JUSIT

IT-Recht
Rechtsinformation
Datenschutz

2/2010

Beiträge

Judikatur

Pbb. Erscheinungsort Wien, Verlagspostamt 1030 Wien, ISSN 1996-8228

LexisNexis®

2/2010, S. 41 – 84
Art.-Nr. 18 – 35

Dipl.-Wirt. Jur. (FH) Thomas Hartmann, LL.M.
Humboldt-Universität Berlin

Novelle des Bundesdienstrechts als Modell für die Nutzung und Kontrolle von Internet am Arbeitsplatz?

Eine vor Kurzem in Kraft getretene Novelle des österreichischen Bundesdienstrechts[1] (§§ 79c bis 79i BDG,[2] die Verweisungen darauf in § 29n VBG[3] und § 206 RStDG[4] sowie begleitende Änderungen im PVG[5]) enthält recht detaillierte Bestimmungen über die Zulässigkeit privater Internetnutzung am Arbeitsplatz sowie über die Kontrollbefugnisse des Dienstgebers. Die wesentlichen neuen Gesetzesbestimmungen der Novelle werden in diesem Beitrag vorgestellt und bewertet. Abschließend wird darauf eingegangen, ob die Regelungen des Bundesdienstrechts auch Modellcharakter für das allgemeine Arbeits- und Datenschutzrecht entfalten können. Den bisherigen Meinungsstand zum Thema hat zuletzt *Goricnik* in jusIT 2009/82, 169[6] dargestellt.

Deskriptoren: Arbeitsvertrag, Betriebsmittel, Betriebsvereinbarung, Datenschutz, E-Mail, Inhaltsdaten, Interessenabwägung, Internet, Internet-Policy, Internet am Arbeitsplatz, IT-Sicherheitsrichtlinien, IT-Stelle, Kommunikationsgeheimnis, Kontrolle, Kontrollmaßnahmen, Menschenwürde, Nachricht, Privatnutzung, Systemadministrator, Überwachung, Verhältnismäßigkeit, Verkehrsdaten

Normen: ArbVG: § 96 Abs 1 Z 3; BDG: §§ 79c, 79d, 79e, 79f, 79g, 79h, 79i; DSG 2000: § 1, § 1 Abs 2, § 4 Z 1, §§ 6, 7, 24; EMRK: Art 8; IKT-NV 2009: §§ 4, 5; RL 2002/58/EG: Art 2, 3, 5; RStDG: § 206; StGG: Art 10a; TKG 2003: §§ 92, 93; VBG: § 29n

1. Private Internetnutzung und private E-Mail am Arbeitsplatz

Unter Heranziehung allgemeiner Normen des Arbeits- und Datenschutzrechts geht die Literatur davon aus, dass im Zweifel der dienstliche Internetzugang in begrenztem Rahmen auch privat genutzt werden darf, soweit der Arbeitgeber keine abweichenden Regelungen getroffen hat und dadurch nicht in nennenswerter Weise geschädigt wird.[7]

Für den öffentlichen Bundesdienst hat der Gesetzgeber mit § 79d S 1 und 2 BDG nun folgende Leitlinien kodifiziert:

„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."

Zwar ist damit auch eine vorsichtige Aufweichung des arbeitsrechtlichen Grundsatzes verbunden, wonach der Arbeitgeber über seine Betriebsmittel und deren betrieblichen Einsatz frei disponieren kann.[8] Die Regelung reagiert jedoch insgesamt mit Augenmaß auf die vielerorts betriebliche Realität des Internetzeitalters. Gelungen erscheint ein zeitgemäßer Interessenausgleich zwischen Dienstgebern und Bediensteten. In der heutigen Arbeits- und Kommunikationswelt wird von Dienstnehmern für gewöhnlich ein hohes Maß an Flexibilität und Einsatzbereitschaft erwartet. Die vertraglich geschuldete Arbeitsleistung orientiert sich weithin orts- und zeitunabhängig etwa an Zielvereinbarungen. Die Entwicklung erreicht neuerdings auch die deutsche Judikatur. „Sozialtypisch" seien die privaten Telefongespräche eines Geschäftsführers auf dem dienstlichen Mobiltelefon.[9] Angesichts verbreiteter Flat-Tarifmodelle führt eine maßvolle, private Internetnutzung (im Inland) heute nicht mehr zu einer zusätzlichen finanziellen Belastung des Arbeitgebers, sodass die in der Arbeitsvertragspraxis oftmals vereinbarte anteilige Abrechnung von Telefon- bzw Internetkosten idR obsolet ist.[10]

Bei einem Fair-Use-Prinzip für die Internetnutzung am Arbeitsplatz stehen die Mitarbeiter besonders in der Verantwortung, ihren Treue- und Rücksichtspflichten im Arbeitsverhältnis gerecht zu werden. Durch nachstehende Fallgruppen führt § 79d BDG dem einzelnen Mitarbeiter vor Augen, welche private Internetnutzung dem Umfang und Inhalt nach jedenfalls zu unterbleiben hat.

1.1. Missbräuchliche Privatnutzung

Missbrauch betrieblicher Informations- und Kommunikationstechnik in engerem Sinne erfolgt etwa durch Amtsmissbrauch, der – falls nicht schon bereits durch andere

1) BGBl I 2009/77.
2) Beamten-Dienstrechtsgesetz BGBl 1979/333.
3) Vertragsbedienstetengesetz BGBl 1948/86.
4) Richter- und Staatsanwaltschaftsdienstgesetz BGBl 1961/305.
5) Bundes-Personalvertretungsgesetz BGBl 1967/133.
6) *Goricnik*, Zur Kontrolle der Internet-Nutzung und des E-Mail-Verkehrs am Arbeitsplatz, jusIT 2009/82, 169.
7) *Goricnik* (FN 6) mwN.
8) Vgl zB *Brodil*, Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis, ZAS 2004, 156.
9) LAG Rheinland-Pfalz, 23. 10. 2008, 10 Sa 787/05 rkr.
10) Vgl ArbG Frankfurt, 18. 6. 2009, 1 Ca 1139/09 Rz 4, 35 rkr; dahin gehend schon im Jahr 2001 *Dellisch*, Private E-Mail- und Internet-Nutzung am Arbeitsplatz – Gestaltung der Nutzung und Kontrolle durch den Dienstgeber, ASoK 2001, 316.

straf- oder dienstrechtliche Vorschriften geahndet – nicht von einer privilegierten privaten Internetnutzung protegiert sein soll. Bei einer Schädigung mag sich der Arbeitgeber zwar in der Regel zivilrechtlich an dem Mitarbeiter schadlos halten. Infolge des ausdrücklichen gesetzlichen Verbots missbräuchlicher Privatnutzung kann der Arbeitgeber aber regelmäßig auch dem Vorwurf eines Mitverschuldens wegen fehlender Regelungen im eigenen Betrieb entgegentreten. Ausweislich der Erläuterungen[11] soll der Missbrauchstatbestand auch eine zeitliche und den Volumina nach überschießende Privatnutzung umfassen. Dieses Exzessverbot wird allerdings schon durch die ausdrückliche Beschränkung der Privatnutzung auf ein „eingeschränktes Ausmaß" deutlich.

1.2. Rufschädigung

Bedienstete dürfen am Arbeitsplatz nicht auf Internetseiten zugreifen, wenn dies dem Dienstgeber ruf- bzw kreditschädigend zugeordnet werden kann. Untersagt ist demnach insbesondere der Zugriff auf Mehrwertdienste im Internet sowie auf pornographische oder strafrechtlich relevante Internetangebote.[12]

Eine typische dienstliche E-Mail-Adresse (Max.Mustermann@firma123.at) weist auf der einen Seite eine hohe Mitarbeiterindividualität auf, andererseits ist sie regelmäßig unmittelbar der Firma des Arbeitgebers zuordenbar. Fraglich ist, ob der Mitarbeiter mit dieser dienstlichen E-Mail-Adresse an internetöffentlichen Diskussionsforen, Weblogs 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 hinterlegen darf. Ein generelles Verbot derartiger Handlungen sieht die Nutzungsverordnung der Bundesregierung zwar nicht vor, allerdings dürfen Bedienstete zB in privaten E-Mails „keinen Hinweis auf ihre dienstliche Stellung oder ihre dienstliche Postadresse aufnehmen", insbesondere darf auch nicht eine dienstliche elektronische Signatur angefügt werden.[13] Bei privaten Rechtsgeschäften am Arbeitsplatz trifft die Bediensteten insoweit eine besondere Sorgfaltspflicht, „als dabei in eindeutiger Weise der private Charakter des Vorgangs ersichtlich" werden muss.[14]

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

Diese primär technisch bzw organisatorisch motivierten Tatbestände stehen häufig in sachlichem Zusammenhang. Grundsätzlich können Privatnutzungen des dienstlichen Internetzugangs zu Störungen der IT-Sicherheit oder der IT-Leistungsfähigkeit führen. So kann ein Mitarbeiter zB ein derart hohes Datenvolumen aus dem Internet herunterladen, dass sich die Leistungsfähigkeit des IT-Servers insgesamt verlangsamt. Aber auch durch das Öffnen eines einzelnen Anhangs einer E-Mail kann Schadsoftware in das System eindringen und seine Funktionsfähigkeit behindern.

Das Gefährdungspotenzial erscheint enorm und ist zugleich gekennzeichnet durch eine hohe Komplexität.[15] Im Zweifel wird es für den einzelnen Mitarbeiter eher schwierig sein zu erkennen, welche Nutzungen die IT-Sicherheit und IT-Leistungsfähigkeit bedrohen können. Generell kann auch durch Anhänge dienstlicher E-Mails oder sonstige dienstliche Internetnutzung Schadsoftware in das betriebseigene System eingeschleust werden, sodass trotz aktueller Schutz- und Datensicherheitsmaßnahmen (zB Firewall, Antiviren-Tools) ein mit dem Internet verbundenes Firmennetzwerk gegen Angriffe aus dem Internet nicht lückenlos geschützt werden kann. Ferner ist auch zu berücksichtigen, dass Mitarbeiter Programme herunterladen und sodann „gemischt" nutzen oder etwa dienstliche Programme einem notwendigen und gegebenenfalls die Systemsicherheit erhöhenden Update zuführen.

Entsprechende Verhaltensregeln sind daher den Bediensteten so konkret und verständlich wie möglich aufzuerlegen. Infolge des rasanten technologischen Fortschritts bedürfen IT-Sicherheitsrichtlinien einer beständigen Fortschreibung. Besondere Gefährdungen der IT-Sicherheit und geeignete Schutzmaßnahmen des Dienstgebers demonstrierte die Bundesregierung exemplarisch in § 4 Abs 4 Z 5 und § 5 Abs 3 IKT-NV für bestimmte Dateitypen, die auffällig häufig Schadsoftware enthalten.

1.4. Zwischenergebnis

Das Nutzungsreglement des § 79d BDG ist weithin zu begrüßen. Es eröffnet den Bundesbediensteten zB die Möglichkeit, während der Pausen Online-Ausgaben von Tageszeitungen abzurufen oder Recherchen durchzuführen, die nicht immer trennscharf der dienstlichen oder der privaten Sphäre zugeordnet werden können. Zugleich sind die Mitarbeiter verstärkt zu einem verantwortungsvollen Umgang mit dem dienstlichen Internetzugang angehalten; die klar benannten Grenzen der Internetnutzung am Arbeitsplatz schaffen ein Problembewusstsein im Betrieb und schützen so letztlich die berechtigten Interessen des Dienstgebers.

2. Grundsätze für Kontrollmaßnahmen

Das von *Kotschy/Reimer* entwickelte Modell stufenweiser Kontrollverdichtung[16] prägt die Bestimmungen der Novelle. Aus Datenschutzsicht ist an den §§ 79e bis 79i BDG positiv das Bestreben hervorzuheben, dass konsequent nur der jeweils gelindeste Eingriff in das Grundrecht auf Datenschutz der Mitarbeiter erfolgen darf.[17] Eben in diesem Sinne formulierten auch die Vertreter der europäischen Datenschutzbehörden im Lichte des Verhältnismäßigkeitsgrundsatzes:

„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."[18]

Weiterhin grundsätzlich unzulässig ist nach § 79e Abs 1 BDG die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren; bislang bestand insoweit im öffentlichen Bundesdienst ein absolutes Kontrollverbot

11) ErläutRV 160 BlgNR 24.GP 3.
12) § 79d S 4 u 5 BDG 1979 iVm § 4 Abs 1 u 4 IKT-NV, IKT-Nutzungsverordnung BGBl II 2009/281.
13) § 79d S 4 u 5 BDG 1979 iVm § 5 Abs 2 IKT-NV.
14) § 79d S 4 u 5 BDG 1979 iVm § 4 Abs 2 IKT-NV.
15) Vgl zB Programm „Innere Sicherheit" der Innenminister von Bund und Ländern in Deutschland („Eine zunehmende Bedeutung haben internetgebundene Angriffe auf Rechnersysteme von Wirtschaftsunternehmen und Regierungsstellen. [...] Das Internet als Tatort wird auch in der Zukunft nur begrenzt kontrollierbar sein."), zit n Handelsblatt v 3. 6. 09.
16) *Kotschy/Reimer*, Die Überwachung der Internet-Kommunikation am Arbeitsplatz: Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht, ZAS 2004, 167.
17) Vgl §§ 1, 6, 7 DSG 2000, Art 8 EMRK.
18) *Artikel 29 Datenschutzgruppe*, Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten 29.

für den Dienstgeber.[19] Das wird nun von zwei Ausnahmen (§ 79e Abs 2 BDG) durchbrochen: Der staatliche Dienstgeber soll personenbezogene Daten der Internetnutzung ausnahmsweise doch kontrollieren dürfen, wenn die Integrität bzw die Funktionsfähigkeit des betrieblichen IT-Systems gefährdet ist oder bei 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,[20] sieht auch die Novelle nicht vor: Ein „absolutes" Zustimmungsrecht der Personalvertretung zu Kontrollmaßnahmen des Dienstgebers, welche die Menschenwürde berühren, ist im öffentlichen Dienst aus verfassungsrechtlichen Gründen nicht möglich.[21]

2.1. Gefährdung des IT-Systems

Der Anlass der Kontrollmaßnahme ist in diesem Fall zumindest primär nicht in der Person des Mitarbeiters, sondern in einer Fehlermeldung des IT-Systems zu sehen. Initiator dieser Datenverwendung ist die IT-Stelle im Unternehmen, die mit maschinell generierten, teils systembedingt personenbezogenen Daten iSd § 4 Z 1 DSG 2000[22] operiert.

Personenbezogene Nutzungsdaten von Mitarbeitern dürfen demnach nur unter Beachtung und nach Maßgabe der folgenden Schutzvorkehrungen verwendet werden:

- Generell dürfen Inhaltsdaten übertragener Nachrichten[23] nicht kontrolliert werden, es sei denn, es ist „unbedingt notwendig"[24] (§ 79e Abs 3 S 1 BDG).
- Die IT-Stelle hat mit ihrem technischen Sachverstand ex ante alle Möglichkeiten zur Fehlerbeseitigung wahrzunehmen, die keiner Inhaltsdaten bedürfen (§§ 79f Abs 1 S 2 BDG).[25]
- Bleiben die Bemühungen der IT-Stelle erfolglos, kann der Dienststellenleiter in anonymisierter Form über Art und Dauer der gefährdenden Internetnutzung informiert werden (§ 79f Abs 1 BDG). Dieser hat sodann umgehend die Mitarbeiter zu informieren und auf die Beseitigung der indizierten Internetnutzung hinzuwirken (§ 79f Abs 2 BDG).
- Erst wenn die Gefahr nun noch fortbesteht, kann über maximal vier Wochen eine namentliche Zuordnung des Mitarbeiters zu der gefährdenden Internetnutzung erfolgen (§ 79f Abs 4 BDG).

Bei einer konkreten, unmittelbaren Gefährdung des IT-Systems aber darf die IT-Stelle nach § 79f Abs 5 BDG sofort mit personenbezogenen Daten operieren, „soweit dies zur Behebung dieser Gefährdung unbedingt notwendig ist." Neben einer insoweit strikten Zweckbeschränkung hat die IT-Stelle in diesen Notverfahren erhöhte Informations- und Protokollpflichten zu beachten.

Eine Hauptverantwortung für den Datenschutz trägt in diesem Zusammenhang die IT-Stelle, die nach der Novelle verstärkt eine besondere Vertrauensstellung einnimmt und insofern mit einer Black Box verglichen werden könnte. Es ist zu hoffen, dass die datenschutzrechtlichen Integritätsanforderungen an die Systemadministratoren von den Dienstgebern respektiert werden, denn die Nichteinhaltung der Datenschutz- und Kontrollgrundsätze der §§ 79e bis 79g BDG „wäre nicht nur allgemein rechtswidrig, sondern würde gleichzeitig die Begehung einer Dienstpflichtverletzung durch die die Kontrollen durchführenden Bediensteten darstellen."[26]

2.2. Verdacht auf gröbliche Dienstpflichtverletzung

Hinsichtlich verhaltensbedingter Kontrollen der Internetnutzung ist zunächst daran zu erinnern, dass nach § 79d BDG den Bundesbediensteten die Privatnutzung in eingeschränktem Ausmaß grundsätzlich erlaubt ist (s oben Kapitel 1). Nur bei einem Verdacht auf eine gröbliche Dienstpflichtverletzung ist die personenbezogene Kontrolle der Internetnutzung am Arbeitsplatz zulässig. Diesfalls hat der Dienstgeber folgende Voraussetzungen zu beachten:

- Ausgangspunkt ist das Bestehen eines begründeten Verdachts einer gröblichen Dienstpflichtverletzung (§ 79e Abs 2 Z 2 BDG). Ein *begründeter Verdacht* muss schon vorliegen, ehe die Kontrollmaßnahme eingeleitet wird; nur dann kann eine Kontrollmaßnahme zur „Klarstellung des Sachverhaltes" iSv § 79e Abs 2 Z 2 lit b BDG legitimiert sein.[27] Der Begriff der *gröblichen Dienstpflichtverletzung* knüpft am Kündigungsgrund des § 32 Abs 2 Z 1 VBG[28] an.[29] Ein Weiterleiten von ein bis zwei Scherz-E-Mails pro Woche an Kollegen[30] etwa wird die Schwelle eines gröblichen Fehlverhaltens iSd §§ 79e, 79g BDG nicht erreichen.
- Zunächst sind zeitliche, inhaltliche oder qualitative Beschränkungen des dienstlichen Internetzugangs zu verhängen, um die Dienstpflichtverletzung durch technische Vorkehrungen zu verhindern (§ 79e Abs 2 Z 2 lit a BDG).
- Verfahrensinitiator ist ausschließlich der Leiter der Dienststelle (§ 79e Abs 2 Z 2 BDG).
- Die IT-Stelle ist schriftlich unter genauer Beschreibung des Verdachtfalls zu beauftragen (§ 79g Abs 1 BDG).
- Die IT-Stelle hat dem Dienststellenleiter zunächst anonymisiert zu berichten (§ 79g Abs 2 BDG). Erst wenn nach der Information der Bediensteten und dem Hinwirken auf Einhaltung der Dienstpflichten (§ 79g Abs 3 BDG) der Verdachtsfall fortbesteht, darf die IT-Stelle innerhalb von maximal vier Wochen dem Dienststellenleiter namentlich in schriftlicher Form berichten (§ 79 Abs 6 BDG).
- Legitimer Zweck ist neben der Verhinderung weiterer Dienstpflichtverletzungen (§ 79e Abs 2 Z 2 lit b BDG) die Klarstellung eines Sachverhalts (lit a leg cit), dem der Verdacht einer gröblichen Dienstpflichtverletzung zugrunde liegt.

19) *Fellner* (Hrsg), BDG (53. Erg Lfg) § 79c: Ein im Vergleich zu § 96 Abs 1 Z 3 ArbVG strengerer Maßstab für den staatlichen Dienstgeber führt dazu, dass nach *Fellner* jede verdeckte Kontrollmaßnahme als Maßnahme anzusehen sei, welche die Menschenwürde berühre.

20) Arbeitsverfassungsgesetz BGBl 1974/22.

21) *Fellner* (Hrsg), BDG (FN 19); *Stiger*, Protokollierung der Internetzugriffe von Dienstnehmern, in *Forgó/Feldner/Witzmann/Dieplinger* (Hrsg), Probleme des Informationsrechts 420 ff.

22) Datenschutzgesetz 2000 BGBl I 1999/165.

23) Zum Begriff u Anwendungsbereich der „Nachricht" s u 2.3 Exkurs.

24) Krit *BM f Justiz*, 14/SN-17/ME 24. GP 2.

25) ErläutRV 160 BlgNR 24. GP 3.

26) ErläutRV 160 BlgNR 24. GP 3; vgl LAG München, 8. 7. 2009, 11 Sa 54/09, rechtskräftig (bestätigt fristlose Kündigung ohne Abmahnung eines Systemadministrators bei unbefugtem Zugriff auf E-Mail).

27) Gegen eine „Suche ins Blaue hinein" ohne tatsächliche Anhaltspunkte für eine schwere Pflichtverletzung auch *Steinkühler/Raif*, „Big Brother" am Arbeitsplatz – Arbeitnehmerüberwachung, AuA 2009, 213 (215).

28) Kasuistik ausführlich in *Ziehensack*, VBG Praxiskommentar (11. Erg Lfg) § 32 Rz 129 ff (gröbliche Dienstpflichtverletzung bejaht zB bei erheblichen Ehrverletzungen, Verletzung des Amtsgeheimnisses bzw Indiskretion, Fernbleiben vom Dienst oder bei dienstlichem Ungehorsam).

29) ErläutRV 160 BlgNR 24. GP 3.

30) OGH 9 Ob A 75/04a ARD 5552/16/2004 (kein Entlassungsgrund).

- Zu beachten ist ein absolutes Kontrollverbot von Inhalten übertragener Nachrichten[31] (§ 79e Abs 3 S 2 BDG).[32]

Relativiert wird dieses abgestufte Verfahren durch seinen Anwendungsbereich: Es kommt nur zum Einsatz, wenn sich der begründete Verdacht nicht gegen einen bestimmten Bediensteten richtet. Es ist davon auszugehen, dass sich ein begründeter Verdacht eines schweren dienstlichen Fehlverhaltens nicht selten gegen einen bestimmten Mitarbeiter wendet. Dann ist unter Beachtung von Verfahrens- und Transparenzpflichten der sofortige Zugriff auf die personenbezogenen Daten eines bestimmten Mitarbeiters zulässig (§ 79g Abs 7 BDG).

2.3. Exkurs: Begriff „Nachricht"

Unklar ist, ob die Bestimmungen der Novelle auch für E-Mails gelten, die über ein Intranet oder ähnliche Netzwerke übertragen werden.

Nachricht ist nach der Legaldefinition des § 79c Z 6 BDG „jede Information, die zwischen einer endlichen Zahl von Beteiligten über einen öffentlichen Kommunikationsdienst ausgetauscht oder weitergeleitet wird." Mit einem Intranet erbringt der Dienstgeber regelmäßig keinen öffentlichen Kommunikationsdienst. Das Kriterium der öffentlichen Zugänglichmachung nach § 79c Z 6 BDG iVm § 92 Abs 3 Z 7 TKG 2003[33] erfüllt der Arbeitgeber nach herrschender Meinung regelmäßig nicht, weil er den Internetzugang nur einem geschlossenen Benutzerkreis, nämlich den Mitarbeitern, zur Verfügung stellen will.[34] Dies unterstreicht auch die insoweit einschlägige Datenschutzrichtlinie für elektronische Kommunikation,[35] die sich ua in den Art 2 lit d, h und Art 3, 5 sowie in Erwägungsgrund 10 durchgängig auf öffentlich zugängliche Kommunikationsdienste und -netze bezieht; ausweislich § 92 Abs 1 TKG 2003 ist auf nicht öffentliche Kommunikationsdienste wie ein Intranet daher die Datenschutzrichtlinie,[36] umgesetzt im DSG 2000, anzuwenden.

De lege lata gilt folglich, dass der Dienstgeber mit dem Betrieb eines Intranets keinen öffentlich zugänglichen Kommunikationsdienst anbietet. Damit sind Inhalte übertragener Nachrichten nicht nach den §§ 79d ff BDG geschützt, wenn die E-Mail eines Bediensteten lediglich (behörden-)intern ohne Inanspruchnahme des allgemein zugänglichen Internets übertragen wird.

Das Ergebnis ist nicht zufriedenstellend, denn der Schutz von Inhaltsdaten vor einer Kontrolle am Arbeitsplatz wäre damit wiederum auf die allgemeinen Regelungen des DSG 2000 zurückgeworfen. Da aber gerade im öffentlichen Dienst eine fast nicht zu überblickende Anzahl von Behörden und staatlichen Einrichtungen auch ohne das allgemein zugängliche Internet digital miteinander vernetzt ist, erscheint das Überwachungspotenzial des Dienstgebers dem bloßen Umfang nach nicht gering. Beschäftigte sind deshalb auch vor einer unrechtmäßigen Kontrolle der in einem Intranet (zB Behördenverbundportal) übertragenen Inhalte mit speziellem Beschäftigtendatenschutzrecht zu schützen. Die mit der Novelle insofern drohende Schutzlücke sollte durch eine legistische Erweiterung des § 79c Z 6 BDG beseitigt werden.

2.4. Zwischenergebnis

Die Kontrollgrundsätze der Novelle sind charakterisiert durch das Modell der stufenweisen Kontrollverdichtung, das Eingriffe in den Datenschutz und das Kommunikationsgeheimnis der Bediensteten nur in der notwendigen Intensität zulässt. Für den einzelnen Dienstnehmer wird vorhersehbar beschrieben, welche Personen auf Dienstgeberseite unter welchen Voraussetzungen Kontrollmaßnahmen einleiten dürfen. Grundsätzlich mit Vorrang ausgestattet sind anonymisierte Auswertungen. Dank der Informationspflichten des Dienstgebers wird dem Mitarbeiter regelmäßig die Gelegenheit gegeben, sein Fehlverhalten einzustellen, ehe es zu einer individuellen Ausforschung seines Nutzungsverhaltens kommt. Zugleich sind expressis verbis legis weitere datenschutzrechtliche Grundprinzipien vorgesehen, die erforderlich sind, damit betroffene Bedienstete ihre Rechte überhaupt wahrnehmen können: Nimmt der Dienstgeber eine (an sich zulässige) Kontrolle der Nutzungsdaten eines betrieblichen Internetzugangs vor, so hat er dies dem Mitarbeiter gegenüber transparent zu stellen.[37] Flankierend ist die zuständige Beschäftigtenvertretung davon zu unterrichten. Des Weiteren können vermöge der Dokumentationsverpflichtungen Kontrollmaßnahmen des Dienstgebers besser nachgeprüft werden.

Lobend hervorzuheben ist auch der eindeutig festgeschriebene, umfassende Schutz von Inhaltsdaten, der insoweit die unausgereifte österreichische Rechtslage der §§ 92 ff TKG 2003 im Bereich von Beschäftigungsverhältnissen mit angemessenem Ergebnis konkretisiert und damit – neben dem Grundrecht auf Datenschutz – das Kommunikationsgeheimnis der Mitarbeiter (§ 93 TKG 2003 iVm Art 10a StGG[38]) stärkt.

Die Rechtslage nach der Novelle könnte damit grob wie folgt zusammengefasst werden: Inhaltsdaten der E-Mail- und Internetnutzung am Arbeitsplatz sind für den Dienstgeber in aller Regel tabu, denn bei berechtigtem Anlass genügen regelmäßig (bevorzugt anonymisierte) Verkehrsdaten, damit der Dienstgeber seine schutzwürdigen Interessen hinreichend wahrnehmen kann.

3. Modellcharakter der Novelle

Der Anwendungsbereich der vorgestellten Novelle erstreckt sich auf Bundesbedienstete gem BDG, VBG und RStDG. Die geltende Rechtslage für Bundesbedienstete ist grundsätzlich nicht mit der Situation im Arbeitsrecht der Privatwirtschaft zu vergleichen. Grundrechte der Bundesbediensteten entfalten gegenüber dem staatlichen Dienstgeber unmittelbare Wirkung.[39] Ein staatlicher Dienstgeber unterliegt deshalb einem strengeren Maßstab als private Arbeitgeber, die grundsätzlich nur eine mittelbare Wirkung der Verfassungsrechte erfahren (Ausnahme § 1 DSG 2000).[40] Nach § 79e Abs 1 BDG ist eine Kontrollmaßnahme des staatlichen Dienstgebers unzulässig, welche die Menschenwürde berührt.[41] Private Arbeitgeber hingegen können grundsätzlich

31) FN 23.
32) Krit *WKÖ*, 7/SN-17/ME 24. GP 3.
33) Telekommunikationsgesetz 2003 BGBl I 2003/70.
34) *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in *IT-LAW.AT* (Hrsg), E-Mail – elektronische Post im Recht, 91 f; *Hattenberger*, Die Bedeutung des Datenschutzrechts für das Arbeitsrecht, in *Resch* (Hrsg), Die Kontrolle des Arbeitnehmers vor dem Hintergrund moderner Medien, 21 ff; *Brodil*, Die Registrierung von Vermittlungsdaten im Arbeitsverhältnis, ZAS 2004, 17 (19); *Parschalk/Otto/Weber/Zuser*, Telekommunikationsrecht FN 671 auf S 209; im Ergebnis auch OGH 13. 6. 2002, 8 ObA 288/01p.
35) Datenschutz-RL für elektronische Kommunikation 2002/58 ABl L 2002/201, 37.
36) Datenschutz-RL 1995/46 ABl L 1995/281, 31.
37) Vgl § 24 DSG 2000.
38) Staatsgrundgesetz BGBl 1867/142 idF BGBl 1974/8.
39) Beachte in diesem Zusammenhang insb den engen Legalitätsvorbehalt des § 1 Abs 2 DSG 2000 sowie der EMRK; *Fellner* (Hrsg), BDG (FN 19).
40) Erforderlich sei deshalb eine grundlegende Differenzierung zum privatrechtlichen Bereich, meint *Stiger*, Protokollierung (FN 21) 420 ff.
41) Krit *WKÖ*, 7/SN-17/ME 24. GP 2.

die Verwendung der Betriebsmittel kontrollieren, soweit die Datenschutz- und Mitbestimmungsvorschriften (insb § 96 Abs 1 Z 3 ArbVG), das Grundrecht auf Datenschutz sowie das Kommunikationsgeheimnis und Persönlichkeitsrechte der Mitarbeiter beachtet werden.

Aufgrund dieser unterschiedlichen Ausgangslage ist eine (direkte) Analogie von Datenschutzbestimmungen aus dem Recht der Bundesbediensteten auf datenschutzrechtliche Fragestellungen im allgemeinen Arbeitsrecht ausgeschlossen.

Davon zu unterscheiden ist, ob die Regelungen der Novelle einen arbeitsrechtlich fairen Interessenausgleich von Nutzungs- und Kontrollmöglichkeiten unter Wahrung des Mitarbeiterdatenschutzes bewirken können. Für einen typischen Arbeitsplatz mit Internetzugang kann die Novelle insoweit weitgehend überzeugen. Arbeitgeber und Mitarbeiter können jeweils ihre Rechte und Pflichten im Umgang mit dem Betriebsmittel Internetzugang deutlich erkennen. Die Bestimmungen der Novelle, ob und inwieweit private Internetnutzung am Arbeitsplatz zulässig ist, überzeugen durch Augenmaß, sachliche Differenzierung und Verständlichkeit. Indem es insbesondere das Grundrecht auf Datenschutz und das Kommunikationsgeheimnis der Beschäftigten hinreichend zur Geltung bringt, erweist sich das abgestufte Verfahren als adäquat, nach dessen Maßgabe Arbeitgeber Kontrollmaßnahmen der Internetnutzung durchführen können.

Der Regelungsgegenstand der Novelle im Recht der Bundesbediensteten ist überwiegend mit identischen Rechts- und Wertungsfragen auch im Arbeitsrecht der Privatwirtschaft anzutreffen.[42] Die Bundesbediensteten können deshalb mit privatrechtlich Beschäftigten auf der einen Seite und der Staat in seiner Eigenschaft als Dienstgeber mit Arbeitgebern aus der Privatwirtschaft auf der anderen Seite grundsätzlich verglichen werden. Dies kann nicht gelten für Spezialbereiche des öffentlichen Bundesdienstes, wie zB die Innere und Äußere Sicherheit[43] oder die Finanzverwaltung.[44] Vor allem in Kernbereichen der Staatsordnung (insbesondere Verfassungsorgane) sind besondere Sicherheitserfordernisse zu berücksichtigen.[45]

Im Falle einer entsprechenden Gesetzesinitiative sollte der Gesetzgeber bereichsspezifische Datenschutzbestimmungen im allgemeinen Arbeitsrecht ausdrücklich als dispositives Recht einführen, soweit sie den Mitarbeitern eine Privatnutzung von Betriebsmitteln einräumen. Ansonsten würde wohl ein Arbeitnehmer(daten)schutz eingeführt, von dem nicht zum Nachteil der Arbeitnehmer abgewichen werden darf. Die Dispositionsfreiheit des Arbeitgebers über seine Betriebsmittel soll jedoch nicht durch die Hintertür mit datenschutzmotivierten Bestimmungen unterlaufen werden. Ein Primat für entsprechende freiwillige Regelungen auf Betriebsebene soll weiterhin gelten. Dem (privaten) Arbeitgeber soll deshalb die Möglichkeit vorbehalten bleiben, eine Privatnutzung des Internetzugangs ausdrücklich zu verbieten und dazu eine gesetzliche Regelung abzubedingen, welche die Zulässigkeit einer beschränkten Privatnutzung vermutet.[46] Wie in Kapitel 1 allerdings dargestellt, erscheint ein Verbot jeglicher Privatnutzung freilich weltfremd und im Übrigen rechtlich nur schwer durchsetzbar.[47]

4. Resümee

Ob das Reglement der Novelle – wie von der *Wirtschaftskammer Österreich* befürchtet – zB über die Judikatur des OGH das allgemeine Arbeitsrecht beeinflussen wird, bleibt zu beobachten.[48] Eine wesentliche rechtspolitische Zielsetzung hat der Gesetzgeber bei der Novelle wie folgt vorgegeben:

„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."[49]

Wünschenswert wäre, dass mehr Arbeitgeber die unübersichtliche Rechtslage erkennen, initiativ werden und auf Betriebsebene angemessene Regelungen für die Internetnutzung (Betriebsvereinbarung, Arbeitsvertrag oder Internet Policy) verankern. Zur Ausgestaltung kann die recht ausgewogene Novelle mit guten Anregungen dienen. Damit würden die Betriebe überfällige Orientierungspunkte für das Internetzeitalter am Arbeitsplatz schaffen. Insgesamt könnte sich so das folgende (leider im Gesetzgebungsverfahren gestrichene) Anliegen aus dem Ministerialentwurf zur Novelle ohne weitere gesetzgeberische Veranlassung erfüllen:

„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."[50]

42) Dahin gehend zB schon der Verweis bei der früheren RV zu § 79c BDG-alt auf § 96 ArbVG zum Thema, ob eine Kontrollmaßnahme die Menschenwürde berühre; vgl *Fellner* (Hrsg), BDG (FN 19).

43) Vgl *BM f Landesverteidigung u Sport*, 11/SN-17/ME 24. GP 3 ff.

44) Vgl DSK E K121.014/0008-DSK/2005.

45) Vgl FN 15.

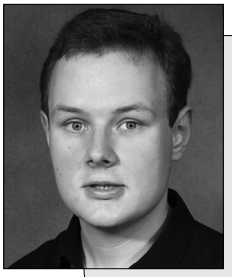
46) Vgl § 79d S 3 BDG 1979 („Die Beamten haben keinen Rechtsanspruch auf eine private IKT-Nutzung.").

47) So auch *Goricnik*, Zur Kontrolle (FN 6); aA zB *Wellhöner/Byers*, Datenschutz im Betrieb – Alltägliche Herausforderung für den Arbeitgeber?! BB 2009, 2310.

48) *WKÖ*, 7/SN-17/ME 24. GP 1.

49) ErläutRV 160 BlgNR 24. GP 2.

50) 17/ME 24. GP Vorblatt Mat.



Der Autor:
Dipl.-Wirt.Jur.(FH) *Thomas Hartmann*, LL.M. befasst sich seit Herbst 2009 im Projekt IUWIS der Deutschen Forschungsgemeinschaft an der Humboldt-Universität zu Berlin insbesondere mit der Entwicklung und Darstellung von Urheberrecht für Wissenschaft und Bildung. Nach einem Studium der Rechts- und Wirtschaftswissenschaften in Pforzheim absolvierte er im Studienjahr 2008/2009 den Universitätslehrgang für Informationsrecht und Rechtsinformation in Wien und war studienbegleitend zunächst beim Verein für Konsumenteninformation (VKI), später bei der Datenschutzkommission tätig.
Publikationen des Autors:
Konzernweiter Kundendatenschutz – mit oder ohne Codes of Conduct (CoC)? Die Kunden ernst nehmen bedeutet auch, Alternativen zu prüfen, DuD 2008, 455-460; Finanzberater dürfen Provisionen nicht verschweigen, Urteilsbesprechung BGH v. 20. 1. 09, Az. XI ZR 510/07, in: *Kolba, Peter* (Hrsg.), Informationen zum Verbraucherrecht 2009/3, 1.