

ZAS

[Zeitschrift für Arbeitsrecht und Sozialrecht]

Schwerpunkt

Neue Medien und Arbeitsrecht

- | | | |
|---|------------|---|
| Beiträge | 156 | Die Kontrolle der Nutzung neuer Medien im Arbeitsverhältnis
Wolfgang Brodil |
| | 167 | Die Überwachung der Internet-Kommunikation am Arbeitsplatz
Waltraut Kotschy, Sebastian Reimer |
| | 172 | Beweisverwertungsverbote im Arbeitsrecht?
Caroline Graf, Elisabeth Schöberl |
| Judikatur-
übersicht | 178 | Nr 101-128 |
| Recht-
sprechung
kommentiert | 183 | Klagemöglichkeit bei Ablehnung einer freiwilligen Leistung
Paul Haslinger |
| | 188 | EuGH zu Bereitschaftszeiten, Ruhezeiten und länger als 48-stündigen Wochenarbeitszeiten
Lukas Stärker |
| | 194 | Kündigungsschutz und Betriebspension
Theodor Tomandl |
| Muster | 200 | Rückersatz von Ausbildungskosten
Christoph Wolf |

Juli 2004

04
MANZ 

Schriftleitung
Theodor Tomandl
Martin E. Risak

Redaktion
Bernhard W. Gruber
Harald Kaszanits
Franz Schrank

ISSN 0044-2321

Die Überwachung der Internet-Kommunikation am Arbeitsplatz

Ein Diskussionsbeitrag aus datenschutzrechtlicher Sicht

Die Zahl der mit Internetzugang ausgestatteten Arbeitsplätze ist in stetem Steigen begriffen.¹⁾ Dadurch wird der Bedarf nach rechtlicher Klarheit über die Zulässigkeit der Aufzeichnung von Daten arbeitsplatzbezogener Internetaktivitäten, die zu einer Überwachung von Arbeitnehmern führen können, immer dringlicher.

Von Waltraut Kotschy und Sebastian Reimer

Inhaltsübersicht:

- A. Die Aufzeichnung von Kommunikationsdaten eines Arbeitsplatzes als Datenschutzproblem
- B. Beseitigung des Grundrechts auf Datenschutz durch privatrechtliche Disposition?
- C. Interessenabwägung in Lehre und Judikatur
- D. Modell stufenweiser Kontrollverdichtung als Ergebnis der Interessenabwägung
 1. Stufe 1: Maschinelle Überwachung zur Gewährleistung der Systemfunktionalität
 2. Stufe 2: Signifikante Abweichungen von der „normalen“ IT-Nutzung
 3. Stufe 3: Zugriff auf Kommunikationsdaten bei Verdacht auf (Vertrags-)Rechtsverletzung
 4. Grundsatz der Verhältnismäßigkeit und des gelindesten Mittels
 5. Anwendung des Stufenmodells in der Praxis
- E. Ergebnis

A. Die Aufzeichnung von Kommunikationsdaten eines Arbeitsplatzes als Datenschutzproblem

Für das Vorliegen eines datenschutzrechtlich relevanten Sachverhalts ist als Vorfrage zu klären, ob die Aufzeichnung von Kommunikationsdaten bei Internet oder E-Mail-Nutzung eine **Verwendung personenbezogener Daten** darstellt. Aufzeichnungen über die Kommunikation vom elektronischen Arbeitsplatz zum öffentlichen Netz (Internet), sog Logfiles, lassen die Zurechnung dieses Kommunikationsvorgangs zum account-Inhaber als Absender oder Empfänger der Nachricht zu. Sie stellen somit zumindest identifizierbare Daten iSd DatenschutzRL 95/46/EG²⁾ und des DSGVO 2000 (§ 4 Z 1) dar und sind daher personenbezogene Daten des account-Inhabers. Ist der Arbeitnehmer account-Inhaber, handelt es sich somit um dessen personenbezogene Daten.³⁾ Dass diese darüber hinaus auch personenbezogene Daten des Arbeitgebers sein können⁴⁾ ist kein Gegenargument: Dass eine Information personenbezogene Daten im Hinblick auf mehrere Personen (in unterschiedlichen Rollen) liefert, ist nichts Ungewöhnliches, sondern bei einer Kommunikation immer dann der Fall, wenn zumindest ein Sender und ein Empfänger vorhanden

sind.⁵⁾ Bei arbeitsrechtlicher Betrachtung wird jedoch die Betroffenheit der Datenschutzrechte außenstehender Kommunikationspartner des Arbeitnehmers (zB Kunden) leicht übersehen. Da aber bei der Aufzeichnung von Kommunikationsdaten deren Datenschutzrechte ebenfalls untrennbar mitbetroffen sind, ist dies in der Folge mit zu berücksichtigen. Daraus ergibt sich bspw, dass arbeitsvertragsrechtliche Einschränkungen des Gebrauchs von Kommunikationsmitteln auf dienstliche Kommunikationen und ein Verbot der Privatnutzung das Problem in seiner Gesamtdimension nicht lösen können, da dadurch die allenfalls bestehenden Rechte des außenstehenden Kommunikationspartners nicht beeinflusst werden können.

Jeder Gebrauch personenbezogener Daten – sofern es sich nicht um allgemein verfügbare oder um indirekt personenbezogene Daten handelt – stellt einen **Eingriff in das Grundrecht auf Datenschutz** dar (§ 1 Abs 1 DSGVO 2000). Dieser ist nur zulässig, wenn

- die Zustimmung aller (!) Betroffenen vorliegt oder
- die Verwendung im lebenswichtigen Interesse eines Betroffenen oder
- im überwiegenden berechtigten Interesse eines anderen notwendig ist.

Aber auch bei Vorliegen einer dieser Rechtfertigungsgründe ist die Datenverwendung dennoch nur in jenem Ausmaß zulässig, das zum (legitimen) Verwendungszweck verhältnismäßig ist, wobei das jeweils gelindeste zum Ziel führende Mittel anzuwenden ist.⁶⁾

1) In Österreich waren zum Jahr 2000 76 % aller Unternehmen mit Internetzugang ausgestattet (Quelle: New technology and respect for privacy at the workplace, EIROOnline, <http://www.eiro.eurofound.eu.int/print/2003/07/study/tf0307101.s.html>, aufgerufen am 7. 5. 2004).

2) RL des Europäischen Parlaments und des Rates vom 24. 10. 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr, ABl 1995 L 281 S 31–50.

3) Dass Verkehrsdaten als personenbezogene Daten iSd DSGVO 2000 anzusehen sind, darf als hL betrachtet werden (abl Rotter, Internetzugang für Arbeitnehmer, ASoK 1999, 118; krit Brodtil, Die Registrierung von Vermittlungsdaten im Arbeitsverhältnis, ZAS 2004/4).

4) Dabei ist zu beachten, dass in Österreich auch juristische Personen Datenschutz genießen.

5) Der Ansicht von Brodtil, ZAS 2004/4, dass sich bei dienstlich angewählten Rufnummern überhaupt die Frage erhebe, ob sie als personenbezogene Daten (des Arbeitnehmers) zu werten seien, kann nicht gefolgt werden. Es handelt sich um personenbezogene Daten sowohl des Arbeitnehmers als auch des Arbeitgebers wie des außenstehenden Kommunikationspartners.

6) Vgl § 1 Abs 2 DSGVO 2000 und die auf Eingriffe in das Grundrecht des Art 8 EMRK Bezug nehmende Judikatur des EGMR (Nachweise bei Wiederin, in Korinek/Holoubek, Österreichisches Bundesverfassungsrecht, Anm 26 ff zu Art 8 EMRK).

ZAS 2004/29

DSG 2000;
DatenschutzRL
95/46/EG

Datenschutz;
Kontrolle;
Internet;
E-Mail

Dies führt zur Frage, inwieweit zivilrechtliche, insb arbeitsrechtliche Vereinbarungen Eingriffe in das Grundrecht auf Datenschutz eines Vertragspartners rechtfertigen können.

B. Beseitigung des Grundrechts auf Datenschutz durch privatrechtliche Disposition?

In der Frage nach der Legitimation eines allfälligen Eingriffs in das Grundrecht auf Datenschutz sieht ein beträchtlicher Teil der Lit⁷⁾ die Zustimmung gem § 4 Z 14 DSGVO 2000 durchaus als geeignetes Legitimationsinstrument an.⁸⁾ Eine **Zustimmung des Arbeitnehmers** – innerhalb oder außerhalb des Arbeitsvertrags – kann jedoch in der Praxis auf Dauer keine brauchbare Rechtsgrundlage ergeben, da sie jederzeit widerrufen werden kann⁹⁾. Es ist uE Mayer¹⁰⁾ zu folgen, wenn er die datenschutzrechtliche Zustimmungserklärung von den zivilrechtlichen Willenserklärungen unterscheidet.

Im Übrigen wird es uU auch an dem Erfordernis der „freien Zustimmung“ iSd § 4 Z 14 DSGVO 2000 fehlen, da die Gefahr des Arbeitsplatzverlustes bei Nicht-Zustimmung die tatsächliche Freiwilligkeit einer erteilten Zustimmung fraglich erscheinen lässt.¹¹⁾ Weiters ist zu beachten, dass, wie oben (Pkt A) dargestellt, die Zustimmung des Arbeitnehmers allein die Aufzeichnung ohnehin in den wenigsten Fällen zulässig macht, da es idR immer an der Zustimmung des Kommunikationspartners mangeln wird. Demnach ist uE grundsätzlich davon auszugehen, dass **allein die Zustimmung des Arbeitnehmers die Erfassung seiner Kommunikationsdaten nicht rechtfertigen kann**.

Neben der Zustimmung des Betroffenen ist als weitere privatrechtliche Disposition noch das im vorliegenden Zusammenhang oft genannte **Verbot privater Internetnutzung** in Form einer Arbeitgeberweisung auf seine datenschutzrechtliche Relevanz hin zu untersuchen: Nach unbestrittener Ansicht¹²⁾ wird zwar das Bestehen eines rechtlichen Anspruchs des Arbeitnehmers auf Internetnutzung verneint, etwas uneinheitlich stellen sich jedoch die Meinungen zur Frage dar, ob und inwieweit der Arbeitgeber die private Internetnutzung verbieten kann.¹³⁾ Während die eine Ansicht¹⁴⁾, in Anlehnung an die zur Telefonüberwachung angestellten Überlegungen, von einem ausnahmsweisen Nutzungsrecht des Arbeitnehmers in dringenden privaten Angelegenheiten¹⁵⁾ ausgeht, wird dies von einer anderen Ansicht¹⁶⁾ mit Hinweis auf die Judikatur des VwGH¹⁷⁾, wonach das Eigentumsrecht des Arbeitgebers an der Telefonanlage ihn zur freien Verfügung darüber berechtige, verneint. Aus datenschutzrechtlicher Sicht ist an dieser Fragestellung aber nur entscheidend, ob aus der uE gegebenen Dispositionsbefugnis des Arbeitgebers eine umfassende, schrankenlose Kontrollbefugnis als Grund für Datenaufzeichnungen abgeleitet werden kann.¹⁸⁾ Dies ist mit Sicherheit zu verneinen, da aus einem privatrechtlich gültigen Verbot noch nicht die Zulässigkeit der Durchsetzung des Verbots unter Beseitigung von Grundrechtspositionen abgeleitet werden kann. Im Gegenteil: Da das Grundrecht auf Datenschutz ein Grundrecht mit Drittwirkung ist¹⁹⁾, ist es jedenfalls vom Arbeitgeber zu beachten.

Festzuhalten ist somit, dass kein Vorrang privatrechtlicher Willenserklärungen gegenüber grundrecht-

lichen Positionen besteht, da dies nur unter Annahme eines Vorrangs des Eigentumsrechts vor dem Grundrecht auf Datenschutz gerechtfertigt werden könnte. Grundrechtskonflikte können jedoch nicht dadurch gelöst werden, dass der Vorrang eines bestimmten Grundrechts vor anderen postuliert wird, sondern nur durch eine umfassende Interessenabwägung.²⁰⁾

Dabei können zwar überwiegende berechnete Interessen das Grundrecht auf Datenschutz einschränken, dies aber nur soweit **als die Einschränkung unbedingt notwendig ist**. Deshalb kann mit Sicherheit die Lösung nicht in einem unbeschränkten Ja oder Nein der Zulässigkeit der Datenverwendung gefunden werden. Sie ist infolge ihrer Natur als Grundrechtseingriff darauf zu prüfen, ob eine konkrete Maßnahme situationsangepasst und erforderlich ist. Deshalb ist es notwendig, sich mit der Typologie von Überwachungssituationen im betrieblichen IT-Gebrauch auseinander zu setzen, um daraus allenfalls ein Modell der **stufenweisen** Zulässigkeit von Kontrollmaßnahmen zu entwickeln (Pkt D).

C. Interessenabwägung in Lehre und Judikatur

Bei einer Abwägung rechtlicher Interessen sind in erster Linie grundrechtlich garantierte Positionen zu berücksichtigen. Auf Arbeitnehmerseite sind dies die Grund-

7) Dellisch, Private E-Mail- und Internetnutzung am Arbeitsplatz, ASoK 2001, 36; Kuderna, Die Zustimmung des Betroffenen zur Übermittlung von Daten, öRdA 1992, 421; Obereder, E-Mail und Internetnutzung aus arbeitsrechtlicher Sicht, öRdA 2001, 75; Wessely, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht?, ÖJZ 1999, 491.

8) Bei Verbot der privaten Internetnutzung geht Dellisch (ASoK 2001, 36) davon aus, dass es für die Aufzeichnung der Verkehrsdaten nicht einmal einer Zustimmung bedarf.

9) Vgl § 8 Abs 1 Z 2 und § 9 Z 6 DSGVO 2000, aber auch zB § 107 Abs 1 TKG 2003.

10) Mayer, Willensmängel im öffentlichen Recht – Zugleich ein Beitrag zur Auslegung des § 7 Abs 1 Z 2 DSGVO, eclex 1992, 812 mwN.

11) Streitberger, Privacy am Rechnerarbeitsplatz (2003) 19 (abrufbar unter http://www.rechtsprobleme.at/doks/privacy_arbeitsplatz-streitberger.pdf, aufgerufen am 7. 5. 2004); Mayer, eclex 1992, 812.

12) Dellisch, ASoK 2001, 36; Kraft, Internet und E-Mail am Arbeitsplatz, ARD 5481/11/2004.

13) Die Regelung der Internetnutzung kann sowohl durch Weisung als auch durch Betriebsvereinbarung erfolgen, wobei die Regelung der privaten Nutzung durch eine Betriebsvereinbarung gem § 97 Abs 1 Z 6 ArbVG, auf Grund des Merkmals „zweckentsprechend“, nicht ganz unumstritten ist (Dellisch, ASoK 2001, 36). Besteht kein Verbot des Arbeitgebers zur Internetnutzung, so ist davon auszugehen, dass eine nicht exzessive Nutzung erlaubt ist (vgl Brodill, Nutzung und Kontrolle von neuen Medien im Arbeitsrecht, eclex 2001, 853; Kraft, ARD 5481/11/2004; Obereder, öRdA 2001, 75; OGH 21. 10. 1998, 9 Ob A 192/98w, RdW 1999, 425, der davon ausgeht, dass private Telefongespräche von Arbeitnehmern in geringem Umfang nicht unüblich sind).

14) Vgl Dellisch, ASoK 2001, 36; Kraft, ARD 5481/11/2004; Laimer/Mayr, Rechtsprobleme der Internetnutzung am Arbeitsplatz, eclex 2003, 113; dies, Zum Spannungsverhältnis von Arbeitgeber- und Arbeitnehmerinteressen rund um die EDV-Nutzung, öRdA 2003, 410; Obereder, öRdA 2001, 75.

15) Dringende private Angelegenheiten, die trotz Verbot der privaten Nutzung ausnahmsweise eine solche legitimieren können, sind in ARD 5323/8/2002 angeführt.

16) Vgl Brodill, eclex 2001, 853; Rotter, ASoK 1999, 118; Thiele, Internet am Arbeitsplatz, eclex 2001, 613.

17) VwGH 9. 11. 1988, 86/01/0069, ARD 4069/7/89.

18) Zust VwGH 9. 11. 1988, 86/01/0069, ARD 4069/7/89; Rotter, ASoK 1999, 118; abl Obereder, öRdA 2001, 75.

19) Vgl § 1 Abs 5 DSGVO 2000, in dem durch eine Rechtswegeggarantie klar zum Ausdruck kommt, dass dieses Grundrecht gegenüber Privaten durchsetzbar ist, und zwar im Wesentlichen vor den ordentlichen Gerichten.

20) Berka, Die Grundrechte (1999) Rz 231.

rechte auf Datenschutz und Wahrung des Telekommunikationsgeheimnisses, auf Arbeitgeberseite vor allem das in Art 5 StGG normierte Grundrecht der Unverletzlichkeit des Eigentums. Außerdem werden die dem Arbeitsvertrag entspringenden Fürsorgepflichten des Arbeitgebers und die Treuepflicht des Arbeitnehmers genannt. Das spielerische Erlernen des Umgangs mit der neuen Technologie kann dabei jedoch kein berechtigtes Interesse des Arbeitnehmers für den nicht unmittelbar dienstlichen Gebrauch von IT-Ausstattung darstellen.²¹⁾

Die Abwägung dieser Interessenlagen führt in Judikatur und Schrifttum allerdings zu recht uneinheitlichen Ergebnissen: Als Grund für die Zulässigkeit der Aufzeichnung und weiteren Verwendung von Kommunikationsdaten werden etwa der Wunsch des Arbeitgebers nach einem funktionsfähigen Kommunikationssystem (freie Leitungen) oder das Ziel der Wirtschaftlichkeit des unternehmerischen Handelns, also Kontrollzwecke, anerkannt.²²⁾ Die Kontrollbefugnis, die geradezu typisch für ein Arbeitsverhältnis ist²³⁾, stellt nach Ansicht von *Obereder*²⁴⁾ hingegen kein überwiegendes, berechtigtes Interesse zur Protokollierung dar, da diesem Interesse auch durch Rundgänge des Arbeitgebers entsprochen werden kann. *Streitberger*²⁵⁾ sieht demgegenüber die Protokollierung als unerlässliches Instrument für die Wartung und Optimierung des Firmennetzwerkes, wobei er sogar die Personenbezogenheit für erforderlich hält. Aus dem Eigentum am Server leitet er auch das Recht des Arbeitgebers zur Kontrolle ab. Seiner Meinung nach macht das Interesse an der Einhaltung eines (teilweisen) Verbots bezüglich der privaten E-Mail-Nutzung eine umfassende Kontrolle notwendig.

D. Modell stufenweiser Kontrollverdichtung als Ergebnis der Interessenabwägung

Bei einer datenschutzrechtlichen Betrachtung muss zunächst davon abgegangen werden, die Datenarten (zB Verkehrsdaten versus Inhaltsdaten²⁶⁾ oder Daten über private Kommunikation versus Daten über dienstliche Kommunikation etc) als Ausgangspunkt der Betrachtung zu wählen. **Entscheidend für Zulässigkeit oder Unzulässigkeit einer Datenverwendung ist in erster Linie der Zweck, zu dem sie durchgeführt werden soll.** Während nämlich Daten eines Auftraggebers für einen bestimmten Zweck verarbeitet werden dürfen, kann die Verwendung derselben Daten beim selben Auftraggeber für einen anderen Zweck unzulässig sein. Welche Zwecke könnten dem Arbeitgeber also die Verwendung von Daten über die IT-Kommunikation auf Arbeitsplätzen erlauben und welche nicht?

1. Stufe 1: Maschinelle Überwachung zur Gewährleistung der Systemfunktionalität

Aus dem Grundrecht auf Eigentum ist zumindest mittelbar abzuleiten, dass der Arbeitgeber als Eigentümer der IT-Ausstattung am Arbeitsplatz ein Recht darauf hat, jene Maßnahmen zu ergreifen, die notwendig sind, um die **Funktionsfähigkeit des betrieblichen IT-Systems** zu gewährleisten. Die hierfür notwendigen Datenermittlungen über Inanspruchnahme und performance des Systems ist ihm – auch in personenbezogener (iden-

tifizierbarer) Form – erlaubt, soweit dies aus dem Zweck der Systemkontrolle und den damit verbundenen technischen Gegebenheiten unerlässlich bzw unvermeidlich ist. Die in der Literatur so heftig geführte Diskussion, ob die Aufzeichnung von Protokolldaten zulässig sei²⁷⁾, geht insofern datenschutzrechtlich ins Leere, als nicht die Aufzeichnung der Protokolldaten²⁸⁾ an sich einer Zulässigkeitsbeurteilung zu unterwerfen ist, sondern der **Zweck**, zu dem sie verwendet werden sollen: Dieser muss einem überwiegenden berechtigten Interesse zugeordnet werden können. Weiters ist zu prüfen, in welcher Weise die Daten für den angegebenen Zweck verarbeitet werden sollen, da hiebei der Grundsatz des gelindesten Mittels beachtet werden muss.

Die Kenntnisnahme von mit Hilfe der betrieblichen IT-Ausstattung durchgeführten Kommunikationsvorgängen zum Zweck der Gewährleistung der Funktionsfähigkeit des Systems stellt somit ein überwiegendes berechtigtes Interesse des Arbeitgebers dar. Doch sollte in dieser obersten Stufe der Systemüberwachung möglichst wenig menschliche Kenntnisnahme von IT-Gebrauchsdaten erfolgen – der **Grundsatz des gelindesten Mittels verlangt die maschinelle Routineprüfung** der Vorgänge, da diesfalls Kommunikationsdaten nur in Ausnahmefällen einem Organ des Dienstgebers bekannt werden.

Unter diesen Zulässigkeitsgrund („Gewährleistung der Systemfunktionalität“) sind alle Maßnahmen zur Abwehr von Viren und sonstigen Attacken Unbefugter auf das System einzureihen. Hier zeigt sich auch deut-

21) *Brodil*, *ecolex* 2001, 853; *Thiele*, *ecolex* 2001, 613; aA *Obereder*, *öRdA* 2001, 75.

22) Vgl *VwGH* 9. 11. 1988, 86/01/0069, *ARD* 4069/7/89.

23) *OGH* 13. 6. 2002, 8 Ob A 288/01 p, wbl 2003/353 (*Thiele*) = *öRdA* 2003/37 (*Preiss*) = *ZAS* 2004/4 (*Brodil*).

24) *ÖRdA* 2001, 75.

25) *Privacy am Rechnerarbeitsplatz* 24 ff.

26) So hält *Jahnel* (*Datenschutz im Internet*, *ecolex* 2001, 84) die Protokollierung der Verbindungsdaten, außer für Verrechnungszwecke und jedenfalls der Inhaltsdaten für datenschutzwidrig.

27) Dass die Protokollierung der Internetnutzung eine Kontrollmaßnahme sei, die die Menschenwürde berührt, wird überwiegend bejaht (BKA-Verfassungsdienst, ZI 810.233/003-V/3/01; *Dellisch*, *ASoK* 2001, 36; *Kraft*, *ARD* 5481/11/2004; *Laimer/Mayr*, *ecolex* 2003, 113; *dies*, *öRdA* 2003, 410; *Obereder*, *öRdA* 2001, 75; *OGH* 8 Ob A 288/01 p, wbl 2003/353 (*Thiele*) = *öRdA* 2003/37 (*Preiss*) = *ZAS* 2004/4 (*Brodil*); *Schwarz*, *Komm* zu *VwGH* 87/01/0034, *EDVUR* 1988, H 1, 26; *Teichmann*, *Komm* *VwGH* 87/01/0034, *öRdA* 1988/23) – andere Ansichten, die nicht von einer Berührung der Menschenwürde ausgehen, verweisen etwa auf die Unberührtheit des Fernmeldegeheimnisses bei Nichtprotokollierung der angewählten Telefonnummern (so etwa der *VwGH* 86/01/0069) bzw darauf, dass bei der Registrierung der Internetkontakte überhaupt keine personenbezogene Daten des Arbeitnehmers gespeichert werden (vgl *Rotter*, *ASoK* 1999, 118; *Brodil*, *ZAS* 2004/4). Letztgenannter Ansicht ist uE nicht zu folgen, da nach der klaren Definition des § 4 Z 1 DSG 2000 personenbezogene Daten, Angaben über Betroffene sind, deren Identität bestimmt oder bestimmbar ist (in diesem Sinne auch BKA-Verfassungsdienst, ZI 810.233/003-V/3/01; *Dellisch*, *ASoK* 2001, 36; *Stiger*, *Die Zulässigkeit der Protokollierung der Internetzugriffe von Dienstnehmern durch den Dienstgeber aus arbeits-, datenschutz- sowie telekommunikationsrechtlicher Sicht* (Masterthese 2000) 26; *Wessely*, *ÖJZ* 1999, 491).

28) Zu welchen mit der Realität nicht in Einklang zu bringenden Schlüssen eine Fixierung auf Datenarten in diesem Zusammenhang führt, zeigt zB *Gruber*, *Überwachung der dienstlichen Verwendung von Internet und E-Mail*, in *Österreichische Juristenkommission* (Hrsg), *Grundrechte in der Informationsgesellschaft* (2001) 172. Dieser bewertet Protokolldaten als „potentiell sensible Daten“, da die Daten sowohl sensibel (§ 4 Z 3 DSG 2000) als auch nicht sensibel sein können. Aus diesem Grund empfiehlt *Streitberger* (*Privacy am Rechnerarbeitsplatz* 15) auch auf Grund des gesetzlichen Schutzzwecks die generelle Behandlung der Protokolldaten als sensible Daten.

lich, dass bei dieser obersten Überwachungsstufe keine sinnvolle Unterscheidung zwischen der Behandlung dienstlicher oder privater Kommunikation getroffen werden kann. Der Grund der Überwachung, nämlich die Bedrohung der Systemfunktionalität, kann ja bei beiden Kommunikationsarten gleichermaßen eintreten. Auch der Streit, ob nur Verfahrensdaten oder auch Inhaltsdaten der Überwachung unterliegen können, geht am Problem vorbei²⁹⁾: Selbstverständlich muss zur Abwehr von Viren der Inhalt der Kommunikation geprüft werden – nur darf dies im Normalfall als gelindestes Mittel nur maschinell erfolgen, wozu ja auch zahlreiche Virenschutzprogramme entwickelt wurden und eingesetzt werden.

Soweit in diesem Zusammenhang überhaupt Menschen in Kenntnis von Kommunikationsdaten kommen dürfen – etwa zur Behandlung von Krisensituationen –, handelt es sich vor allem um jene Kategorie von Organen des Arbeitgebers, die in den ErlRV³⁰⁾ zu § 119 StGB als Systemadministratoren bezeichnet werden. § 119 StGB³¹⁾ betrifft die Strafbarkeit der Verletzung des Telekommunikationsgeheimnisses. Sie bringt zwar keine eindeutige Klarheit darüber, inwieweit der innerbetriebliche Teil einer Telekommunikation der Vertraulichkeit unterliegt, enthält aber eine wichtigen Hinweis auf die Wertungen des Gesetzgebers, da die Strafbarkeit von Datenermittlungen und -Weiterverwendungen an die Eigenschaft als „Unbefugter“ geknüpft ist. Den Materialien zur der diese Bestimmung einführenden Novelle des StGB BGBl I 2002/143 lässt sich – neben der zweifelsfreien Reduktion des Schutzgegenstands auf Inhaltsdaten – entnehmen, dass „Unbefugtheit“ eine andere Eigenschaft darstellt, als bloß „Nicht-Adressat der Nachricht“ zu sein: Der Hinweis in den Materialien, dass Systemadministratoren jedenfalls Befugte seien³²⁾, bedeutet, dass sich zumindest diese Personengruppe straffrei Kenntnis vom Inhalt von Nachrichten, die nicht für sie bestimmt sind, verschaffen kann. Da Systemadministratoren jeweils als Organ ihrem Arbeitgeber zuzurechnen sind, ergibt sich daraus wohl eindeutig, dass der Gesetzgeber davon ausging, dass ein Arbeitgeber jedenfalls hinsichtlich der üblicherweise von einem Systemadministrator wahrgenommenen Aufgaben Einblick in den Inhalt von Kommunikationen haben dürfe. Daraus leitet sich auch (argumento a maiore ad minus) die Strafflosigkeit der Kenntnisnahme von Verkehrsdaten durch den Systemadministrator ab.

2. Stufe 2: Signifikante Abweichungen von der „normalen“ IT-Nutzung

Bei der maschinellen Überwachung der Systemfunktionen fallen auch Daten an, die signifikante Abweichungen vom normalen IT-Gebrauch erkennen lassen. Dies führt üblicherweise zur Kenntnisnahme dieser Abweichungsdaten durch ein Organ des Arbeitgebers. Dem können nun auch Maßnahmen folgen, deren Zweck nicht mehr (nur) die Gewährleistung der Funktionsfähigkeit des Systems ist, sondern die Kontrolle von Arbeitnehmern. Dieser Zweck der Datenverwendung ist zweifellos datenschutzrechtlich kritischer als die generelle maschinelle Systemüberwachung, dennoch ist uE ein überwiegendes berechtigtes Interesse des Arbeitgebers an der Kenntnisnahme nicht zu ver-

neinen. Daraus folgt auch das Recht des Arbeitgebers, die Ursache der Abweichung zu ermitteln. In dieser Konstellation kann von einer ungerechtfertigten Datenermittlung durch den Arbeitgeber nicht gesprochen werden, da es die Treuepflicht des Arbeitnehmers erfordert, ihm zur Verfügung gestellte Arbeitsmittel nicht zum erheblichen Nachteil des Arbeitgebers, insb für nicht dienstliche Zwecke zu verwenden. Daraus folgt allerdings wiederum, dass nur erheblich kostenrelevante Abweichungen zum Anlass von verdichteter Kontrolle genommen werden dürfen.

Um in diesem Zusammenhang eine angemessene Interessenabwägung zu erzielen, ist es wichtig, die Grenzwerte für die Abweichung so zu definieren, dass die Abweichungskontrolle zu keiner unverhältnismäßige Kontrolle des Arbeitnehmers führt. Ein grundrechtsrelevantes Berühren der Menschenwürde ist insb dann anzunehmen, wenn die Maßnahmen beim Arbeitnehmer das Gefühl dauernd im Einsatz befindlicher Kontrolle hervorrufen.³³⁾ Das Bundeskanzleramt-Verfassungsdienst geht in Zl 810.233/003-V/3/01 davon aus, dass jede verdeckte Kontrollmaßnahme, insb solche zur qualitativen oder quantitativen Kontrolle der Arbeitsleistung an Bildschirmgeräten, als Maßnahme anzusehen ist, die die Menschenwürde berührt.³⁴⁾ Auch ausreichende Information über die Existenz von Kontrolle wird daher als Element einer verhältnismäßigen, den Grundsatz des gelindesten Mittels berücksichtigenden Kontrolle gewertet werden müssen.

3. Stufe 3: Zugriff auf Kommunikationsdaten bei Verdacht auf (Vertrags-)Rechtsverletzung

Aus einer Kontrollmaßnahme nach Stufe 2, aber auch aus besonderen externen oder betriebsinternen Ereignissen.

29) Die inhaltliche Kontrolle, worunter auch das Lesen der E-Mails verstanden werden muss, wird allgemein (*Dellisch*, ASoK 2001, 36; *Laimer/Mayr*, öRdA 2003, 410; Ablehnung nur bezüglich der rein privaten E-Mails: *Kraft*, ARD 5481/11/2004; *Obereder*, öRdA 2001, 75; *Thiele*, *ecolex* 2001, 613) abgelehnt, wobei es auch hier Gegenansichten gibt (etwa *Streltberger*, *Privacy am Internetarbeitsplatz* 30); *Laimer/Mayr*, öRdA 2001, 410, bejahen sogar einen Schutz von E-Mails durch § 118 StGB und sehen den Schutz des Briefgeheimnisses (Art 10 StGG) nicht nur für verschlüsselte, sondern auch für unverschlüsselte E-Mails. Zustimmung hinsichtlich verschlüsselter mails *Jahnel*, *ecolex* 2001, 84, wobei *Jahnel* nicht von der Anwendbarkeit des Art 10 StGG, sondern des Art 10 a StGG ausgeht; *Obereder*, öRdA 2001, 75; *Wagner*, Unbefugter Zugriff auf E-Mail, *ecolex* 2000, 273. Hinsichtlich unverschlüsselter Mails *Gassauer-Fleissner*, Geheimhaltung, Offenbarung und Veröffentlichung von Daten in Informationsnetzwerken, *ecolex* 1997, 102. AA *Wagner*, *ecolex* 2000, 273; *Obereder* öRdA 2001, 75.

30) ErlRV 1166 BlgNR 20. GP.

31) „Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation (§ 3 Z 13 TKG) oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.“

32) „Fallkonstellationen, in denen etwa Systemadministratoren befugterweise (den Inhalt von) E-Mails analysieren, sind – ohne dass dies ausdrücklich gesagt werden müsste – straffrei ...“

33) EA Linz 1985, ZAS 1986, 171.

34) Im Gegensatz zu § 96 Abs 1 Z 3 ArbVG sehen die §§ 79 c BDG, 29 n VBG, 76 g RDG vor, dass Kontrollsysteme, die die Menschenwürde berühren, nicht einer speziellen Zustimmung wie etwa durch die Personalvertretung bedürfen, sondern schlichtweg unzulässig sind. Vgl im Übrigen zur besonderen rechtlichen Situation im öffentlichen Dienst *Stiger*, Protokollierung der Internetzugriffe 32.

nissen kann sich der begründete Verdacht einer Dienstpflichtverletzung oder sogar einer strafrechtlich relevanten Handlung ergeben, die durch Gebrauch der betrieblichen IT-Ausstattung begangen wurde.³⁵⁾ Soweit zur Aufklärung des Verdachts der Zugriff auf Kommunikationsdaten – Verkehrsdaten wie auch Inhaltsdaten – notwendig ist, kann dem Arbeitgeber das Grundrecht auf Datenschutz nicht prinzipiell eingewendet werden, sondern nur allenfalls hinsichtlich der Einhaltung geeigneter Garantien für den Schutz des Betroffenen in der Durchführung der Kontrollmaßnahme. Als solche Garantien käme etwa die Beiziehung von Vertrauenspersonen wie betrieblichen Datenschutzbeauftragten oder Mitgliedern des Betriebsrats etc in Frage. Ein Monopol gerichtlicher Untersuchungsmaßnahmen kann dabei uE nicht erfolgreich behauptet werden, da § 119 StGB die Grenze zur unbefugten Kenntnisnahme von Kommunikationsdaten offenbar außerhalb des Arbeitsverhältnisses zieht.

4. Grundsatz der Verhältnismäßigkeit und des gelindesten Mittels

In jeder der drei Stufen der Kontrolle ist der für Grundrechtseingriffe maßgebliche Grundsatz der Verhältnismäßigkeit und das Gebot der Anwendung des jeweils gelindesten Eingriffsmittels zu beachten. Vor allem bei Kontrollmaßnahmen ist die dem österreichischen Recht immanente Wertung zu berücksichtigen, dass ein Eingriff in den **Inhalt einer Kommunikation** als **schwerwiegender** gewertet wird **als** die Kenntnisnahme von **Verkehrsdaten**. Die Einsicht von Organen des Arbeitgebers in Kommunikationsinhalte als Kontrollmaßnahme sollte daher auf die absolut notwendigen Fälle beschränkt werden.

Zusätzlich zu den oben dargestellten Grundsätzen der stufenweisen Kontrolle wäre hinsichtlich des Zugriffs auf fremde Web-Seiten zu sagen, dass es dem Arbeitgeber selbstverständlich erlaubt ist, den **Zugriff auf bestimmte Web-Seiten** von betrieblicher IT-Ausstattung aus zu **sperren**. Es ist dabei das gelindere Mittel, bei Zugriffsversuchen den Arbeitnehmer automatisch zu warnen, als die Zugriffe zu registrieren und ihn sodann „händisch“ abzumachen.³⁶⁾

Die **Befassung von Vorgesetzten des Arbeitnehmers** sollte jeweils erst erfolgen, wenn der Kontakt des Systemadministrators mit dem betreffenden Arbeitnehmer keine befriedigende Erklärung für die Abweichung im IT-Ressourcenverbrauch oder hinsichtlich des Verdachtsfalles ergeben hat. Über festgestellte, aber bereits im Gespräch mit dem Betroffenen zufriedenstellend aufgeklärte Kontrollanlassfälle sollte Verschwiegenheitspflicht des Systemadministrators bestehen.

5. Anwendung des Stufenmodells in der Praxis

Die Art und Weise und die Bedingungen, unter welchen das oben dargestellte Modell einer stufenweise verdichteten Kontrolle ausgeübt werden, sind für ein zufriedenstellendes Gesamtergebnis von entscheidender Bedeutung. Es kommt auf die angemessene Zeitdauer der Speicherung von Kommunikationsdaten ebenso an wie auf einen ausreichenden Informationsstand der Arbeitnehmer³⁷⁾ über die zu gewärtigenden Kontroll-

maßnahmen. Personen, die die Funktion von Systemadministratoren ausüben, sollte die Verantwortung ihrer Position besonders bewusst gemacht werden.³⁸⁾ Weiters ist ein Verfahren der Streitschlichtung vorzusehen. Dies und andere Details könnten sinnvollerweise zum Gegenstand von Betriebsvereinbarungen über den IT-Gebrauch am Arbeitsplatz gemacht werden.

Diese Grundideen haben auch bereits Eingang in die **Judikatur** gefunden: Der OGH³⁹⁾ schlägt zur ausgewogenen Berücksichtigung der beiderseitigen Interessen bei einer Telefon-Rufdatenerfassungsanlage vor allem den Abschluss einer Betriebsvereinbarung vor, in der die Nutzung der Anlage sowie Maßnahmen zum Schutz des Arbeitnehmers vor übermäßiger Kontrolle geregelt werden sollten. Den widerstreitenden Interessen soll dabei durch eine schrittweise Erhöhung der Kontrolldichte im Verdachtsfall entsprochen werden. Damit sei gesichert, dass keine überschießende⁴⁰⁾ Datenermittlung stattfindet, da immer nur so viele Daten ermittelt werden, als für die Verfolgung der legitimen Interessen des Arbeitgebers gerade benötigt werden. Erst bei Weiterbestehen der Verdachtsmomente sei bspw ein direktes Gespräch mit dem betroffenen Arbeitnehmer sowie allenfalls weitere Kontrollen denkbar. Die Einsicht in die Rufdaten sollte nur im Verdachtsfall und unter Beiziehung des Betriebsrates erfolgen.

Ein diesen Vorstellungen entsprechendes System wurde auch in praxi bereits in Form der *Instruction on the use of the Council of Europe's information system*⁴¹⁾ umgesetzt. In dieser Anordnung an die Bediensteten des Europarates werden diese zunächst davon informiert, dass der Gebrauch der IT-Ausstattung zum Zweck der Gewährleistung der Funktionsfähigkeit des Systems dauernd überwacht wird („*monitoring*“). Weiters festgehalten, dass ein privater Gebrauch der dienstlichen IT-Ausstattung erlaubt ist, soweit hiedurch weder die Erfüllung der Dienstpflichten des Betroffenen

35) Interessant erscheint in diesem Zusammenhang die Feststellung von *Jahnel*, Das Versenden von e-Mails aus datenschutzrechtlicher Sicht, in IT-LAW.AT (Hrsg), e-Mail, elektronische Post im Recht 89, wonach der Arbeitgeber als datenschutzrechtlicher Auftraggeber der E-Mails des Arbeitnehmers anzusehen sei; ähnlich *Streitberger*, Privacy am Rechnerarbeitsplatz 28. Dies würde die Rechtfertigung für Kontrollmaßnahmen stark untermauern, da aus der Auftraggebereigenschaft auch die Verantwortung für den Inhalt versendeter E-Mails abzuleiten ist.

36) Nach Ansicht *Stigers* (Protokollierung der Internetzugriffe 34) ist die Kontrolle der Internetzugriffe überschießend und daher ein unzulässiger Eingriff in das Grundrecht auf Datenschutz. Dem kann als Kontrollmaßnahme der Stufe 1 gefolgt werden; da kompromittierende Seiten ohnehin gesperrt werden können, sollte individueller Web-Gebrauch nur im Falle der Notwendigkeit von Maßnahmen nach Kontrollstufe 2 einer Überprüfung unterzogen werden.

37) Die Informationspflicht des datenschutzrechtlichen Auftraggebers gem § 24 DSGVO 2000 ist zu beachten, sodass bei einer Protokollierung der Verkehrsdaten über die Datenanwendung informiert werden müsste (vgl *Thiele*, *ecolox* 2001, 613 bzw *Streitberger*, Privacy am Internetarbeitsplatz 25).

38) *Streitberger* (Privacy am Internetarbeitsplatz 24) macht auf die Verpflichtung gem § 14 Abs 2 Z 7 DSGVO 2000 aufmerksam, wonach der Arbeitgeber auch zur Protokollierung seiner Kontrollzugriffe auf die Logfiles verpflichtet sei.

39) OGH 13. 6. 2002, 8 Ob A 288/01p, wbl 2003/353 (*Thiele*) = öRdA 2003/37 (*Preiss*) = ZAS 2004/4 (*Brodil*).

40) Überschießend ist ein Eingriff in das Grundrecht auf Datenschutz, wenn er nicht dem Gebot des gelindesten Mittels (§ 1 Abs 2 letzter Satz DSGVO 2000) entspricht, wenn also von den verschiedenen Eingriffsmöglichkeiten die zum Ziel führen, nicht die Option gewählt wird, die das Grundrecht am wenigsten beeinträchtigt.

41) In Kraft gesetzt durch den Generalsekretär des Europarates am 28. Okt. 2003. Der Europarat hat etwa 2000 Bedienstete.

noch die Funktionsfähigkeit des IT-Systems oder der gute Ruf des Europarates gefährdet sind. Die Bediensten dürfen auch als privat gekennzeichnete files einrichten, deren Vertraulichkeit grundsätzlich respektiert wird; die Notwendigkeit einer Einsichtnahme in besonderen Verdachtsfällen kann jedoch nicht ausgeschlossen werden. In Punkt 4.2 dieser *policy* wird zugesichert, dass das *monitoring* so weit als möglich automationsunterstützt und vor allem anonym – zu Zwecken der Überwachung der Systemleistung – durchgeführt wird. Personalisierte Überwachungen sind nicht vorgesehen, es sei denn, sie sind für den reibungslosen Betrieb des Systems, das Ansehen des Europarates oder die Einhaltung rechtlicher Bestimmungen erforderlich oder erfolgen auf Anweisung einer zuständigen Stelle. Telefonkommunikationen werden nur bei ungewöhnlich hohen Kosten überprüft. Die Kontrolle des E-Mail-Verkehrs ist in einem eigenen Absatz geregelt, wobei inhaltliche Kontrolle nur bei Verdacht der Handhabung illegaler Informationen und auf Anordnung einer zuständigen Stelle erfolgen kann. Im Fall einer solchen inhaltsbezogenen Kontrollmaßnahme wird – außer bei Gefahr im Verzug – der Betroffene und die Personalvertretung verständigt.

Dieses Beispiel zeigt, dass es durchaus möglich ist, Regeln über den IT-Gebrauch im Betrieb aufzustellen bzw zu vereinbaren, die einen fairen Interessenausgleich bewirken.

E. Ergebnis

Unter Aufrechterhaltung des grundsätzlichen Verfügungsrechts des Arbeitgebers über die von ihm zur Verfügung gestellte IT-Ausstattung kann den berechtigten Schutzanliegen der Arbeitnehmer vor unverhältnismäßiger Überwachung durch **stufenweise verdichtete Kontrolle** gut entsprochen werden, wobei von diesem Schutz nicht nur „private“ Kommunikation – die ohnehin ohne Inhaltsprüfung nicht verlässlich als solche erkannt werden kann – erfasst ist, sondern auch dienstliche Nachrichtenübermittlung. Unverhältnismäßig und damit auch datenschutzwidrig ist jedenfalls eine Kontrolle, die dem Arbeitnehmer den Eindruck vermittelt, unausgesetzter Überwachung zu unterliegen, deren Ergebnisse laufend ausgewertet werden und in die Beurteilung seiner Arbeitsleistung mit entsprechenden Konsequenzen und Sanktionen einfließen.

→ In Kürze

Die Aufzeichnung und Verarbeitung von Kommunikationsdaten des Arbeitnehmers kann datenschutzrechtlich *nicht* durch dessen diesbezügliche Zustimmung begründet werden, sondern nur durch eine Abwägung der Arbeitgeber- und Arbeitnehmerinteressen. Ergebnis dieser Interessenabwägung ist ein stufenweises Kontrollmodell, das auf jeder Stufe den Grundsatz der Verhältnismäßigkeit und das Gebot der Anwendung des jeweils gelindesten Eingriffsmittels zu beachten hat.

→ Zum Thema

Über den Autor:

Dr. Waltraut Kotschy ist Leiterin und Mag. Sebastian Reimer ist Mitarbeiter der Abteilung V/3 (Datenschutz, Geschäftsstellen des Datenschutzrates und der Datenschutzkommission, rechtliche Angelegenheiten der Verwaltungsreform) des Verfassungsdienstes des Bundeskanzleramts. Kontaktadresse: Ballhausplatz 1, A-1014 Wien. <http://www.dsk.gv.at>.

