nach dem TKG 2003 zur Folge hat. Es erscheint mit *Brodil* und *Mazal/Risak* zumindest erwägenswert, im Sinne einer Einheit der Rechtsordnung die grundlegenden Wertungen des Kommunikationsgeheimnisses über § 16 ABGB bzw. einer datenschutzrechtlichen Interessenabwägung einfließen zu lassen.[54]

[53] Ob der Reichweite des Fernmeldegeheimnisses in Deutschland bezüglich der Kontrollmöglichkeiten des Arbeitgebers bestehe Rechtsunsicherheit, wenn im Betrieb keine Zulässigkeitsregelung der privaten Internetnutzung getroffen wurde, so jüngst der *GDD e.V.*, Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages am 11.05.2009, S. 5

[54] *Brodil*, ZAS 2009, 121 (124); *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 62

4. Zulässigkeit privater E-Mail- und Internetnutzung

4.1. Geltende Rechtslage

Für die Arbeitgeber bestehen momentan drei Optionen (vgl Abb. 5), wie sie mit der privaten Internetnutzung ihrer Mitarbeiter umgehen können.[55] Der Arbeitgeber kann erstens die private Nutzung von E-Mail und Internet am Arbeitsplatz ausdrücklich verbieten. Zweitens kann der Arbeitgeber zu dieser Thematik schweigen. Schließlich kann der Arbeitgeber eine elaborierte Regelung vorgeben, unter welchen Voraussetzungen den Mitarbeitern die private Nutzung von E-Mail und Internet am Arbeitsplatz gestattet sein soll.

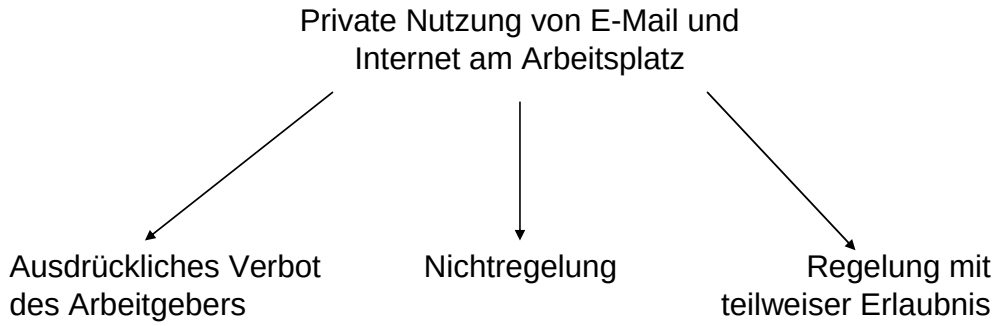

Abb. 5 Regelungsoptionen Privatnutzung des betrieblichen Internetzugangs für Arbeitgeber
Quelle: eigene Darstellung

4.1.1. Ausdrückliches Verbot

Der Arbeitgeber kann den Mitarbeitern nach herrschender Auffassung einseitig die private Nutzung von E-Mail und Internet verbieten. Dies folgt aus allgemeinen arbeitsrechtlichen Grundsätzen. Demnach hat der Arbeitgeber eine uneingeschränkte Verfügungsbefugnis über die Betriebsmittel, zu denen der Computer einschließlich eines Internetzugangs gehört. Der Mitarbeiter schuldet dem Arbeitgeber während der Arbeitszeit seine volle Arbeitskraft und hat insoweit – abgesehen von Notsituationen[56] – keinen Anspruch auf private Verrichtungen.[57] *Obereder* vertritt in diesem Zusammenhang, dass ein

[55] *ISPA*, Internet sicher nutzen, S. 38; *Laimer/Mayr*, DRdA 2003, 410 (412f)

[56] Was darunter (bei Telefongesprächen) zu verstehen ist, thematisiert der OGH ausdrücklich nicht (OGH 13.06.02, 8 Ob A 288/01p); *Thiele*, Internet am Arbeitsplatz, ecolex 2001, 613; *Brodil*, ecolex 2001, 853

[57] OGH 10.1.1984, 4 Ob 164/83, DRdA 1985, 389; *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 51ff; BAG, Urteil v 31.05.07, Az 2 AZR 200/06=NJW 2007, 2653; *Härting*, ITRB 2008, 88; *Bundesbeauftragter für Datenschutz*, Datenschutzrechtliche Grundsätze bei der dienslitchen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, S. 4; *GDD e.V.*,

Betriebsrat nach § 97 Abs 1 Z 6 ArbVG mit einer erzwingbaren Betriebsvereinbarung für einen Interessenausgleich sorgen könne.[58]

Beachtlich ist die Entscheidung eines deutschen Arbeitsgerichts: Wenn es im Betrieb grundsätzlich verboten wird, privat Internet zu surfen, so sei diese Anweisung nicht eindeutig und eine Kündigung des insoweit pflichtwidrig handelnden Mitarbeiters ohne Abmahnung nicht zu rechtfertigen. Das grundsätzliche Verbot könne von den Mitarbeitern wie im Rahmen des juristischen Sprachgebrauchs verstanden werden, so dass damit nicht jegliche private Nutzung von vornherein ohne Wenn und Aber verboten gewesen wäre.[59]

Der Arbeitgeber ist deshalb auch dazu befugt, die Infrastruktur mit Hardware und Software nur insoweit einzurichten, als sie zum Dienstbetrieb erforderlich ist. So können sich mittels technischer Zugriffsperren die Nutzungsmöglichkeiten eines Internetanschlusses auf bestimmte, (wenige) Internetseiten erschöpfen.[60] Auch die Kommunikation mittels E-Mail kann zB auf die an das betriebliche Intranet angeschlossenen Mitarbeiter reduziert werden. An diese Entscheidungsbefugnis des Arbeitgebers erinnert auch der Gesetzesentwurf ausdrücklich, indem das Bestehen eines Rechtsanspruchs der Mitarbeiter auf private IKT-Nutzung ausgeschlossen wird.[61]

Da die Informations- und Wissensgesellschaft auch die Arbeitswelt erfasst hat, erscheint es allerdings regelmäßig fraglich, ob ein Verbot der

---

Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages am 11.05.2009, S. 5; *Gerlach*, Der gesetzliche Schutz von Arbeitnehmerdaten, S. 2; *ISPA*, Internet sicher nutzen, S. 38; *Naderhirn*, Kollektives Arbeitsrecht und Arbeitnehmerkontrolle, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 109; nicht lückenlos durchsetzbar *Freudhofmeier*, taxlex 2006, 41; Mindermeinung *Thiele*, ecolex 2001, 613*; Laimer/Mayr*, ecolex 2003, 114; unzeitgemäß und sittenwidrig nach *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 419

[58] *Obereder*, RdA 2001, 75

[59] LAG Nürnberg, Urteil v 26.10.04, Az 6 Sa 348/03 = CR 2006, 61; aber nach Revision beim BAG zurückverwiesen, da das LAG den Verhältnismäßigkeitsgrundsatz überspannt habe, so BAG, Urteil v 12.01.06, Az 2 AZR 179/05 (insb Rz 50ff)

[60] *Gerhartl*, ASoK 2008, 147 (151); technische Zugriffssperren des Arbeitgebers unterliegen insoweit nur einem Willkürverbot. Problematisch wäre wohl eine Anordnung, nach welcher alle nichtgesperrten Internetseiten in bestimmtem Umfang auch nichtdienstlich genutzt werden könnten, die Auswahl der nichtgesperrten Internetseiten aber nicht nach dienstlichen Gesichtspunkten, sondern gezielt zugunsten bzw. zum Nachteil bestimmter Mitarbeiter erfolgen würde (vgl arbeitsrechtliches Gleichbehandlungsgebot, aber zB auch das Grundrecht auf Informationsfreiheit iSd Art 10 EMRK).

[61] § 79d S 3 des Gesetzesentwurfs

Privatnutzung unternehmenspolitisch adäquat ist: Geschuldete Arbeitsleistungen werden zunehmend orts- und zeitunabhängig von den Arbeitnehmern erbracht; oftmals wird stillschweigend von Angestellten erwartet, dass diese auch außerhalb der Kernarbeitszeiten telefonisch erreichbar sind, sich mittels Internet am Wochenende auf Besprechungen vorbereiten oder abends dienstliche E-Mail beantworten. Der Gedanke eines Fair-Use-Prinzips der dienstlichen IT-Geräte drängt sich vor diesem Hintergrund auf; es ist nicht ersichtlich, weshalb in einem solchen Rahmen ein partnerschaftliches Miteinander von Arbeitgeber und Mitarbeiter ein absolutes Verbot der Privatnutzung erfordern würde. Vielmehr vermag ein Fair-Use-Prinzip ein vertrauensvolles, den Mitarbeiter motivierendes und eigenverantwortliches Arbeiten und insoweit ein insgesamt stimuliertes Beschäftigungsverhältnis zu befördern.[62]

4.1.2. Nichtregelung

Oftmals wird der Arbeitgeber sich nicht ausdrücklich im Wege einer arbeits- oder kollektivvertraglichen Regelung bzw. einer sonstigen Anordnung dazu geäußert haben, ob und ggf inwieweit die Mitarbeiter die dienstlichen Computer auch zur privaten E-Mail- und Internetnutzung benutzen dürfen.[63]
Gesetzliche konkrete Regelungen zur Zulässigkeit einer privaten Internetnutzung am Arbeitsplatz fehlen im Datenschutz- oder Arbeitsrecht. Es wird unter Beachtung allgemeiner Rechtsnormen nach überwiegender Auffassung der Lehre von einer stillschweigenden Duldung des Arbeitgebers in eine die betrieblichen Interessen nicht zuwiderlaufenden Privatnutzung auszugehen sein;[64] zugleich werden allerdings die Mitarbeiter in besonderer Wese zur Einhaltung ihrer Treue- und Rücksichtspflichten angehalten sein. Diese Betrachtung wird unterstützt durch sich verändernde Vorzeichen in der

[62] Mit ähnlichen Überlegungen *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 418ff

[63] Vgl dazu die unten (Kap 4.2.) angeführte Studie

[64] OGH 2001/ARD 5323/8/2002; *Freudhofmeier*, taxlex 2006, 41; *Laimer/Mayr*, DRdA 2003, 410 (413); *Naderhirn*, Kollektives Arbeitsrecht und Arbeitnehmerkontrolle, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 107; *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S. 18; *ISPA*, Internet sicher nutzen, S. 39; *Thiele*, ecolex 2001, 613; LAG Köln, Urteil v 11.02.05, Az 4 Sa 1018/04 rkr; aA strenge ständige Rspr des BAG Urteil v 31.05.07, Az 2 AZR 200/06; BAG, Urteil v 12.01.06, Az 2 AZR 179/05; BAG, Urteil v 07.07.05, Az 2 AZR 581/04: Demzufolge kann ausschweifendes privates Surfen ohne Genehmigung des Arbeitgebers ein außerordentlicher Kündigungsgrund sein, beachte aber auch die Einschätzung der BAG Präsidentin, Ingrid Schmidt: „Die derzeitige Rechtslage ist zu unklar. (...) Der Gesetzgeber muss eine klare Ansage machen, was geht und was nicht." (Quelle: Handelsblatt v 29.01.09)

Arbeitswelt: Zusehends basieren Beschäftigungsverhältnisse nicht mehr auf reinen Arbeitszeitmodellen, vielmehr etablieren sich zielorientierte Kern- und Vertrauensarbeitszeiten.

Hinzu kommt, dass Beschäftigte zwar zunehmend auch Betriebsmittel wie Laptops oder Geschäftstelefone außerhalb der Diensträumlichkeiten benutzen können, damit aber zugleich auch die (oftmals unausgesprochene) Erwartung seitens des Arbeitgebers verbunden sein wird, dass der Beschäftigte auch im nichtdienstlichen Bereich erreichbar ist bzw. von zu Hause aus E-Mail beantwortet. Betriebsmittel wie Laptops sind weiters in den letzten Jahren zunehmend günstiger geworden, eine maßvolle private Internutzung verursacht angesichts von Flat-Tarifmodellen wohl zumeist nur marginale Zusatzkosten beim Arbeitgeber.[65] Ferner ist vorstellbar, dass der Arbeitgeber zB von privatem Internetsurfen auch profitiert, etwa wenn der Beschäftigte von zu Hause aus eingehende auch betriebsbezogene Recherchen im Wissenspool des weltweiten Internets durchführt, betrieblich veranlasste Administration abwickelt[66] oder wenn zB Vertriebs- oder PR-Beschäftigten durch eine stetige aktive Präsenz in sozialen Netzwerken im Internet Kontakt zu wichtigen bzw. potentiellen Geschäftspartnern befördern.[67] Es erscheint insoweit im Rahmen einer Gesamtbetrachtung des Beschäftigungsverhältnisses nicht unbillig, dass im Zweifel, dh bei fehlenden Vorgaben des Arbeitgebers, eine maßvolle private Internetnutzung vom Arbeitgeber stillschweigend toleriert wird und damit kein pflichtwidriges Verhalten des Beschäftigten begründet.[68]

In diesem Kontext stufte es kürzlich das deutsche Landesarbeitsgericht Rheinland-Pfalz als „sozialtypisch“ ein, wenn Geschäftsführer private Telefongespräche auf dem dienstlichen Mobiltelefon führen, falls die

[65] Insofern erscheint das Kostenargument zulasten des Arbeitgebers als kündigungsrelevante Pflichtverletzung überholt (BAG Urteil v 31.05.07, Az 2 AZR 200/06 = NZA 2007, 922ff); Internetkosten geringer als Telefonkosten, meinte schon im Jahr 2001 *Dellisch*, ASoK 2001, 316

[66] Vorsichtig *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 56f (die Ticketinformation und -einholung online bei der ÖBB könne zB zu einer „objektiv nachvollziehbaren Entlastung des Arbeitgebers führen“)

[67] *Obereder* erkannte schon im Jahr 2001, „dass die elektronische Kommunikation bereits im hohen Ausmaß Alltagscharakter angenommen hat, ein Umstand, der sich in den nächsten Jahren weiter steigern wird“. Seine Folgerung daraus, die Nutzung der Neuen Medien sei übliche Form des Verkehrs mit Dritten, die nicht der ausschließlichen Disposition des Arbeitgebers überlassen werden könne, ist aber zu weitgehend (*Obereder*, RdA 2001, 75).

[68] *BITKOM e.V.*, Presseinformation v. 03.08.2008, S. 1 (2)

Privatnutzung nicht ausdrücklich verboten wurde.[69] Ein ausdrückliches Verbot ließe sich nicht einer Arbeitsanweisung des Arbeitgebers entnehmen, wonach die Mitarbeiter auf den Handy-Rechnungen ihre Privatgespräche zur Verrechnung mit dem Gehalt zu markieren haben.[70] Diese Entscheidung ist besonders bemerkenswert, da das deutsche Bundesarbeitsgericht bisher in ständiger Rechtsprechung umfangreiche unerlaubt und heimlich geführte Privattelefonate auf Kosten des Arbeitgebers als wichtigen Grund für eine außerordentliche Kündigung anerkannte.[71] Es bleibt somit abzuwarten, ob das Urteil des Landesarbeitsgerichts Rheinland-Pfalz ein Ausreißer ist, oder ob es − auch im Wege der aufgezeigten veränderten Rahmenbedingungen − zu einer Änderung der Judikaturlinie kommen wird.

Unstrittig hingegen ist, dass der Beschäftigte jedenfalls nicht zu einer exzessiven Privatnutzung berechtigt ist.[72] Unzulässig ist demnach insbesondere, wenn der Beschäftigte strafbare und pornographische[73] Internetseiten aufsucht[74] oder privat erhebliche Datenmengen auf betriebliche Datensysteme herunterlädt, Anhänge von E-Mail öffnet, die als Schadsoftware die IT-Sicherheit beim Arbeitgeber (zB durch Computerviren)[75] gefährden kann.[76] Auf einem dienstlichen Computer gespeicherte bebilderte Scherzdateien über die polnische Bevölkerungsgruppe oder Männer sind nach der Judikatur per se weder menschenverachtend noch ausländerfeindlich, haben keine konkreten Auswirkungen auf den Betriebsfrieden und rechtfertigen deshalb keine fristlose Kündigung.[77] Der OGH sieht keinen Entlassungsgrund, wenn ein Mitarbeiter ein bis zwei Scherz-E-Mail pro

[69] LAG Rheinland-Pfalz, Urteil v 23.10.08, Az. 10 Sa 787/05 rkr (Zu beachten ist allerdings, dass das LAG zwischen dem vorliegenden Fall eines Geschäftsführerdienstvertrages und einem Arbeitsverhältnis differenziert.)

[70] LAG Rheinland-Pfalz, Urteil v 23.10.08, Az. 10 Sa 787/05 rkr

[71] BAG Urteil v 31.05.07, Az 2 AZR 200/06 = NZA 2007, 922 ff; Besprechung von *Raif/Kunze*, SAE 01/2009, 19ff

[72] *ISPA*, Internet sicher nutzen, S. 39

[73] Diffizile Abgrenzung von (kinder-)pornographischen und nichtpornographischen (geschmacklosen) Internetinhalten bei LAG Rheinland-Pfalz, Urteil v 23.10.08, Az 10 Sa 787/05 rkr; Herunterladen und geordnetes Speichern umfangreicher pornographischer Dateien als verhaltensbedingter Kündigungsgrund zB ArbG Frankfurt, Urteil v 02.01.02**,** Az 2 Ca 5340/01

[74] Die mögliche Rufschädigung des Arbeitgebers bei öffentlichem Bekanntwerden des Vorfalls ist dabei insbesondere zu bedenken.

[75] Zur Haftung des Arbeitnehmers bei Virenbefall des EDV-Systems *Laimer/Mayr*, DRdA 2003, 410 (415f) mwN; zur Anwendung des DNHG *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 60; *Freudhofmeier*, taxlex 2006, 41

[76] Oftmals gefährliche Dateiformate wie „.exe“ oder „.bat“ könnten in E-Mail vom Systemadministrator unterdrückt werden, so *Bundesbeauftragter für Datenschutz*, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, S. 5

[77] LAG Rheinland-Pfalz, Urteil v 23.10.08, Az 10 Sa 787/05

Woche an Kollegen weiterleitet.[78] Weiterhin ist allerdings anerkannt, dass der Beschäftigte beim (nicht nur kurzzeitigen) Betrachten von Videofilmen, Computerspielen oder anderen Unterhaltungsinhalten des Internets nicht mehr seine arbeitsvertraglich geschuldete Arbeitsleistung erbringen kann.[79]

4.1.3. Regelung mit teilweiser Erlaubnis

Der Arbeitgeber kann den Mitarbeitern nach freien Billigkeitserwägungen erlauben, den dienstlichen Computer auch privat zu nutzen.

Eine solche Erlaubnis kann der Arbeitgeber einseitig verfügen und − insbesondere infolge eines Widerrufsvorbehalts dann ohne Angabe von Gründen − auch wieder aufheben. Zu denken wäre in diesem Zusammenhang etwa an „Nutzungsbedingungen für betriebliche IT-Geräte“ (IT-Policy), die der Arbeitgeber vermöge seiner Systemadministratoren erstellt und dann für den gesamten Betrieb vorgibt. Gleichsam vorstellbar ist auch eine entsprechende Bestimmung im Arbeitsvertrag des einzelnen Beschäftigten; insbesondere sind hier keine Anhaltspunkte für eine Klausel in den Formulararbeitsverträgen erkennbar, welche nach einer AGB-Inhaltskontrolle grundsätzlich rechtswidrig wäre. Allenfalls zu beachten sind auch an dieser Stelle allgemeine arbeitsrechtliche Prinzipen wie etwa der Gleichbehandlungsgrundsatz in einem Betrieb.[80] Weiters kann der Arbeitgeber Regelungen zur privaten Nutzung der IT-Infrastruktur auch im Wege einer freiwilligen Betriebsvereinbarung implementieren.

Das Exzess- und Schädigungsverbot des Bediensteten gilt jedenfalls auch dann, wenn die private Internetnutzung am Arbeitsplatz grundsätzlich gestattet ist. Mitarbeiter dürfen den dienstlichen Internetzugang zeitlich nicht zu intensiv nutzen oder zB auf pornographische Internetseiten zugreifen.[81]

---

[78] OGH 9 Ob A 75/04a, ARD 5552/16/2004

[79] BAG Urteil v 31.05.07, Az 2 AZR 200/06 = NZA 2007, 922 ff; BAG Urteil v 07.07.05, Az 2 AZR 581/04 = MMR 2006, 94ff; der Arbeitgeber hat freilich einen konkreten Sachvortrag zu erbringen, in welchem zeitlichen Umfang der Beschäftigte den Dienst-PC privat genutzt und seine Dienstpflichten vernachlässigt hat, LAG Rheinland-Pfalz, Urteil v. 23.10.08, Az 10 Sa 787/05; bei der Darlegungs- und Beweislast stecke für den Arbeitgeber der Teufel im Detail, meinen *Raif/Kunze*, SAE 01/2009, 19 (20)

[80] Vgl dazu auch unten Kap 5.1.1. (Verknüpfung von erforderlicher Zustimmung zu Kontrollen mit Erlaubnis für Privatnutzung)

[81] BAG, Urteil v 07.07.05, Az 2 AZR 581/04; *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 55

4.2. Zwischenergebnis und Würdigung

Wie eine aktuelle Studie zeigt, hatte im Jahr 2008 fast jedes zweite Unternehmen in Deutschland seinen Mitarbeitern verboten, den dienstlichen Internetzugang zur privaten Kommunikation zu nutzen. Weitere 42 Prozent der deutschen Unternehmen hingegen stellte es ihren Mitarbeitern frei, auch privat das Internet am Arbeitsplatz zu nutzen und private E-Mail zu senden.[82]

Gerade die letztgenannte Situation ist aus rechtlicher Sicht sowohl für den Arbeitgeber als auch für die Mitarbeiter nicht ohne Gefahren. Für den Mitarbeiter fehlen klare Vorgaben, an denen er sein Handeln orientieren könnte.[83] Die oben überblicksartig vorgebrachten rechtlichen Abwägungen sind teils hochkomplex und umstritten, die schmalen Grenzen für den Mitarbeiter im Einzelfall nicht ohne weiteres erkennbar. Selbst wenn eine rechtswidrige Privatnutzung des Mitarbeiters vorliegt, so wird man ihm oftmals sein Handeln nicht vorwerfen können, da er die Rechtswidrigkeit bzw. Schuldhaftigkeit nicht erkennen konnte.

Auch der Arbeitgeber läuft Gefahr, sich regelmäßig zumindest in einem rechtlichen Graubereich zu bewegen. Wie noch zu zeigen sein wird, richten sich die Kontrollmöglichkeiten der Internetnutzung am Arbeitsplatz maßgeblich auch danach, zu welchen Nutzungen die Mitarbeiter berechtigt sind.

Besteht also der Verdacht, ein Mitarbeiter nutze den Computer in unzulässiger Weise privat, so wird eine Verfolgung regelmäßig umso schwieriger, falls sich der Arbeitgeber zu den Grenzen der im Betrieb erlaubten Privatnutzung nicht geäußert hat.

---

[82] Studie „IT-Security 2008“ von der Fachzeitschrift InformationWeek und Steria Mummert Consulting AG, Quelle *Steria Mummert Consulting AG*, Pressemitteilung v. 29.01.09 und *Jung/Bube*, Fallstricke beim Verbot privater Emails am Arbeitsplatz, in InformationWeek v 30.01.09; die weithin verbreitete Nichtregelung als Risiko für den Arbeitgeber darstellend *Haar*, iX Nr. 6/2009, 90 (91); *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S. 39

[83] So kürzlich auch die Präsidentin des BAG, Ingrid Schmidt: „Die derzeitige Rechtslage ist zu unklar. (...) Der Gesetzgeber muss eine klare Ansage machen, was geht und was nicht.“ Beim Blick in das Bundesdatenschutzgesetz könnten Schmidts Aussage zufolge sowohl Arbeitnehmer als auch Arbeitgeber nicht erkennen, was ihre Rechte und Pflichten seien. (Quelle: Handelsblatt v 29.01.09)

Der österreichische Gesetzgeber hatte sich bislang nicht dazu geäußert, ob und ggf unter welchen Voraussetzungen Mitarbeiter die moderne Informationsinfrastruktur des Arbeitgebers auch zu privaten Zwecken nutzen können, gerade wenn darüber keine Regelungen auf Betriebsebene errichtet wurden.

4.3. Die Regelungen des Gesetzesentwurfs

Für die Beschäftigten im österreichischen öffentlichen Dienst[84] brachte das Bundeskanzleramt am 24.03.2009 einen Gesetzesentwurf ein, der unter anderem einem neuen § 79d BDG „Grundsätze der IKT-Nutzung“ beinhaltet.

Der Gesetzesentwurf gibt zunächst den Wesenskern eines Beschäftigungsverhältnisses wieder: Die Arbeitnehmer haben die Betriebsmittel anhand der Weisungen des Arbeitgebers zu nutzen und dürfen sie nicht zu privaten Zwecken einsetzen, verwenden, modifizieren oder in sonstiger Weise benutzen.

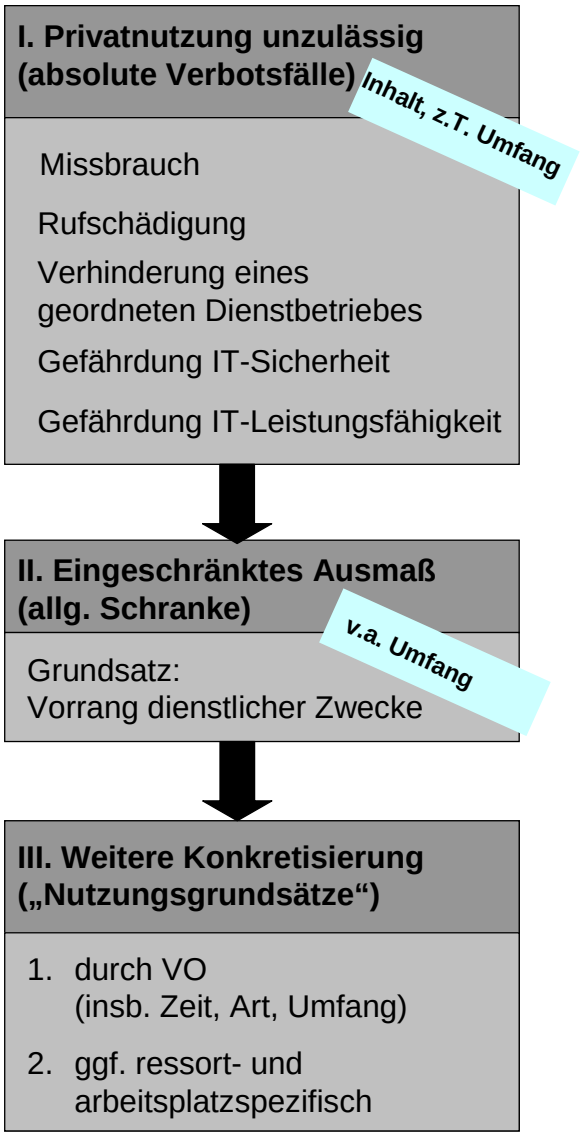

Abb. 6 Privatnutzung des dienstlichen Internetzugangs (nach Gesetzesentwurf)
Quelle: eigene Darstellung

[84] Dass Länder und Gemeinden nicht eingebunden worden seien, kritisiert das *Amt der Niederösterreichischen Landesregierung*, Stellungnahme, S. 2 (siehe Anhang)..

Diesen Grundsatz kraft Gesetz lockernd dürfen Mitarbeiter die IKT-Infrastruktur in eingeschränktem Ausmaß auch privat nutzen.[85] Die Erlaubnis bewirkt keinen Rechtsanspruch auf private Nutzung der betrieblichen Informations- und Kommunikationstechnik und ist neben der generellen Einschränkung des Ausmaßes durch fünf konkret benannte Interessen des Arbeitgebers beschränkt (vgl Abb. 6).

a.) Missbräuchliche Privatnutzung

Die private Nutzung in eingeschränktem Ausmaß darf nicht missbräuchlich erfolgen. Dieser Tatbestand ist in hohem Maß strafrechtlich sowie durch eine subjektive Komponente geprägt. Missbrauch in engerem Sinne erfolgt etwa durch Amtsmissbrauch, der – falls nicht schon bereits durch andere straf- oder dienstrechtliche Vorschriften geahndet – nicht von einer privilegierten, privaten Internetnutzung protegiert sein soll. Darüber hinaus soll wohl auch erfasst sein, wenn der Mitarbeiter betriebliche Informations- und Kommunikationstechnik (vorsätzlich) nutzt, um seinen Arbeitgeber zu schädigen. Zwar mag sich in diesem Fall der Arbeitgeber jedenfalls zivilrechtlich an dem Mitarbeiter schadlos halten. Infolge des ausdrücklichen gesetzlichen Verbots missbräuchlicher Privatnutzung dürfte sich der Arbeitgeber grundsätzlich auch nicht dem Vorwurf eines Mitverschuldens wegen fehlender Regelungen im eigenen Betrieb ausgesetzt sehen.

Wie den Erläuterungen zu entnehmen ist, soll der Missbrauchstatbestand auch eine zeitlich und den Volumina nach überschießende Privatnutzung umfassen.[86] Ein solches ausdrückliches Exzessverbot wird allerdings regelmäßig schon durch die ausdrückliche Beschränkung der Privatnutzung auf ein „eingeschränktes Ausmaß“ deutlich. Allfällige Präzisierungen, zB hinsichtlich des maximalen Datenvolumens, sind – so wie es die Erläuterungen vorsehen – kann die Regierung per Verordnung in den Nutzungsgrundsätzen festlegen.

[85] Entschiedener Widerstand der *Wirtschaftskammer Österreich*, Stellungnahme, S. 1 (siehe Anhang): Die gesetzliche Zulassung der Privatnutzung von betrieblicher Hard- und Software sei höchst problematisch „unter dem Aspekt der Sparsamkeit und Steuerzahlerkosten insbesondere für widmungswidrige Verwendung von Dienstzeiten“.

[86] Erläuterungen zum Gesetzesentwurf, S. 3 (Anhang)

b) Rufschädigung

Ein offenbar in der Praxis häufiger Fall ist es, dass in der Öffentlichkeit Mitarbeiter in einer den Arbeitgeber schädigenden Weise auftreten. Mitarbeiter haben es daher zu unterlassen, am Arbeitsplatz auf rechtswidrige oder sittlich verpönte Internetseiten zuzugreifen. Regelmäßig ist es für den Arbeitgeber ruf- und kreditschädigend, wenn Mitarbeiter zB Internetseiten mit pornografischem Inhalt aufsuchen und die Zugriffe dann öffentlich dem Arbeitgeber zugeordnet werden.

In diesem Zusammenhang enthalten der Gesetzesentwurf und die dazugehörigen Erläuterungen keine Hinweise, wie sich der Mitarbeiter mit seiner dienstlichen E-Mail-Adresse zu verhalten hat. Die heute typische dienstliche E-Mail-Adresse (Max.Mustermann@firma123.at) weist einerseits eine hohe Mitarbeiterindividualität auf, auf der anderen Seite ist sie regelmäßig unmittelbar der Firma des Arbeitgebers zuordenbar. Fraglich ist, ob der Mitarbeiter mit dieser dienstlichen E-Mail-Adresse an internetöffentlichen Diskussionsforen, Web-Bloggs und ähnlichen Meinungsplattformen teilnehmen darf. Ebenfalls zu prüfen ist, inwieweit ein Mitarbeiter für (private) Kunden-Accounts zB bei Online-Auktionshäusern, im elektronischen Versandhandel oder bei Online-Banking seine dienstliche E-Mail-Adresse soll hinterlegen dürfen. Diese Fragestellungen sind regelmäßig dazu geeignet, alle Mitarbeiter eines Betriebes gleichermaßen zu betreffen und würden daher sinnvollerweise einer betriebseinheitlichen Regelung bedürfen. Vorliegend hat der Gesetzgeber für den öffentlich-rechtlichen Beschäftigungssektor diese Konstellation tatbestandlich nicht ausdrücklich geregelt. Es ist aber von folgender Betrachtung auszugehen:

Dass privat veranlasste Meinungsäußerungen unter erkennbarer Verwendung dienstlicher E-Mail-Adressen unzulässig sind, wird sich in der Regel unter den Tatbestand einer möglichen Rufschädigung für den öffentlichen Dienstgeber subsumieren lassen. Dies gilt im öffentlichen Dienst erst recht, weil insbesondere Beamte ex officio grundsätzlich zu (partei-)politischer Neutralität verpflichtet sind.

Rechtsgeschäftliche (private) Betätigungen über den dienstlichen Internetzugang werden hingegen grundsätzlich nicht unzulässig sein.

Es wird insbesondere zu beachten sein, ob die Regierung in den per Verordnung zu erlassenden Nutzungsgrundsätzen solche praktisch bedeutsamen Fallgruppen erfassen wird.

c.) Aufrechterhaltung eines geordneten Dienstbetriebes, Gefährdung von IT-Sicherheit und IT-Leistungsfähigkeit

Diese Tatbestände stehen in engem sachlichen Zusammenhang, denn eine instabile Systemsicherheit bzw. eine verminderte Leistungsfähigkeit des Systems können regelmäßig zu einer wesentlichen Beeinträchtigung des geordneten Dienstbetriebs führen.

Grundsätzlich kann eine private Nutzung dienstlicher Informations- und Kommunikationstechnik qualitativ oder bzw. und quantitativ derart erfolgen, dass es zu Störungen der IT-Sicherheit oder der IT-Leistungsfähigkeit kommt. Ein Mitarbeiter kann ein derart hohes Datenvolumen aus dem Internet herunterladen, dass sich die Leistungsfähigkeit des IT-Servers insgesamt verlangsamt. Aber auch allein durch das Öffnen eines einzelnen Anhangs einer E-Mail kann Schadsoftware in das System eindringen und seine Funktionsfähigkeit behindern.

Das Gefährdungspotential erscheint enorm und ist zugleich gekennzeichnet durch eine hohe Komplexität.[87] Im Zweifel wird es allerdings für den Mitarbeiter eher schwierig sein zu erkennen, welche Nutzungen die IT-Sicherheit und IT-Leistungsfähigkeit bedrohen könnten. Es ist aber zugleich darauf hinzuweisen, dass ein absolutes Verbot von Datenverkehr weder bewerkstelligbar noch sinnvoll wäre: Auch durch Anhänge dienstlicher E-Mail oder sonstige dienstliche Internetnutzung kann Schadsoftware in das

[87] Jüngst stellten die Innenminister von Bund und Ländern in Deutschland in einem Programm Innere Sicherheit fest: „Angriffe auf die Integrität und Sicherheit von Datensystemen bergen in unserer modernen Informationsgesellschaft ein hohes Gefahrenpotential. (...) Eine zunehmende Bedeutung haben internetgebundene Angriffe auf Rechnersysteme von Wirtschaftsunternehmen und Regierungsstellen. (...) Deutsche Firmen stellen auf Grund der hohen Innovationskraft ein überdurchschnittlich attraktives Ziel für fremde Nachrichtendienste dar. (...) Das Internet als Tatort wird auch in der Zukunft nur begrenzt kontrollierbar sein.“ (Quelle: Handelsblatt v 03.06.09)

betriebseigene System eingeschleust werden und trotz der aktuellen Schutz- und Datensicherheitsmaßnahmen (zB Firewall, Antiviren-Tools) gegen Angriffe aus dem Internet wird ein an das Internet angebundene Firmennetzwerk nicht absolut sicher sein können. Ferner ist auch zu berücksichtigen, dass Mitarbeiter Programme herunterladen und sodann „gemischt" nutzen oder aber etwa dienstliche Programme einem notwendigen und ggf die Systemsicherheit erhöhenden Update zuführen.

Vorliegend ist es daher geboten, das Verbot systemgefährdender Internetnutzungen mittels Anordnung zu konkretisieren und damit die Mitarbeiter verständlich zu instruieren.[88] Sinnvoll erscheint ein abgestuftes Vorgehen: ZB für das Thema Anhänge von E-Mail könnte in den EDV-Sicherheitsrichtlinien folgendes vorgegeben sein:

1.) Bestimmte Dateitypen (*Gefährdungstyp rot*) werden systemseitig vom E-Mail-Clienten entfernt. Der Mitarbeiter kann diese (technisch) erst gar nicht öffnen.
2.) Bestimmte (und dem Mitarbeiter unbekannte) Dateitypen (*Gefährdungstyp gelb*) dürfen erst nach Rücksprache mit dem Absender und/oder mit der IT-Sicherheitsabteilung geöffnet werden.
3.) Dateitypen von dem Mitarbeiter unbekannten Absendern dürfen solange nicht geöffnet werden, bis die (vertrauenswürdige) Identität des Absenders bestimmt werden konnte.
4.) Bei Zweifeln hat der Mitarbeiter vor Öffnen der Datei den zuständigen IT-Administrator oder den Vorgesetzten zu unterrichten.

Abb. 7 Ausschnitt aus EDV-Sicherheitsrichtlinien bezüglich Anhängen von E-Mails
Quelle: eigene Darstellung

[88] Eine Dienstvereinbarung für technische und organisatorische Fragen empfiehlt dem Dienstherrn auch der *Bundesbeauftragte für Datenschutz*, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, S. 4

4.4. Ergebnis und Würdigung

Soweit keine besonderen Gründe in den individuellen Anforderungen eines Arbeitsplatzes liegen und insoweit abteilungsspezifische Abweichungen indizieren (zB bei Grundbuchbeamten, in der Finanzverwaltung oder in der Justiz)[89], ist das Reglement des Gesetzesentwurfs zu begrüßen. Es eröffnet den öffentlich Bediensteten zB die Möglichkeit, sich rechtmäßig in Pausen in Online-Ausgaben von Tageszeitungen zu informieren. Zugleich wird deutlich vor Augen geführt, dass private Internetnutzung zu unterbleiben hat, wenn berechtigte Interessen des Dienstgebers bestehen. So dürfen Mitarbeiter zB nicht unbekannte Anhänge privater E-Mail öffnen, wenn damit die Funktionsfähigkeit der IT-Infrastruktur gefährdet werden kann.

[89] Weitere Sonderbereiche des öffentlichen Diensts vgl unten Kap 6.

5. Kontrolle der Internetnutzung durch Arbeitgeber

5.1. Geltende Rechtslage

Bei der Nutzung des betrieblichen Internetzugangs fallen personenbezogene Verkehrs- und Inhaltsdaten des einzelnen Mitarbeiters an.[90] Möchte der Arbeitgeber auf diese personenbezogenen Daten zugreifen, so handelt es sich regelmäßig um ein Verarbeiten von Daten iSd § 4 Z 9 DSG 2000, dessen Zulässigkeit sich insbesondere nach dem Grundrecht auf Datenschutz des § 1 DSG 2000 sowie nach den §§ 6ff DSG 2000 richtet. Zugleich können ─ neben dem Arbeitsvertrag ─ die arbeitsrechtlichen Bestimmungen insbesondere der §§ 96 Abs. 1 Z 3, 96a ArbVG und § 10 AVRAG relevant sein.

5.1.1. Arbeitsrecht

Zu beachten ist in Betrieben, in denen ein Betriebsrat eingerichtet ist, vor allem dessen zwingende Mitbestimmungskompetenz nach § 96 Abs 1 Z 3 ArbVG bei der Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren.[91] Die Einführung und Aufrechterhaltung derartiger Kontrollmaßnahmen ohne den Abschluss einer Betriebsvereinbarung ist demnach rechtswidrig.[92]

Nach herrschender Auffassung in der Literatur genügt primär bereits die abstrakte Eignung eines EDV-Systems zur Kontrolle der Mitarbeiter, um einen notwendige Mitbestimmung auszulösen.[93] Die Rechtsprechung sieht die Menschenwürde iSd § 96 Abs 1 Z 3 ArbVG bei einer betrieblichen Telefonanlage auch dann berührt, wenn durch eine Taste am Telefongerät die Endziffern der Rufnummer im System unterdrückt werden können.[94]

---

[90] Vgl oben Kap 2

[91] ausführlich *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 123ff, 232ff

[92] *Gerlach*, Der gesetzliche Schutz von Arbeitnehmerdaten, S. 1; *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 229; *Obereder*, RdA 2001, 75; *Naderhirn*, Kollektives Arbeitsrecht und Arbeitnehmerkontrolle, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 94

[93] *Thiele*, ecolex 2001; *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 230; *Obereder*, RdA 2001, 75; aA *Sacherer*, RdW 2005, 627: Allzu optimistisch erscheint aber sein Argument, dass ein Arbeitgeber auch bei einem Verbot der Privatnutzung ausschließlich Daten protokolliert, die für eine sichere Abwicklung der Dienste technisch notwendig seien. Keine notwendige Mitbestimmung, falls nicht speziell Kontrollmechanismen adaptiert wurden, fordert *Dellisch*, ASoK 2001, 316.

[94] OGH 13.06.02, 8 ObA 288/01p; dazu krit Besprechungsaufsatz von *Brodil*, ZAS 2004, 17

Eine teleologische Reduktion dahingehend, dass § 96 Abs 1 Z 3 ArbVG nur bei tatsächlich durchgeführten Kontrollmaßnahmen angewendet werden soll, wird in der Lehre zwar angedacht, aber insbesondere eine Einschränkung des Merkmals „Berühren der Menschenwürde“ [95] angesichts der technischen Möglichkeit eines gläsernen Angestellten nicht gefordert.[96] Nicht ganz wortgleich, da nicht nur die Einführung entsprechender Systeme, sondern auch deren (fortdauernde) Verwendung unter einen Zustimmungsvorbehalt gestellt wird, ordnet § 10 AVRAG für Betriebe ohne Betriebsrat ein Zustimmungserfordernis der einzelnen Arbeitnehmer an.

§ 10 AVRAG erscheint datenschutzrechtlich nicht unbedenklich. Eine datenschutzrechtliche Einwilligung in eine Datenverwendung muss nach eindeutiger europarechtlicher Vorgabe freiwillig erfolgen.[97] Zu Recht steht deshalb die herrschende Lehre in Deutschland und wohl auch in Österreich datenschutzrechtlichen Einwilligungen eines Arbeitnehmers skeptisch und teils ablehnend gegenüber, da dem Arbeitnehmer aufgrund dem Abhängigkeitscharakter des Arbeitsverhältnisses zumindest mittelbar Nachteile bei einer Zustimmungsverweigerung drohen.[98]

Dieser – wenn auch nur unterschwellige – Druck auf den Arbeitnehmer dürfte regelmäßig zu der dogmatischen Einschätzung führen, dass ein schriftliches Einverständnis nach § 10 AVRAG keine hinreichende datenschutzrechtliche Einwilligung sein kann, sondern nur die Kenntnisnahme des Arbeitnehmers

---

[95] Dieses Tatbestandsmerkmal besteht in Deutschland de lege lata nicht, vgl § 87 Abs 1 Z 6 dBetrVG: „Der Betriebsrat hat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, in folgenden Angelegenheiten mitzubestimmen: Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Die Pflicht zu einer erzwingbaren Betriebsvereinbarung wird demnach zB ausgelöst durch den Einsatz einer Software zum Datenabgleich; vgl *Steinkühler/Raif*, AuA 2009, 213 (215). Ein Datenabgleich oder eine Überwachung anlässlich eines konkreten Verdachtsmoments sei schon von dem allg. Überwachungsrecht des Betriebsrats (§ 80 dBetrVG) erfasst, meint *Haar*, iX Nr. 6/2009, S. 90f; ausführlich zur Zuständigkeit nach dBetrVG *Trittin/Fischer*, NZA 2009, 343ff; ähnlich auch *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S. 15

[96] *Stiger* ,Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 417; *Eichinger/Kreil/Sacherer*, Basiswissen Arbeits- und Sozialrecht, S. 94f; anders noch *Rotter*, ASoK 1999, 118

[97] Art. 2 lit. h RL 95/46/EG (Datenschutzrichtlinie), *Ehmann/Helfrich*, EG-Datenschutzrichtlinie Kurzkommentar, Art 2 Rz 66

[98] *Bergmann/Möhrle/Herb*, Datenschutzrecht Kommentar, § 4a, Rz 5a; *Büllesbach*, Beschäftigtendatenschutz, in *Roßnagel (Hrsg)*, Handbuch Datenschutzrecht, Rz 13ff; *Kotschy/Reimer*, ZAS 2004, 167; *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 37f; aA *Eichinger/Kreil/Sacherer*, Basiswissen Arbeits- und Sozialrecht, S. 95f; *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 251; *Brodil*, Individualarbeitsrechtliche Fragen der Kontrolle des Arbeitnehmers, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 75

von der gegenständlichen Datenverwendung nach § 24 DSG 2000 bezeugt. Empfindlich erhöht wird der Druck auf den einzelnen Mitarbeiter, Kontrollmaßnahmen nach § 10 AVRAG zuzustimmen, wenn der Arbeitgeber bestimmte Vorteile (insbesondere Privatnutzung) zum Ausgleich in Aussicht stellt. Es ist nicht verständlich, dass *Löschnigg* trotz des so direkt erzeugten Zustimmungsdrucks – ohne weitere Begründung – keine unsachliche Benachteiligung von nicht zustimmenden Arbeitnehmern erblicken will;[99] *Sacherer* empfiehlt es Arbeitgebern sogar, die Zustimmung an die Zulässigkeit der Privatnutzung zu binden.[100]

5.1.2. Grundrecht auf Datenschutz

Jeder Mitarbeiter hat nach der Verfassungsbestimmung des § 1 Abs 1 DSG 2000 Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.

Daten von Arbeitnehmern werden nach österreichischer Lehrmeinung generell als besonders schutzwürdig angesehen.[101] Das Grundrecht auf Datenschutz nach § 1 DSG 2000 ist eine österreichische Besonderheit: Es handelt sich um eine Verfassungsbestimmung mit unmittelbarer Drittwirkung auch im Privatrechtsverkehr.[102] Verletzungen des Grundrechts auf Datenschutz können gemäß § 1 Abs 5 DSG 2000 auch gegen private Rechtssubjekte im Zivilrechtsweg geltend gemacht werden[103]; insbesondere wirkt es auch unmittelbar zwischen Dienstgeber und Dienstnehmer.[104] Ein Eingriff in das Geheimhaltungsinteresse des Mitarbeiters ist demnach nur dann gerechtfertigt, wenn die Datenverwendung durch den Arbeitgeber

[99] *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 255
[100] Im Satz zuvor noch betont er, dass der Arbeitnehmer „frei von Zwang zugestimmt" haben müsse, *Sacherer*, RdW 2005, 173
[101] *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 162 mwN
[102] *Kotschy/Reimer*, ZAS 2004, 167; *Stärker*, DSG, S. 26; *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 62; grundlegend *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 120f: Eine unmittelbare Drittwirkung der Grundrechte komme nach hM in Ö weitgehend nicht in Frage. Dazu und zur mittelbaren Drittwirkung über auslegungsbedürftige Generalklauseln (§ 16 ABGB) auch *Brodil*, Kontrolle und Datenschutz im Arbeitsrecht, 121 (122); *Brodil*, Individualarbeitsrechtliche Fragen der Kontrolle des Arbeitnehmers, in *Rech (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 71
[103] *Jahnel*, Datenschutzrecht, in *Jahnel/Schramm/Staudegger (Hrsg)*, Informatikrecht, S. 251
[104] *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 424f

1.) im lebenswichtigen Interesse des Mitarbeiters steht,

2.) aufgrund einer Zustimmung des Mitarbeiters erfolgt oder

3.) sich auf überwiegende Interessen[105] stützt.

Über das Grundrecht des einzelnen Mitarbeiters kann nicht von Dritten disponiert werden, dh eine Betriebsvereinbarung nach § 96 Z 3 ArbVG bewirkt per se keine hinreichende Eingriffsgrundlage in das Grundrecht des § 1 DSG 2000; auch der disponible Bereich des Persönlichkeitsschutzes bestimmt sich grundsätzlich nicht nach betriebsverfassungsrechtlichen Zulassungsvorschriften.[106] Jedoch wird in einer höchstgerichtlichen Entscheidung der Abschluss einer solchen Betriebsvereinbarung herangezogen, um überwiegende berechtigte Interessen des Arbeitgebers iSd § 1 DSG 2000 zu rechtfertigen.[107] Unabhängig vom Vorliegen einer Betriebsvereinbarung darf der der Arbeitgeber keine Kontrollmaßnahmen durchführen, welche den unverzichtbaren Kern des Persönlichkeitsschutzes des Arbeitnehmers berühren bzw. verletzen würden.[108]

Außerordentlich problematisch erscheint, welcher Qualität eine Zustimmungserklärung des Mitarbeiters nach § 1 Abs 2 DSG 2000 bedarf.[109] Zu erinnern ist in diesem Zusammenhang insbesondere auch an § 10 AVRAG sowie an § 8 Abs 1 Z 2 DSG 2000 bzw. für sensible Daten an § 9 Z 6 DSG 2000. Ident sprechen die drei Vorschriften von „Zustimmung", welche der Mitarbeiter zur Datenverwendung erteilen muss.[110] Gemessen an der Reichweite der Zustimmungserklärung bzw. des Schutzzwecks sind an eine datenschutzrechtlich wirksame Zustimmungserklärung (als Grundlage in den Eingriff des Grundrechts auf Datenschutz iSd § 1 DSG 2000) höhere

---

[105] Vgl dazu auch unten das nächste Kapitel zu den §§ 8 und 9 DSG 2000.

[106] Zu den dogmatischen Schwierigkeiten bzw. zur Rangordnung der hier einschlägigen Rechtsnormen angesichts von Grundrecht, Mitbestimmungsrecht und einfachgesetzlichen Bestimmungen *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 233ff (differenziert die Position des Arbeitnehmers vor allem danach, ob die Kontrollmaßnahme den unverzichtbaren Kern oder den disponiblen Bereich seines Persönlichkeitsbereichs betrifft.)

[107] So der OGH leider ohne weitere Begründung für eine Telefonanlage mit elektronischem Telefonkontrollsystem, wenn im Rahmen einer Betriebsvereinbarung nach § 96 Abs 1 Z 3 ArbVG ein umfassender Interessenausgleich zwischen Arbeitgeber und Betriebsrat zustande gekommen ist (OGH 13.06.2002, 8 Ob A 288/01p).

[108] *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 233

[109] Ausführlich *Reimer*, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung, in *Jahnel/Siegwart/Fercher (Hrsg)*, Aktuelle Fragen des Datenschutzrechts, S. 183ff

[110] Nur scheinbar folgerichtig benennt *Dellisch* daher in einem Atemzug, dass das Einvernehmen schriftlich mit den „ausdrücklichen Zustimmungen des Dienstnehmers gemäß § 10 AVRAG und §§ 1 und 9 Z 6 DSG 2000" vereinbart werden sollte, *Dellisch*, ASoK 2001, 316.

Anforderungen zu stellen als an die arbeitsrechtliche Bestimmung des § 10 AVRAG. Dies gilt insbesondere bezüglich der Informiertheit und der Freiwilligkeit iSd § 4 Z 14 DSG 2000 des Mitarbeiters.[111]

Grundsätzlich sind Datenverwendungen zulässig, wenn der Betroffene zugestimmt hat. Es wäre demnach zu überlegen, ob ein Mitarbeiter zB in stichprobenartige Kontrollen der Einhaltung einer Internet Policy datenschutzrechtlich wirksam einwilligen kann. Eine datenschutzrechtliche Zustimmung kann nur freiwillig, dh ohne Zwang, abgegeben werden. An der Freiwilligkeit würde es mangeln, wenn der Mitarbeiter infolge einer Verweigerung oder späteren Rücknahme der Zustimmung tatsächliche oder potentielle Nachteile zu befürchten hätte. Mit gleicher Argumentation möchte die Artikel 29 Datenschutzgruppe die Einwilligung des Beschäftigten nur dann als Ausweichmöglichkeit vorsehen, falls der Beschäftigte eine „echte Wahl" habe, und bekräftigt die Erfordernisse an eine datenschutzrechtlich gültige Einwilligungserklärung (vgl. Abb. 8).[112]

> *„Angesichts der besonderen Merkmale eines Beschäftigungsverhältnisses kann die Einwilligung im Normalfall die Verarbeitung von Beschäftigtendaten nicht rechtfertigen. Wird darauf zurückgegriffen, muss die Einwilligung stets freiwillig, muss die Einwilligung stetes freiwillig, für den konkreten Fall und in Kenntnis der Sachlage erfolgen."*[113]

Der verbreiteten Auffassung über eine informierte Einwilligungserklärung folgend, die für bestimmte Datenarten und festgelegte Verarbeitungszwecke[114] bis auf Widerruf abgegeben werden kann, erscheint eine deutsche Einzelmeinung verfehlt, die bei erlaubter Privatnutzung erkennen will, dass der Arbeitgeber den Arbeitnehmer bei jeder (rechtmäßigen) Prüfung einzeln um Erlaubnis bitten müsse, wenn der Arbeitgeber nicht ausdrücklich für die private Nutzung die Bedingung von stichprobenartigen Kontrollen gestellt

---

[111] *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 252ff; *Reimer*, Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung, in *Jahnel/Siegwart/Fercher (Hrsg)*, Aktuelle Fragen des Datenschutzrechts, S. 183 (199ff)

[112] *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 27f; so auch DSK 08.03.06, ARD 5784/11/2007

[113] *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 34

[114] OGH 27.01.99, 7 Ob 170/98w = ecolex 1999, 182

hat.[115] Weil nicht die gegenständliche Ausgangslage bezüglich Kontrollmöglichkeiten in einem Beschäftigungsverhältnis vor Augen, vermag eine abschließende Klärung für das vorliegende Thema auch eine Entscheidung des OGH nicht zu leisten, dass ein Betroffener iSd DSG 2000 „in Kenntnis der Sachlage für den konkreten Fall" wirksam zustimmen könne.[116]

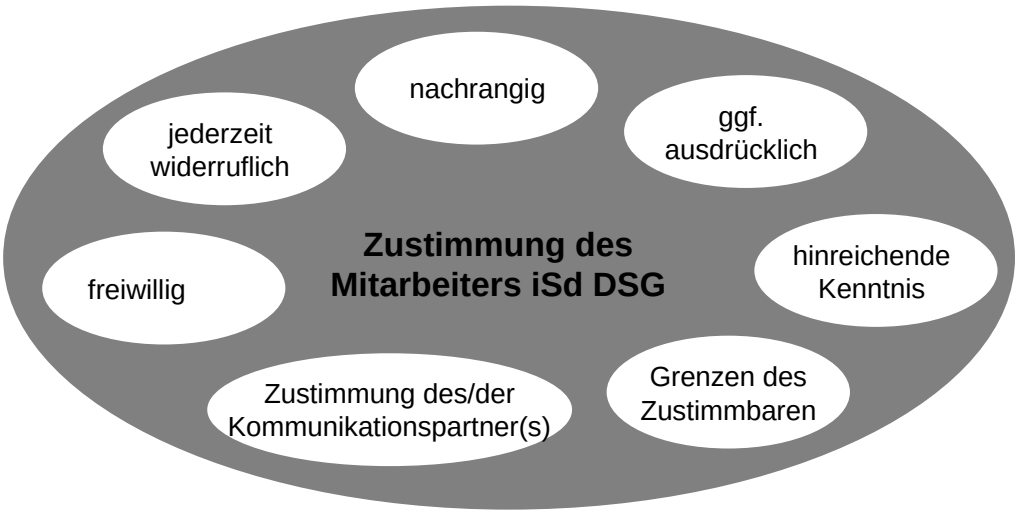

Abb. 8 Anforderungen an eine datenschutzrechtlich wirksame Zustimmungserklärung
Quelle: eigene Darstellung

Weiterhin ist insbesondere zu beachten, dass Arbeitnehmer ihre Zustimmung grundsätzlich[117] jederzeit frei zurücknehmen können.[118] Allein auf Zustimmungen begründete Datenverwendungen erscheinen deshalb in einem Betrieb kaum praktikabel. Der OGH verneint darüber hinaus eine gültige Zustimmung, wenn der Betroffene auf sein Widerrufsrecht nicht hingewiesen wurde.[119]

[115] Ohne weitere Begründung jüngst *Haar*, iX Nr. 6/2009, 90 (91); zu konzedieren ist allerdings, dass auch die *Artikel 29 Datenschutzgruppe* die Einwilligung nur „für den konkreten Fall" zulassen will (vgl oben FN 113); aA *Bundesbeauftragter für Datenschutz*, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, S. 4 und *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S. 27f (Erlaubnis der Privatnutzung darf mit angemessener Art der Kontrolle verknüpft werden.)

[116] OGH 22.03.2001 = ecolex 2001, 438

[117] Es sei denn, die Zustimmungserklärung wurde nach § 10 Abs 2 AVRAG schriftlich und befristet abgegeben; beachte aber auch weiter unten die jederzeitige Widerruflichkeit nach Datenschutzrecht.

[118] Das fristlose Kündigungsrecht der Zustimmung deutlich mit einem allg. Schikaneverbot bzw. mit den Maßstäben der Sittenwidrigkeit einschränken, wollen *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 68

[119] OGH 19.11.2002, 4 Ob 179/02f.

5.1.3. Datenschutzgesetz 2000

Die Zulässigkeit der Verwendung von Daten des Mitarbeiters zu Kontrollmaßnahmen des Arbeitgebers richtet sich nach den §§ 6ff DSG 2000. Stets zu beachten bei der Verwendung personenbezogener Daten hat der Arbeitgeber die allgemeinen datenschutzrechtlichen Grundsätze der §§ 6f DSG 2000, das sind insbesondere eine strenge Zweckbindung, Beachtung der Verhältnismäßigkeit sowie das Prinzip des gelindesten Mittels zur Zweckerreichung.[120] Zulässigkeitsvoraussetzungen für eine Verwendung von Internetnutzungsdaten durch den Arbeitgeber ergeben sich aus dem § 8 DSG 2000 (nichtsensible Daten) oder dem § 9 DSG 2000 (sensible Daten).

§ 9 DSG 2000 ist nur anzuwenden auf sensible Daten: Wie oben gezeigt, sind entgegen der herrschenden Lehre Verkehrsdaten der Internetnutzung von Mitarbeitern grundsätzlich nicht per se sensiblen Daten, wenn der Arbeitgeber in zulässiger Weise die Internetnutzung seiner Mitarbeiter kontrolliert.[121] Ist ausnahmsweise doch von sensiblen Daten auszugehen, so ist nach § 9 DSG 2000 ein grundsätzliches Verwendungsverbot sensibler Daten mit taxativem Ausnahmenkatalog zu befolgen.

a) Ausdrückliche Zustimmung des Betroffenen (§ 9 Z 6 DSG 2000)

Vorstellbar ist, dass der Mitarbeiter einer Kontrolle seines Internetzugangs ausdrücklich zustimmt. Zu den Anforderungen an eine datenschutzrechtlich wirksame Zustimmung gelten die vorherigen Ausführungen.[122] Bei § 9 Z 6 DSG 2000 tritt das Merkmal der Ausdrücklichkeit hinzu, infolge dessen die Zustimmung nachstehende Kriterien zusätzlich zu erfüllen hat: [123]

- keine Klausel in AGB
- Hervorhebung
- gesonderte Unterzeichnung

[120] *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 2f; auch *Brodil*, ZAS 2009, 121 (122)
[121] Vgl oben Kap 2.3.
[122] Vgl oben Kap 5.1.1. und 5.1.2.
[123] Vgl zu Form und Inhalt einer ausdrücklichen Zustimmungserklärung insbesondere das Rundschreiben des Verfassungsdiensts des BKA, 810.008/1-V/1a/85 v 10.8.1965. Entgegen des gesetzlichen Wortlautes sei auch eine konkludente Zustimmung möglich, ist Mindermeinung von *Sacherer*, RdW 2005, 173.

- detaillierte Beschreibung der Datenanwendung
- Hinweis auf jederzeitige Widerrufsmöglichkeit
- Schriftform de facto erforderlich[124]

b) Spezialvorschrift Arbeits- und Dienstrecht (§ 9 Z 11 DSG 2000)

Die Bedeutung von § 9 Z 11 DSG 2000 ist wohl eher gering einzuschätzen, obgleich es sich prima facie um eine einschlägige Spezialvorschrift handeln könnte.[125] Nach einer höchstgerichtlichen Entscheidung bringe diese auf Arbeitsverhältnisse bezogene Sonderregelung eine Erleichterung für Unternehmen, wohl ist dies allerdings nicht auf den vorliegenden Kontext beziehbar. Angesprochen werden nämlich – ausweislich auch Art 8 Abs 2 lit b der RL 95/46/EG –[126] gesetzlich vorgeschriebene Verarbeitungen und Übermittlungen sensibler Beschäftigtendaten wie zB nach sozialversicherungsrechtlichen Vorschriften oder für vorhandene Lohnpfändungen[127], die ohne § 9 Z 11 DSG 2000 nur mit ausdrücklicher Zustimmung jedes Mitarbeiters zulässig wären.[128] Genau dies fordert aber *Jahnel*, der die ausdrückliche Zustimmung der einzelnen Mitarbeiter als einzige Zulässigkeitsgrundlage einer Protokollierung des E-Mail-Verkehrs anerkennt.[129] Für *Hattenberger* ist das ein datenschutzrechtliches Problem, das für den Arbeitgeber nur durch Aufzeichnungsverzicht lösbar sei.[130]

Der explizit für das Arbeits- und Dienstrecht vorgesehene § 9 Z 11 DSG 2000 erfährt in der Lehre teils große Kritik, da der Tatbestand missverständlich sei.[131] Die Verwirrung verstärkend ist eine höchstgerichtliche Entscheidung,

---

[124] *Dohr/Pollirer/Weiss*, Datenschutzrecht, § 9 Anm 9 (Schriftform wird „dringend empfohlen".)

[125] Die *Artikel 29 Datenschutzgruppe* benennt als relevante österreichische Datenschutzvorschriften für Beschäftigte neben dem DSG 2000 und § 96 ArbVG den § 9 Z 11 DSG als „besondere Vorschrift" (*Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 10).

[126] Vgl auch *Ehmann/Helfrich*, EG-Datenschutzrichtlinie Kurzkommentar, Art 8 Rz 23ff

[127] *Brodil*, ZAS 2004, 156 (159)

[128] OGH 29.6.06, 6 Ob A 1/06z; so auch *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 173; irreführend *Brodil*, der beim Tatbestand des § 9 Z 11 DSG 2000 von Interessenabwägung spricht (*Brodil*, ZAS 2004, 156 (159)), denn der taxative Katalog an Erlaubnistatbeständen des § 9 DSG 2000 sieht gerade keine überwiegenden berechtigten Interessen des Auftraggebers vor; vgl zutreffend *Stärker*, DSG, S. 72f; *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 50

[129] *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *IT-LAW.AT (Hrsg)*, E-Mail – elektronische Post im Recht, S. 98

[130] *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg.)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 43f

[131] Eingehend *Brodil*, ZAS 2004, 156 (158ff); *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner

die sich damit zu befassen hatte, ob sich auf § 9 Z 11 DSG 2000 eine Aktivlegitimation gründen lässt; dies wurde aus für das DSG 2000 rechtssystematisch zweifelsfrei richtigen Überlegungen abgewiesen.[132]

Zu verkürzt ist die Meinung von *Dohr/Pollierer/Weiss*, die für die Zulässigkeit von Kontrollmaßnahmen in den Bestimmungen des Arbeitsverfassungsrechts „eine durchaus befriedigende Antwort" erblicken und den § 9 Z 11 DSG 2000 insoweit offenbar erschöpft sehen.[133] ME sind nach § 9 Z 11 DSG 2000 folgende zwei Voraussetzungen kumulativ zu erfüllen:[134]

1.) Die Datenverwendung (zu Kontrollmaßnahmen) muss erforderlich sein, um den Rechten des Arbeitgebers Rechnung zu tragen.

Mit der Umschreibung von Rechten und Pflichten auf dem Gebiet des Arbeits- oder Dienstrechts ist mE eine umfassende Betrachtung geboten, d.h. der Arbeitgeber wird regelmäßig darzulegen haben, welche schutzwürdigen Interessen aus dem Beschäftigungsverhältnis er mit den Kontrollmaßnahmen verfolgt, weiters ob diese geeignet, erforderlich und verhältnismäßig sind und schließlich, ob nicht schutzwürdige Geheimhaltungsinteressen des Mitarbeiters überwiegen

2.) Die Datenverwendung muss nach „besonderen Rechtsvorschriften" zulässig sein.

Ist eine Kontrollmaßnahme nach 1.) zulässig, so bedarf sie zusätzlich noch einer besonderen Rechtsvorschrift. Eine solche ist insbesondere in

---

Medien, S. 49ff; *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 173; *Gerhartl*, ASoK 2008, 147 (151)

[132] OGH 29.6.06, 6 Ob A 1/06z mit Anm *Hattenberger*

[133] *Dohr/Pollirer/Weiss*, Datenschutzrecht, § 9 Anm 14; so offenbar auch *Stärker*, DSG, S. 274 und *Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in *Österreichische Juristenkommission (Hrsg)*, Grundrechte in der Informationsgesellschaft, S. 173

[134] Im Ergebnis ähnlich *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 173; *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 49ff mwN; aA *Brodil*, ZAS 2004, 159 FN 42 (sieht die beiden Voraussetzungen wohl alternativ)

§ 96 Abs. 1 Z 3 ArbVG zu erblicken,[135] mE – wenn auch mit großen Bedenken (vgl oben Kap 5.1.1. und 5.1.2.) – für Betriebe ohne Betriebsrat auch in § 10 AVRAG.

Löschnigg lehnt eine Zustimmung nach § 10 AVRAG als „besondere Rechtsvorschrift" ab und will eine solche nur bei normativ wirkenden Rechtsquellen (Betriebsvereinbarungen, Kollektivverträge, Satzungen) annehmen.[136] Überlagert wird diese Betrachtung mE aber von der (ausdrücklich gewollten) gesetzgeberischen Gleichstellung bzw. Auffanglösung des § 10 AVRAG für Unternehmen und Mitarbeiter, die offenbar auch im Ergebnis nicht bloß ob des Fehlens eines Betriebsrats datenschutzrechtlich anders behandelt werden sollen. Dahin könnte eventuell auch *Löschniggs* Aussage an anderer Stelle gedeutet werden, dass die Bestimmung des § 96 Abs 1 Z 3 ArbVG „inhaltlich für Betriebe ohne Betriebsrat auch im § 10 AVRAG abgebildet" worden sei.[137]

Zu beachten ist ferner in diesem Zusammenhang der genaue Wortlaut, der darauf abstellt, ob die Voraussetzungen der einschlägigen besonderen Rechtsvorschrift erfüllt sind. Kontrollmaßnahmen oder technische Systeme, welche die Menschenwürde berühren, sind nach § 96 Abs. 1 Z 3 ArbVG nur zulässig, wenn der Betriebsrat ihrer Einführung zugestimmt hat. In Betrieben ohne Betriebsrat ist nach § 10 AVRAG die Zustimmung des Arbeitnehmers erforderlich. Der insoweit von der österreichischen Lehre hinzugezogene Vergleich mit der Rechtslage in Deutschland ist zutreffend:[138] Nach § 4 Abs 1 dBDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener

---

[135] *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg.)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 51; *Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in *Österreichische Juristenkommission (Hrsg)*, Grundrechte in der Informationsgesellschaft, S. 173f; aA *Sacherer*, RdW 2005, 173; *Brodil*, ZAS 2004, 156 (159): Die Rechtsvorschriften müssten leges speciales außerhalb des DSG und des ArbVG bzw. des AVRAG sein.

[136] *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 174; so auch *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *IT-LAW.AT (Hrsg)*, E-Mail – elektronische Post im Recht, S. 98; so vorsichtig auch *Brodil*, ZAS 2004, 156 (159); aA *Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in *Österreichische Juristenkommission (Hrsg)*, Grundrechte in der Informationsgesellschaft, S. 173

[137] *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 229, zum Ersetzungseffekt von § 10 AVRAG in betriebsratslosen Betrieben auch auf S. 255; ähnlich *Mazal/Risak (Hrsg)*, Das Arbeitsrecht − System und Praxiskommentar Kap X.6., Rz 68; *Laimer/Mayr*, DRdA 2003, 410 (414f); *Posch*, Die e-Mail-Nutzung aus arbeitsrechtlicher Sicht, in *IT-LAW.AT (Hrsg)*, e-Mail – elektronische Post im Recht, S. 83

[138] Vergleichend, aber im Ergebnis für Österreich ablehnend *Brodil*, ZAS 2004, 156 (159)

Daten „nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat." Unstrittig sind in Deutschland Betriebsvereinbarungen normativ wirkende Rechtsvorschriften im Sinne dieser datenschutzrechtlichen Vorschrift.[139]

§ 9 Z 11 DSG 2000 unterstreicht also das Erfordernis einer Betriebsvereinbarung (bzw. einer Zustimmung des Arbeitnehmers), ohne die eine Datenverwendung jedenfalls nicht nach § 9 Z 11 DSG 2000 zulässig ist. Im Umkehrschluss kann als Beispiel für das Fehlen einer „besonderen Rechtsvorschrift" angeführt werden: Nach dem BDG idgF sind Systeme zu Kontrollmaßnahmen, welche die Menschenwürde berühren, jedenfalls unzulässig (§ 79c BDG idgF), dh im Beamtendienstrecht sind nach geltendem Recht Kontrollmaßnahmen und entsprechende technische Systeme auch gemäß § 9 Z 11 DSG 2000 keinesfalls zulässig.

c) Zustimmung des Betroffenen (§ 8 Abs 1 Z 2 DSG 2000)

Grundsätzlich können Betroffene in die Verwendung ihrer personenbezogenen Daten einwilligen, wobei die Zustimmungserklärung jederzeit pro futuro widerruflich ist.[140]

Zur Problematik der Zustimmungserklärung im Beschäftigungsverhältnis ist auf obige Ausführungen (lit a) dieses Kapitels sowie Kap 5.1.1. und 5.1.2.) zu verweisen.

d) Zur Erfüllung einer arbeitsvertraglichen Verpflichtung (§ 8 Abs 1 Z 4 iVm § 8 Abs 3 Z 4 DSG 2000)

Würde der Arbeitgeber mit den Kontrollmaßnahmen einer Verpflichtung aus dem Arbeitsvertrag genügen, so könnten diese nach § 8 Abs 1 Z 4 iVm § 8 Abs 3 Z 4 DSG 2000 rechtmäßig sein. Es wäre aber überschießend, eine Kontrolle der Internetnutzung zur Erfüllung arbeitsvertraglicher Pflichten per se als erforderlich einzustufen. Welche Datenarten und welche Verwendungszwecke gewöhnlich zur Erfüllung arbeitsvertraglicher Pflichten erforderlich sind, kann insbesondere der Standard-Datenanwendung „SA002

[139] BAG 27.05.1986, 1 ABR 48/84 = DB1986, 2080
[140] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie Kurzkommentar, Art. 2 Rz 72f

Personalverwaltung für privatrechtliche Dienstverhältnisse“ der Standard- und Muster-Verordnung 2004 (Anlage 1)[141] entnommen werden. Personenbezogene Daten über die Internetnutzung eines Mitarbeiters gehören regelmäßig nicht dazu.

e) Überwiegende berechtigte Interessen des Arbeitgebers (§ 8 Abs 1 Z 4 DSG 2000)

Geboten erscheint eine umfassende Feststellung schutzwürdiger Interessen des Arbeitnehmers und des Arbeitgebers, wobei zugunsten des Arbeitnehmers stets das Grundrecht auf Datenschutz (§ 1 DSG 2000), das Recht auf Privat- und Familiensphäre (Art 8 EMRK) sowie das Kommunikationsgeheimnis (Art.10a StGG iVm TKG 2003) zu berücksichtigen sein werden. Auf Seiten des Arbeitgebers sind neben arbeitsvertraglichen Berechtigungen (insbesondere Direktionsrecht) das in Art 5 StGG normierte Grundrecht der Unverletzlichkeit des Eigentums einzubeziehen.[142]

Umstritten ist in der österreichischen Lehre der grundlegende Ausgangspunkt des Arbeitsrechts: Zur Beurteilung der Zulässigkeit von Kontrollmaßnahmen geht *Brodil* von einer für ein Beschäftigungsverhältnis wesenstypischen umfassenden Kontrollunterworfenheit des Arbeitnehmers aus.[143] Schädlich und irreführend hingegen ist nach Meinung *Hattenbergers* eine Betonung der Kontrollunterworfenheit, weil sie eine unbeschränkte Kontrollbefugnis des Arbeitgebers suggeriere; Kontrolle dürfe auch im Arbeitsrecht kein Selbstzweck sein, vielmehr habe sich die Kontrollintensität nach den datenschutzrechtlichen Prüfschritten Erforderlichkeit und gelindestes Mittel an den arbeitsvertraglichen Verpflichtungen des Arbeitnehmers zu orientieren und insoweit auch zu beschränken.[144]

Die Schutzwürdigkeit des Arbeitnehmers wird sich regelmäßig auch daran zu orientieren haben, welche (private) Internetnutzung dem Arbeitnehmer erlaubt

---

[141] Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 - StMV 2004), BGBl. II Nr. 312/2004

[142] OGH 13.06.2002, 8 Ob A 288/01p; *Kotschy/Reimer*, ZAS 2004, 167

[143] *Brodil*, ZAS 2009, 121f, so schon auch in ZAS 2004, 156, 166; ähnlich *Sacherer*, RDW 2005, 173

[144] *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg.)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 42f

ist (vgl Kap 4).[145] Anschließend hat eine Abwägung der beiderseitigen schutzwürdigen Interessen für den konkreten Einzelfall zu erfolgen. Dieser Ansatz einer umfassenden Interessenabwägung ist dem Arbeits- und dem Datenschutzrecht nicht fremd.

Auf Arbeitgeberseite mag eingewendet werden, dass Kontrollen damit de facto nur eng anlassbezogen rechtmäßig durchführbar sein werden. Dem ist entgegenzuhalten, dass eine willkürliche Überwachung nicht erwünscht sein kann. Vielmehr gilt, was schon ausgeführt wurde (Kap 4): Ist den Arbeitnehmern durch gesetzliche oder bzw. und betriebliche Regelungen klar verständlich, welche Internetnutzung erlaubt ist, so hat eine Überwachung innerhalb der erlaubten Nutzung grundsätzlich hintenan zu stehen.

Umgekehrt wird der Arbeitgeber bei Übertretungen klarer Vorgaben ein berechtigtes Interesse an Kontrollen haben; die Interessen des Arbeitnehmers treten diesfalls bei Missachtung klarer Vorgaben in den Hintergrund.[146] Nicht nachvollziehbar ist allerdings das Fazit des deutschen Branchenverbands *BITKOM e.V.*, dass wegen fehlender Judikatur zur Interessenabwägung „überwiegende Interessen des Arbeitgebers anzunehmen und dem Arbeitgeber so einen großen Spielraum bei der Wahrnehmung seiner Datenverarbeitungsinteressen zu gewähren“ sein soll.[147]

Die datenschutz- und arbeitsrechtliche Interessenabwägung ist mE zumindest für den konkreten Einzelfall durch klare Zulässigkeitsbestimmungen zur Internetnutzung am Arbeitsplatz weithin determinierbar, was im Sinne von allseitiger Transparenz und Rechtssicherheit zu begrüßen ist.[148]

Auf die besondere Problematik von Wirtschaftskriminalität, Korruption und anderen Compliance-Themen in Unternehmen kann in dieser Arbeit nicht näher eingegangen werden; ob bzw. inwieweit in diesem Zusammenhang

[145] *Bundesbeauftragter für Datenschutz*, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, S. 1; sogar entscheidend nach *Haar*, iX Nr. 6/2009, 90 (91); *Sacherer*, RdW 2005, 173; und *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S 39

[146] So auch *Brodil*, Kontrolle und Datenschutz im Arbeitsrecht, 121 (122); *Eichinger/Kreil/Sacherer*, Basiswissen Arbeits- und Sozialrecht, S. 94

[147] *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S. 39

[148] Gegenmeinung zumindest für Deutschland *Haar*, iX Nr. 6/2009, 90 (92)

präventive Mitarbeiterkontrollen sinnvolle und legitime Instrumente sein können, ist Gegenstand einer laufenden Diskussion.[149]

5.1.4. Absolute Grenzen der Kontrolle

Zu beachten sind jedenfalls die beiden datenschutzrechtlichen Prinzipien, dass eine Datenverwendung nur innerhalb der billigen Grenzen eines legitimen Zwecks erfolgen darf und zugleich das schonendste Mittel zur Erreichung des Zwecks darstellt.[150] Eine Totalüberwachung (vergleichbar zB einer permanenten Beobachtung mittels Videoüberwachung) und damit Vollkontrolle der Beschäftigten ist jedenfalls unzulässig.[151]

Die Kontrolle der Internetnutzung kann dem legitimen Ziel dienen, die Einhaltung der im Betrieb vereinbarten Nutzungsregelungen (ggf ausdrückliches Verbot der Privatnutzung) des Betriebsmittels Internetzugang zu gewährleisten (vgl Abb. 9).[152]

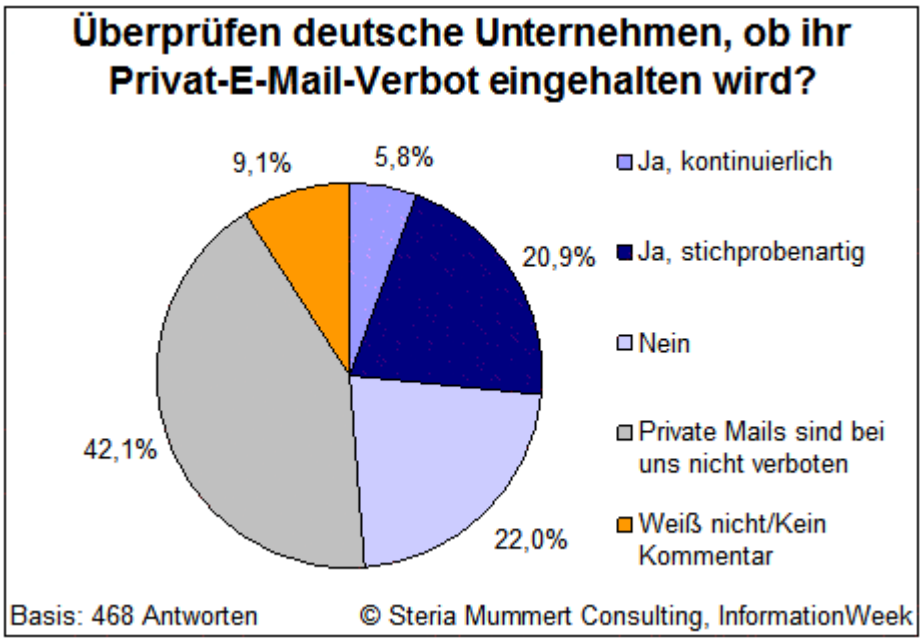

Abb. 9

[149] Vgl stellvertretend für viele jüngst *Steinkühler/Raif*, AuA 2009, 213 (Jedes zweite Unternehmen sei in Deutschland schon einmal Opfer von Wirtschaftskriminalität geworden, durchschnittlicher Schaden pro Unternehmen: 3,5 Mio. Euro.); *Haar*, iX Nr. 6/2009, S. 90

[150] Vgl § 1 Abs 2 letzter Satz und § 6 DSG 2000; *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 2f, 30; *Kotschy/Reimer*, ZAS 2004, 167; *Gerlach*, Der gesetzliche Schutz von Arbeitnehmerdaten, S. 1; *ISPA*, Internet sicher nutzen, S. 39

[151] *Bundesbeauftragter für Datenschutz*, Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet- und E-Mail-Nutzung am Arbeitsplatz, S. 2; *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 124f

[152] OGH 13.06.02, 8 Ob A 288/01p; *Dellisch*, ASoK 2001, 316

Ein besonders wichtiges Anliegen aus Datenschutzsicht müssen in diesem Zusammenhang aber folgende Hinweise für die betriebliche Praxis sein:

1.) Selbst wenn der Arbeitgeber die private Nutzung des betrieblichen Internetzugangs ausdrücklich verboten hat, so berechtigt ihn das gerade nicht zu einer systematischen, fortdauernden Kontrolle oder etwa zu einem willkürlichen Ausspähen („Scannen“) bestimmter Inhalte bzw. bestimmter Kommunikationspartner des Mitarbeiters. Im Gegensatz zu idR angemessenen punktuellen Stichproben wäre es zB jedenfalls unzulässig, das Nutzungsverhalten des Mitarbeiters[153] im Internet systematisch zu analysieren,[154] indem über einen längeren Zeitraum detailliert die aufgesuchten Internetseiten hinsichtlich der privaten, ggf intimen Vorlieben des Mitarbeiters ausgewertet würden.[155] Eine solche Dauerüberwachung im Stile „Big Brother am Arbeitsplatz“ verletzt jedenfalls das allgemeine Persönlichkeitsrecht in Verbindung mit der Menschenwürde des Mitarbeiters und wäre schon deshalb rechtswidrig.[156]

2.) Selbst wenn der Arbeitgeber die private Nutzung des betrieblichen Internetzugangs ausdrücklich verboten hat, so berechtigt ihn das regelmäßig nicht dazu, die privaten Inhalte von E-Mail zu lesen.[157] Vielmehr wird regelmäßig schon an den Empfängeradressen der E-Mail bzw. an den Dateinamen heruntergeladener Internetinhalte die private oder betriebliche Bestimmung zu erkennen sein.[158] Sollte eine E-Mail-Adresse eine Zuordnung

---

[153] Der Einsatz von Software, die Arbeitsgewohnheiten der Mitarbeiter aufzeichnet, („Spionage Software“) ist jedenfalls rechtswidrig, so die Materialien zum Gesetzesentwurf, S. 3 (siehe Anhang)

[154] Unerträglich auch hinsichtlich Art 8 EMRK, meint OGH 13.06.02, 8 Ob A 288/01p

[155] Gefährlich und abzulehnen ist deshalb die folgende Zusammenfassung *Brodils*: Aus datenschutzrechtlicher Sicht sei „die Erfassung sämtlicher Vermittlungs- bzw Verkehrsdaten (insb E-Mail-Adressen, Logfiles) sowohl bei dienstlicher als auch privater Nutzung wegen der überwiegenden Interessen des Arbeitgebers zulässig.“ (*Brodil*, ZAS 2004, 156 (162))

[156] Zum Funktionsreichtum heimlich auf Betriebsrechnern operierender „Schnüffel-Software“ *Haar*, iX Nr. 6/2009, 90 (92), dass solche Programme aber unter Einbindung des Betriebsrats und bei einem Verbot von Privatnutzung laut *Haar* eingesetzt werden dürfen, ist aufgrund der weitgehenden Durchleuchtung abzulehnen; so zutreffend auch *Steinkühler/Raif*, AuA 2009, 213; *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S 12; *Naderhirn*, Kollektives Arbeitsrecht und Arbeitnehmerkontrolle, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 111; *Eichinger/Kreil/Sacherer*, Basiswissen Arbeits- und Sozialrecht, S. 95

[157] *Gerlach*, Der gesetzliche Schutz von Arbeitnehmerdaten, S. 1; *Haar*, iX Nr. 6/2009, S. 90 (91f); *ISPA*, Internet sicher nutzen, S. 39; *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in Resch *(Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 53f

[158] Als privat identifiziert sind zB die Endung „pps“, der Dateiname „Ein Bauer braucht einen Zuchtbullen“ oder der Dateiordner „Eigene Bilder“, so LAG Rheinland-Pfalz, Urteil v 23.10.08, Az

nicht erlauben, so kann dann noch aus der Betreffzeile auf das Thema und damit die betriebliche oder private Veranlassung geschlossen werden.[159]

Der Arbeitgeber wird somit regelmäßig schon an der E-Mail-Adresse erkennen können, ob der Mitarbeiter den dienstlichen Internetzugang unberechtigt privat genutzt hat. Wird so – ohne die Inhalte der E-Mail zu lesen – eine arbeitsrechtliche Pflichtverletzung des Arbeitnehmers festgestellt, so wird der Arbeitgeber eine Abmahnung bzw. bei Wiederholung auch eine Kündigung erwirken können.[160] Ein Lesen der Inhalte der E-Mail ist demnach regelmäßig nicht erforderlich und würde gegen das Grundrecht auf Datenschutz und gegen das Kommunikationsgeheimnis verstoßen.[161]

5.2. Zwischenergebnis und Würdigung

Datenschutzrechtlich kann nach geltendem Recht nur im Rahmen einer umfassenden Interessenabwägung festgestellt werden, ob ein Arbeitgeber die Internetnutzung seiner Mitarbeiter kontrollieren darf.[162] Diese erforderliche Abwägung der Interessenlagen nach Verfassungs-, Datenschutz- und Arbeitsrecht führt – wie *Kotschy/Reimer* schon im Jahr 2004 festhielten – in Judikatur und Schrifttum zu recht uneinheitlichen Ergebnissen.[163]

> *„Jede Überwachung muss (...) eine angemessene Reaktion eines Arbeitgebers auf die Risiken sein, mit denen er konfrontiert ist, wobei der legitime Anspruch auf Schutz der Privatsphäre und andere Interessen der Beschäftigten zu berücksichtigen sind.“*[164]

---

10 Sa 787/05; *Naderhirn*, Kollektives Arbeitsrecht und Arbeitnehmerkontrolle, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 111

[159] *Freudhofmeier*, taxlex 2006, 41 (Ein gleicher Name in Absender- und Empfänger-E-Mail-Adresse biete Anhaltspunkte für Familienpost, „Rendevousz“ in der Betreffzeile deute ebenso auf nichtdienstliche Veranlassung hin.)

[160] Vgl dazu die bisher für Arbeitnehmer strenge BAG-Judikatur zu privater Computer- und Internetnutzung als Kündigungsgrund: BAG Urteil v 31.05.07, Az 2 AZR 200/06 = NZA 2007, 922ff (vgl dazu oben Kap 4, insb FN 54); *Raif/Kunze*, SAE 01/2009, 19ff; *ISPA*, Internet sicher nutzen, S. 38

[161] *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch (Hrsg)*, Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, S. 53ff;*Thiele*, ecolex 2001, 614; *Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in *Österreichische Juristenkommission (Hrsg)*, Grundrechte in der Informationsgesellschaft, S. 172;; aA *ISPA*, Internet sicher nutzen, S. 39 (arg falls der Mitarbeiter nur eine E-Mail-Adresse hat, so müsse er damit rechnen, dass auch private Nachrichten gelesen würden)

[162] *Gerlach*, Der gesetzliche Schutz von Arbeitnehmerdaten, S. 1

[163] *Kotschy/Reimer*, ZAS 2004, 167

[164] *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 29

In Unternehmen mit Betriebsrat muss der Arbeitgeber jedenfalls zusätzlich eine Betriebsvereinbarung nach § 96 Z 3 ArbVG einholen;[165] dies bedeutet jedoch im Umkehrschluss nicht, dass Kontrollen datenschutzrechtlich zulässig sind, wenn eine einschlägige Betriebsvereinbarung eingeholt wurde.[166]
Angesichts der Einschlägigkeit von Datenschutz- und Betriebsverfassungsrecht konstatiert *Hattenberger* zutreffend für die Verarbeitung personenbezogener Daten im Arbeitsverhältnis einen „doppelten Filter".[167]

In betriebsratslosen Unternehmen ist eine datenschutzrechtlich nicht zufriedenstellende Situation festzustellen. Weil nach vorzugswürdiger Ansicht eine Einwilligung von Mitarbeitern nach § 10 AVRAG nicht automatisch datenschutzrechtlich wirksame Zustimmungserklärung begründen und im Übrigen wegen des jederzeitigen Widerrufsrechts des Arbeitnehmers dem Organisationsbedürfnis des Arbeitgebers nicht genügen kann,[168] erschöpft sich die datenschutzrechtliche Rechtsgrundlage diesfalls in einer umfassenden Interessenabwägung für den Einzelfall unter Beachtung der allgemeinen Datenschutzprinzipien[169].

Weithin nicht zielführend erscheint die Argumentation von Teilen in der Literatur, die die Kontrollzulässigkeit zuvorderst nicht wie dargestellt am Zweck der Datenverwendung sondern nach einer Unterteilung in private und dienstliche Veranlassung gliedern wollen.[170] Was zunächst konsequent anmutet, ist weder mit verhältnismäßigem Aufwand für den Arbeitgeber durchführbar noch mit rechtlichen Grundüberlegungen konform: Der Arbeitgeber kann objektiv ex ante regelmäßig nicht in private und dienstliche

---

[165] *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 229ff; *Hattenberger*, RdA 2007/45 (401)

[166] *Löschnigg*, Datenermittlung im Arbeitsverhältnis, S. 233f; so auch in Deutschland: Das dBDSG ist nach § 1 Abs 3 dBDSG nicht subsidiär zu dem dBetrVG, vielmehr ist eine Betriebsvereinbarung danach zu prüfen, ob sie 1.) die Mitbestimmungskompetenz nach § 87 Abs 1 Nr. 6 dBetrVG ausfüllt und, davon getrennt, ob sie 2.) eine datenschutzrechtliche Erlaubnisgrundlage iSd § 4 dBDSG setzt, so *Trittin/Fischer*, NZA 2009, 343 (345); Mitbestimmung im Vorfeld von Datenschutz, meint *BITKOM e.V.*, Die Nutzung von E-Mail und Internet im Unternehmen, S. 14f (zeitlich umgekehrt: Mitbestimmung könne erst bei datenschutzrechtlicher Zulässigkeit einsetzen, meint *Sacherer*, RdW 2005)

[167] *Hattenberger*, RdA 2007/45 (401)

[168] *Kotschy/Reimer*, ZAS 2004, 167 mwN

[169] Diese erläuternd *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten, S. 2ff

[170] So insbesondere *Brodil*, Kontrolle und Datenschutz im Arbeitsrecht, 121 (124ff); *Sacherer*, RdW 2005, 173; *Dellisch*, ASoK 2001, 316; aA *Kotschy/Reimer*, ZAS 2004, 167

Nutzung unterteilen, so dass ein danach differenzierender Maßstab erst gar nicht angelegt werden könnte.[171] Selbst wenn mit erheblichem Aufwand der Mitarbeiter dazu verpflichtet würde, am dienstlichen Internetzugang eine Art Parallelstruktur für die private Kommunikation anzulegen, so erhebt sich für den Arbeitgeber die Frage nach der Kontrollierbarkeit bzw. auch der Verantwortlichkeit, falls der Mitarbeiter vom betrieblichen Internetzugang aus dennoch rechtswidrig im Internet agiert.

Verschärfend macht die angeführte Judikatur zu privaten Telefongesprächen am Arbeitsplatz deutlich, dass der durch das Kommunikationsgeheimnis teils höchstpersönliche Charakter von Telefongesprächen (und anderer vergleichbarer Kommunikation) den Arbeitgeber grundsätzlich zu keinem Überwachen berechtigt – ungeachtet der Veranlassung und auch bei ausdrücklichem Verbot des privaten Telefonierens bzw. der privaten Internetnutzung.[172]

5.3. Regelungen des Gesetzesentwurfs

Für Kontrollen des Internetverhaltens am Arbeitsplatz zieht der Gesetzesentwurf ein Modell stufenweiser Kontrollverdichtung[173] heran. Positiv hervorzuheben ist aus datenschutzrechtlicher Sicht, dass das Prinzip des den Eingriff in das Datenschutzrecht schonendsten Mittels konsequent gesetzlich vorgegeben wird. Im Gesetzesentwurf unverändert zum geltenden § 79c BDG bleibt, dass die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, unzulässig ist.[174] Dieses bislang im öffentlichen Dienst absolute Kontrollverbot für den staatlichen Arbeitgeber wird nun von zwei Ausnahmen durchbrochen (Abb. 10): Der staatliche Arbeitgeber soll personenbezogene Daten der Internetnutzung ausnahmsweise doch kontrollieren dürfen, wenn die Funktionsfähigkeit des betrieblichen IT-Systems gefährdet ist oder bei

[171] *Haar*, iX Nr. 6/2009, 90 (92); *Freudhofmeier*, taxlex 2006, 41
[172] Vgl oben Kap 5.1.1. (insb FN 94); zum abgestuften Kommunikationsgeheimnis auch *Brodil*, ZAS 2004, 156 (165f)
[173] Nach *Kotschy/Reimer*, ZAS 2004, 167
[174] Beachte ergänzend zu den obigen Ausführungen, wann die Menschenwürde (Kap 5.1.) berührt ist, für das Beamtendienstrecht *Fellner (Hrsg)*, BDG, § 79c: Ein strengerer Maßstab für den staatlichen Dienstgeber führt dazu, dass nach *Fellner* jede verdeckte Kontrollmaßnahme als Maßnahme anzusehen sei, die die Menschenwürde berühre.

Verdacht auf gröbliche Dienstpflichtverletzungen. Eine hinzutretende echte Mitbestimmungskompetenz der Personalvertretung für die Einführung und Ausübung von Kontrollmaßnahmen vergleichbar insbesondere § 96 Abs 1 Z 3 ArbVG sieht auch der Gesetzesentwurf nicht vor: Ein „absolutes" Zustimmungsrecht der Personalvertretung zu Kontrollmaßnahmen des Dienstgebers, welche die Menschenwürde berühren, ist im öffentlichen Dienst aus verfassungsrechtlichen Gründen nicht möglich.[175]

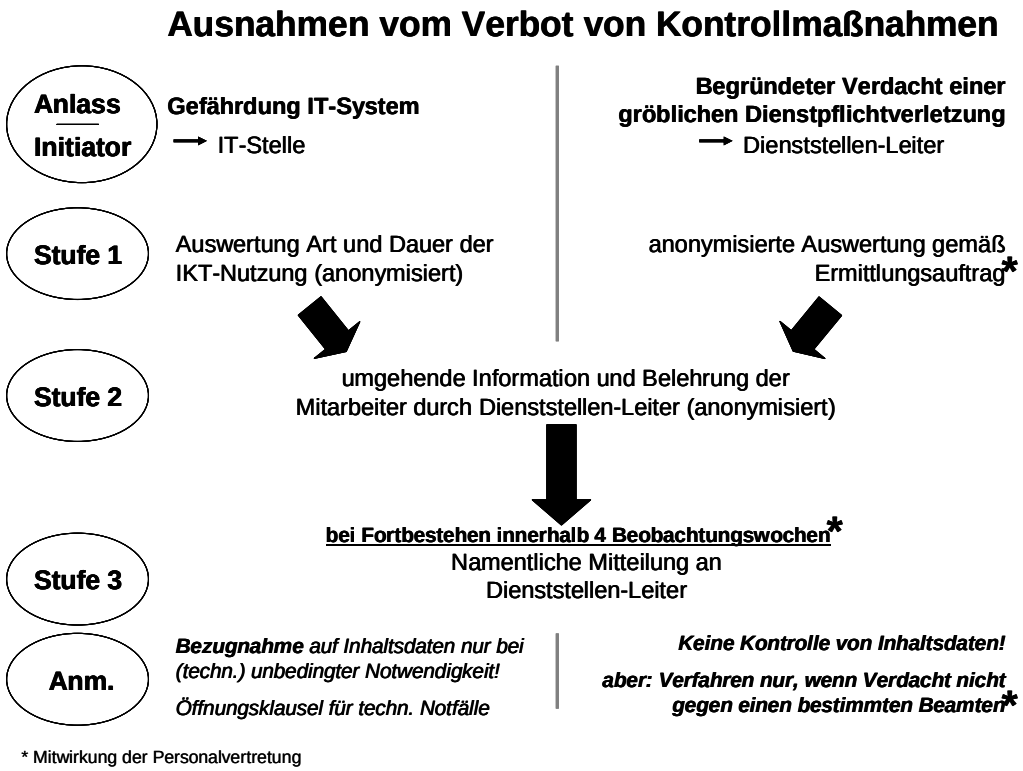

Abb. 10 Kontrollgrundsätze nach der Regierungsvorlage
Quelle: eigene Darstellung

5.3.1. Kontrolle wegen Gefährdung des IT-Systems

Aus Datenschutzsicht erscheint es unbedenklich, wenn der Arbeitgeber zur Abwehr von Schäden an der IT-Infrastruktur auch personenbezogene Daten benötigt. Der Anlass der Datenverwendung ist in diesem Fall nicht in der Person des Arbeitnehmers, sondern in einer Fehlermeldung des IT-Systems zu sehen. Initiator dieser Datenverwendung ist die IT-Stelle im Unternehmen. Weiter dürfen personenbezogene Nutzungsdaten von Mitarbeitern nach dem

[175] *Fellner (Hrsg)*, BDG, § 79c; *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 420ff

Gesetzesentwurf nur unter Beachtung und nach Maßgabe der folgenden Schutzvorkehrungen verwendet werden:

- Generell dürfen Inhaltsdaten übertragener Nachrichten nicht kontrolliert werden, es sei denn, es ist unbedingt notwendig.[176]
- Die IT-Stelle hat zunächst alle Möglichkeiten zur Fehlerbeseitigung wahrzunehmen, die keiner personenbezogenen Daten bedürfen.
- Bleiben die Bemühungen der IT-Stelle erfolglos, kann der Dienststellenleiter in anonymisierter Form über Art und Dauer der gefährdenden Internetnutzung informiert werden. Dieser hat sodann umgehend die Mitarbeiter zu informieren und auf die Beseitigung der indizierten Internetnutzung hinzuwirken.
- Erst wenn nunmehr die Gefahr noch fortbesteht, so kann über maximal vier Wochen eine namentliche Zuordnung des Mitarbeiters zu der gefährdenden Internetnutzung erfolgen.

Auf dieses abgestufte Procedere[177] darf nur dann ausnahmsweise verzichtet werden, wenn das IT-System aufgrund einer Internetnutzung von einer konkreten, unmittelbaren Gefährdung bedroht ist. Ein solch unabdingbares Notverfahren erfordert eine strikte Zweckbeschränkung und eine umgehende Information des betroffenen Mitarbeiters. Weiters hat die IT-Stelle den Vorfall zu protokollieren und dabei insbesondere die Gefährdung des IT-Systems sowie die verwendeten personenbezogenen Daten festzuhalten.

Die beschriebene Datenverwendung anlässlich einer technischen (drohenden) Störung hat in der betrieblichen Praxis möglicherweise einen Schwachpunkt: die IT-Stelle. Die Funktion der IT-Stelle nach dem Gesetzesentwurf könnte mit einer Black Box verglichen werden: Die IT-Stelle nimmt für den Arbeitgeber weisungsabhängig Aufgaben wahr, zugleich ist sie dem Arbeitgeber gegenüber zur Verschwiegenheit verpflichtet. Nur als ultima ratio

[176] Stellvertretend auch für andere zu dieser Formulierung die Stellungnahme (S. 2, siehe Anhang) des *Bundesministeriums für Justiz*: Neben dem Begriff einer „gröblichen Dienstpflichtverletzung“ (s.u. Kap 5.3.2.) lasse „unbedingt notwendig“ einen derart großen Interpretationsspielraum, der sich nur schwer mit einem drohenden schwerwiegenden Eingriff in die Persönlichkeitsrechte eines Beamten und Dritter in Einklang bringen ließe.

[177] Nicht nachvollziehbar ist daher die Befürchtung der Gewerkschaft *Öffentlicher Dienst*, dass mit dieser Bestimmung jegliche dauerhafte Kontrollmaßnahme gerechtfertigt werden könnte (Stellungnahme, S. 1f, siehe Anhang).

darf die IT-Stelle die personenbezogenen Nutzungsdaten an einen Vorgesetzten herausgeben. Es ist zu hoffen, dass die datenschutzrechtlichen Integritätsanforderungen an die Systemadministratoren, welche der Gesetzesentwurf vor Augen hat, von den Arbeitgebern respektiert werden.[178]

5.3.2. Kontrolle wegen Verdachts auf gröbliche Dienstpflichtverletzung

Heikler als der soeben erläuterte technische Anlass ist die personenbezogene Kontrolle der Internetnutzung am Arbeitsplatz wegen Verdachts auf eine gröbliche Dienstpflichtverletzung. In diesem Fall liegt der Anlass zur Kontrolle unmittelbar im Verhalten des einzelnen Mitarbeiters; die Kontrollmotivation des Arbeitgebers besteht darin, dass die Regeln zur Nutzung des betrieblichen Internetzugangs im Betrieb auch befolgt werden. Für die nachstehenden Regelungen zur Zulässigkeit personenbezogener Kontrollen ist daran zu erinnern, dass nach dem Gesetzesentwurf den öffentlich Bediensteten die Privatnutzung in eingeschränktem Ausmaß grundsätzlich erlaubt ist.

Nach dem Gesetzesentwurf dürfen personenbezogene Daten über die Internetnutzung am Arbeitsplatz nur unter folgenden Voraussetzungen verwendet werden:

- Der begründete Verdacht einer gröblichen Dienstpflichtverletzung muss vorliegen.
- Zunächst sind zeitliche, inhaltliche oder qualitative Beschränkungen des dienstlichen Internetzugangs zu verhängen, um die Dienstpflichtverletzung durch technische Vorkehrungen zu verhindern.
- Verfahrensinitiator ist ausschließlich der Leiter der Dienststelle.[179]

[178] Ähnlich auch die Stellungnahme (S. 1f, siehe Anhang) des *Österreichischen Gewerkschaftsbunds*: Schon bei der Besetzung der IT-Stelle müsse verstärkt beachtet werden, dass es sich bei den Aufgaben der IT-Stelle nach dem Gesetzesentwurf um ein hoch sensibles Gebiet handle.

[179] Nach Stellungnahme des *Amtes der Salzburger Landesregierung* (Stellungnahme, S. 2, siehe Anhang) muss es auch zulässig sein, dass die IT-Stelle den Dienststellenleiter beim Verdacht einer gröblichen Dienstpflichtverletzung (zB wenn in großem Maß Internet-Domains ohne dienstlichen Bezug angesurft würden) informiert und so ein Kontrollverfahren ausgelöst werden kann; das *Bundesministerium für Justiz* (Stellungnahme, S.4, siehe Anhang) erinnert daran, dass eine solche Ermittlungsfunktion und -entscheidung grundsätzlich der Disziplinarkommission im Wege eines Disziplinarverfahrens obliege.

- Die IT-Stelle ist schriftlich unter genauer Beschreibung des Verdachtfalls zu beauftragen.
- Die IT-Stelle hat dem Dienststellenleiter zunächst anonymisiert zu berichten. Erst wenn nach der Information der Mitarbeiter und dem Hinwirken auf Einhaltung der Dienstpflichten der Verdachtsfall fortbesteht, darf die IT-Stelle innerhalb von maximal vier Wochen dem Dienststellenleiter namentlich in schriftlicher Form berichten.
- Legitimer Zweck ist neben der Verhinderung weiterer Dienstpflichtverletzungen auch die Klarstellung des Sachverhalts.
- Zu beachten ist ein absolutes Verbot einer Kontrolle von Inhaltsdaten übertragener Nachrichten.[180]

Durch das abgestufte Verfahren und die materiellen Voraussetzungen wird das Recht auf Datenschutz und das Kommunikationsgeheimnis der Mitarbeiter geschützt.[181] Relativiert wird das Verfahren allerdings durch seinen Anwendungsbereich: Es kommt nur zum Einsatz, wenn sich der begründete Verdacht nicht gegen einen bestimmten Bediensteten richtet. Es ist aber davon auszugehen, dass sich ein begründeter Verdacht eines schweren dienstlichen Fehlverhaltens regelmäßig gegen einen bestimmten Mitarbeiter wendet. Dann ist unter Beachtung von Verfahrens- und Transparenzpflichten der sofortige Zugriff auf die personenbezogenen Daten des Mitarbeiters zulässig.[182] Anderes ist dann anzunehmen, wenn in einer Abteilung von mehreren Bediensteten ein zumindest ähnliches grobes Fehlverhalten gesetzt wird oder gar wissentlich Dienstpflichten in schwerwiegender Weise missachtet werden.

[180] Dies ist nach Meinung der *Wirtschaftskammer Österreich* unvertretbar und nicht nachvollziehbar; es würden dadurch Missbrauchsmöglichkeiten eröffnet, „die eigentlich in ihren Auswirkungen horrend sind." (Stellungnahme, S. 3, siehe Anhang)

[181] Praxisfremdes Verfahren im Hinblick auf die rasche Verbreitung von Schädlingen und die dadurch drohenden immensen Schäden, meint das *Amt der Salzburger Landesregierung*, Stellungnahme, S. 2 (siehe Anhang); deshalb werde es für das Verfahren erst gar keine Anwendungsfälle geben, meint das *Amt der Niederösterreichischen Landesregierung*, Stellungnahme, S. 3 (siehe Anhang)

[182] Zusätzlich fordern das *Bundesministerium für Wirtschaft, Familie und Jugend* (Stellungnahme, S. 1f, siehe Anhang) sowie das *Bundesministerium für Landesverteidigung und Sport* (Stellungnahme, S. 2f, siehe Anhang), dass bei einem konkreten Verdachtsmoment gegen einen bestimmten Beamten nach § 79e Abs 7 Gesetzesentwurf auf eine Gröblichkeit der Dienstpflichtverletzung verzichtet werden sollte.

Kommt das beschriebene Verfahren zum Einsatz, so ist der Ausgangspunkt der begründete Verdacht einer gröblichen Dienstpflichtverletzung.[183] Der Gesetzesentwurf sieht vor, dass ein Bediensteter nicht schon ob einer kleinen Verfehlung eine Kontrolle seiner Internetnutzung befürchten muss.[184] Nach den Materialien zum Gesetzesentwurf knüpft der Begriff der gröblichen Dienstpflichtverletzung am Kündigungsgrund des § 32 Abs 2 Z 1 VBG[185] an.[186] Hinsichtlich des notwendigen begründeten Verdachts ist − in Abwesenheit einer Erläuterung in den Materialien − klarzustellen, dass der begründete Verdacht schon vorliegen muss, ehe die Kontrollmaßnahme eingeleitet wird.[187] Der „Zweck der Klarstellung des Sachverhaltes" bedeutet also, dass ein Sachverhalt, der den begründeten Verdacht einer gröblichen Dienstpflichtverletzung verursacht, schon vorliegen muss, ehe die Internetnutzung kontrolliert wird.[188] Das Kontrollverfahren kann dann zweckgemäß zu einer Erhärtung oder zu einer Entkräftung des begründeten Verdachts führen. Nicht zulässig wäre es, wenn ein Sachverhalt ohne sachlich hinreichend begründeten Verdacht mithilfe einer Kontrolle der betrieblichen Internetnutzung klargestellt werden soll.

5.4. Der Begriff „Nachricht" im Gesetzesentwurf

Einzugehen ist auf die Wirkung der geplanten Legaldefinition der Nachricht in § 79g Z 5 des Gesetzesentwurfs. Nachricht ist demnach definiert als „jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht wird." Nicht unberechtigt ist der Hinweis in der Stellungnahme des *Innenministeriums*, dass damit die Reichweite des Nachrichtenbegriffs unklar sei. Zu hinterfragen ist in der Tat, ob ein über das Intranet versandtes E-Mail zwischen zwei Bediensteten über

[183] Konkrete Verdachtsmomente fordert auch *Haar*, iX Nr. 6/2009, 90 (92)

[184] So auch das Verständnis des *Amts der Niederösterreichischen Landesregierung*, die allerdings eine Präzisierung (und Lockerung) des Begriffs „gröblichen Dienstpflichtverletzung" fordert (Stellungnahme, S. 2f, siehe Anhang).

[185] Kasuistik ausführlich in *Ziehensack*, VBG Praxiskommentar, § 32 Rz 129ff (gröbliche Dienstpflichtverletzung bejaht zB bei erheblichen Ehrverletzungen, Verletzung des Amtsgeheimnisses/Indiskretion, Fernbleiben vom Dienst oder bei dienstlichem Ungehorsam)

[186] Erläuterungen zum Gesetzesentwurf, S. 3 (siehe Anhang)

[187] Gegen eine „Suche ins Blaue hinein" ohne tatsächliche Anhaltspunkte für eine schwere Pflichtverletzung *Steinkühler/Raif*, AuA 2009, 213 (215)

[188] Möglichkeiten effizienter, spontaner und stichprobenartige Ermittlungen fordert im Gegensatz dazu die *Wirtschaftskammer Österreich*, Stellungnahme, S. 3 (siehe Anhang); unklar bleibt es für das *Amt der Salzburger Landesregierung*, auf welche Art der Leiter der Dienstelle den Verdacht gewonnen haben muss (Stellungnahme, S.1f, siehe Anhang).

einen „öffentlichen Kommunikationsdienst“ abgewickelt wird. Wie oben (Kap 3) ausführlich aufgezeigt, erbringt der Dienstgeber selbst regelmäßig gerade keinen öffentlichen Kommunikationsdienst.[189] Es muss daher erst recht gelten, dass der Dienstgeber mit dem Betrieb eines Intranets keinen öffentlich zugänglichen Kommunikationsdienst anbietet. Während die in Bezug genommene Richtlinie 2002/58/EG durchgängig von öffentlich zugänglichen Kommunikationsdiensten und -netzen spricht, so stellt sie zudem in Erwägungsgrund 10 klar, dass für nicht öffentliche Kommunikationsdienste (zB Intranet) die Richtlinie 95/46/EG (umgesetzt im öDSG 2000) gelten soll.
Dies bedeutet, dass der Schutz für Inhalte übertragener Nachrichten nach den §§ 79c Abs. 3. 79d Abs 1 Satz 2 und Abs 4 Satz 2 des Gesetzesentwurf in Ermangelung einer begriffsentsprechenden Nachricht nicht einschlägig ist, wenn die E-Mail eines Bediensteten lediglich (behörden-)intern ohne Inanspruchnahme des allgemein zugänglichen Internets versendet wird.

Das Ergebnis ist nicht zufriedenstellend, denn es würde der Schutz von Inhaltsdaten entfallen, der, wie bereits festgestellt, im Vergleich zu Verkehrsdaten aus Datenschutzsicht besonders wichtig ist. Da gerade im öffentlichen Dienst eine fast nicht zu überblickende Anzahl von Behörden und staatlichen Einrichtungen auch ohne das allgemein zugängliche Internet digital miteinander vernetzt sind, erscheint das Überwachungspotential dem Umfang nach nicht gering. Die Mitarbeiter sind deshalb auch vor einer unrechtmäßigen Kontrolle der in einem Intranet (oder zB in Behördenverbundportalen) übertragenen Inhaltsdaten gesetzlich zu schützen.

[189] Der Rückgriff auf die Besprechung der relevanten Normen des TKG 2003 erscheint nicht nur anhand der Terminologie, sondern auch ausweislich der Erläuterungen zum Gesetzesentwurf unausweichlich: Diesen zufolge orientiere sich der Begriff der Nachricht an § 92 Abs 3 Z 7 TKG 2003 und dessen zugrunde liegender Begriffsbestimmung in Art 2 lit d RL 2002/58/EG, vgl Erläuterungen zum Gesetzesentwurf, S. 3f (Anhang)

5.5. Ergebnis und Würdigung

Die Kontrollgrundsätze des Gesetzesentwurfs sind charakterisiert durch das Modell der stufenweisen Kontrollverdichtung, das Eingriffe in den Datenschutz stets nur in der notwendigsten Intensität zulässt.[190] Es ist klar beschrieben, welchen Personen auf Arbeitgeberseite unter welchen Voraussetzungen Kontrollmöglichkeiten eingeräumt werden.[191]

Mit einem zwingenden Vorrang ausgestattet sind grundsätzlich anonymisierte Auswertungen des Mitarbeiterverhaltens am dienstlichen Internetzugang. Durch dazu korrespondierend vorgeschriebene Informationspflichten des Arbeitgebers wird dem Mitarbeiter regelmäßig die Gelegenheit gegeben, sein (nicht gröbliches) Fehlverhalten einzustellen, ehe es zu einer personenbezogenen Ausforschung seines Nutzungsverhaltens kommt.

Zugleich sind weitere datenschutzrechtliche Grundbedingungen, die erforderlich sind, damit betroffene Bedienstete ihre Rechte überhaupt wahrnehmen können, expressis verbis legis vorgesehen: Nimmt der Arbeitgeber eine (an sich zulässige)[192] Kontrolle der Nutzungsdaten eines betrieblichen Internetzugangs vor,[193] so hat er dies dem Mitarbeiter gegenüber transparent zu stellen.

Flankierend ist auch die zuständige Beschäftigtenvertretung davon in Kenntnis zu setzen. Werden Kontrollverfahren durchgeführt, so sind Dokumentationsverpflichtungen vorgesehen, um neben der Transparenz für den betroffenen Mitarbeiter auch die Rechtmäßigkeit der Kontrolle überprüfen zu können.

---

[190] So schon das zentrale Petitum im Jahr 2004 von *Kotschy/Reimer*, ZAS 2004, 167

[191] „Aufbau von bürokratischen Hürden für den Dienstgeber" kritisiert das *Amt der Niederöstereichischen Landesregierung*, Stellungnahme, S. 1 (siehe Anhang)

[192] OGH 13.06.02, 8 Ob A 288/01p

[193] Weitgehend ist die Forderung *Obereders*, der den Arbeitgeber auch von einer Einsicht der Verkehrsdaten des betrieblichen Internetzugangs ausschließen will mit Ausnahme der Gesamtnutzungsdauer und der dadurch verursachten Kosten, vgl *Oberede*r, RdA 2001, 75; ähnlich auch *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 417

Lobend hervorzuheben ist auch der eindeutig festgeschriebene umfassende Schutz von Inhaltsdaten, der insoweit die va legistisch unpräzise österreichische Rechtslage der §§ 92ff TKG 2003 im Bereich von Beschäftigungsverhältnissen mit angemessenem Ergebnis konkretisiert und damit das Kommunikationsgeheimnis der Mitarbeiter stärkt.

Die diesbezügliche Rechtslage nach dem Gesetzesentwurf könnte grob wie folgt zusammengefasst werden: Inhaltsdaten der E-Mail- und Internetnutzung am Arbeitsplatz sind für den Arbeitgeber in aller Regel tabu.[194] Bei berechtigtem Anlass genügen regelmäßig die Verkehrsdaten, damit der Arbeitgeber seine schutzwürdigen Interessen wahrnehmen kann.[195]

[194] „Bei Einsicht in die inhaltlichen, personenbezogenen Daten wäre wohl eine noch restriktivere, die schutzwürdigen Interessen der Betroffenen im Sinne der Bestimmungen des DSG und des Artikels 8 MRK sowie des Briefgeheimnisses berücksichtigende Regelung einzuführen." So das *Bundesministerium für Justiz*, Stellungnahme, S. 3 (siehe Anhang); würde der öffentliche Dienstgeber Inhaltsdaten der Internetnutzung protokollieren, so wäre dies ein Verstoß gegen Art. 8 EMRK, meint *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 421f

[195] Vernichtende Bewertung des *Bundesministeriums für Finanzen*: „Das vorliegende Normsetzungsverfahren erscheint widersprüchlich, normlogisch inhomogen und (...) rechtlich systemwidrig." (Stellungnahme, S. 2, siehe Anhang)

6. Resümee: Modellcharakter des Gesetzesentwurfs

Zu bedenken ist, dass der Gesetzesentwurf **nur öffentlich Bedienstete** (Beamte, Vertragsbedienstete, Richter, Lehrer ua) erfasst. Ob die geplanten Gesetzesregelungen auch für die Privatwirtschaft geeignet sein können, ist wie folgt zu behandeln:

Es ist festzuhalten, dass die geltende Rechtslage im Beamtendienstrecht nicht mit der Situation im Arbeitsrecht der Privatwirtschaft zu vergleichen ist. Nach § 79c BDG ist dem staatlichen Dienstgeber momentan jede Kontrollmaßnahme ausnahmslos verboten.[196] Private Arbeitgeber hingegen können die Verwendung der Betriebsmittel kontrollieren, soweit die Mitbestimmungsvorschriften, das DSG 2000 und die Grundrechte auf Datenschutz und Kommunikationsgeheimnis der Mitarbeiter eingehalten werden. Aufgrund dieser gegensätzlichen Ausgangslage ist eine (direkte) Analogie von datenschutzrechtlichen Vorschriften des Beamtendienstrechts auf datenschutzrechtliche Fragestellungen im privaten Arbeitsrecht ausgeschlossen.

Davon zu unterscheiden ist die Frage, ob die Regelungen des Gesetzesentwurfs einen arbeitsrechtlich fairen Interessenausgleich betreffend Nutzungs- und Kontrollmöglichkeiten bewirken und zugleich die datenschutzrechtliche Position der Mitarbeiter wahren können. Für einen typischen Arbeitsplatz mit Internetzugang kann der Gesetzesentwurf weitgehend überzeugen:[197] Arbeitgeber und Mitarbeiter können jeweils ihre Rechte und Pflichten im Umgang mit dem Betriebsmittel Internetzugang deutlich erkennen.[198]

---

[196] Unakzeptabler Zustand nach Meinung der *Wirtschaftskammer Österreich*, Stellungnahme, S. 2 (siehe Anhang); auch wegen einer regelmäßig entsprechend kritischen Berichterstattung über Missbrauchsvorfälle öffentlicher Bediensteter und wegen „gegebenen historischen Begriffsverständnisses zum ‚Dienstrecht'" sei der *Amt der Niederösterreichischen Landesregierung* zufolge eine auch „gegenüber Dienstnehmern in anderen (privaten) Bereichen höhere Kontrolldichte" im öffentlichen Dienst grundsätzlich zulässig (Stellungnahme, S.2, siehe Anhang); offen bleibt freilich mE, wie diese Analyse durch die geltende Rechtslage insb des § 79c BDG abgebildet ist.

[197] Widersprüchlich erscheint die Stellungnahme der *Wirtschaftskammer Österreich*: Einerseits dürfe das, was der Bund als Dienstgeber für angemessen oder vertretbar hält, nicht zum zwingenden Maßstab für die privaten Dienstgeber werden, zugleich wird aber eine Gleichbehandlung öffentlich Bediensteter und privat Beschäftigter eingefordert (Stellungnahme, S. 1ff, siehe Anhang).

[198] Vorsichtig für die Rechtslage in Deutschland vergleichbar feststellend die *GDD e.V.*, Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages am 11.05.2009, S. 4 (in einzelnen Zweifelsfällen könne es „angezeigt sein, gesetzgeberische Zielvorgaben für die Beurteilung der Zulässigkeit des Einsatzes der modernen

Die Bestimmungen, ob und inwieweit private Internetnutzung am Arbeitsplatz zulässig ist, überzeugen durch Augenmaß, sachliche Differenzierung und Verständlichkeit (Kap 4). Ebenso überzeugen die Regelungen, unter welchen Voraussetzungen der Arbeitgeber Kontrollmaßnahmen der Internetnutzung durchführen kann mittels eines abgestuften Verfahrens, das insbesondere die Verfassungsrechte der Beschäftigten angemessen berücksichtigt (Kap 5).

Der Gesetzesentwurf wäre, so er zu Gesetzeskraft erwächst, anzuwenden auf den Staat als Arbeitgeber und auf dessen öffentlichen Bediensteten. Über diesen Anwendungsbereich ist der Sachverhalt, den der Gesetzesentwurf als Regelungsgegenstand vor Augen hat, zwar zunächst eindeutig und ausschließlich dem öffentlich-rechtlichen Dienstrecht gewidmet. Der beamtendienstrechtliche Sachverhalt indessen scheint ganz überwiegend mit identischen Rechts- und Wertungsfragen auch im Arbeitsrecht der Privatwirtschaft gegenständlich zu sein.[199] Es können daher die öffentlich-rechtlich Bediensteten mit privatrechtlich Beschäftigten auf der einen Seite und der Staat in seiner Eigenschaft als Dienstgeber mit Arbeitgebern aus der Privatwirtschaft auf der anderen Seite insoweit grundsätzlich verglichen werden. Wesentliche Abweichungen davon ergeben sich allerdings insbesondere,

- wenn die (private) Internetnutzung die Ausführung hoheitlicher Aufgaben unmittelbar beeinträchtigen könnte. Soweit also vom Aufgabenfeld öffentlich Bediensteter Rechtsgüter oder staatstragende Prinzipien wie zB Innere und Äußere Sicherheit,[200] Vertretung von Verfassungsorganen oder Schutz richterlicher Unabhängigkeit tangiert sind, so kann nicht mehr von einer Vergleichbarkeit mit einem

---

Techniken im Arbeitsverhältnis aufzustellen."); kürzlich so auch die Präsidentin des BAG, Ingrid Schmidt: „Die derzeitige Rechtslage ist zu unklar. (...) Der Gesetzgeber muss eine klare Ansage machen, was geht und was nicht." Beim Blick in das Bundesdatenschutzgesetz könnten Schmidts Aussage zufolge sowohl Arbeitnehmer als auch Arbeitgeber nicht erkennen, was ihre Rechte und Pflichten seien. (Quelle: Handelsblatt v 29.01.09)

[199] So auch der Verweis der RV zu § 79c BDG idgF auf § 96 ArbVG dazu, ob eine Kontrollmaßnahme die Menschenwürde berühre; vgl *Fellner (Hrsg)*, BDG, § 79c

[200] Dahingehendes lässt das *Bundesministerium für Landesverteidigung und Sport* (Stellungnahme, S. 3ff, siehe Anhang) erkennen, indem es auf sensibelste dienstliche Informations- und Kommunikationsinfrastruktur (zB streng geheime EU-Dokumente) oder die Sicherstellung der Bereitschaft des Bundesheers auch durch Kontrollen hinweist. Eine Sonderstellung haben auch IT-Stellen, die sich mit der militärisch motivierten Sicherheit der IKT-Einrichtung befassen.

privatrechtlichen Beschäftigungsverhältnis ausgegangen werden.[201] Im Vordergrund stehen vielmehr die besonderen Treuepflichten des staatlich Bediensteten;

- weil bestimmte staatliche Einrichtungen (zB Verfassungsorgane) verstärkt das Ziel von Hackerangriffen sind;[202] angesichts der Manipulationsgefahr wäre in diesen Bereichen ein restriktiveres Reglement gerechtfertigt, das über die ministerielle Verordnung oder ressortspezifische Sicherheitsbestimmungen implementiert werden könnte;
- durch die unmittelbare Bindung des Staates an das Verfassungsrecht: Die Verfassungsrechte der öffentlich-rechtlich Bediensteten entfalten gegenüber dem staatlichen Dienstgeber unmittelbare Wirkung.[203] Eine die Menschenwürde berührende Kontrollmaßnahme wäre ein unzulässiger Eingriff des österreichischen Staates als Dienstgeber in durch die Europäische Menschenrechtskonvention geschützte Rechte der öffentlich Bediensteten.[204] Ein staatlicher Dienstgeber unterliegt deshalb einem strengeren Maßstab als private Arbeitgeber, die grundsätzlich nur eine mittelbare Wirkung der Verfassungsrechte erfahren (Ausnahme § 1 DSG 2000).[205]

Der Gesetzgeber sollte in einem nächsten Schritt die Ansätze des nun für das Arbeitsrecht im Öffentlichen Dienst geplanten Regelungsmodells im privatrechtlichen Arbeitsrecht berücksichtigen; solche neuen bereichsspezifischen Datenschutzregelungen wären ausdrücklich als *dispositives* Recht einzuführen. Denn es ist daran zu erinnern, dass Arbeitsrecht vorwiegend Arbeitnehmerschutzrecht und insoweit grundsätzlich ius cogens ist, von dem nicht zum Nachteil der Arbeitnehmer abgewichen werden darf.

---

[201] Besondere Vorkehrungen gegen missbräuchliche Zugriffe bestehen zB auch im Bereich der Finanzverwaltung (Steuergeheimnis), so dass ex officio die Pflicht zu einer anlassunbezogenen laufenden Protokollierung beim Umgang mit Steuerdaten erwächst − vgl DSK E K1212.014/0008-DSK/2005 und vgl *Bundesministerium für Finanzen*, Stellungnahme (siehe Anhang), S. 3.

[202] Vgl oben Kap 4.3. lit c) und FN 37

[203] Beachte in diesem Zusammenhang insb auch den engen Legalitätsvorbehalt des § 1 Abs 2 DSG 2000.

[204] *Fellner (Hrsg)*, BDG, § 79c

[205] Erforderlich sei deshalb eine grundlegende Differenzierung zum privatrechtlichen Bereich, meint *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in: *Forgó/Feldner/Witzmann/Dieplinger (Hrsg)*, Probleme des Informationsrechts, S. 420ff

Wie beschrieben, gehört ein Internetzugang zu den Betriebsmitteln, auf deren Privatnutzung die Beschäftigten grundsätzlich keinen Anspruch haben. Dieser arbeitsrechtliche Grundgedanke sollte nicht unterlaufen werden durch eine den Arbeitnehmer begünstigende gesetzliche Regelung wie die des im Gesetzesentwurf geplanten § 79d Satz 2 BDG.[206] Der (private) Arbeitgeber soll weiterhin die Möglichkeit haben, die private Nutzung des Internetzugangs ausdrücklich zu verbieten und deshalb eine gesetzliche Regelung wie die des geplanten § 79d Satz 2 BDG abbedingen können. Ein entsprechendes Primat für eine Regelung auf Betriebsebene soll weiterhin gelten.[207]

In den zahlreichen Unternehmen allerdings, die auf betrieblicher Ebene momentan keine Bestimmungen zur privaten Internetnutzung implementiert haben, würde eine gesetzliche Regelung wie die des Gesetzesentwurfs Transparenz und Rechtssicherheit bewirken können bzw. den Arbeitgeber – ggf mit dem Betriebsrat – dazu anregen können, betriebliche Bestimmungen (Internet Policy, Betriebsvereinbarung) zu erarbeiten.

[206] „In einem eingeschränkten Ausmaß ist auch die private Nutzung der für den Dienstbetrieb zur Verfügung stehenden IKT-Infrastruktur erlaubt, (...)."
[207] *GDD e.V.*, Stellungnahme zur Sachverständigenanhörung, S. 5

Literaturverzeichnis

Artikel 29 Datenschutzgruppe (unabhängiges Beratungsgremium der EU in Datenschutzfragen),
Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten vom 13.09.2001, Brüssel 2001

Bergmann, Lutz/Möhrle, Roland/Herb, Armin,
Datenschutzrecht Kommentar (Band 1), Stuttgart 2004, Loseblatt 38. Erg.Lfg./Januar 2009

Brodil, Wolfgang,
Kontrolle und Datenschutz im Arbeitsrecht, ZAS 2009, 121

Brodil, Wolfgang,
Individualarbeitsrechtliche Fragen der Kontrolle des Arbeitnehmers, in *Resch, Reinhard (Hrsg),* Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, Wien 2005, S. 69-90

Brodil, Wolfgang,
Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis – Kontrollbefugnisse des Arbeitgebers zwischen Datenschutz und Persönlichkeitsrechten, ZAS 2004, 156

Brodil, Wolfgang,
Die Registrierung von Vermittlungsdaten im Arbeitsverhältnis – zugleich eine Besprechung der Entscheidung OGH 8 Ob A 288/01p, ZAS 2004, 17

Brodil, Wolfgang,
Nutzung und Kontrolle von neuen Medien im Arbeitsrecht, ecolex 2001, 853

Büllesbach, Alfred,
Beschäftigtendatenschutz, in *Roßnagel, Alexander (Hrsg),* Handbuch Datenschutzrecht, München 2003, S. 949-1064

Bundesbeauftragter für Datenschutz (Schaar, Peter),
Datenschutzrechtliche Grundsätze bei der dienstlichen/privaten Internet und E-Mail-Nutzung am Arbeitsplatz, Bonn 2008

Bundesministerium für Arbeit und Soziales (Hrsg),
BMAS plant eigenständiges Arbeitnehmerdatenschutzgesetz (Pressemitteilung vom 16.02.2009), Berlin 2009

Bundesministerium für Inneres (Hrsg),
Bundeskabinett beschließt Grundsatzregelung zum Datenschutz der Arbeitnehmer (Pressemitteilung vom 18.02.2009), Berlin 2009

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM e.V.),
Die Nutzung von E-Mail und Internet im Unternehmen – Rechtliche Grundlagen und Handlungsoptionen (Version 1.5), Berlin 2008

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM e.V.),
Presseinformation „Jeder Dritte geht am Arbeitsplatz ins Internet“ vom 03.08.2008, Berlin 2008

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM e.V.),
Presseinformation „Jeder Vierte nutzt am Arbeitsplatz das Internet“ vom 12.07.2007, Berlin 2007

Dellisch, Karin,
Private E-Mail- und Internet-Nutzung am Arbeitsplatz – Gestaltung der Nutzung und Kontrolle durch den Dienstgeber, ASoK 2001, 316

Dohr, Walter/Weiss, Ernst M./Pollirer, Hans-Jürgen,
Kommentar Datenschutzrecht, 2. Auflage Wien 2002, Loseblatt 8. Erg.Lfg./Januar 2009

Ehmann, Eugen/Helfrich, Marcus,
EG-Datenschutzrichtlinie Kurzkommentar, Köln 1999

Eichinger, Julia/Kreil, Linda/Sacherer, Remo,
Basiswissen Arbeits- und Sozialrecht (Stand 1.1.2009), 4. Auflage, Wien 2009

Fellner, Wolfgang (Hrsg),
Beamten-Dienstrechtsgesetz 1979 - BDG, Wien, Loseblatt 53. Erg.Lfg./Februar 2009

Freudhofmeier, Martin,
Aspekte der privaten Nutzung des Internet durch den Arbeitgeber, taxlex 2006, 41

Gerhartl, Andreas,
Datenschutz im Arbeitsrecht, ASoK 2008, 147

Gerlach, Roland,
Der gesetzliche Schutz von Arbeitnehmerdaten (Vortragshandreichung anlässlich eines Jour-Fixe des Universitätslehrgangs für Informationsrecht und Rechtsinformation, Universität Wien, 26.03.2009), Wien 2009

Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD e.V.),
Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages am 11.05.2009, Bonn 2009

Gola, Peter/Klug, Christoph,
Die Entwicklung des Datenschutzrechts in den Jahren 2007/2008, NJW 2008, 2481

Gruber, Bernhard W.,
Überwachung der dienstlichen Verwendung von Internet und E-Mail, in *Österreichische Juristenkommission (Hrsg),* Grundrechte in der Informationsgesellschaft, Wien 2001, S. 167-176

Haar, Tobias,
Mitarbeiterüberwachung: Was ist erlaubt? Reingeschaut, iX (Magazin für professionelle Informationstechnik) Nr. 6/2009, 90

Härting, Niko,
Internetsurfen am Arbeitsplatz, ITRB 2008, 88

Hattenberger, Doris,
Glosse zu OGH 29.6.2006, 6 Ob A 1/06z (Keine Befugnisse des Betriebsrates zur Durchsetzung des DSG), RdA 2007/45 (401)

Hattenberger, Doris,
Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch, Reinhard (Hrsg),* Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, Wien 2005, S.13-68

Internet Service Providers Austria (ISPA, Verband der österreichischen Internet-Anbieter),
Internet sicher nutzen – ein Leitfaden der ISPA, Wien 2008

Jahnel, Dietmar,
Datenschutzrecht, in *Jahnel, Dietmar/Schramm, Alfred/Staudegger, Elisabeth (Hrsg),* Informatikrecht, 2. Auflage, Wien 2003, S. 241-272

Jahnel, Dietmar,
Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *Wissenschaftliche Interessensgemeinschaft für Informationsrecht IT-LAW.AT (Hrsg),* e-Mail – elektronische Post im Recht, Wien 2003, S. 89-100

Jung, Jakob/Bube, Lars,
Fallstricke beim Verbot privater Emails am Arbeitsplatz (zur Studie „IT-Security 2008“), in InformationWeek v. 30.01.2009

Kotschy, Waltraut/Reimer, Sebastian,
Die Überwachung der Internet-Kommunikation am Arbeitsplatz: Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, ZAS 2004, 167

Laimer, Barbara/Mayr, Klaus,
Zum Spannungsverhältnis von Arbeitgeber- und Arbeitnehmerinteressen rund um die EDV-Nutzung, DRdA 2003, 410

Leitner, Armin,
Speicherung dynamisch vergebener IP-Adressen, lex:itec 2006, 23

Löschnigg, Günther,
Datenermittlung im Arbeitsverhältnis, Wien 2009

Mayer-Schönberger, Viktor/Brandl, Ernst O.,
Datenschutzgesetz, 2.Auflage, Wien 2006

Mazal, Wolfgang/Risak, Martin E. (Hrsg),
Das Arbeitsrecht – System und Praxiskommentar, Kapitel X. 6. Private Verrichtungen des Arbeitnehmers während der Arbeitszeit (Bearbeiter *Brodil, Wolfgang*), Wien, Stand 11. Erg.Lfg./Mai 2008

Naderhirn, Johanna H.,
Kollektives Arbeitsrecht und Arbeitnehmerkontrolle, in *Resch, Reinhard (Hrsg),* Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, Wien 2005, S. 91-115

Obereder, Alois,
E-Mail und Internetnutzung aus arbeitsrechtlicher Sicht, RdA 2001, 75

Parschalk, Martin/Otto, Gerald/Weber, Jan/Zuser, Alexander,
Telekommunikationsrecht, Wien 2006

Posch, Katharina,
Die e-Mail-Nutzung aus arbeitsrechtlicher Sicht, in *Wissenschaftliche Interessensgemeinschaft für Informationsrecht IT-LAW.AT (Hrsg)*, e-Mail – elektronische Post im Recht, Wien 2003, S. 75-88

Pracher, Petra,
Datenschutz in der Telekommunikation, in *Forgó, Nikolaus/Feldner, Birgit/Witzmann, Martin/Dieplinger, Simone (Hrsg)*, Probleme des Informationsrechts, Wien 2003, S. 351-377

Raif, Alexander/Kunze, Kati,
Internetsurfen als Kündigungsgrund – keine leichte Aufgabe für den Arbeitgeber, in Sammlung Arbeitsrechtlicher Entscheidungen (SAE) 01/2009, S. 19-25

Reimer, Sebastian,
Verfassungs- und europarechtliche Überlegungen zur datenschutzrechtlichen Zustimmung, in *Jahnel, Dietmar/Siegwart, Stefan/Fercher, Natalie (Hrsg)*, Aktuelle Fragen des Datenschutzrechts, Wien 2007, S. 183-210

Reindl, Susanne,
Computerstrafrecht im Überblick, Wien 2004

Rotter, Erwin,
Internet-Zugang für Arbeitnehmer – Mustervereinbarung gibt dem Dienstnehmer klare Verhaltensmaßregeln, ASok 1999, 118

Ruhle, Ernst-Olav/Freund, Natascha/Kronegger, Dieter/Schwarz, Maria,
Das neue österreichische Telekommunikations- und Rundfunkrecht, Wien 2004

Sacherer, Remo,
Internet am Arbeitsplatz als zustimmungspflichtige Kontrollmaßnahme?, RdW 2005, 627

Sacherer, Remo,
Datenschutzrechtliche Aspekte der Internetnutzung von Arbeitnehmern, RdW 2005, 173

Schönfeld, Anja/Strese, Franziska/Flemming, Anne,
Ausgewählte Probleme der Nutzung des Internet im Arbeitsleben, MMR 2001, 8

Stärker, Lukas,
Datenschutzgesetz (DSG), Wien 2008

Steinkühler, Bernhard/Raif, Alexander,
„Big Brother“ am Arbeitsplatz − Arbeitnehmerüberwachung, AuA 2009, 213

Steria Mummert Consulting AG,
Jedes vierte Unternehmen kontrolliert das Verbot privater E-Mails am Arbeitsplatz (Pressemitteilung vom 29.01.2009 zur Studie „IT-Security 2008“), Hamburg 2009

Stiger, Christoffer,
Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó, Nikolaus/Feldner, Birgit/Witzmann, Martin/Dieplinger, Simone (Hrsg),* Probleme des Informationsrechts, Wien 2003, S. 407-438

Stratil, Alfred (Hrsg),
Telekommunikationsgesetz 2003, 3. Auflage, Wien 2004

Thiele, Clemens,
Internet am Arbeitsplatz ─ Erste arbeitsrechtliche Konfliktfälle, ecolex 2001, 613

Trittin, Wolfgang/Fischer, Esther D.,
Datenschutz und Mitbestimmung – Konzernweite Personaldatenverarbeitung und die Zuständigkeit der Arbeitnehmervertretung, NZA 2009, 343

Zanger, Georg/Schöll, Liselotte,
Telekommunikationsgesetz – Kommentar zum TKG 2003, 2.Auflage, Wien 2004

Ziehensack, Helmut,
Vertragsbedienstetengesetz Praxiskommentar, Wien 2003, Loseblatt 11. Erg.Lfg./Mai 2009

Anhang zum Gesetzesentwurf:
Gesetzestext, Erläuterungen und Stellungnahmen

Gesetzestext (Regierungsvorlage)

160 d.B. (XXIV. GP)
Regierungsvorlage betreffend Bundesgesetz, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz und das Bundes-Personalvertretungsgesetz geändert werden

(Vorangegangener Ministerialentwurf: ME Beamten-Dienstrechtsgesetz 1979, Vertragsbedienstetengesetz 1948 u. a., Änderung, 17/ME [XXIV. GP])

Regierungsvorlage

Bundesgesetz, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz und das Bundes-Personalvertretungsgesetz geändert werden

Der Nationalrat hat beschlossen:

INHALTSVERZEICHNIS

Artikel 1
Änderung des Beamten-Dienstrechtsgesetzes 1979

Das Beamten-Dienstrechtsgesetz 1979, BGBl. Nr. 333, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. XXX/XXXX und die Bundesministeriengesetz-Novelle 2009, BGBl. I Nr. 3, wird wie folgt geändert:

1. An die Stelle des § 79c samt Überschrift treten folgende Bestimmungen samt Überschriften:

„5a. Unterabschnitt
IKT-Nutzung und Kontrollmaßnahmen

Begriffsbestimmungen

§ 79c. Im Sinne der §§ 79d bis 79h bedeuten die folgenden Begriffe:

1. „IKT“ (Informations- und Kommunikationstechnologie oder -technik): alle Einrichtungen zur elektronischen oder nachrichtentechnischen Übermittlung, Speicherung und Verarbeitung von Sprache, Text, Stand- und Bewegbildern sowie Daten,
2. „IT-Stelle“: die für die technische Ermöglichung oder die Sicherheit der IKT-Nutzung zuständige Organisationseinheit,
3. „IKT-Infrastruktur“: alle Geräte („Hardware“), die vom Dienstgeber zur Verfügung gestellt werden oder im Einvernehmen mit dem Dienstgeber für dienstliche Zwecke benutzt werden und der Informationsverarbeitung für Zwecke des Dienstgebers dienen, sowie die darauf befindlichen Programme und Daten („Software“),
4. „IKT-Nutzung“: Nutzung der IKT-Infrastruktur,
5. „korrekte Funktionsfähigkeit“: Wahrung der Vertraulichkeit, der Integrität und Verfügbarkeit der IKT-Infrastruktur,
6. „Nachricht“: jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird.

Grundsätze der IKT-Nutzung

§ 79d. Die IKT-Infrastruktur darf von den Beamten grundsätzlich nur für dienstliche Zwecke genutzt werden. In einem eingeschränkten Ausmaß ist auch die private Nutzung der für den Dienstbetrieb zur Verfügung stehenden IKT-Infrastruktur erlaubt, sofern sie nicht missbräuchlich erfolgt, dem Ansehen des öffentlichen Dienstes nicht schadet, der Aufrechterhaltung eines geordneten Dienstbetriebes nicht entgegensteht und sie die Sicherheit und die Leistungsfähigkeit der IKT-Infrastruktur nicht gefährdet. Die Beamten haben keinen Rechtsanspruch auf eine private IKT-Nutzung. Die Beamten sind verpflichtet, sich an die durch Verordnung der Bundesregierung festzulegenden Nutzungsgrundsätze sowie allfällige weitere ressort- oder arbeitsplatzspezifische Nutzungsregelungen für eine private IKT-Nutzung zu halten. Mit diesen Nutzungsgrundsätzen werden inhaltliche Vorgaben für die Zulässigkeit einer privaten IKT-Nutzung festgelegt, wobei insbesondere der zeitliche Rahmen, der Umfang und die Art einer zulässigen privaten IKT-Nutzung geregelt werden.

Grundsätze der Datenverwendung, Kontrollmaßnahmen

§ 79e. (1) Die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, ist unzulässig.

(2) Personenbezogene Daten der IKT-Nutzung dürfen nach Maßgabe der §§ 79f und 79g zu Kontrollzwecken nur verwendet werden, wenn dies

1. zur Abwehr von Schäden an der IKT-Infrastruktur oder zur Gewährleistung ihrer korrekten Funktionsfähigkeit oder
2. bei einem begründeten Verdacht einer gröblichen Dienstpflichtverletzung über Auftrag des Leiters der Dienststelle
   a) zum Zweck der Verhinderung weiterer Dienstpflichtverletzungen, wenn zeitliche, inhaltliche oder quantitative Beschränkungen der bereitgestellten IKT-Nutzung dafür nicht ausreichen, oder
   b) zum Zweck der Klarstellung des Sachverhaltes

erfolgt.

(3) Inhalte übertragener Nachrichten dürfen für die Zwecke des Abs. 2 Z 1 nur dann kontrolliert werden, wenn dies für deren Erreichung unbedingt notwendig ist. Sie dürfen nicht Gegenstand von Kontrollmaßnahmen im Sinne des Abs. 2 Z 2 sein.

(4) Kontrollmaßnahmen dürfen sich nur auf Organisationseinheiten mit mindestens fünf Bediensteten beziehen. Bei Organisationseinheiten mit weniger als fünf Bediensteten ist für die Durchführung einer Kontrollmaßnahme die jeweils übergeordnete Organisationseinheit miteinzubeziehen. Wenn bestimmte Programme und Anwendungen auch unter Einbeziehung der übergeordneten Organisationseinheiten weniger als fünf Bediensteten zur Verfügung stehen, dürfen Kontrollmaßnahmen auch auf diesen kleineren Bedienstetenkreis bezogen durchgeführt werden.

(5) In anderen Bundesgesetzen enthaltene Regelungen über die Zulässigkeit der Überprüfung der ordnungsgemäßen Verwendung von Daten bleiben unberührt.

Kontrolle zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit

§ 79f. (1) Geht von einer IKT-Nutzung die Gefahr eines Schadens für die IKT-Infrastruktur oder eine Gefahr für die Gewährleistung ihrer korrekten Funktionsfähigkeit aus, hat die IT-Stelle, wenn sie die Gefahr nicht selbst abwenden kann, den Leiter der Dienststelle in anonymisierter Form über Art und Dauer dieser IKT-Nutzung zu informieren. Auf Inhalte übertragener Nachrichten darf dabei nicht Bezug genommen werden.

(2) Der Leiter der Dienststelle hat die von einer Kontrollmaßnahme betroffenen Beamten über die Information gemäß Abs. 1 umgehend in Kenntnis zu setzen und

1. auf die Beseitigung der Gefahr gemäß Abs. 1 hinzuwirken,
2. die betroffenen Beamten über die Möglichkeit einer namentlichen Ausforschung innerhalb eines vier Wochen nicht übersteigenden Beobachtungszeitraumes, wenn innerhalb dieses Zeitraumes die Gefahr fortbesteht oder eine gleichgelagerte Gefahr auftritt, nachweislich zu informieren und
3. die IT-Stelle vom Zeitpunkt der Information gemäß Z 2 zu unterrichten.

(3) Ein längerer als der in Abs. 2 Z 2 vorgesehene Beobachtungszeitraum darf nur in begründeten Ausnahmefällen festgesetzt werden.

(4) Besteht die Gefahr nach erfolgter Information gemäß Abs. 2 weiter, hat die IT-Stelle dem Leiter der Dienststelle die betreffenden IKT-Nutzungen namentlich und in schriftlicher Form zur Kenntnis zu bringen. Auf Inhalte übertragener Nachrichten darf dabei nicht Bezug genommen werden.

(5) Besteht aufgrund einer IKT-Nutzung eine konkrete unmittelbare Gefährdung für die IKT-Infrastruktur oder ihre korrekte Funktionsfähigkeit, darf die IT-Stelle abweichend von Abs. 1 bis 4 die personenbezogenen Daten der IKT-Nutzung verwenden, soweit dies zur Behebung dieser Gefährdung unbedingt notwendig ist. Diese Daten dürfen nicht für andere Zwecke verwendet werden. Der Beamte ist über die Verwendung der Daten umgehend zu informieren. Die IT-Stelle hat über die Gefährdung, die verwendeten Daten und die erfolgte Information des Beamten Protokoll zu führen. Die den Beamten betreffenden Daten des Protokolls sind ihm auf sein Verlangen zur Verfügung zu stellen.

Kontrolle bei begründetem Verdacht einer gröblichen Dienstpflichtverletzung

§ 79g. (1) Besteht der begründete, aber nicht gegen einen bestimmten Beamten gerichtete Verdacht einer gröblichen Dienstpflichtverletzung, kann der Leiter der Dienststelle die IT-Stelle beauftragen, auf diesen Verdachtsfall Bezug habende Daten der IKT-Nutzung zu ermitteln. Ein solcher Ermittlungsauftrag hat schriftlich zu ergehen und den Verdachtsfall genau zu umschreiben.

(2) Die IT-Stelle hat dem Leiter der Dienststelle über die IKT-Nutzungen im Umfang des Ermittlungsauftrags in anonymisierter Weise zu berichten.

(3) Der Leiter der Dienststelle hat die von einer Kontrollmaßnahme betroffenen Beamten über den Ermittlungsauftrag gemäß Abs. 1 und die Information gemäß Abs. 2 umgehend in Kenntnis zu setzen und

1. auf die Einhaltung der Dienstpflichten hinzuwirken,
2. die betroffenen Beamten über die Möglichkeit einer namentlichen Ausforschung innerhalb eines vier Wochen nicht übersteigenden Beobachtungszeitraumes, wenn innerhalb dieses Zeitraumes der im Ermittlungsauftrag gemäß Abs. 1 genannte Verdachtsfall fortbesteht oder ein gleichgelagerter Verdachtsfall auftritt, nachweislich zu informieren und
3. die IT-Stelle vom Zeitpunkt der Information gemäß Z 2 zu unterrichten.

(4) Ein längerer als der in Abs. 3 Z 2 vorgesehene Beobachtungszeitraum darf nur in begründeten Ausnahmefällen festgesetzt werden.

(5) Der Leiter der Dienststelle kann innerhalb des Beobachtungszeitraumes von der IT-Stelle Auskunft über Daten verlangen, die sich auf einen Verdachtsfall im Sinne des Abs. 3 Z 2 beziehen.

(6) Die IT-Stelle hat dem Leiter der Dienststelle über die IKT-Nutzungen im Umfang des Verlangens nach Abs. 5 namentlich und in schriftlicher Form zu berichten. Der betroffene Beamte ist vom Leiter der Dienststelle umgehend zu informieren.

(7) Besteht der begründete Verdacht einer gröblichen Dienstpflichtverletzung gegen einen bestimmten Beamten, kann der Leiter der Dienststelle abweichend von Abs. 1 bis 6 und § 79e Abs. 4 die IT-Stelle beauftragen, auf diesen Verdachtsfall Bezug habende Daten der IKT-Nutzung des Beamten zu ermitteln. Ein solcher Ermittlungsauftrag hat schriftlich zu ergehen und den Verdachtsfall unter Nennung des Beamten genau zu umschreiben. Die IT-Stelle hat dem Leiter der Dienststelle über die IKT-Nutzungen im Umfang des Ermittlungsauftrags in schriftlicher Form zu berichten. Der Beamte ist vom Leiter der Dienststelle umgehend über den Bericht der IT-Stelle und den diesem vorausgegangenen Ermittlungsauftrag zu informieren.

Sonstige zulässige Datenverwendungen

§ 79h. Unbeschadet des § 79e darf die IT-Stelle Daten über die IKT-Nutzung eines Beamten verwenden, soweit dies auf sein Ersuchen zum Zweck der Erbringung von Serviceleistungen im Zusammenhang mit der IKT-Nutzung dieses Beamten erfolgt.

Ausnahmebestimmung

§ 79i. Die §§ 79e Abs. 2 bis 5, 79f und 79g sind auf Beamte der Parlamentsdirektion nicht anzuwenden.“

2. In § 140 Abs. 3 treten an die Stelle der den Verfassungsgerichtshof betreffenden Zeile folgende Bestimmungen:

„für den leitenden Beamten des Generalsekretariats	
des Verfassungsgerichtshofes	Generalsekretär
für den leitenden Beamten des Präsidiums	
des Verfassungsgerichtshofes	Präsidialdirektor“

3. Anlage 1 Z 1.3.8 lautet:

„**1.3.8.** der Generalsekretär und der Präsidialdirektor im Verfassungsgerichtshof,“

Artikel 2
Änderung des Vertragsbedienstetengesetzes 1948

Das Vertragsbedienstetengesetz 1948, BGBl. Nr. 86, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. XXX/XXXX und die Bundesministeriengesetz-Novelle 2009, BGBl. I Nr. 3, wird wie folgt geändert:

§ 29n samt Überschrift lautet:

„IKT-Nutzung und Kontrollmaßnahmen

§ 29n. Die §§ 79c bis 79i BDG 1979 sind anzuwenden.“

Artikel 3
Änderung des Richter- und Staatsanwaltschaftsdienstgesetzes

Das Richter- und Staatsanwaltschaftsdienstgesetz, BGBl. Nr. 305/1961, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. XXX/XXXX, wird wie folgt geändert:

§ 206 erster Satz lautet:

„Im Übrigen ist der Allgemeine Teil des BDG 1979 mit Ausnahme des 5. Unterabschnitts und 5a. Unterabschnitts des 6. Abschnitts, des 7. und des 8. Abschnitts sinngemäß anzuwenden.“

Artikel 4
Änderung des Bundes-Personalvertretungsgesetzes

Das Bundes-Personalvertretungsgesetz, BGBl. Nr. 133/1967, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. XXX/XXXX und die Bundesministeriengesetz-Novelle 2009, BGBl. I Nr. 3, wird wie folgt geändert:

1. In § 9 Abs. 2 wird am Ende der lit. m der Punkt durch einen Strichpunkt ersetzt und werden folgende lit. n und o angefügt:

„n) bei der Durchführung einer Kontrollmaßnahme unter Verwendung von personenbezogenen Daten der IKT-Nutzung bei einem begründeten Verdacht einer gröblichen Dienstpflichtverletzung;

o) bei der Festsetzung eines längeren Beobachtungszeitraumes als vier Wochen zur Durchführung einer Kontrollmaßnahme unter Verwendung von personenbezogenen Daten der IKT-Nutzung.“

2. In § 9 Abs. 3 wird am Ende der lit. n der Punkt durch einen Strichpunkt ersetzt und wird folgende lit. o angefügt:

„o) der Zeitpunkt der Information im Sinne des § 79g Abs. 3 Z 2 des Beamten-Dienstrechtsgesetzes (BDG 1979), BGBl. Nr. 333, die namentliche Auswertung der IKT-Nutzungen nach § 79g Abs. 6 BDG 1979 und der Datenzugriff nach § 79g Abs. 7 BDG 1979 im Rahmen der Kontrolle bei begründetem Verdacht einer gröblichen Dienstpflichtverletzung.“

3. § 14 Abs. 3 letzter Satz entfällt.

4. In § 15 Abs. 5a entfällt der Zitatteil „ BGBl. Nr. 333,“

Erläuterungen

160 d.B. (XXIV. GP)
Regierungsvorlage betreffend Bundesgesetz, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz und das Bundes-Personalvertretungsgesetz geändert werden

(Vorangegangener Ministerialentwurf: ME Beamten-Dienstrechtsgesetz 1979, Vertragsbedienstetengesetz 1948 u. a., Änderung, 17/ME [XXIV. GP])

Vorblatt

Problem:

Die zunehmende Ausstattung von Arbeitsplätzen mit moderner Informationstechnologie führt zur Fragestellung, in welchem Umfang und in welcher Weise die Kontrolle der Bediensteten durch den Dienstgeber zulässig ist. Auch viele Bedienstete im Bundesdienst haben bereits Zugang zu Internetdienstleistungen, wie dem World Wide Web (WWW) oder E-Mail. Obwohl dadurch der Aktionsradius der Bediensteten wesentlich erweitert wird, bringen die neuen Kommunikationstechnologien nicht nur Vorteile mit sich. Zum einen wird auf Seiten der Bediensteten ein nicht zu unterschätzendes Missbrauchspotential geschaffen, zum anderen entstehen aufgrund der Datenvernetzung bisher nicht vorhandene Kontrollmöglichkeiten auf Seiten des Dienstgebers.

Ziel:

Durch den vorliegenden Entwurf soll ein dem Verhältnismäßigkeitsprinzip entsprechender Ausgleich dieser diametral entgegenstehenden und teilweise grundrechtlich geschützten Interessen auf Bediensteten- und Dienstgeberseite betreffend Nutzungs- und Kontrollmöglichkeiten geschaffen werden.

Inhalt:

Schaffung einer gesetzlichen Grundlage für die Zulässigerklärung der privaten IKT-Nutzung, insbesondere auch von Internet und E-Mail, durch die Bediensteten und für die Festlegung von Nutzungsgrundsätzen durch Verordnung der Bundesregierung; Festlegung von Kontrollgrundsätzen, mit denen eine überschießende und damit unverhältnismäßige Kontrolle durch den Dienstgeber hintangehalten werden soll.

Alternativen:

Keine.

Finanzielle Auswirkungen:

Keine. Es ist davon auszugehen, dass eventuell erforderliche Adaptierungen der Software aus den laufenden Budgets bedeckt werden können. Keine Zusatzkosten sollten auch durch die Zulässigerklärung der privaten IKT-Nutzung entstehen, da diese nicht jene Kosten übersteigen sollte, die durch eine bisherige – vom Dienstgeber tolerierte – private IKT-Nutzung entstanden sind.

Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Keine.

Auswirkungen auf die Verwaltungslasten für Unternehmen:

Es sind keine Informationsverpflichtungen für Unternehmen vorgesehen.

Auswirkungen in umweltpolitischer Hinsicht, insbesondere Klimaverträglichkeit:

Das Regelungsvorhaben ist nicht klimarelevant.

Auswirkungen in konsumentenschutzpolitischer sowie sozialer Hinsicht:

Keine.

Geschlechtsspezifische Auswirkungen:

Keine.

Besonderheiten des Normerzeugungsverfahrens:

Keine.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Die vorgesehenen Regelungen sind mit dem Gemeinschaftsrecht, insbesondere der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995 S. 31, vereinbar.

Erläuterungen

I. Allgemeiner Teil

Die zunehmende Ausstattung von Arbeitsplätzen mit moderner Informationstechnologie führt zur Fragestellung, in welchem Umfang und in welcher Weise die Kontrolle der Bediensteten durch den Dienstgeber zulässig ist. Auch viele Bedienstete im Bundesdienst haben bereits Zugang zu Internetdienstleistungen, wie dem World Wide Web (WWW) oder E-Mail. Obwohl dadurch der Aktionsradius der Bediensteten wesentlich erweitert wird, bringen die neuen Kommunikationstechnologien nicht nur Vorteile mit sich. Zum einen wird auf Seiten der Bediensteten ein nicht zu unterschätzendes Missbrauchspotential geschaffen, zum anderen entstehen aufgrund der Datenvernetzung bisher nicht vorhandene Kontrollmöglichkeiten auf Seiten des Dienstgebers.

Durch den vorliegenden Entwurf soll ein dem Verhältnismäßigkeitsprinzip entsprechender Ausgleich dieser diametral entgegenstehenden und teilweise grundrechtlich geschützten Interessen auf Bediensteten- und Dienstgeberseite betreffend Nutzungs- und Kontrollmöglichkeiten geschaffen werden.

Die Bediensteten sind vor übermäßiger Kontrolle am Arbeitsplatz durch den Dienstgeber zu schützen. Eine Balance zwischen dem Schutz der Bediensteten und den berechtigten Interessen des Dienstgebers ist in diesem Sinne zu gewährleisten. Transparenz in Form von Grundsätzen für die private IKT-Nutzung ist daher besonders wichtig, damit die Bediensteten ihr Verhalten zulässig gestalten und somit eine Kontrolle vermeiden können. Sind Kontrollen aus den gesetzlich festgelegten Gründen dennoch erforderlich, so sind diese dem gegenständlichen Entwurf zufolge grundsätzlich einem Modell stufenweiser Kontrollverdichtung entsprechend vorzunehmen (zu diesem Modell *Kotschy/Reimer*, Die Überwachung der Internet-Kommunikation am Arbeitsplatz, ZAS 2004, 169).

Der Entwurf legt Kontrollgrundsätze für den Dienstgeber fest, die eine überschießende und damit unverhältnismäßige Kontrolle der IKT-Nutzung durch die Bediensteten hintanhalten sollen. Im Verfahren einer stufenweisen Kontrollverdichtung wird die Protokollierung von Daten aus technischen Gründen zwar maschinen- und damit auch personenbezogen vorgenommen. Die Kontrolle erfolgt allerdings vorerst nur durch die IT-Stelle. Erst und bloß im Fall des Weiterbestehens einer Gefahr für die IKT-Infrastruktur bzw. ihre korrekte Funktionsfähigkeit oder einer pflichtwidrigen Nutzung ist – in einem zweiten Schritt – die Offenlegung der personenbezogenen Daten gegenüber dem Leiter oder der Leiterin der jeweils zuständigen Dienststelle vorgesehen. Ausgenommen von diesem Verfahren einer stufenweisen Kontrollverdichtung sind nur die Fälle einer konkreten unmittelbaren Gefährdung für die IKT-Infrastruktur oder ihre korrekte Funktionsfähigkeit und ein bereits vorliegender begründeter Verdacht einer gröblichen Dienstpflichtverletzung gegen einen bestimmten Bediensteten oder eine bestimmte Bedienstete. Durch die im Entwurf ebenfalls vorgesehene Änderung des PVG werden die Mitwirkungsrechte der Personalvertretung bei der Durchführung von Kontrollmaßnahmen festgelegt.

Gleichzeitig wird eine gesetzliche Grundlage für die Zulässigerklärung der privaten Nutzung der IKT-Infrastruktur, insbesondere auch von Internet und E-Mail, durch die Bediensteten und für die Festlegung von Nutzungsgrundsätzen durch Verordnung der Bundesregierung geschaffen.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Erlassung des vorgeschlagenen Bundesgesetzes ergibt sich hinsichtlich der Art. 1 bis 4 (BDG 1979, VBG, RStDG, PVG) aus Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

II. Besonderer Teil

Zu Art. 1, Art. 2, Art. 3 (§§ 79c bis 79i BDG 1979, § 29n VBG, § 206 erster Satz RStDG):

Zu § 79c Z 1 BDG 1979:

Der Begriff IKT ist die zusammenfassende Bezeichnung für Computer- und Kommunikationstechnik. Er erfasst alle Einrichtungen und Netze für die Übertragung sowie die für Empfang, Versand und Verarbeitung erforderlichen Endgeräte.

Zu § 79d BDG 1979:

Sowohl im öffentlichen Dienst als auch in der Privatwirtschaft ist es Realität, dass die IKT-Infrastruktur, die für dienstliche bzw. betriebliche Zwecke zur Verfügung steht, von den Bediensteten bzw. Arbeitnehmern auch privat genutzt wird. Diese Realität wird im Regelfall in einem gewissen Ausmaß und – sofern dies mit den in § 45 BDG 1979 und § 5b VBG normierten Dienstpflichten in Einklang gebracht

werden kann – vom Dienstgeber toleriert. Mit der gegenständlichen Bestimmung soll klargestellt werden, dass die IKT-Infrastruktur grundsätzlich nur dienstlichen Zwecken dienen soll, in einem eingeschränkten Ausmaß und unter Einhaltung gewisser Nutzungsbedingungen aber auch privat genutzt werden darf. Diese Nutzungsbedingungen, die – unbeschadet weiterer ressort- bzw. arbeitsplatzspezifischer Nutzungsregelungen – durch Verordnung der Bundesregierung festzulegen sind, haben sich auf den zeitlichen Rahmen sowie Art und Umfang einer zulässigen privaten Nutzung zu beziehen. Sie haben damit auch näher festzulegen, was unter einer missbräuchlichen Nutzung zu verstehen ist, womit einerseits eine exzessive zeitliche und quantitative Nutzung gemeint ist, andererseits aber auch die Art der Nutzung wie beispielsweise eine missbräuchliche Berufung auf die dienstliche Stellung eines Beamten für private Zwecke. Wie Beispiele aus der Vergangenheit gezeigt haben, schadet dem Ansehen des öffentlichen Dienstes der Zugriff auf rechtswidrige oder aus sittlichen Gründen verpönte Internetseiten wie z.B. Seiten mit pornografischem Inhalt. Die Aufrechterhaltung eines geordneten Dienstbetriebes und die Sicherheit sowie die Leistungsfähigkeit der IKT-Infrastruktur sind schließlich ebenfalls einerseits durch eine exzessive Nutzung, andererseits aber durch das Herunterladen von bestimmten, besonders für deren Anfälligkeit für Schadprogramme bekannten, ausführenden Dateitypen beeinträchtigt bzw. gefährdet.

Die Beamten haben keinen Anspruch auf eine private Nutzung der für den Dienstbetrieb zur Verfügung stehenden IKT-Infrastruktur. Da sich eine private Nutzung immer nur auf die für den Dienstbetrieb bestehende IKT-Infrastruktur beziehen kann, steht es dem Dienstgeber frei zu entscheiden, ob bzw. welche IKT-Infrastruktur zur Verfügung steht. Es steht ihm damit prinzipiell auch frei zu entscheiden, welche Zugriffsmöglichkeiten er auf das Internet ermöglicht, da Ausgangspunkt immer die für den Dienstbetrieb erforderlichen Zugriffsmöglichkeiten sind. Er darf daher auch Filtersoftware zum Einsatz bringen. Werden jedoch nicht nur für den Dienstbetrieb erforderliche, sondern auch weitere Internetangebote allgemein zugänglich gemacht, so ist bei einer Beschränkung nach sachlichen, durch diese Bestimmung vorgezeichneten Motiven vorzugehen (vgl. in diesem Zusammenhang zum in Art. 10 EMRK verbürgten Grundrecht auf Informationsfreiheit EGMR 19. 12. 1994, ÖJZ 1995/23).

Zu § 79e BDG 1979:

Abs. 1 entspricht dem Wortlaut des bisherigen § 79c. Die Datenverwendung in anderen als den in Abs. 2 genannten Fällen bzw. unter Nichteinhaltung der Vorschriften der §§ 79f und 79g – sowohl durch den Dienstgeber als auch durch die IT-Stelle – zu Kontrollzwecken ist unzulässig (zB. der Einsatz von Software, die Arbeitsgewohnheiten der Bediensteten aufzeichnet [„Spionage-Software“]). Vom Begriff der Kontrolle nicht umfasst ist jedoch der Einsatz von Software-Programmen, die zur vollautomatischen Abwehr von Computerviren oder Ähnlichem bzw. als Spamfilter dienen. Schon nach geltendem Recht dürfen Kontrollmaßnahmen nur dann eingeführt werden, wenn diesbezüglich ein Einvernehmen mit dem Zentralausschuss im Sinne des § 10 PVG hergestellt wird (§ 14 Abs. 3 erster Satz PVG).

Die §§ 79e bis 79g BDG 1979 legen Kontrollgrundsätze fest, die eine überschießende und damit unverhältnismäßige Kontrolle durch den Dienstgeber hintanhalten sollen. Ihre Nichteinhaltung wäre nicht nur allgemein rechtswidrig, sondern würde gleichzeitig die Begehung einer Dienstpflichtverletzung durch die die Kontrollen durchführenden Bediensteten darstellen.

Im Hinblick auf das Vorliegen eines begründeten Verdachtes der Begehung von Dienstpflichtverletzungen soll ein überschießender Zugriff auf Daten der Bediensteten dadurch verhindert werden, dass nicht jegliches pflichtwidrige Verhalten eine Kontrolle der IKT-Nutzung von Bundesbediensteten legitimieren kann, sondern nur ein solches, das eine gröbliche Verletzung von Dienstpflichten bedeutet (Abs. 2 Z 2). Mit dem Begriff der gröblichen Dienstpflichtverletzung wird – da diese Bestimmung für Beamte und Vertragsbedienstete gleichermaßen gelten soll – an den Kündigungsgrund des § 32 Abs. 2 Z 1 VBG angeknüpft.

Gemäß Abs. 3 dürfen Inhalte übertragener Nachrichten (Inhaltsdaten) nicht Gegenstand von Kontrollmaßnahmen sein, die im Hinblick auf das Bestehen eines begründeten Verdachtes einer gröblichen Dienstpflichtverletzung erfolgen. Auch zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit dürfen Inhaltsdaten nur dann kontrolliert werden, wenn dies zur Erreichung dieser Zwecke unbedingt notwendig ist. Die zuständige IT-Stelle hat daher aufgrund ihres technischen Sachverstandes im Einzelfall jeweils zu prüfen, ob es – in einer Betrachtung ex ante – nicht möglich ist, diese Zwecke anders als durch den Zugriff auf Inhaltsdaten zu erreichen. Selbst für diesen Fall wird im § 79f Abs. 1 und 4 jedoch festgelegt, dass diese Daten von der IT-Stelle nicht an den Leiter oder die Leiterin der zuständigen Dienststelle weitergegeben werden dürfen. Die Definition des Begriffes „Nachricht“ in § 79c Z 6 orientiert sich dabei am § 92 Abs. 3 Z 7 TKG 2003 und damit ebenso wie diese Bestimmung (vgl. RV 128 BlgNR 22. GP, 17 f.) an der entsprechenden Begriffsbestimmung des Art. 2 lit. d der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener

Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. Nr. L 201 vom 12. Juli 2002 S. 37.

Bei der Durchführung von Kontrollmaßnahmen ist darauf Bedacht zu nehmen, dass davon nicht mehr Bedienstete erfasst werden, als es zur Verfolgung einer der Zwecke des Abs. 2 erforderlich ist. Abs. 4 definiert den Kreis der von Kontrollmaßnahmen potentiell betroffenen Bediensteten unter zwei Gesichtspunkten: Zum einen soll dieser Kreis nicht zu klein sein, um die Anonymität der Bediensteten nicht zu gefährden. Zum anderen soll er aber auch nicht so umfangreich sein, dass eine zu große Zahl an Bediensteten, die mit jenen IKT-Nutzungen, auf Grund derer ein Kontrollverfahren eingeleitet wird, nichts zu tun haben, Adressat einer Kontrollmaßnahme wird. Der Entwurf legt daher als Minimum des zu kontrollierenden Personenkreises fünf Bedienstete fest. Nur wenn eine Organisationseinheit diese Anzahl an Bediensteten unterschreitet, dürfen die Bediensteten der nächstgrößeren Organisationseinheit in die Kontrollmaßnahme miteinbezogen werden. Ausnahmsweise darf jedoch auch ein kleinerer Bedienstetenkreis kontrolliert werden, nämlich dann, wenn eine bestimmte Anwendung oder ein bestimmtes Programm, das von einer Kontrollmaßnahme erfasst werden soll, selbst bei Ausdehnung der Kontrollmaßnahme auf die übergeordneten Organisationseinheiten weniger als fünf Bediensteten zur Verfügung steht.

Abs. 5 nimmt schließlich darauf Bedacht, dass es gesetzliche Regelungen gibt, die die Überprüfung des Datenzugriffs von Beamten normieren (vgl. z.B. § 14 Abs. 2 Z 7 DSG 2000). Mit dieser Bestimmung wird klargestellt, dass derartige Regelungen vom gegenständlichen Gesetzesentwurf unberührt bleiben und somit die Protokollierung der Zugriffe von Bediensteten etwa auf Kundendaten oder die generalpräventive auswertende Kontrolle der Protokolle zum Zweck der Feststellung und künftigen Unterbindung unzulässiger Zugriffe zur Verwirklichung der Datensicherheit im Rahmen dieser Bestimmungen möglich bzw. geboten ist. § 79e Abs. 5 erstreckt sich auch auf die §§ 79f und 79g.

Zu § 79f BDG 1979:

Durch die IKT-Nutzung kann es nicht nur zu einer Gefahr eines Schadens für die IKT-Infrastruktur kommen (zB Datenverluste, kompletter Ausfall durch Überlastung u.a.), sondern auch zu einem Fehlverhalten der IKT-Infrastruktur. Bei einer Infektion durch Schadsoftware kann es durchaus sein, dass die IKT noch reibungslos funktioniert, jedoch Informationen an Dritte übermittelt (zB durch Trojaner, die Passwort-Eingaben aufzeichnen und versenden) oder E-Mails mit problematischem Inhalt aus dem Netzwerk nach außen verschickt werden. Ebenso kann die Bedienung der IKT-Geräte durch eine große CPU-Belastung wesentlich verlangsamt werden. IKT-Nutzungen im Sinne des § 79f Abs. 1 BDG 1979 müssen nicht notwendigerweise gleichzeitig auch Dienstpflichtverletzungen darstellen. Zu Beginn der stufenweisen Kontrollverdichtung soll bei einer Gefahr eines Schadens für die IKT-Infrastruktur oder einer Gefahr für die Gewährleistung ihrer korrekten Funktionsfähigkeit eine anonymisierte Auswertung über Art und Dauer der IKT-Nutzungen erfolgen. Damit wird garantiert, dass diesfalls keine personenbezogenen Daten aus dem Einflussbereich des zuständigen Systemadministrators übermittelt werden. Das Verfahren nach § 79f BDG 1979 wird somit von der IT-Stelle initiiert, woraufhin der Leiter oder die Leiterin der für die betroffene Organisationseinheit zuständigen Dienststelle die Bediensteten dieser Organisationseinheit über die Information der IT-Stelle in Kenntnis zu setzen, auf die Beseitigung der Gefahr hinzuwirken und die Bediensteten über die Möglichkeit einer namentlichen Ausforschung bei Fortbestehen der Gefahr innerhalb eines vierwöchigen Beobachtungszeitraumes nachweislich zu informieren hat. Der Beobachtungszeitraum darf in begründeten Ausnahmefällen die Dauer von vier Wochen überschreiten (Abs. 3). Ein begründeter Ausnahmefall wird dann vorliegen, wenn technische Probleme nur zu gewissen – beispielsweise monatlichen – Stichtagen auftreten oder in einer Organisationseinheit, in der sich Bedienstete längere Zeit auf Urlaub oder im Krankenstand befinden. Die Dauer für eine Verlängerung muss sich daher immer aus einem sachlichen Grund heraus rechtfertigen lassen, der eine auf maximal vier Wochen beschränkte Kontrolle als nicht zielführend erscheinen lässt. Die nachweisliche Information der Bediensteten ist ein wesentliches Element der stufenweisen Kontrollverdichtung, um die Verhältnismäßigkeit von Maßnahmen, die der Abwehr von Schäden an der IKT-Infrastruktur und der Gewährleistung ihrer korrekten Funktionsfähigkeit dienen, zu sichern. Die personenbezogene Übermittlung bei Fortbestand der Gefahr darf daher erst dann erfolgen, wenn der Dienststellenleiter oder die Dienststellenleiterin den zuständigen Systemadministrator von der erfolgten Information gemäß Abs. 2 unterrichtet hat und nach diesem Zeitpunkt die Gefahr weiterbesteht. Liegt hingegen eine konkrete unmittelbare Gefährdung für die IKT-Infrastruktur oder ihre korrekte Funktionsfähigkeit vor (Abs. 5), ist ein sofortiger Zugriff auf personenbezogene Daten gerechtfertigt, soweit dies zur Behebung dieser Gefährdung unbedingt notwendig ist. Über einen derartigen Zugriff ist ein Protokoll zu führen, das auf ein entsprechendes Verlangen dem oder der Bediensteten zur Verfügung zu stellen ist.

Zu § 79g BDG 1979:

Liegt ein begründeter Verdacht einer gröblichen Dienstpflichtverletzung vor, so können zwecks Verhinderung allfälliger weiterer Dienstpflichtverletzungen und/oder zur Klarstellung des Sachverhaltes in einem ersten Schritt wiederum anonymisierte Auswertungen über Auftrag des Dienststellenleiters oder der Dienststellenleiterin erfolgen. Sollen ausschließlich weitere Dienstpflichtverletzungen verhindert werden, ist dabei jedoch – § 79e Abs. 2 Z 2 lit. a entsprechend – vorher zu überprüfen, ob es möglich ist, diese durch zeitliche, inhaltliche oder quantitative Beschränkungen der IKT-Nutzung hintanzuhalten.

Der Verdacht muss von der Dienststelle ausgehen, die IT-Stelle kann das Verfahren nicht initiieren. Der anonymisierte Bericht der IT-Stelle im Umfang des Ermittlungsauftrages (Abs. 2) kann auch eine Leermeldung sein. Die Information der Bediensteten nach Abs. 3 erster Satzteil hat aber in jedem Fall (auch im Fall einer Leermeldung) zu erfolgen. In den Anwendungsfällen des § 79g ist die IT-Stelle vom Zeitpunkt der Information gemäß Abs. 3 Z 2 zu verständigen. Für die Festsetzung eines längeren als vierwöchigen Beobachtungszeitraumes gilt das zu § 79f Abs. 3 Ausgeführte (Abs. 4). Besteht innerhalb einer Beobachtungsfrist ein Verdachtsfall im Sinne des Abs. 3 Z 2 (weiter), so sind dem Leiter oder der Leiterin der Dienststelle auf dessen oder deren Verlangen (Abs. 5) die Daten über die IKT-Nutzungen personenbezogen zur Kenntnis zu bringen. Der oder die ausgeforschte Bedienstete muss nicht der- oder diejenige sein, der oder die den ursprünglichen Verdachtsfall gesetzt hat. Das ist deshalb gerechtfertigt, weil dieser Maßnahme eine allgemeine Information im Sinne der Ankündigung eines Beobachtungszeitraumes vorangeht. Nach Ablauf des Beobachtungszeitraumes auftretende Verdachtsfälle lösen jeweils ein neues Verfahren aus. Der betroffene Beamte oder die betroffene Beamtin ist über die namentliche Auswertung der IKT-Nutzungen im Umfang des Verlangens nach Abs. 5 umgehend zu informieren (Abs. 6). Liegt hingegen ein begründeter Verdacht gegen eine bestimmte Person wegen eines konkreten Vorfalls vor, muss das Verfahren einer stufenweisen Kontrollverdichtung nicht eingehalten werden, sondern ist, da hier jedenfalls die Klärung des Sachverhaltes erforderlich ist, unter Einhaltung der Verfahrensschritte des Abs. 7 der sofortige Zugriff auf die Daten der betreffenden Person zulässig. Auch in diesem Fall ist der betroffene Beamte oder die betroffene Beamtin über den erfolgten Datenzugriff und sein Ergebnis zu informieren.

Zu § 79h BDG 1979:

In jenen Fällen, in denen ein Benutzer oder eine Benutzerin um Serviceleistungen im Zusammenhang mit der IKT-Nutzung ersucht, handelt es sich nicht um Kontrollmaßnahmen gemäß den §§ 79e bis 79g. Unter Serviceleistungen sind insbesondere die Hilfestellung durch die IT-Stelle bei der Wiederherstellung von Dokumenten oder die Überprüfung von technischen Abläufen, die zur Verhinderung des Empfanges eines E-Mails (etwa wegen Spam-Verdachtes oder Virenbefalles) geführt haben, zu verstehen. Mit Ersuchen ist eine datenschutzrechtliche Zustimmung im Sinne des § 4 Z 14 DSG 2000 gemeint.

Zu § 79i BDG 1979:

Da im Bereich des Parlaments in der EDV-Verwaltung keine Trennung zwischen Bundesbediensteten und Abgeordneten und deren Mitarbeitern und Mitarbeiterinnen gemäß Klubfinanzierungsgesetz 1985 und Parlamentsmitarbeitergesetz vorhanden ist, könnte eine Kontrollmaßnahme gegenüber Beamten und Beamtinnen sowie Vertragsbediensteten der Parlamentsdirektion zu einer ungewollten Kontrolle der den Abgeordneten und deren Mitarbeitern und Mitarbeiterinnen zur Verfügung stehenden IKT-Infrastruktur führen. Um dieses Problem hintanzuhalten, sind die Bediensteten der Parlamentsdirektion von den Bestimmungen betreffend die Kontrolle der IKT-Nutzung ausgenommen. Gelten sollen für sie jedoch die Begriffsbestimmungen des § 79c, die in § 79d festgelegten Nutzungsgrundsätze sowie der dem früheren § 79c entsprechende § 79e Abs. 1, sodass insofern die bisherige Rechtslage für die Parlamentsbediensteten weiter gilt. Ebenso soll § 79h für Parlamentsbedienstete anwendbar sein; damit wird klargestellt, dass Serviceleistungen im Zusammenhang mit der IKT-Nutzung auch für Parlamentsbedienstete nicht unter den Begriff „Kontrollmaßnahme“ fallen.

Zu § 140 Abs. 3 und Anlage 1 Z 1.3.8 BDG 1979:

Organisatorische Änderungen im Verfassungsgerichtshof machen eine Anpassung der taxativ aufgelisteten Richtverwendungen sowie der Verwendungsbezeichnungen erforderlich.

Zu § 206 erster Satz RStDG:

Die Bestimmungen des BDG 1979 sind trotz der Zusammenfassung des Dienstrechtes von Richtern und Staatsanwälten im Richter- und Staatsanwaltschaftsdienstgesetz teilweise noch auf Staatsanwälte anwendbar. Die Neufassung des ersten Satzes bezweckt, dass Staatsanwälte vom Anwendungsbereich der Bestimmungen des 5a. Unterabschnittes des 6. Abschnittes des BDG 1979 über die IKT-Nutzung und Kontrollmaßnahmen nicht erfasst sind.

Zu Art. 4 (§§ 9 Abs. 2, 9 Abs. 3 und 14 Abs. 3 letzter Satz PVG):

Zu § 9 Abs. 2 PVG:

Als Pendant zu den dienstrechtlichen Vorschriften betreffend die Kontrolle der IKT-Nutzung der Bundesbediensteten enthalten die neuen Bestimmungen in lit. n und o Regelungen über die Mitwirkung der Organe der Personalvertretung bei derartigen Kontrollmaßnahmen. Sowohl bei der Durchführung einer Kontrollmaßnahme bei einem begründeten Verdacht einer gröblichen Dienstpflichtverletzung gemäß § 79e Abs. 2 Z 2 BDG 1979 als auch bei der Festsetzung eines längeren Beobachtungszeitraumes zur Durchführung einer Kontrollmaßnahme (§§ 79f Abs. 3 und 79g Abs. 4 BDG 1979) ist das Einvernehmen mit dem jeweils zuständigen Organ der Personalvertretung herzustellen. Im Fall einer Kontrollmaßnahme auf Grund des Verdachtes einer gröblichen Dienstpflichtverletzung ist die Personalvertretung somit sowohl hinsichtlich der beabsichtigten Durchführung einer Kontrollmaßnahme als auch im Hinblick auf ihr Ergebnis (§ 79g Abs. 7 letzter Satz BDG 1979) in das Verfahren eingebunden. Da gemäß § 79e Abs. 5 BDG 1979 in anderen Bundesgesetzen enthaltene Regelungen über die Zulässigkeit der Überprüfung der ordnungsgemäßen Verwendung von Daten von den Kontrollvorschriften des BDG 1979 unberührt bleiben, bezieht sich auch das Mitwirkungsrecht der Personalvertretung nicht auf diese Vorschriften.

Zu § 9 Abs. 3 PVG:

In den Anwendungsfällen des § 79g BDG 1979 ist zusätzlich zur IT-Stelle das zuständige Organ der Personalvertretung vom Zeitpunkt der Information gemäß § 79g Abs. 3 Z 2 BDG 1979 zu verständigen. Neben dem betroffenen Beamten oder der betroffenen Beamtin (§ 79g Abs. 6 BDG 1979) ist auch das zuständige Organ der Personalvertretung über die namentliche Auswertung der IKT-Nutzungen im Umfang des Verlangens nach § 79g Abs. 5 BDG 1979 zu informieren. Auch bei einer auf eine bestimmte Person abzielenden Kontrollmaßnahme gemäß § 79g Abs. 7 BDG 1979 ist das zuständige Organ der Personalvertretung über den erfolgten Datenzugriff und sein Ergebnis zu informieren.

Zu § 14 Abs. 3 letzter Satz PVG:

Die bisherige Verordnungsermächtigung entfällt, da sie aufgrund der umfassenden gesetzlichen Regelungen über die Kontrolle der IKT-Nutzung in den dienstrechtlichen Bestimmungen entbehrlich ist.

Stellungnahmen zum vorangegangenen Ministerialentwurf

(Vorangegangener Ministerialentwurf: ME Beamten-Dienstrechtsgesetz 1979, Vertragsbedienstetengesetz 1948 u. a., Änderung, 17/ME [XXIV. GP])

In der Arbeit zitierte Stellungnahmen:

- *Amt der Niederösterreichischen Landesregierung*, Stellungnahme 1/SN-17/ME (XXIV. GP)
- *Amt der Salzburger Landesregierung*, Stellungnahme 6/SN-17/ME (XXIV. GP)
- *Wirtschaftskammer Österreich*, Stellungnahme 7/SN-17/ME (XXIV. GP)
- *Gewerkschaft Öffentlicher Dienst, Zentralsekretariat*, Stellungnahme 9/SN-17/ME (XXIV. GP)
- *Bundesministerium für Landesverteidigung und Sport*, Stellungnahme 11/SN-17/ME (XXIV. GP)
- *Bundesministerium für Finanzen*, Stellungnahme 12/SN-17/ME (XXIV. GP)
- *Bundesministerium für Wirtschaft, Familie und Jugend*, Stellungnahme 13/SN-17/ME (XXIV. GP)
- *Bundesministerium für Justiz*, Stellungnahme 14/SN-17/ME (XXIV. GP)
- *Österreichischer Gewerkschaftsbund*, Stellungnahme 15/SN-17/ME (XXIV. GP)

Alle Stellungnahmen abrufbar unter:
http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00017/pmh.shtml (zuletzt abgerufen am 23.06.2009)

AMT DER NIEDERÖSTERREICHISCHEN LANDESREGIERUNG
Gruppe Landesamtsdirektion
Abteilung Landesamtsdirektion/Verfassungsdienst
Postanschrift 3109 St. Pölten, Landhausplatz 1

Amt der Niederösterreichischen Landesregierung, 3109

An das
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Beilagen

LAD1-VD-12136/049-2009
Kennzeichen (bei Antwort bitte angeben)

Bürgerservice-Telefon 02742-9005-9005
In Verwaltungsfragen für Sie da. Natürlich auch außerhalb der Amtsstunden: Mo-Fr 07:00-19:00, Sa 07:00-14:00 Uhr

-	Bezug	BearbeiterIn	(0 27 42) 9005 Durchwahl	Datum
	BKA-920.196/0002-III/1/2009	Dr. Josef Gundacker	14171	27. Jänner 2009

Betrifft
Bundesgesetz, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungsgesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden

Die NÖ Landesregierung hat in ihrer Sitzung vom 27. Jänner 2009 beschlossen, zum Entwurf eines Bundesgesetzes, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungsgesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden, wie folgt Stellung zu nehmen:

1. Das im Vorblatt dargestellte Ziel der Schaffung eines „dem Verhältnismäßigkeitsprinzip entsprechenden Ausgleichs der diametral entgegenstehenden und teilweise grundrechtlich geschützten Interessen auf Bediensteten- und Dienstgeberseite betreffend die Kontrollmöglichkeiten“ scheint insofern nicht gelungen, als diese Möglichkeiten der Kontrolle durch den Aufbau von bürokratischen Hürden für den Dienstgeber massiv eingeschränkt werden sollen.

Weiters ist der in den Erläuterungen geäußerte Wunsch, dass der vorliegende Entwurf Beispielcharakter für den öffentlichen und privaten Bereich entwickelt, nicht nachvollziehbar. Dies gilt umso mehr, als eine Einbindung der Länder und Gemeinden nicht erfolgt ist.

Bei allem notwendigen Schutz der Privatsphäre der öffentlich Bediensteten ist zu bedenken, dass der Dienstgeber die IKT-Betriebsmittel den Bediensteten vorrangig zur Erbringung einer öffentlichen Dienstleistung zur Verfügung stellt, die auch entsprechend zu kontrollieren ist.

Insofern bestehen eben im Vergleich zur Wirtschaft für die Mitarbeiter des öffentlichen Dienstes wegen des berechtigten öffentlichen Interesses und des gegebenen historischen Begriffsverständnisses zum „Dienstrecht“ weitergehende Verpflichtungen, da es hier um das Erscheinungsbild des öffentlichen Dienstes in der Allgemeinheit geht.

Dass die Sensibilität der Öffentlichkeit bei Missbrauch durch öffentlich Bedienstete eine höhere ist als bei vergleichbaren Fällen in der Wirtschaft, manifestiert sich regelmäßig in einer entsprechend kritischen medialen Berichterstattung über derartige Vorfälle.

Da sich die öffentlichen Bediensteten dieser erhöhten Dienstpflichten bewusst sind, ist auch eine gegenüber Dienstnehmern in anderen (privaten) Bereichen gerechtfertigte höhere Kontrolldichte grundsätzlich zulässig.

2. **Zu § 79c BDG:**

Der in Abs. 2 verwendete unbestimmte Gesetzesbegriff „gröbliche Dienstpflichtverletzung“ müsste präzisiert werden.

Es stellt sich aber die Frage, ob mit dieser Einschränkung der Zulässigkeit einer Kontrolle auf „überschießendes“ Verhalten eine Kontrolltätigkeit in der Praxis nicht überhaupt in der überwiegenden Anzahl der Fälle ausgeschlossen wird. Surft ein Mitarbeiter beispielsweise an einem einzigen Tag eine gewisse Zeit auf nicht dienstlichen Seiten, so wird das keine „gröbliche“ Dienstpflichtverletzung darstellen, tut

er dies jedoch fortgesetzt, dann wohl. Eine Feststellung dieses Verhaltens durch die Dienststellenleitung (etwa durch Output-Vergleiche) wird aber in der Praxis in der überwiegenden Anzahl solcher Situationen nicht möglich sein, da ein Verdacht auf eine nicht-gröbliche Dienstpflichtverletzung für die Setzung von Datenkontrollen nicht ausreicht.

Die weiteren Beschränkungen in zeitlicher und quantitativer Hinsicht sind im Hinblick auf den Zweck der bereitgestellten Medien und Systeme praxisfremd, in inhaltlicher Hinsicht wird das auch bei einer erheblichen Zahl von Betroffenen wegen deren Tätigkeitsbereich nicht möglich sein.

Letztlich wird es wohl erforderlich sein, die Möglichkeit der Auftragserteilung nicht nur der jeweiligen Dienststellenleitung, sondern auch übergeordneten Einrichtungen oder sachlich zuständigen Kontrollstellen einzuräumen.

Bei dem im Abs. 3 festgelegten Verbot der Inhaltskontrolle stellt sich die Frage, wie nach der Begriffsdefinition des § 79g Z. 5 des Entwurfes (Austausch über einen „öffentlichen Kommunikationsdienst“) der Nachrichtenaustausch über die internen Kommunikationsstrukturen zu sehen ist.

Eine Klarstellung wäre erforderlich.

3. **Zu § 79d BDG:**

Auch diese Regelung geht im Hinblick auf die rasche Verbreitung von Schädlingen und die möglichen immensen Schäden (vgl. zuletzt die Probleme in der Kärntner Landesverwaltung) an der Praxis völlig vorbei. Schon bei der Verlangsamung der Infrastruktur oder einer möglichen Gefahr von Datenverlusten ist unverzügliches Handeln geboten. Für die Bestimmungen der Abs. 1-4 wird es daher keine Anwendungsfälle geben.

Die Erfahrung hat gezeigt, dass ein Tätigwerden der IT-Stelle im Sinne der formulierten Regelung des Abs. 5 in der überwiegenden Anzahl der Fälle zur Feststellung von (meist schweren) Dienstpflichtverletzungen geführt hat. Es ist daher nicht nachvollziehbar, wieso diese Daten „nicht für andere Zwecke“ verwendet werden

dürfen und welche Reichweite diesem Verbot zukommen soll. Ebenso ist nicht verständlich, wieso nach der geplanten Regelung zwar der Bedienstete, nicht aber auch seine Dienststellenleitung informiert werden muss.

4. **Zu § 79e BDG:**

   Neben den bereits zu § 79c dargestellten grundsätzlichen Überlegungen ist anzunehmen, dass das hier geregelte, verdichtete förmliche Verfahren aufgrund seines bürokratischen Aufwandes in sehr vielen Fällen auch bei einem zureichenden Verdacht dazu führen wird, dass die Dienststellenleitung, wegen der damit verbundenen Prozedur von einem derartigen Verfahren Abstand nimmt.

   Die Erfahrung aus den vergangenen Jahren zeigt nämlich, dass zumeist ein Verdacht gegen einen bestimmten Bediensteten im Zusammenhang mit der IKT-Nutzung zunächst nicht vorgelegen ist (sondern eben ein genereller Verdacht aufgrund sachlicher Indizien, wobei nicht einmal bestimmte Dienststellen ausgeschlossen werden konnten), sodass es für die vergleichsweise unbürokratische, abweichende Regelung des Abs. 7 nur selten einen Anwendungsfall geben wird.

5. Aus systematischen Gründen sollten die Begriffsbestimmungen des § 79g zu Beginn des Unterabschnittes eingefügt werden. Weiters sollte die in § 79g Z. 2 vorgesehene Ausnahme der Fernsprechanlagen überdacht werden, da diese Anlagen zunehmend mit der sonstigen IKT – Infrastruktur verbunden sind.

Eine Ausfertigung dieser Stellungnahme wird unter einem dem Präsidium des Nationalrates elektronisch übermittelt.

Ergeht an:

1. **An das Präsidium des Nationalrates,**

---

2. An das Präsidium des Bundesrates
3. An alle vom Lande Niederösterreich entsendeten Mitglieder des Bundesrates
4. An alle Ämter der Landesregierungen (zu Handen des Herrn Landesamtsdirektors)
5. An die Verbindungsstelle der Bundesländer, Schenkenstraße 4, 1014 Wien
6. An das Bundesministerium für Gesundheit, Familie und Jugend, Radetzkystrasse 2, 1030 Wien
7. Landtagsdirektion

NÖ Landesregierung

Dr. P R Ö L L

Landeshauptmann

Land Salzburg

Für unser Land!

LEGISLATIV- UND VERFASSUNGSDIENST

Bundeskanzleramt
Ballhausplatz 2
1014 Wien

E-Mail: stanislav.horvat@bka.gv.at

SALZBURG feel the inspiration!

CHIEMSEEHOF
✉ POSTFACH 527, 5010 SALZBURG
landeslegistik@salzburg.gv.at
FAX (0662) 8042 - 2164
TEL (0662) 8042 - 2290
Herr Mag. Feichtenschlager

ZAHL
2001-BG-65/55-2009

DATUM
5.2.2009

BETREFF
Entwurf eines Bundesgesetzes, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungsgesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden; Stellungnahme

Bezug: Zl BKA-920.196/0002-III/1/2009

Sehr geehrte Damen und Herren!

Zu dem im Gegenstand bezeichneten Gesetzentwurf gibt das Amt der Salzburger Landesregierung folgende Stellungnahme bekannt:

Zu den §§ 79c und 79e BDG 1979:

1. Im Fall eines nicht gegen eine bestimmte Person gerichteten Verdachts einer gröblichen Dienstpflichtverletzung in einer Dienststelle dürfen personenbezogene Daten nur über Auftrag des Dienststellenleiters verwendet werden (§ 79c Abs 2 Z 2 BDG 1979). Der Leiter der Dienststelle kann die IT-Stelle beauftragen, auf diesen Verdachtsfall Bezug habende Daten der IKT-Nutzung zu ermitteln. Die IT-Stelle hat dem Leiter der Dienststelle über die IKT-Nutzungen im Umfang des Ermittlungsauftrags in anonymisierter Weise zu berichten (§ 79e Abs 1 und 2 BDG 1979). Die Erläuterungen zum geplanten § 79e BDG 1979 halten dazu fest, dass „der Verdacht von der Dienststelle ausgehen (muss) und die IT-Stelle das Verfahren nicht initiieren (kann).“ Unklar ist jedoch, auf welche Art der Leiter der Dienststelle einen Verdacht auf eine Dienstpflichtverletzung gewonnen haben muss,

um einen Auftrag an die IT-Stelle zu rechtfertigen und um eine Datenverwendung im Sinn des § 79c Abs 2 Z 2 BDG zuzulassen.

Soweit die geplanten §§ 79c Abs 2 Z 2 und 79e BDG einschränkend dahingehend zu verstehen sind, dass Datenverwendungen im Sinn des § 79c Abs 2 Z 2 BDG nicht zulässig sind, wenn diese ihren Ausgangspunkt in (an den Leiter der Dienststelle übermittelte) Beobachtungen oder Feststellungen der IT-Stelle, etwa im Rahmen der Leistungsabrechnung haben, kann dem nicht zugestimmt werden: Eine Datenverwendung im Sinn des § 79c Abs 2 Z 2 BDG 1979 muss auch dann möglich sein, wenn die IT-Stelle von sich aus den Leiter der Dienststelle vom Vorliegen eines Verdacht einer gröblichen Dienstpflichtverletzung informiert, etwa dann, wenn diese feststellt, dass in großem Maß Internet-Domains angesurft werden, die in keinem Bezug zur dienstlichen Tätigkeit stehen. Darüber hinaus sollte eine Datenverwendung im Sinn des § 79c Abs 2 Z 2 BDG 1979 auch auf der Grundlage der von der IT-Stelle erstellten Leistungsabrechnungen und auf der Grundlage von anonymisierten Statistiken zur Nutzung der IKT-Infrastruktur im Rahmen der Dienstaufsicht zulässig sein.

Nicht nachvollziehbar ist auch die im geplanten § 79d Abs 5 BDG 1979 enthaltene Einschränkung, dass die im Rahmen einer Beseitigung einer konkreten unmittelbaren Gefährdung für die IKT-Infrastruktur von der IT-Stelle gewonnenen personenbezogenen Daten nur insoweit verwendet werden dürfen, als dies zur Behebung der Gefährdung unbedingt notwendig ist (§ 79d Abs 5 BDG 1979). Auch diese Daten sollten zur Feststellung von Dienstpflichtverletzungen herangezogen werden können; § 79 Abs 5 BDG 1979 ist daher dahingehend zu ergänzen, dass die IT-Stelle auch den Leiter der Dienststelle über die verwendeten Daten zu informieren hat.

2. Nicht geregelt ist die Frage, bis zu welchem Zeitpunkt Daten aus der Vergangenheit zulässigerweise verwendet werden dürfen. Ist dafür ausschließlich der Ermittlungsauftrag des Leiters der Dienststelle an die IT-Stelle maßgeblich?

Zu § 79d BDG 1979:

Im Hinblick auf die rasche Verbreitung von Schädlingen und die dadurch bedingten immensen Schäden erscheint das im Abs 1 bis 4 geregelte Verfahren praxisfremd.

Zu § 79g BDG 1979:

Die Begriffsbestimmungen sollten an den Beginn des geplanten neuen Abschnitts und nicht an dessen Ende gestellt und um eine Bestimmung des in den §§ 79c Abs 3 und 79d Abs 1 BDG 1979 verwendeten Begriffs der „Inhalte“ (verstanden als Datenvolumina oder Häufigkeiten genutzter Internet- oder Mail-Domains) ergänzt werden.

Diese Stellungnahme wird der Verbindungsstelle der Bundesländer, den anderen Ämtern der Landesregierungen, dem Präsidium des Nationalrates und dem Präsidium des Bundesrates ue zur Verfügung gestellt.

Mit freundlichen Grüßen
Für die Landesregierung:
Dr. Heinrich Christian Marckhgott
Landesamtsdirektor

Ergeht nachrichtlich an:

1. – 8. E-Mail an: Alle Ämter der Landesregierungen
9. E-Mail an: Verbindungsstelle der Bundesländer vst@vst.gv.at
10. E-Mail an: Präsidium des Nationalrates begutachtungsverfahren@parlinkom.gv.at
11. E-Mail an: Präsidium des Bundesrates peter.michels@parlament.gv.at
12. E-Mail an: Bundeskanzleramt iii1@bka.gv.at
13. E-Mail an: Institut für Föderalismus institut@foederalismus.at
14. E-Mail an: Landesinformatik zu do Zl 2002-105/682-2009

zur gefl Kenntnis.

WIRTSCHAFTSKAMMER ÖSTERREICH

Bundeskanzleramt
Abteilung III/1
Ballhausplatz 2
1014 Wien

per E-Mail:
iii1@bka.gv.at
stanislav.horvat@bka.gv.at

Wirtschaftskammer Österreich
Wiedner Hauptstraße 63 | 1045 Wien
T +43 (0)5 90 900-DW | F +43 (0)5 90 900-DW
W http://wko.at/sp

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sacharbeiter	Durchwahl	Datum
920.196/0002-III/1/2009 9. Jänner 2009	Sp 675/09/Dr.RT/KR Dr. Rainer Thomas	4394	4.2.2009

Bundesgesetz, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungsgesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden; Begutachtungsverfahren - Stellungnahme der WKÖ.

Sehr geehrte Damen und Herren!

Obwohl der Entwurf unmittelbar und ausschließlich den öffentlichen Dienst erfassen soll, sind in den Erläuterungen zum Gesetzestext angesprochenen Wechselwirkungen zwischen öffentlichen und privaten Bereich, sowie auch Auswirkungen im Bereich des privaten Arbeitsrechts zu erwarten (etwa über die Judikatur des OGH). Im Vorblatt zu den Erläuterungen ist unter dem Punkt „Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich" zu lesen: *Nicht nur denkbar, sondern auch erwünscht ist, dass der vorliegende Entwurf Beispielcharakter sowohl im öffentlichen als auch im privaten Bereich entwickelt und somit zumindest indirekt die Unternehmenskultur in Österreich positiv beeinflusst.*

Die Wirtschaftskammer Österreich hält fest, dass die gesetzliche Zulassung der Privatnutzung der IKT-Struktur als solche durch Bedienstete in der Dienstzeit unter Präjudizaspekten, aber auch unter dem Aspekt der Sparsamkeit und Steuerzahlerkosten insbesondere für widmungswidrige Verwendung von Dienstzeiten, höchst problematisch ist und keinesfalls so auf die Wirtschaft ausdehnbar ist. Auch aus Gründen der Gleichbehandlung kann dem Entwurf nicht gefolgt werden: würden sonst Arbeitnehmer des Bundes im Verhältnis zu Arbeitnehmer im privaten Bereich ohne ersichtlichen Grund privilegiert werden. Im Bereich des privaten Arbeitsrechts muss auch die Nichtzulassung bzw. ein Verbot der IKT-Nutzung den Dienstgebern vorbehalten bleiben. Was der Bund als Dienstgeber für angemessen oder vertretbar hält, darf nicht zum zwingenden Maßstab für private Dienstgeber werden.
Aus diesen Gründen lehnt die Wirtschaftskammer Österreich den Gesetzesentwurf zum Beamten-Dienstrecht ab.

1. Rechtslage im privaten Arbeitsrecht

Zum privaten Arbeitsrecht hat die Judikatur zur Frage privater Tätigkeiten am Arbeitsplatz bereits geklärt, dass es zulässig ist, etwa private Telefonate zu verbieten (OGH 4 Ob 65/82,

Arb 10.118 - ausgenommen kurze unbedingt erforderliche Mitteilungen) oder auch nach Aufzeichnungen zu verrechnen (OGH 9 Ob A 192/98 w). Die Einrichtung einer Telefongesprächsregistrierung zur Kostenkontrolle und nicht zum Abhören von Telefongesprächen verstößt auch nicht gegen die Menschenwürde (zB VwGH 86/01/0069).

Die private Nutzung des PC sowie des Internets ist ähnlich wie die private Nutzung des firmeneigenen Telefons zu betrachten. Es ist daher zulässig, dass der Arbeitgeber die private Nutzung des Internets untersagt. Kurze dringende private e-mails sind daher ebenso wie kurze private Telefonate trotz des Verbots der privaten Nutzung als zulässig anzusehen. Ebenso die vereinzelte Weiterleitung von „Spaß-e-mails", die die Arbeitszeit nur in geringem Ausmaß beansprucht, durch eine seit 20 Jahren unbeanstandet beschäftigte Arbeitnehmerin (OGH 9 Ob A 75/04 a).

Bei einem eindeutigen Verbot durch den Arbeitgeber, welches dieser jederzeit aussprechen kann, sind somit nur äußerst geringe Spielräume für die private Nutzung gegeben und kann der Arbeitgeber bei vorhergehenden Verwarnungen und einem neuerlichen Anlassfall mit entsprechender Mindestintensität eine Entlassung aussprechen.

Zur Kontrolle sieht § 96 Abs 1 Z 3 ArbVG (bzw § 10 Abs 1 AVRAG) vor, dass die Zustimmung des Betriebsrates erforderlich ist, wenn Kontrollmaßnahmen und technische Systeme zur Kontrolle der Arbeitnehmer eingeführt werden sollen, sofern diese Maßnahmen die Menschenwürde berühren. In Betrieben ohne Betriebsrat ist die Zustimmung der Arbeitnehmer erforderlich (§ 10 Abs 2 AVRAG). Wird die Zustimmung nicht erteilt, so dürfen die geplanten Maßnahmen nicht umgesetzt werden.

2. Zur Rechtslage, die sich aus dem Entwurf zur Gesetzesänderung ergeben würde

Aufgrund des von der Judikatur vorgegebenen rechtlichen Rahmens im Bereich des privaten Arbeitsrechts ist nun zu hinterfragen, ob der vorliegende Entwurf, der (aufgrund des oben erwähnten Punktes im Vorblatt) Beispielcharakter entwickeln soll, im Bereich dieses Rahmens liegt oder diesen einengt bzw. erweitert.

Nach dem Entwurf zum § 79c Abs. 1 des Beamten-Dienstrechtsgegesetzes ist die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren, unzulässig. Wie bereits ausgeführt, sind solche Maßnahmen im privaten Arbeitsrecht sehr wohl mit Zustimmung des Betriebsrates bzw. in Betrieben ohne Betriebsrat mit Zustimmung der Arbeitnehmer zulässig. Es ist nicht einzusehen, warum dies im Bereich des Beamten-Dienstrechts nicht mit Zustimmung der Personalvertretung, die ihre Zustimmung von entsprechenden Einschränkungen im Interesse der Belegschaft abhängig machen könnte, möglich sein soll. Auch für den Bund kann hier nur jene Lösung akzeptabel sein, die für den privaten Bereich durch § 96 Abs. 1 Z. 3 ArbVG bzw. § 10 AVRAG gilt, nämlich entsprechende Mitbestimmung der Belegschaftsvertretung bzw. der Betroffenen.

Durch die vorgeschlagene Norm besteht die Gefahr des Ausdehnens der absoluten Unzulässigkeit der Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, auf die Privatwirtschaft, zumal die bisherige Rechtsprechung das Berühren der Menschenwürde sehr schnell annimmt und so den Betrieben auch zumutbare Kontrollmöglichkeiten genommen würden, wenn sich dieser Standard, den § 79c Beamten-Dienstrechtsgesetz normieren möchte, durchsetzt. Zu befürchten ist auch, dass dieser Bundesstandard die Rechtsprechung zum Nachteil der Betriebe beeinflussen würde.

Abzulehnen ist weiters § 79c Abs. 3 2. Satz Beamten-Dienstrechtsgesetz. Warum auch in begründeten Verdachtsfällen ilnhalte übertragener Nachrichten nicht kontrolliert werden dür-

fen, ist unvertretbar und nicht nachvollziehbar. Insofern würden sich Nutzungs- bzw. Missbrauchsmöglichkeiten eröffnen, die eigentlich in ihren Auswirkungen horrend sind.

Die §§ 79d und 79e des Entwurf zum Beamten-Dienstrechtsgesetz sind primär auf vorherige Information der von der Kontrolle betroffenen Beamten und nicht auf effiziente Ermittlungen abgestellt und können auch nicht spontan oder stichprobenartig durchgeführt werden, weil sie einen begründeten Verdacht voraussetzen.

Im privaten Arbeitsrecht wäre hingegen eine Kontrolle, die sich bloß auf das Ziel der Zugriffe des Arbeitnehmers im Internet beschränkt und keine personenbezogenen Daten speichert, auch ohne die Zustimmung des Betriebsrats (bzw. der Arbeitnehmer nach § 10 AVRAG) zulässig. Ebenso wäre die Information des betroffenen Arbeitnehmers nicht erforderlich.

Freundliche Grüße

Dr. Christoph Leitl
Präsident

Mag. Anna Maria Hochhauser
Generalsekretärin

Österreichischer Gewerkschaftsbund
GEWERKSCHAFT ÖFFENTLICHER DIENST
1010 Wien, Teinfaltstraße 7, Telefon 01/53 454-0

An das
Bundeskanzleramt / Sektion III
z.Hd. Frau AL MR Dr. Anita Pleyer

Hohenstaufengasse 3
1010 Wien

Unser Zeichen	Ihr Zeichen	Datum
Zl. 1.598/2009 – Mag. Ab/Fö	BKA-920.196/0001-III/1/2009 BKA-920.196/0002-III/1/2009	Wien, 5.2.2009

Betrifft: **Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bundesbedienstete (IKT-Nutzungsverordnung) sowie BG mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetendienstgesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungsgesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden; Stellungnahme der GÖD**

Sehr geehrte Frau Ministerialrätin!

Binnen offener Frist wird die Stellungnahme der Gewerkschaft öffentlicher Dienst zum Begutachtungsentwurf betreffend „Kontrolle der IT-Nutzung“ sowie der „IKT-Nutzungsverordnung“ eingebracht.

Grundsätzlich begrüßt die Gewerkschaft Öffentlicher Dienst (GÖD) die Schaffung von nachvollziehbaren Regelungen für Kontrollmaßnahmen bezüglich Nutzung der IKT – Infrastruktur sowie das Verankern der Möglichkeit der privaten Nutzung der IKT – Infrastruktur des Bundes durch die Bundesbediensteten in der IKT – Nutzungsverordnung. Das formulierte Ziel, die Dienstnehmer „vor übermäßiger Kontrolle am Arbeitsplatz durch den Dienstgeber zu schützen“ wird ebenfalls begrüßt.

Zum vorliegenden Begutachtungsentwurf werden folgende Forderungen erhoben:

Beamtendienstrechtsgesetz:

§ 79c Abs. 2:
Die Ziffer 1 sollte dahingehend präzisiert und klargestellt werden, dass solche Maßnahmen nur in begründeten Einzelfällen gesetzt werden dürfen. Der derzeitige Text lässt einen erheblichen Interpretationsspielraum zu und könnte in die Richtung

missverstanden werden, dass mit dieser Bestimmung jegliche dauerhafte Kontrollmaßnahme gerechtfertigt wird.
Die Protokolle über die Kontrollmaßnahme sind dem jeweiligen Personalvertretungsorgan zur Verfügung zu stellen.

§ 79c Abs. 4:
Die Begrenzung der Kontrollmaßnahmen gem. Abs. 4 bei Organisationseinheiten mit weniger als 5 Bediensteten dient dazu, die Anonymität der Bediensteten nicht zu gefährden.
Diese Anonymität kann nach Ansicht der GÖD aber auch nicht bei 5 Bediensteten gewahrt werden, weshalb eine Erhöhung der Anzahl von Bediensteten auf mindestens 10 Bedienstete gefordert wird.

§ 79d Abs. 2, 4 und 5:
Die GÖD fordert, dass der Dienststellenleiter verpflichtet wird, auch das jeweils zuständige Personalvertretungsorgan unmittelbar über die Kontrollmaßnahme zu informieren.

§ 79e:
Die GÖD fordert, dass sowohl in Abs. 1 und 2 als auch in Abs. 7 festgelegt wird, dass eine Kopie des schriftlichen Ermittlungsauftrages sowie des Berichtes unverzüglich dem zuständigen Organ der Personalvertretung sowie im Abs. 7 dem betroffenen Beamten zu übermitteln ist.

Bundes-Personalvertretungsgesetz:

Die GÖD begrüßt die Normierung der Einvernehmenstatbestände in § 9 Abs. 2 n) und o).

IKT-Nutzungsverordnung:

Die Schaffung von klaren Regelungen über die private Nutzung der IKT-Infrastruktur wird von der GÖD begrüßt.
Nach Auffassung der GÖD muss jedoch klargestellt werden, dass Einschränkungen der privaten Nutzung an bestimmte, klar zu definierende Gründe gebunden sein müssen (Ausschluss von Willkür).

Die Gewerkschaft Öffentlicher Dienst ersucht um die Einarbeitung o.a. Forderungen sowie um Bekanntgabe eines Termins für die Schlussverhandlung.

Mit dem Ausdruck vorzüglicher Hochachtung

Vorsitzender

Ergeht an: begutachtungsverfahren@parlament.gv.at sowie an
iii1@bka.gv.at und an
stanislav.horvat@bka.gv.at

Bundesministerium
für Landesverteidigung und Sport
Abteilung Fremdlegislative und
Internationales Recht

Sachbearbeiterin:
Mag. Barbara FREISTÄTTER, MBA
Tel: 050201 10 21640
Mobil: 0664/622 1103
E-Mail: fleg.ref2@bmlv.gv.at

GZ S91043/3-FLeg/2009

Entwurf eines Bundesgesetzes, mit dem das BDG 1979 u.a geändert wird

Stellungnahme

An das
Präsidium des Nationalrates
Parlament
1017 Wien

Das Bundesministerium für Landesverteidigung und Sport beehrt sich nachstehend die Ressortstellungnahme zu dem vom Bundeskanzleramt versendeten **Entwurf eines Bundesgesetzes, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungsgesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden** (GZ BKA-920.196/0002-III/1/2009), zu übermitteln.

Die gegenständliche Stellungnahme wird ausschließlich auf elektronischem Weg an die Adresse begutachtungsverfahren@parlament.gv.at übermittelt.

06.02.2009
Für den Bundesminister:
i.V. MOSER

Bundesministerium
für Landesverteidigung und Sport
Abteilung Fremdlegislative und
Internationales Recht

DRINGEND

Sachbearbeiterin:
Mag. Barbara FREISTÄTTER, MBA
Tel: 050201 10 21640
Mobil: 0664/622 1103
E-Mail: fleg.ref2@bmlv.gv.at

GZ S91043/3-FLeg/2009

Entwurf eines Bundesgesetzes, mit dem das BDG 1979 u.a geändert wird;

Stellungnahme

An das
BKA/Sektion III
iii@bka.gv.at
z.Hd. Abt. 1
Hohenstauffengasse 3
1010 Wien

Zu dem übermittelten **Entwurf eines Bundesgesetzes, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungsgesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden** (do. GZ BKA-920.196/0002-III/1/2009), nimmt das Bundesministerium für Landesverteidigung und Sport wie folgt Stellung:

I. <u>Zum BDG 1979</u>:

a) Aus ho. Sicht erscheint die im **§ 79c Abs. 2 Z 2** gewählte Formulierung „*Verdacht einer gröblichen Dienstpflichtverletzung*“ nicht zielführend und sollte durch die Formulierung „*Verdacht einer Dienstpflichtverletzung*“ ersetzt werden.

Erstere Diktion würde dazu führen, dass ein weiter Bereich von Dienstpflichtverletzungen unterhalb der Qualifikation der Gröblichkeit nicht kontrolliert und nicht disziplinär geahndet werden dürfte. Die Differenzierung zu Dienstpflichtverletzungen, die nicht im Bereich der privaten Nutzung der

Informations- und Kommunikationstechnik-Infrastruktur des Bundes verwirklicht werden, erscheint sachlich nicht gerechtfertigt. ZB. könnten dadurch mündliche Beschimpfungen zwischen Bediensteten disziplinär geahndet werden, gleichartige Beschimpfungen per E-mail jedoch nicht. Darüber hinaus erscheint die Formulierung „*gröblich*“ für die Anwendungspraxis der Disziplinarbehörden zu wenig determiniert.

b) Nach dem vorliegenden Entwurf ist die Verwendung personenbezogener Daten zu Kontrollzwecken ausnahmslos an die normierten – oft langwierigen – Kontrollverfahren gebunden. Insbesondere im ho. Ressorts würde das bedeuten, dass auch in Zusammenhang mit sensibelster dienstlicher IKT (zB. zur Bearbeitung streng geheimer EU-Dokumente, etc.) eine ad hoc-Kontrollmöglichkeit auch dann nicht gegeben ist, wenn die Gefahr der Vereitelung der Einsatzbereitschaft des Bundesheeres oder der Einschränkung der Interessen der umfassenden Landesverteidigung vorliegt. Aus diesem Grund erscheint es unumgänglich, dass in ausdrücklich definierten Ausnahmefällen eine Verwendung dieser Daten zu Kontrollzwecken möglich sein sollte. Aus ho. Sicht könnte dabei eine Anlehnung an die Definition dieser Ausnahmefälle, zB. im Rahmen der Meldepflicht gemäß § 17 Abs. 3 des Datenschutzgesetz 2000, BGBl. I Nr. 165/1999, – DSG 2000, oder im Rahmen der Auskunftserteilung gemäß § 26 Abs. 1 DSG 2000, erfolgen.

Das ho. Ressort ersucht demgemäß um Aufnahme des folgenden **(neuen) Abs. 2 im § 79c** – unter gleichzeitiger Neunummerierung der Folgeabsätze:

„(2) Personenbezogene Daten der IKT-Nutzung dürfen zu Kontrollzwecken für Zwecke der Sicherung der Einsatzbereitschaft des Bundesheeres oder der Sicherstellung der Interessen der umfassenden Landesverteidigung verwendet werden.“

c) Zu **§ 79g** wird angemerkt:

i. Im ho. Ressort gibt es – neben der für die Errichtung und den Betrieb der IKT-Nutzung zuständigen Organisationseinheit – auch eine für die militärische Sicherheit der IKT-Einrichtungen zuständige Organisationseinheit. Diese wäre nach der vorliegenden Definition kein Teil der „IT-Stelle“. Aus diesem Grund wird ersucht, Z 1 wie folgt zu formulieren:

„1. „IT-Stelle“: die für die technische Ermöglichung oder die Sicherheit der IKT-Nutzung zuständige Organisationseinheit,“

ii. Zur Herausnahme von Fernsprechanlagen aus der Definition der „IKT-Infrastruktur“ wird angemerkt, dass dies aus ho. Sicht ein allfälliges Problem in Zusammenhang mit der Internettelefonie (zB. „VoIP – Voice over Internet Protocol“) darstellen kann. Aus ho. Sicht ist in diesen Fällen eine Trennung zwischen Geräten zur Datenübertragung und jenen zur Sprachtelefonie nicht möglich, weshalb aus ho. Sicht – zB. in den Erläuterungen – der Begriff „Fernsprechanlagen“ genauer zu definieren wäre.

II. Zum PVG:

Die Verpflichtung, bei der Durchführung von Kontrollmaßnahmen unter Verwendung von personenbezogenen Daten der IKT-Nutzung bei einem begründeten Verdacht einer gröblichen Dienstpflichtverletzung das Einvernehmen mit dem Dienststellenausschuss herstellen zu müssen, wird auch aus der Sicht des BMLVS ausdrücklich befürwortet.

Es wird jedoch darauf hingewiesen, dass eine verpflichtende zweiwöchige Vorausinformation des Dienststellenausschusses (§ 10 Abs. 2 PVG) und ein „Abwarten“ auf dessen Zustimmung bei **Gefahr in Verzug** (zB. Virusgefahr, etc.) einen nicht wieder gut zu machenden Schaden im Bereich der technischen und betrieblichen Sicherheit verursachen kann. Aus diesem Grund wäre aus ho. Sicht – **ausschließlich bei Gefahr in Verzug** – abweichend von der vorgeschlagenen Regelung eine unverzügliche Meldung an den Dienststellenausschuss sowie dessen Recht, nach Prüfung des Sachverhalts die sofortige Einstellung der Kontrollmaßnahme zu verlangen, zu normieren. Ähnliche Konstruktionen finden sich in der geltenden Rechtsordnung etwa bereits in

- **§ 2 Abs. 5 KSE-BVG**: Zu Entsendungen zu Maßnahmen der humanitären Hilfe und der Katastrophenhilfe ist dem Grunde nach die Bundesregierung (BReg) im Einvernehmen mit dem Hauptausschuss des Nationalrates (HA) berufen. Bei besonderer Dringlichkeit kann der Bundeskanzler zusammen mit dem Bundesminister für europäische und internationale Angelegenheiten und allfälligen anderen zuständigen Bundesministern die unverzügliche Entsendung zur humanitären Hilfe und Katastrophenhilfe veranlassen. Darüber muss unverzüglich der BReg und dem HA berichtet werden, wobei der HA innerhalb von 2 Wochen gegen die Entsendung Einspruch erheben kann – in diesem Fall ist die Entsendung sofort zu beenden.
- **§ 22 Abs. 8 MBG**: Grundsätzlich ist eine Datenermittlung durch militärische Organe nur mit ausdrücklicher Zustimmung des Rechtsschutzbeauftragten zulässig. Besteht jedoch die Gefahr eines nicht wieder gutzumachenden, schweren Schaden

für die nationale Sicherheit, insbesondere für die Einsatzbereitschaft des Bundesheeres oder für die Sicherheit von Menschen, kann eine entsprechende Datenermittlung sofort unter gleichzeitiger Information des Rechtsschutzbeauftragten erfolgen. Diese Ermittlung ist bei Einspruch des Rechtsschutzbeauftragten sofort zu beenden.

Aus ho. Sicht könnte somit dem § 9 Abs. 2 folgender Satz angehängt werden:

„Eine Kontrollmaßnahme nach lit. n darf jedoch sofort nach Kenntnisnahme durch den Dienststellenausschuss begonnen werden, wenn bei weiterem Zuwarten ein nicht wieder gutzumachender Schaden für die nationale Sicherheit, insbesondere der Einsatzbereitschaft des Bundesheeres eintreten würde. Eine solche Kontrollmaßnahme ist unverzüglich zu beenden, wenn der Dienststellenausschuss dagegen Einspruch erhoben hat.“

Eine Ausfertigung der vorliegenden Stellungnahme wurde dem Präsidium des Nationalrates auf elektronischem Weg übermittelt.

06.02.2009
Für den Bundesminister:
i.V. MOSER

BMF
BUNDESMINISTERIUM FÜR FINANZEN

BMF - I/4 (I/4)
Hintere Zollamtsstraße 2b
1030 Wien

Sachbearbeiterin:
Mag. Beate Sternig
Telefon +43 (1) 514 33 501167
Fax 01514335901167
e-Mail Beate.Sternig@bmf.gv.at
DVR: 0000078

Bundeskanzleramt
Ballhausplatz 2
1014 Wien

GZ. BMF-110500/0003-I/4/2009

Betreff: GZ BKA-920.196/0002-III/1/2009 sowie GZ BKA-920.196/0001-III/1/2009 vom 9. Jänner 2009; Entwurf eines Bundesgesetzes, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungs-gesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden sowie Entwurf einer Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bundesbedienstete (IKT-Nutzungsverordnung – IKT-NV); Stellungnahme des Bundesministeriums für Finanzen

Das Bundesministerium für Finanzen beehrt sich, zu den mit E-Mail vom 12. Jänner 2009 unter den Geschäftszahlen GZ BKA-920.196/0002-III/1/2009 sowie GZ BKA-920.196/0001-III/1/2009 übermittelten und im Betreff näher bezeichneten Begutachtungsentwürfen innerhalb offener Frist wie folgt Stellung zu nehmen:

I.
Zusammenfassende Feststellungen

Das vorliegende Normsetzungsvorhaben erscheint widersprüchlich, normlogisch inhomogen und mit mehreren, den weiteren Ausführungen dieser Stellungnahme zu entnehmenden Feststellungen rechtlich systemwidrig. Insbesondere ist die im Vorblatt zum Ausdruck gebrachte Intention der Schaffung einer gesetzlichen Grundlage für die Zulässigerklärung der privaten IKT-Nutzung nicht durchgehend vorhanden, da einzelne Bestimmungen weit darüber hinaus gehende Regelungsvorhaben erkennen lassen. Es darf in diesem Kontext auch auf die nicht durchgängig nachvollziehbare, jedenfalls ohne Einbindung der Expertise des Bundesministeriums für Finanzen finalisierte Erstellung der vorliegenden Entwürfe hingewiesen werden.

Der zur Begutachtung vorgelegte Gesetzesentwurf und der Entwurf einer IKT-Nutzungsverordnung ist daher aus rechtlichen Erwägungen seitens des Bundesministeriums für Finanzen einer neuerlichen intensiven fachbezogenen Beratungsphase zu unterziehen.

Abgesehen von den nachstehend dargestellten rechtlichen Bedenken wäre eine Ausnahme entsprechend der offenbar in Art. 3 des Entwurfes für Bereiche des Justizressorts intendierten Regelung auch für Bereiche des Finanzressorts zu überlegen.

Selbstverständlich würde auch bei Fortsetzung der Arbeiten am gegenständlichen, wohl redimensionierten Vorhaben und entsprechend zeitgerechter Einbindung die Expertise des Bundesministeriums für Finanzen aktiv eingebracht werden.

II.
Zum Vorblatt des Gesetzesentwurfs

Die bereits angesprochene Intention des Normsetzungsvorhabens, eine gesetzliche Grundlage für die Zulässigerklärung der privaten IKT-Nutzung (insbesondere Internet und E-Mail) durch die Bediensteten des Bundes zu schaffen, ist aus der Sicht des Bundesministeriums für Finanzen – wie nicht zuletzt auch die Erfahrungen in einem

Verfahren vor der DSK im vergangenen Jahr gezeigt haben – aufgrund der damit verbundenen Rechtssicherheit von Vorteil und somit die einzig nachvollziehbare Zielausrichtung. So sollte der Anwendungsbereich der Vorschriften des BDG auch auf diesen Bereich der Privatnutzung beschränkt werden.

Im Gegensatz zu dieser zentralen Themenstellung lässt der Wortlaut des Entwurfs aber eine Einschränkung auf den Bereich der privaten Nutzung vermissen. § 79c Abs. 2 des Entwurfs enthält vielmehr eine Regelung für die Verwendung von personenbezogenen Daten der IKT-Nutzung zu Kontrollzwecken, durch die nicht nur die Kontrolle der Privatnutzung, sondern jegliche Kontrolltätigkeit seitens des Dienstgebers erfasst wird.

Die Problematik im Zusammenhang mit bestehenden gesetzlichen Verpflichtungen betreffend die Gewährleistung von Datensicherheit scheint völlig ignoriert. Gerade im Bereich der Finanzverwaltung genießen der sorgsame Umgang mit Steuerdaten und das Steuergeheimnis oberste Priorität, ein Umstand auf den sich die Steuerpflichtigen schon bisher verlassen konnten und der auch für die Zukunft gewahrt bleiben muss. Um dieser Anforderung gerecht werden zu können, bedarf es einer adäquaten Kontrolltätigkeit auf der Grundlage des § 14 DSG 2000. Die Protokollierung der Zugriffe von Bediensteten der Finanzverwaltung auf Steuerdaten von Bürgern und auswertende Kontrolle der Protokolle zum Zweck der Feststellung und künftigen Unterbindung unzulässiger Zugriffe, stellt ein nach dem Stand der Technik allgemein anerkanntes Mittel zur Verwirklichung von Datensicherheit in Form von Generalprävention gegen unzulässige Zugriffe dar (vgl. K121.040/0018-DSK/2005). Die DSK hat in diesem Zusammenhang festgehalten, dass aus § 14 DSG 2000 nicht nur die Verpflichtung erkennbar ist, Abfragedaten zu protokollieren, sondern auch die Verpflichtung, Protokolldaten über die Überprüfung der Zulässigkeit der Verwendung des Datensatzes heranzuziehen.

III.

Zu den einzelnen Bestimmungen des Gesetzesentwurfes

1. Ad Art 1 - Änderung des Beamtendienstrechtsgesetzes 1979 (BDG)

a) Ad § 79c BDG:

Der Erfüllung der unter Punkt II. dargestellten Verpflichtung steht nun aber der Wortlaut des § 79c des vorgelegten Entwurfs entgegen. Da Protokolldaten im Sinne des § 14 Abs. 1 Z 7 DSG 2000 gemäß den Definitionen des Entwurfes für § 79g Z 2 und 3 BDG als personenbezogene Daten der IKT-Nutzung zu verstehen sind, dürften diese nach § 79c Abs. 2 Z 2 ausschließlich bei begründetem Verdacht auf gröbliche Dienstpflichtverletzung herangezogen werden.

Bereits das Erfordernis eines begründeten Verdachts ist bei präventiv gesetzten Datensicherheitsmaßnahmen nicht in jedem Fall gegeben. Hinzu kommt, dass angesichts der geforderten „gröblichen Dienstpflichtverletzung“ Kontrolle überhaupt dann zu unterbleiben hätte, wenn nicht von Vornherein feststünde, dass ein in weiterer Folge allenfalls feststellbarer unzulässiger Datenzugriff jedenfalls diese „gröbliche Verletzung“ der Dienstpflichten darstellt. Um ein erforderliches, adäquates Sicherheitsniveau für die Steuerdaten gewährleisten zu können, muss Kontrolle – in den heute bereits bestehenden rechtlichen Grenzen - auch dort zugelassen werden, wo (noch) kein Verdacht besteht. Die DSK führte dazu in der Entscheidung K121.014/0008-DSK/2005 aus, dass es sich bei der generellen, laufenden Kontrolle der Protokolldaten um eine gesetzliche Verpflichtung des Auftraggebers handelt, die gänzlich unabhängig von tatsächlichen Vorfällen besteht.

Die vorliegenden Normansätze würden die Gewährleistung des von der Bundesabgabenordnung und dem Datenschutzgesetz geforderten Schutzes der Steuerdaten verhindern.

b) Ad §79c Abs. 2 Z 2 iVm § 79e BDG:

Der Begriff der „gröblichen Dienstpflichtverletzung“ erscheint unklar und sollte vor dem Hintergrund der § 53 BDG bzw. § 78 StPO zumindest um „strafrechtliche Verdachtsmomente“ ergänzt werden.

Verdachtsmomente in Richtung von Dienstpflichtverletzungen könnten sich beispielsweise auch bei wiederholter Herbeiführung von Gefährdungen für die IKT ergeben. Die diesbezüglichen Sachverhaltsfeststellungen wären aber bei einer Beschränkung der Verwendungsmöglichkeit der Daten im Sinne des § 79d Abs. 5 BDG nicht möglich.

c) Ad §§ 79c ff BDG:

Um begriffliche Unschärfen zu vermeiden, wäre eine exakte Legaldefinition des Begriffes IKT zu ergänzen. Aus dieser sollte sich eine klare Abgrenzung beispielsweise von der Allgemeinheit zugänglichen IKT-Bereichen zu diversen im Dienstbetrieb verwendeten Datenbanken mit eingeschränkten Zugriffsrechten auf hochsensible Daten ergeben.

Eine ganz grob gegliederte Gruppierung von Themen mit völlig unterschiedlichem Regelungsbedarf könnte aus den drei „Gruppen“ Internetanwendungen, email–Anwendungen und Datenbanken bestehen. Jede dieser Gruppen weist sowohl technisch als auch inhaltlich gesehen einen völlig unterschiedlichen Regelungsbedarf auf, wobei es dabei um eine möglichst prägnante Regelung von unterschiedlichsten vielschichtigen Themenstellungen gehen muss.

Das Ergebnis der Neufassung des gegenständlichen Gesetzesvorhabens wird jedenfalls auch die Wahrnehmung von Verpflichtungen im Sinne des DSG zu berücksichtigen haben. Ein besonderes Augenmerk wird auf die Erfordernisse einer rechtskonformen Sachverhaltsdokumentation im Zusammenhang mit allfälliger missbräuchlicher Verwendung von Datenbanken des Dienstgebers zu geben sein.

d) Ad § 79c Abs. 3 BDG:

Der Grund für die Verankerung einer über die bestehende Regelung in § 9 Abs. 2 lit. f PVG hinausgehenden Normierung einer Einvernehmensbestimmung gemäß § 10 PVG ist nicht nachvollziehbar, weshalb diese Bestimmung abgelehnt werden muss.

Darüber hinaus ist diese sowie die mehrfach dem § 79e BDG des vorliegenden Entwurfs zu entnehmende Normierung von personalvertretungsrechtlichen Bestimmungen in der legistischen Konstruktion von leges fugitivae als rechtssystemwidrig und fragwürdig zu bezeichnen.

Wie bereits oben ausgeführt, fehlt es dem gegenständlichen Vorhaben aus Sicht der Finanzverwaltung im Besonderen an der Zulässigkeit generalpräventiv begründeter Kontrollmaßnahmen; § 79c Abs. 3 stellt sogar dies wiederum unklar – es ist nicht erkennbar, was unter Kontrollsystemen für Kontrollmaßnahmen zu verstehen wäre.

e) Ad § 79c Abs. 4 BDG:

Der gegenständliche Regelungsversuch erscheint widersprüchlich; es ist nicht klar, ob bei Vorliegen einer so genannten „gröblichen Dienstpflichtverletzung“ diese im System der „Kontrollverdichtung“ nur zulässig wäre, wenn es sich um Organisationseinheiten von mehr als fünf Bediensteten handelt.

f) Ad § 79e Abs. 3 Z 2 BDG:

Unklar scheint weiters die Verwendung des Begriffes „belehren“. Die Belehrung ist in der Systematik des BDG eine individuelle Maßnahme im Sinne des § 109 Abs. 2 BDG und richtet sich an einen konkreten Bediensteten. Wenn hier von „belehren“ gesprochen wird, sollte dieser Umstand Berücksichtigung finden, um Missverständnisse zu vermeiden. Eine Belehrung als auf das Individuum ausgerichtete Maßnahme kann nicht im Verdachtsbereich gegen eine namentlich nicht konkretisierte Gruppe von Bediensteten ausgesprochen werden.

g) Ad § 79e Abs. 3 Z 3 BDG:

Zur fehlenden Systematik und Ausgestaltung als lex fugitiva wird auf die obigen Ausführungen verwiesen. Darüber hinaus ist aber die hier verankerte Information an die Personalvertretung im Ermittlungsstadium als verfahrensrechtlich höchst bedenklich

einzustufen. Inwieweit diese Informations- bzw. Befassungsverpflichtung mit § 46 BDG in Konflikt steht, ist zu prüfen.

Insgesamt ist jedoch der Sinn der Mitteilung der Belehrung an die IT-Stelle und an die Personalvertretung überhaupt nicht nachvollziehbar. Diesem auf die Zuordnung von dienstbehördlichen bzw. dienstaufsichtsbezogenen Aufgaben an diese Stellen abgestellte Ansatz ist nicht zu folgen.

h) Ad § 79e Abs. 4 BDG:

Diese Bestimmung stattet wiederum die Personalvertretung (PV) mit Aufgaben und Befugnissen aus, die ihr aufgrund der gesamten Systematik des Personalvertretungsrechts nicht zukommen. Ein Grund, warum gerade in derart sensiblen Bereichen – noch dazu ohne Gestaltungsmöglichkeit des bzw. der betroffenen Bediensteten – die PV (auch hier) mit dienstbehördlichen bzw. dienstaufsichtsbezogenen Befugnissen auszustatten wäre, ist nicht erkennbar.

i) Ad § 79e Abs. 6 und 7 BDG:

Die Absätze 6 und 7 im vorliegenden Entwurf des § 79e BDG stehen in erheblichem Widerspruch mit straf- bzw. verfahrensrechtlichen Bestimmungen. Durch die darin vorgesehenen Berichtspflichten würde – für die Fälle der erforderlichen Ermittlungen bei gröblichen Dienstpflichtverletzungen – in laufende Verfahrensschritte eingegriffen und die Erforschung der materiellen Wahrheit beeinträchtigt, wenn nicht vereitelt. Dass mit den so genannten „gröblichen Dienstpflichtverletzungen“ häufig auch in (Ideal)-konkurrenz die Prüfung von Tatbeständen des StGB verbunden sind, sei hier nur ergänzt.

Eine Abstimmung dieser Regelung mit dem bestehenden § 109 BDG dürfte in der Erstellung des gegenständlichen Entwurfes nicht vorgenommen worden sein.

Besonders rechtlich bedenklich – gerade auch vom Gesichtspunkt des Schutzes der Interessen der betroffenen Bediensteten – erscheint die auch in dieser Bestimmung wiederum gewählte Variante der Zuordnung dienstbehördlicher Agenden an die Personalvertretung; dies ist, um es nochmals festzuhalten, jedenfalls abzulehnen.

j) Ad § 79g BDG:

Wie bereits oben ausgeführt, sollte eine Definition und Schärfung des Begriffs „IKT“ vorgenommen werden.

Zur Definition des Begriffs „IT-Stelle“ gemäß § 79g Z 1 BDG:

Der Gesetzesentwurf geht davon aus, dass es lediglich der für „die technische Ermöglichung der IKT-Nutzung“ zuständigen Stelle möglich ist, Kontrollmaßnahmen (Auswertungen von Zugriffen, Datenermittlung) zu setzen und schließt andere Organisationseinheiten in diesem Zusammenhang vom Ermittlungsverfahren aus. Im Bereich des Finanzressorts wurden derartige Auswertungsmöglichkeiten – in Anbetracht der bereits erwähnten Sensibilität der verwalteten Steuerdaten – zumindest in Teilbereichen auch dem ho. Büro für Interne Angelegenheiten (BIA) zur Verfügung gestellt. Nachdem das BIA entsprechend dem Entwurf der Legaldefinition nicht die IKT-Nutzung ermöglicht, wären dessen (repressiven bzw. präventiven) Ermittlungen hinkünftig unzulässig. Es wird angeregt, entweder

- eine allgemeinere Formulierung zu finden, die auch Raum für Ermittlungen anderer Stellen eröffnet oder
- es den Ressorts selbst zu überlassen, wer derartige Datenermittlungen durchzuführen hat.

Es wird nochmals festgehalten, dass im Sinne der Rechtsklarheit und Rechtssicherheit eine (Legal)Definition hilfreich wäre. In einigen Ressorts wird die Festnetztelefonie über Internet („Voice over Internet Protocol - VOIP“) abgewickelt, was aber für die Nutzer nicht erkennbar ist. Fällt daher die Nutzung des Festnetzanschlusses auch unter den Begriff „Internetnutzung“?

Zur Definition des Begriffs „IKT-Infrastruktur“ gemäß § 79g Z 2 BDG:

Die Wortfolge „mit Ausnahme der Fernsprechanlagen“ wäre dahingehend klarzustellen, dass nur analoge Fernsprechanlagen gemeint sind.

2. Ad Art 4 – Änderung des Bundes-Personalvertretungsgesetzes (PVG)

Zu privaten Nutzung:

Als Eigentümer wäre es dem Dienstgeber unbenommen, direkt oder indirekt ein gänzliches Privatnutzungsverbot auszusprechen. In der einschlägigen Literatur wird überwiegend die

Auffassung vertreten, dass die Variante einer Nutzungsregelung mit klaren Prämissendefinitionen effizienter in der Handhabung ist.

Zu bedenken ist, dass ohne ausdrückliches Verbot oder Regelung der Privatnutzung, ob bzw. in welchem Umfang der Internetzugang für private Zwecke genutzt werden darf, davon auszugehen sein wird, dass eine Privatnutzung im „üblichen“ Ausmaß gestattet ist.

Wie bereits zum Vorblatt ausgeführt, erscheint eine Regelung mit bundesweiter Gültigkeit und allfälliger Erweiterbarkeit durch die Ressorts entsprechend den spezifischen Bedürfnissen zweckmäßig. Diese Regelung muss aber an ein von Vornherein klar ausgeschildertes, transparentes Kontrollsystem im Sinne einer Überwachungsmöglichkeit des Dienstgebers hinsichtlich der in seinem Eigentum stehenden IKT gekoppelt sein.

Jedenfalls sollte eine derartige Regelung systematischer Weise im Bereich der dienstrechtlichen Normen, nicht aber im PVG Verankerung finden.

Im Speziellen ist die Normierung einer Verordnungsermächtigung für die Bundesregierung im PVG – noch dazu mit diesem Regelungsinhalt – systemwidrig und rechtlich äußerst fragwürdig, weshalb eine solche Regelung vom Bundesministerium für Finanzen jedenfalls abgelehnt wird.

Die derzeit geltende Bestimmung des § 14 Abs. 3 PVG sieht eine Mitwirkung des Zentralausschusses vor, deren Ausgestaltung durch Verordnung der Bundesregierung vorzunehmen ist, was die Verordnungsgrundlage im PVG rechtfertigt. Bei der vorgeschlagenen gesetzlichen Grundlage fehlt hingegen bei der Verordnungsermächtigung jegliche Anknüpfung an eine Mitwirkung der Personalvertretung, was die Verankerung der gesetzlichen Grundlage für die IKT-Nutzung im Bundesdienst im PVG als nicht zweckmäßig erscheinen lässt.

IV.
Zu den einzelnen Bestimmungen eines Entwurfs einer IKT-Nutzungsverordnung

Aufgrund obiger Ausführungen wird auf eine umfassende Auseinandersetzung mit dem Verordnungstext verzichtet. Zu einzelnen Punkten wird inhaltlich wie folgt ausgeführt:

1. Die Textfolge in § 2 ist sprachlich nicht völlig verständlich, lassen die Sätze 1 und 2 mit den Worten „Die Nutzung ... für private Zwecke ... hat ... am Arbeitsplatz zu erfolgen“ doch einen inhaltlichen Widerspruch zur privaten Nutzung an sich erkennen.

2. Im nahezu gesamten Verordnungstext sind völlig unsystematisch begriffliche Verweise auf das Beamten-Dienstrechtsgesetz erkennbar.

3. Es wird angeregt, im letzten Satz des § 2 das Wort „eigenmächtige“ aufznehmen, sodass dieser lautet: „Insbesondere ist eine eigenmächtige Veränderung der zur Verfügung gestellten IKT-Infrastruktur (Hard- und Software) unzulässig“.

4. In § 3 Abs. 4 Z 4 wird die exemplarische Anführung kostenpflichtiger Datenbanken vorgeschlagen. Z 4 würde demnach lauten: „der Zugriff auf Seiten, die eine Zahlungsverpflichtung des Dienstgebers (z.B. kostenpflichtige Datenbanken) verursachen ....“

5. Es scheint nicht ratsam, in § 3 Abs. 4 Z 5 undifferenziert das Herunterladen „großer Datenmengen“ anzuführen. Besser wäre es, stattdessen von „nicht zu rechtfertigenden Datenvolumina“ zu sprechen. In diesem Sinn sollten auch nicht Bilddateien genannt werden, ohne auf deren Größe abzustellen. Es wird daher empfohlen, die Z 5 in folgender Weise umzuformulieren: „das Herunterladen nicht zu rechtfertigender Datenvolumina (z.B. Videodateien, MP3-Dateien oder große Bilddateien)“.

V.
Zu den Verwaltungslasten für Unternehmen

Abschließend ist zu beiden Begutachtungsentwürfen hinsichtlich der Verwaltungslasten für Unternehmen festzuhalten, dass gemäß §14a Abs. 1 BHG iVm § 2 Abs. 3

Standardkostenmodell-Richtlinien, BGBl. II Nr. 233/2007 bei Gesetzes- und Verordnungsentwürfen die Auswirkungen auf die Verwaltungslasten für Unternehmen in den Erläuterungen darzustellen sind.

Gemäß dem Rundschreiben des Bundeskanzleramtes vom 6. November 2007, GZ BKA-6000.824/0005-V/2/2007 betreffend die Darstellung der Auswirkungen von Rechtsetzungsvorhaben wird angeregt, in den Vorblättern eine Überschrift „Auswirkungen auf die Verwaltungslasten für Unternehmen“ und die Erläuterung „Es sind keine Informationsverpflichtungen für Unternehmen vorgesehen.“ aufzunehmen.

Das Bundesministerium für Finanzen ersucht um entsprechende Berücksichtigung oben stehender Ausführungen. Dem Präsidium des Nationalrates wurde diese Stellungnahme zum gegenständlichen Entwurf in elektronischer Form zugeleitet.

03.02.2009
Für den Bundesminister:
i.V. Mag. Hans-Jürgen Gaugl
(elektronisch gefertigt)

Bundesministerium für
Wirtschaft, Familie und Jugend

Bundeskanzleramt, Sektion III
Wollzeile 1-3
1014 Wien

Name/Durchwahl:
Mag. Lebschik / 5669
Geschäftszahl:
BMWA-12.010/0002-Pers/4/2009
Ihre Zahl:
BKA-920.196/0002-III/1/2009
Antwortschreiben bitte unter Anführung der Geschäftszahl an die E-Mail-Adresse post@pers4.bmwfj.gv.at richten.

Fremdlegistik; Bund; BKA; Bundesgesetz, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948 und andere Bundesgesetze geändert werden; ME; Begutachtung

Zu o.a. legistischem Vorhaben wird seitens des Bundesministeriums für Wirtschaft, Familie und Jugend wie folgt Stellung genommen:

Grundsätzlich wird die – mit ggstl. Entwurf verfolgte – Intention der Schaffung näherer Regelungen betreffend Datenverwendung, Kontrollmaßnahmen und der Ermöglichung der Festlegung von Nutzungsgrundsätzen der IKT-Infrastruktur mittels Verordnung begrüßt.

ad Begriff der „gröblichen Dienstpflichtverletzung“:

Das BDG kennt außer im § 133 BDG 1979 (disziplinäre Verantwortlichkeit der Beamten des Ruhestands) den Begriff der gröblichen Dienstpflichtverletzung nicht. Inhaltlich ist § 133 BDG 1979 (iwF bezieht sich jeder Paragraf auf das BDG 1979) bzw. dieser Tatbestand auf eine Verletzung des Amtsgeheimnisses (§ 46) und Verletzung bestimmter Meldepflichten (§ 53 Abs. 2), bzw. bei unter sechzigjährigen Ruhestandsbeamten noch Verletzung der Meldepflicht von Nebenbeschäftigungen (§ 56 Abs. 3) und Genehmigungspflicht bei Erstellung außergerichtlicher Sachverständigen Gutachten (§ 57) beschränkt. In diesem Zusammenhang ist anzumerken, dass bei diesen Tatbeständen die Zuordnung zu einer bestimmten Person leicht möglich ist und dadurch die Schwere der Tat - auch im Vorfeld - eher einschätzbar ist. Im Übrigen ist das Verhältnis zwischen Beamten und Dienstbehörde durch die Ruhestandsversetzung idR sehr „gelockert“.

Abt. PERS/4 - BUNDES-BEDIENSTETENSCHUTZ
1011 Wien • Stubenring 1 • Tel.: +43 (0)1 711 00 - 5304 • Fax: +43 (0)1 711 00 - 15304
E-Mail: post@pers4.bmwfj.gv.at • DVR 0037257

Die disziplinäre Verantwortlichkeit der Beamten des Aktivstandes richtet sich jedoch in der Praxis primär nach den §§ 43f (vgl. Kucsko-Stadlmayer, Das Disziplinarrecht der Beamten, 3. Auflagen, Seiten 98 bis 176). Hier bedarf es gerade des Disziplinarverfahrens um abschließend die Schwere der Tat zu beurteilen. Eine wie immer geartete „Gröblichkeitsprüfung" – noch dazu im Vorfeld des Verfahrens - ist nicht vorgesehen. Der Begriff „gröbliche Dienstpflichtverletzung" wird daher aus Sicht des BMWFJ als zu unbestimmt ansehen.
Außerdem ist aus den EB ersichtlich, dass eine Verletzung der Kontrollgrundsätze eine Dienstpflichtverletzung der die Kontrolle durchführenden Bediensteten darstellen würde. Somit wäre, trotz des Verdachtes einer Dienstpflichtverletzung durch einen Bediensteten, aufgrund von Zweifeln an der „Gröblichkeit" dieser Dienstpflichtverletzung, jede weitere Vorgehensweise praktisch unmöglich.
Da der Begriff „gröbliche Dienstpflichtverletzung" einen zu weiten Interpretationsspielraum offen lässt, wird daher anempfohlen die Einschränkung („*gröbliche*") zu streichen.

Jedenfalls wird jedoch um Streichung des Wortes „*gröblicherr*" im § 79e Abs. 7 (konkreter Verdachtsmoment gegen einen bestimmten Beamten) ersucht. Dies würde auch der Abstufung nach Kontrollverdichtung der EB entsprechen.

ISd § 9 PVG wird auch – anstelle der „allgemeinen" Informationspflicht in § 79e Abs. 3 Z 3, Abs. 6 und Abs. 7 letzter Satz – um konkrete Normierung der Pflicht zur **schriftlichen Verständigung** des zuständigen Personalvertretungsorgans, wie schon bisher bei Disziplinaranzeigen (9 Abs. 3 lit. c PVG) geboten, ersucht.

ergeht in Kopie an:
das Präsidium des Nationalrates
per Mail an: **begutachtungsverfahren@parlament.gv.at**

Mit freundlichen Grüßen
Wien, am 05.02.2009
Für den Bundesminister:
i.V. Mag.iur Gregor Lebschik

Elektronisch gefertigt.

Abt. PERS/4 - BUNDES-BEDIENSTETENSCHUTZ 2
1011 Wien • Stubenring 1 • Tel.: +43 (0)1 711 00 - 5304 • Fax: +43 (0)1 711 00 - 15304
E-Mail: post@pers4.bmwfj.gv.at • DVR 0037257

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR JUSTIZ
BMJ-A231.00/0006-Pr 6/2009

Museumstraße 7
1070 Wien

Briefanschrift
1016 Wien, Postfach 63

e-mail
Kzl.A@bmj.gv.at

Telefon (01) 52152-0*
Telefax (01) 52152 2727

Sachbearbeiter(in): Mag. Gerhard Nogratnig
*Durchwahl: 2289

An das Bundeskanzleramt
Sektion III

iii@bka.gv.at

An das
Präsidium des Nationalrates

begutachtungsverfahren@parlament.gv.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem das BDG 1979, das VBG und andere Bundesgesetze geändert werden (IKT-Nutzung) – Stellungnahme

Das Bundesministerium für Justiz beehrt sich, zu dem in Rede stehenden Begutachtungsentwurf folgende Stellungnahme abzugeben:

Eingangs ist anzumerken, dass im Entwurf (§ 79c Abs. 2) **lediglich Bestimmungen zu Kontrollmaßnahmen** vorgesehen sind, sich jedoch keine Grundlage für die Zulässigkeit der Aufzeichnung der personenbezogenen Daten und deren Sammlung an sich findet. Eine solche Datensammlung bildet jedoch die Voraussetzung für die Möglichkeit der Einsichtnahme, bevor in einem dritten Schritt deren weitere Verwendung zu regeln ist.

In § 79c Abs. 2 ist weiters von **personenbezogenen Daten der IKT-Nutzung** die Rede, wobei sich die Frage stellt, ob darunter alle personenbezogenen Daten fallen (auch dienstliche Emails) oder nur jene Daten, die der privaten Nutzung zuzuordnen sind. Überdies wird dabei **nicht zwischen persönlichen Daten des IKT-Nutzers und jenen von dritten Personen**, mit denen dieser in Kontakt steht, **unterschieden**. Mit den vorgesehenen Kontrollmaßnahmen sind jedenfalls auch Eingriffe in die Persönlichkeitsrechte Dritter möglich bzw. verbunden, weshalb den Bestimmungen des Datenschutzgesetzes auch außerhalb des Dienstverhältnisses besondere Bedeutung zukommt (§ 1 und §§ 17ff DSG).

Im konkreten Fall soll die Kontrolle einerseits Schäden an der IKT-Infrastruktur vorbeugen andererseits im Fall eines begründeten Verdachts einer „gröblichen“ Dienstpflichtverletzung zum Zweck der Verhinderung weiterer Dienstpflichtverletzungen, wenn zeitliche, inhaltliche oder quantitative Beschränkungen der bereitgestellten IKT-Nutzung dafür nicht ausreichen, oder zum Zweck der „Klarstellung“ des Sachverhalts eingesetzt werden dürfen (§ 79c Abs. 2 BDG 1979 in der Fassung des Entwurfs).

Zur Kontrolle bei begründetem Verdacht einer gröblichen Dienstpflichtverletzung (§ 79e BDG in der Fassung des Entwurfs) ist zu bemerken,

- dass damit – nicht nur Fall der Anordnung im Fall des Verdachts gegen einen konkreten Bediensteten gemäß Abs. 7 - der strafprozessuale Regelungsbereich der Auskunft über Daten einer Nachrichtenübermittlung sowie der Überwachung von Nachrichten (§§ 134, 135 StPO) unterlaufen wird, die grundsätzlich den Verdacht einer vorsätzlich begangenen Straftat voraussetzt, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist;
- dass zwar in § 79c Abs. 3 BDG 1979 in der Fassung des Entwurfs klargestellt wird, dass Inhalte übertragener Nachrichten nicht Gegenstand von Kontrollmaßnahmen zum Zweck der Verhinderung weiterer Dienstpflichtverletzungen oder zum Zweck der „Klarstellung“ des Sachverhalts sein dürfen, jedoch im Übrigen der Datenbegriff des Entwurfs ebenso wie der zentrale Begriff der „**gröblichen Dienstpflichtverletzung**“ keiner inhaltlich ausreichenden Determinierung zugeführt werden kann (nur als Beispiel: unter welchen Bedingungen wäre eine Verletzung der §§ 2 bis 4 der IKT-Verordnung als „gröblich“ zu bezeichnen?). Ebenso wirft der Begriff „**unbedingt notwendig**“ Unklarheiten und Widersprüche auf und schafft einen großen Interpretationsspielraum. Ein derart schwerwiegender Eingriff in die Persönlichkeitsrechte eines Beamten und/oder Dritter bedarf einer genauen Determinierung der Umstände, unter welchen die Interessen des Dienstgebers unter Berücksichtigung des Verhältnismäßigkeitsprinzips die schutzwürdigen Interessen der Betroffenen verdrängen. Insbesondere wird erst nach Einschau in den Inhalt der Nachrichten beurteilt werden können, ob die inhaltliche Kontrolle „unbedingt notwendig“ ist, weshalb diese Bestimmung einen unlösbaren inneren Widerspruch in sich birgt.

Auf beide Fragen gehen im Übrigen auch die Erläuterungen nicht ein.

Verfassungsrechtlich können Ermittlungsbefugnisse vergleichbarer Art wohl nur dann gerechtfertigt werden, wenn man – wie die **arbeitsrechtlichen Senate des OGH** (8 ObA 288/01p; 9 ObA 109/06d) – davon ausgeht, dass bestimmte Daten einer IKT-Nutzung nicht dem Bereich des Fernmeldegeheimnisses unterliegen (Artikel 10a StGG). Gerade dann wäre es jedoch unentbehrlich, die angesprochenen Datenkategorien im Gesetz genau zu umschreiben.

Der OGH erklärt in diesen beiden Entscheidungen, welche nur die lückenlose Erfassung „äußerer“ und nicht inhaltlicher Grunddaten betreffen, dass solche Kontrollsysteme (dort betreffend die Telefonanlage bzw. Fingerscanning) die Menschenwürde berühren können, weshalb die Zustimmung des Betriebsrates iSd § 96a ArbVG einzuholen sei. Auch werde bei Verwendung der oben angeführten Systeme das schutzwürdige Interesse an der Geheimhaltung personenbezogener Daten gemäß § 1 Abs. 1 DSG nicht berücksichtigt. In seiner Begründung zur Entscheidung zu 8 ObA 288/01p erklärte der OGH, dass es den beiderseitigen Interessen entspräche, eine Betriebsvereinbarung abzuschließen, wo Schutzmaßnahmen vor übermäßiger Kontrolle in folgender Weise festgeschrieben werden sollten: Die Rufdatenerfassung **sollte nur im Verdachtsfall unter Einbeziehung des Betriebsrates geöffnet werden können**. Im Falle des Weiterbestehens von Verdachtsmomenten sollten diese nach Information des Betriebsrates **mit dem jeweiligen Dienstnehmer erörtert werden** und weitere Erhebungen sollten erst möglich sein, wenn der Dienstnehmer die Verdachtsmomente nicht entsprechend entkräften könne.

Werden die vom OGH festgelegten Grundsätze auf den vorliegenden Gesetzesentwurf übertragen, wäre die **Personalvertretung bereits vor und bei Einsichtnahme** in die aufgezeichneten „äußeren“ Daten einzubeziehen. Hier wäre zum Schutz auch eine **automatische Protokollierung** der Einschau wünschenswert, um – wie im Datenschutzrecht üblich - Missbrauch zu verhindern bzw. nachvollziehbar zu machen.

Bei **Einsicht in die inhaltlichen, personenbezogenen Daten** wäre wohl eine noch restriktivere, die schutzwürdigen Interessen der Betroffenen im Sinne der Bestimmungen des DSG und des Artikels 8 MRK sowie des Briefgeheimnisses berücksichtigende Regelung einzuführen.

Die **Strafsenate des OGH** sehen das freilich grundsätzlich anders und beziehen Vermittlungs- oder Verkehrsdaten regelmäßig in den Anwendungsbereich der

Bestimmungen über die Überwachung einer Telekommunikation ein (13 Os 161/95; zuletzt 11 Os 57/05z).

Das ist jedoch unabhängig von diesem Lehrenstreit deshalb von Bedeutung, weil Verwertungsverbote damit auf dem Umweg eines Disziplinarverfahrens unterlaufen werden können, wenn der Verdacht der Dienstpflichtverletzung zugleich den Verdacht einer Straftat begründet, die für sich genommen keine Anordnung und Bewilligung einer Maßnahme nach den §§ 134 und 135 StPO rechtfertigen würde. Dafür besteht aus Sicht des Bundesministeriums für Justiz ausgehend von einem „Stufenbau“ der Strafrechtsordnungen (und dem Grundsatz der Verhältnismäßigkeit) keine Rechtfertigung. Gleichzeitig besteht aber auch die Gefahr einer Verhinderung sinnvoller strafprozessualer Überwachungsmaßnahmen, weil die betroffenen Bediensteten umgehend von dem Ermittlungsauftrag in Kenntnis zu setzen sind (§ 79e Abs. 3 und 7 BDG 1979 in der Fassung des Entwurfs).

Schließlich wird dem Leiter der Dienststelle damit aber auch eine Ermittlungsfunktion übertragen, die grundsätzlich den Disziplinarkommissionen obliegt; im Fall eines begründeten Verdachts ist wohl ein Disziplinarverfahren einzuleiten und von der Kommission zu entscheiden, welche Ermittlungen zur Klärung des Verdachts durchzuführen sind.

Soweit in § 79e des Entwurfes davon ausgegangen wird, dass der Leiter einer Dienststelle die IT-Stelle beauftragen kann, auf einen Verdachtsfall Bezug habende Daten der IKT-Nutzung zu „ermitteln“, ergibt sich die Frage, ob die daran geknüpften Pflichten (Abs 2 und Abs 3) auch ausgelöst werden, wenn die Zugriffsmöglichkeit des Dienstgebers (der IT-Stelle) auf eine Datensammlung bereits – ohne Übergabe eines bestimmten Codes oder mittels Einschaltung einer dritten Person – besteht, weil sich die Daten in seiner Gewahrsame befinden und keine Protokollierung der Nutzung dieser Zugriffsmöglichkeit stattfindet.

Weiters ergeben sich **Zweifel, ob** vom Begriff der IKT-Nutzung **auch elektronische Akten erfasst** sind. Die Begriffsbestimmungen in § 79g geben dahingehend Aufschluss, dass als IKT-Infrastruktur alle Geräte, die vom Dienstgeber zur Verfügung gestellt werden oder im Einvernehmen mit dem Dienstgeber für dienstliche Zwecke benützt werden und der Informationsverarbeitung für Zwecke des Dienstgebers dienen, sowie die darauf befindlichen Programme und Daten mit der Ausnahme von Fernsprechanlagen zu verstehen sind. Elektronische Akten sind jedoch weder vom Dienstgeber speziell dem Dienstnehmer zur Verfügung gestellt

noch im Einvernehmen mit dem Dienstgeber für dienstliche Zwecke zu benützen, sondern im Rahmen der Gesetze, der Approbationsbefugnisse, Zuständigkeiten und des Weisungszuges. Daher dürften elektronische Akten wohl nicht unter diese Definition fallen. Dies sollte aber klargestellt werden. Bei der Einbeziehung elektronischer Akten würde sich wiederum das Problem stellen, ob die Grundsätze der Datenverwendung auch auf jene Personen anzuwenden ist, denen Einsichtsbefugnisse kraft ihrer Amtsstellung im Verfahren zukommen.

Zur Systematik des Entwurfs ist zu bemerken, dass die Bestimmungen zT nicht recht klar geordnet sind. So soll gemäß § 79e Abs. 1 ein schriftlicher Ermittlungsauftrag zu ergehen haben, auf Grund dessen einerseits die IT- Stelle über die IKT-Nutzungen im Umfang des Ermittlungsauftrags in anonymisierter Weise (Abs. 2) zu berichten, andererseits dem Leiter der Dienststelle über die IKT-Nutzungen im Umfang des Verlangens nach Abs. 5 namentlich und in schriftlicher Form zu berichten (Abs. 6) haben. Erst aus dem Zusammenhalt der Bestimmungen des Abs. 5 mit jener des Abs. 3 Z 2 ergibt sich, dass diese namentliche Berichterstattung nur in dem Fall zulässig ist, dass der im Ermittlungsauftrag gemäß Abs. 1 genannte Verdachtsfall fortbesteht oder ein gleichgelagerter Verdachtsfall auftritt.

Gleiches gilt auch für die zulässige Dauer der Überwachung, weil sich diese bloß aus der verpflichtenden Mitteilung gemäß § 79e Abs. 3 BDG 1979 in der Fassung des Entwurfs ergibt. Nach der Formulierung des Abs. 4 dieser Bestimmung („Ein längerer als der in Abs. 3 Z 2 vorgesehene Beobachtungszeitraum darf nur in begründeten Ausnahmefällen festgesetzt werden.“) ist wiederum zweifelhaft, ob eine Verlängerung zulässig ist.

Die Formulierung des Abs. 7 lässt wiederum nicht eindeutig bestimmen, ob der Beamte nach Übermittlung eines Berichts der IT- Stelle umgehend zu informieren ist oder bereits vom Ermittlungsauftrag, die Formulierung des letzten Satzes lässt beide Auslegungsvarianten offen („Der Beamte und das zuständige Organ der Personalvertretung sind vom Leiter der Dienststelle umgehend über den Ermittlungsauftrag und über den Bericht der IT-Stelle zu informieren.“).

Zuletzt wäre zu klären, in welchem Verhältnis die neuen Mitwirkungsrechte der Personalvertretung gemäß § 9 Abs. 2 lit. n und o PVG zum bestehenden Mitwirkungsrecht nach lit. f stehen (bzw. weiter greifend, in welchem Verhältnis die da bzw. dort angesprochenen Maßnahmen zueinander stehen).

*****

Zusammenfassend wird angeregt, das **Grundkonzept** insbesondere im Zusammenhang mit den Bestimmungen des Datenschutzes und der Judikatur zu den Persönlichkeitsrechten zu **überdenken** und zu verfeinern, eine Befugnis zur „Klarstellung von Dienstpflichtverletzungen“ (§ 79c Abs. 2 Z 2 BDG 1979 idF des Entwurfs) (i.S. eines bloßen Erkundungsbeweises) sollte damit nicht verbunden sein.

05. Februar 2009
Für die Bundesministerin:
Dr. Anton Paukner

Elektronisch gefertigt

Österreichischer
Gewerkschaftsbund

Sozialpolitik · Fachbereich Rechtspolitik

ÖGB

Bundeskanzleramt
Sektion III
Ballhausplatz 2
1014 Wien

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Bearbeiter/in	Klappe (DW) Fax (DW)	Datum
BKA-920.196/0002-III/1/2009	Mag[a]Fr/Mic	440/463	05.01.2009

Bundesgesetz, mit dem das Beamten-Dienstrechtsgesetz 1979, das Vertragsbedienstetengesetz 1948, das Richter- und Staatsanwaltschaftsdienstgesetz, das Bundes-Personalvertretungsgesetz, das Landeslehrer-Dienstrechtsgesetz und das Land- und forstwirtschaftliche Landeslehrer-Dienstrechtsgesetz geändert werden.

Der Österreichische Gewerkschaftsbund dankt für die Übermittlung des oben angeführten Gesetzesentwurfs und nimmt hierzu wie folgt Stellung:

Durch den vorliegenden Entwurf soll eine gesetzliche Grundlage für die Zulässigerklärung der privaten IKT-Nutzung, insbesondere auch von Internet und E-Mail, durch die Bediensteten geschaffen werden. Weiters soll durch die Festlegung von Kontrollgrundsätzen eine überschießende und damit unverhältnismäßige Kontrolle durch den Dienstgeber hintangehalten werden.

Diese Maßnahme wird vom Österreichischen Gewerkschaftsbund grundsätzlich begrüßt, wobei insbesondere auf das Einvernehmen mit der Personalvertretung gem. § 9 Abs 2 PVG großer Wert gelegt wird.

Kritisch gesehen wird jedoch die Rolle der IT-Stelle, welche im § 79g lediglich als Organisationseinheit, die für die technische Ermöglichung der IKT-Nutzung zuständig ist, definiert wird. Auf Grund der Tatsache, dass es sich bei den der IT-Stelle zukommenden Aufgaben um ein hoch sensibles Gebiet handelt, in welchem sie Einsicht in persönliche Daten von möglicherweise unbetroffenen Personen erlangt, regt der Österreichische

ADRESSE
1010 Wien, Laurenzerberg 2

Telefon +43 1 534 44-Dw
Telefax +43 1 534 44-Dw
ZVR-Nr.: 576439352

Internet www.oegb.at
E-Mail oegb@oegb.or.at
DVR-Nr.: 0046655

BAWAG AG, Kto. Nr. 01010-225-007
PSK, Kto. Nr. 1808.005
ATU 162 731 00

Gewerkschaftsbund an, dass schon bei der Besetzung der IT-Stelle diesem Umstand verstärkt Rechnung getragen wird.

Der Österreichische Gewerkschaftsbund ersucht um Berücksichtigung seiner Stellungnahme.

Erich Foglar
gf. Präsident

Mag. Bernhard Achitz
Leitender Sekretär