Ortstagung Hamm am 18. September 2013

Am 18. September 2013 begrüßte *Dr. Holger Schrade*, Präsident des Landesarbeitsgerichts Hamm, den Referenten *Prof. Dr. Jacob Joussen*, Ruhr-Universität Bochum. In seinem Vortrag vor der Arbeitsgemeinschaft Hamm im Deutschen Arbeitsgerichtsverband e. V. setzte sich *Joussen* mit dem Thema „Compliance und Datenschutz beim Gebrauch von Kommunikationsmitteln im Arbeitsverhältnis“ auseinander und schlug - nach eigenen Worten - eine „Schneise“ in das Dickicht arbeitsrechtlichen Datenschutzes.

Joussens wesentliche Thesen lassen sich wie folgt zusammenfassen:

Das Thema „Datenschutz am Arbeitsplatz“ ist seit geraumer Zeit von dauerhafter Aktualität. Ausgelöst durch Überwachungsmaßnahmen von Arbeitgebern bestimmter Wirtschaftszweige hat der Gesetzgeber - bislang erfolglos - verschiedene Anläufe unternommen, ein umfassendes Regelungswerk zu schaffen. Derzeit kann im Arbeitsrecht im Wesentlichen nur auf die Regelung in § 32 BDSG zurückgegriffen werden. Trotz der weitreichenden Bedeutung dieser Vorschrift ist sie nicht immer ohne Weiteres anzuwenden. Im Rahmen der Nutzung von Kommunikationsmitteln ist gedanklich zunächst eine klare Trennlinie zu ziehen zwischen *dienstlicher* und *privater* Nutzung von Telefon, Mail und Internet. Ist nur eine dienstliche Nutzung gestattet, bestehen geringere Hürden für eine Kontrolle als bei einer erlaubten privaten Nutzung.

I. Vorbemerkungen

1. Der Ausgangspunkt: die Entscheidung des Arbeitgebers

Im Zentrum steht zunächst die Entscheidung des Arbeitgebers, im Rahmen des ihm zustehenden Weisungsrechts gemäß § 106 GewO eine private Nutzung von Kommunikationsmitteln überhaupt zu erlauben. Die private Nutzung elektronischer Ressourcen ist bei einer fehlenden ausdrücklichen Gestattung oder Duldung des Arbeitgebers grundsätzlich nicht erlaubt (vgl. BAG 7. Juli 2005 - 2 AZR 581/04 -). *Joussen* merkte an, dass der Arbeitgeber gut daran täte, die private Nutzung stärker oder auch generell zu untersagen. Hierdurch ließen sich zahlreiche rechtliche Probleme bereits vorab vermeiden. Doch sei klar, dass dies in der betrieblichen Praxis unrealistisch sei.

Neben dem einseitigen Gebrauch des Weisungsrechts durch den Arbeitgeber kommt zudem der Abschluss einer Vereinbarung in Betracht, sei es individualvertraglich oder durch Be-

triebsvereinbarung. Nach Auffassung *Joussens* können sich „Ob“ und „Wie“ des Gebrauchs von Kommunikationsmitteln auch aus betrieblicher Übung ergeben.

2. Der Arbeitgeber als Adressat des Telemediengesetzes/ Telekommunikationsgesetzes?

Zur Beantwortung der strittigen Frage, inwieweit der Arbeitgeber als etwaiger Adressat des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) die Nutzung von Kommunikationsmitteln kontrollieren kann und welcher Kontrollmaßstab anzulegen ist, ist auch insoweit eine Differenzierung zwischen der Kontrolle der *dienstlichen* Nutzung auf der einen und der *privaten* Nutzung auf der anderen Seite vorzunehmen.

Die Kontrolle von Kommunikationsmitteln bei deren rein dienstlicher Nutzung unterliegt nach wohl überwiegender Meinung nicht dem TMG und TKG. Der Arbeitgeber bietet in diesem Fall nicht geschäftsmäßig Dienste im Sinne der gesetzlichen Regelungen an (vgl. § 2 Nr. 1 und 2 TMG, § 3 Nr. 6 TKG). Stattdessen verbleiben die allgemein bestehenden Grenzen, vor allem die Regelungen in § 32 BDSG.

Im Fall privater Nutzung - soweit sie erlaubt ist - geht die wohl herrschende Auffassung im Schrifttum hingegen davon aus, dass der Arbeitgeber Diensteanbieter im Sinne des Telekommunikationsrechts ist. Betroffen ist nicht mehr das eigentliche Arbeitsverhältnis. Prinzipiell greift damit zum Teil Telekommunikationsrecht. Nach *Joussens* Auffassung ist die Anwendung des Telekommunikationsrechts auf diese Sachverhalte jedoch wenig überzeugend, da die entsprechenden Regelungen erkennbar nicht hierfür geschaffen worden sind.

II. Kontrollmöglichkeiten bei ausschließlich dienstlicher Nutzung

Bei ausschließlich dienstlicher Nutzung gilt an sich lediglich Datenschutzrecht und damit § 32 BDSG. Dennoch darf der Arbeitgeber nicht grenzenlos alles kontrollieren. Den Rahmen bilden stets das allgemeine Persönlichkeitsrecht des Arbeitnehmers und das darin enthaltene Recht auf informationelle Selbstbestimmung.

1. Die Kontrolle dienstlich geführter Telefonate

Im Rahmen der Kontrolle dienstlich geführter Telefonate ist zunächst das Fernmeldegeheimnis zu beachten (vgl. z. B. bereits BVerfG 20. Juni 1984 - 1 BvR 1494/78 -). Hier steht die Vertraulichkeit des gesprochenen Worts im Vordergrund. Nicht nur das Abhören, auch das Aufnehmen von Telefonaten stellt einen Eingriff in das allgemeine Persönlichkeitsrecht dar. Eingriffe sind nur selten gerechtfertigt.

Die strafrechtliche Grenze bildet - als hohe Hürde - § 201 StGB. Eine Rechtfertigung, gegebenenfalls gemäß § 34 StGB, kommt nur in wenigen Fällen in Betracht, wenn das Arbeitgeberinteresse überwiegt. Dies kann eventuell im Fall des Beweisnotstands angenommen werden und könnte in der Praxis beispielsweise bei Korruptionsfällen eine Rolle spielen.

Datenschutzrechtlich bildet § 32 Abs. 1 Satz 2 BDSG - als nicht ganz so hohe Hürde - die Grenze für Eingriffe in das Recht auf informationelle Selbstbestimmung des Arbeitnehmers.

2. Die Kontrolle dienstlicher E-Mails

Bei der Kontrolle dienstlicher E-Mails sind weder die Regelung in § 201 StGB noch die Regelungen im TMG bzw. TKG einschlägig. Anwendbar ist allein § 32 BDSG. Hier gelten im Wesentlichen die allgemeinen datenschutzrechtlichen Grundsätze (wie z. B. zur Geschäftspost). Hierbei sind nicht nur Rahmendaten kontrollfähig, sondern auch Inhalte, dies allerdings in Grenzen. Dem Arbeitgeber steht keine Vollkontrolle zu. Denn auch insoweit ist das Recht des Arbeitnehmers auf informationelle Selbstbestimmung zu beachten.

3. Die Kontrolle der Nutzung des Internets

Bezüglich der Kontrolle der Internetnutzung bestehen im Grundsatz keine Unterschiede zur Kontrolle dienstlicher E-Mails. Sonderfragen können sich zum Beispiel bei der Verwendung von Filtern ergeben.

III. Kontrollmöglichkeiten bei erlaubter privater Nutzung

1. Telefon- und Telefondatenüberwachung

Bei erlaubter Privatnutzung von Kommunikationsmitteln „mutiert“ der Arbeitgeber nach wohl überwiegender Auffassung im Schrifttum zum Diensteanbieter im Sinne des Telekommunikationsrechts. Es gilt unter anderem § 88 TKG:

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. …

…“

Der Arbeitgeber darf somit nicht mehr tun als zur Aufrechterhaltung der angebotenen Dienste erforderlich. Kontrollfähig sind nur abrechnungsrelevante Daten. Telefonnummern dürfen beispielsweise nicht gespeichert werden. Auch eine Anwendung der Regelung in § 32 BDSG führt zu keinem anderen Ergebnis.

2. Mail und Internet

Bei E-Mail und Internet ist im Fall erlaubter privater Nutzung weiter zu differenzieren, ob eine Kontrolle *während* oder *nach* dem Übermittlungsakt bzw. der Übertragung erfolgt. Das Bundesverfassungsgericht führt wie folgt aus (16. Juni 2009 - 2 BvR 902/06 - m. w. N.):

> „Der Grundrechtsschutz erstreckt sich nicht auf die außerhalb eines laufenden Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation. Der Schutz des Fernmeldegeheimnisses endet insoweit in dem Moment, in dem die E-Mail beim Empfänger angekommen und der Übertragungsvorgang beendet ist.“

Während des Übermittlungsakts ist wiederum § 88 TKG der Maßstab. Im Fall des Versands von E-Mails sind diese bis zur Ankunft beim Empfänger geschützt.

Nach der Übertragung ist Telekommunikationsrecht wiederum nicht anwendbar. Einschlägig ist § 32 BDSG. Nur äußere Daten sind kontrollfähig. Zudem muss ein berechtigtes Interesse des Arbeitgebers an der Kontrolle bestehen. Problematisch ist, wenn zwar eine E-Mail bereits den Empfänger erreicht hat, sich aber noch eine Kopie auf dem Server des Providers

befindet - vgl. auch insoweit die Entscheidung des Bundesverfassungsgerichts vom 16. Juni 2009 - 2 BvR 902/06 -:

> „Hierbei ist zu berücksichtigen, dass die Sicherstellung und Beschlagnahme von E-Mails- auf dem Mailserver des Providers in der Regel nicht heimlich, sondern offen vollzogen wird, die Daten punktuell und auf den Ermittlungszweck begrenzt außerhalb eines laufenden Kommunikationsvorgangs erhoben werden und der Betroffene Einwirkungsmöglichkeiten auf den von ihm auf dem Mailserver seines Providers gespeicherten E-Mail-Bestand hat."

Die Rechtslage ist schwierig, wenn eine Erlaubnis zur privaten Nutzung von E-Mail und Internet besteht, sie aber eingeschränkt erteilt wurde. Dies ist etwa bei Zeitfenstern der Fall, in denen eine private Nutzung erfolgen darf.

Kernproblem ist aber vor allem die Erkennbarkeit, ob eine E-Mail oder Internetnutzung dienstlicher oder privater Natur ist.

IV. Besonderheiten beim sog. „Bring your own Device"

Nutzen Arbeitnehmer eigene Kommunikationsgeräte, bringt dies in der praktischen Nutzung Vor- und Nachteile mit sich. Das Schrifttum hat sich - soweit erkennbar - bislang nicht eingehend mit dieser Thematik auseinandergesetzt. Fraglich ist, ob und inwieweit die Grundsätze im Fall der Gestellung von Kommunikationsmitteln durch den Arbeitgeber übertragen werden können.

1. Bestimmung der verantwortlichen Stelle im Sinne des BDSG

In jedem Fall ist hier der Arbeitnehmer „verantwortliche Stelle" im Sinne des § 3 Abs. 7 BDSG.

2. Arbeitsrechtliche Fragen

Die Nutzung von Geräten des Arbeitnehmers unterliegt nicht dem Weisungsrecht des Arbeitgebers. Erforderlich ist eine Vereinbarung, die gegebenenfalls dem Recht der Allgemeinen Geschäftsbedingungen unterliegt. Gegen die Möglichkeit des Abschlusses einer Betriebsvereinbarung könnten mangels Kompetenz des Betriebsrats Bedenken bestehen. Diese Frage ist jedoch strittig. In Betracht kommt als Grundlage § 87 Abs. 1 Nr. 6 BetrVG.

Das „Bring your own device“ wirft zahlreiche Fragen zum Inhalt einer abzuschließenden Vereinbarung, zu Haftung und etwaigen Ersatzansprüchen des Arbeitgebers (eventuell zu handhaben nach den Grundsätzen, die beispielsweise im Fall des Abhandenkommens eines Koffers auf der Dienstreise gelten) und - wohl kaum zu lösen - zum Arbeitszeitrecht auf. Auch hier problematisch ist die Abgrenzung privater und dienstlicher Nutzung.

3. Kontrollfragen

Die Kontrolle der Kommunikation durch den Arbeitgeber bei der Nutzung von Arbeitnehmergeräten ist grundsätzlich genauso zu behandeln wie im Fall der Nutzung von Arbeitgebergeräten.

a) Die Kontrolle des privaten Bereichs

Mangels in der Regel vorhandener Einwilligung des Arbeitnehmers richtet sich die Möglichkeit der Kontrolle des privaten Bereichs nach § 32 BDSG. An einer Rechtfertigung wird es mangels überwiegenden Arbeitgeberinteresses regelmäßig fehlen.

b) Die Kontrolle des dienstlichen Bereichs

Bei der Kontrolle des dienstlichen Bereichs ergeben sich keine Unterschiede zur Nutzung von Arbeitgebergeräten. Fraglich ist hier auch und insbesondere die Unterscheidung zwischen privatem und dienstlichem Bereich. Technisch dürfte ohne Weiteres eine Trennung möglich und ratsam sein.

V. Arbeitsrechtliche Folgen aus Verstößen gegen Datenschutzbestimmungen

1. Materiellrechtliche Folgen

Verstößt der Arbeitgeber gegen Datenschutzbestimmungen, könnte dem Arbeitgeber gemäß § 273 BGB - mangels Gegenseitigkeit nicht § 320 BGB - ein Zurückbehaltungsrecht zustehen, dann ist allerdings eine besondere Schwere der Pflichtverletzung zu verlangen.

2. Prozessuale Folgen: Beweisverwertungsverbot?

Rechtswidriges Verhalten einer Prozesspartei bei der Informationsgewinnung kann unter bestimmten Umständen zu einem Beweisverwertungsverbot führen. Dies ist dann der Fall,

wenn mit der gerichtlichen Verwertung ein erneuter Eingriff in rechtlich geschützte, hochrangige Positionen der anderen Prozesspartei oder die Perpetuierung eines solchen Eingriffs verbunden ist, und dies auch durch schutzwürdige Interessen der Gegenseite nicht gerechtfertigt werden könnte, vgl. hierzu die Entscheidung des Bundesarbeitsgerichts vom 16. Dezember 2010 - 2 AZR 485/08 - m. w. N.:

> „Dennoch kann rechtswidriges Verhalten einer Prozesspartei bei der Informationsgewinnung zu einem Verwertungsverbot führen. Das ist der Fall, wenn eine solche Sanktion unter Beachtung des Schutzzwecks der verletzten Norm zwingend geboten erscheint. In einem gerichtlichen Verfahren ist darauf Bedacht zu nehmen, dass das Gericht den Verfahrensbeteiligten in Ausübung staatlicher Hoheitsgewalt gegenübertritt. … Daraus folgt für den Zivilprozess zwar nicht, dass jede unzulässig erlangte Information prozessual unverwertbar wäre … Sie ist es im Einzelfall aber dann, wenn mit ihrer gerichtlichen Verwertung ein erneuter Eingriff in rechtlich geschützte, hochrangige Positionen der anderen Prozesspartei oder die Perpetuierung eines solchen Eingriffs verbunden wäre, und dies auch durch schutzwürdige Interessen der Gegenseite … nicht gerechtfertigt werden könnte …“

Aus einer datenschutzwidrigen Erlangung der auf einem Arbeitsplatzrechner vorgefundenen abgespeicherten Chatprotokolle folgt nach der Rechtsprechung des Landesarbeitsgerichts Hamm (10. Juli 2012 - 14 Sa 1711/10 -) insbesondere dann kein Beweisverwertungsverbot, wenn der Arbeitgeber seinen Arbeitnehmern lediglich eine gelegentliche private Nutzung elektronischer Ressourcen gestattet und zugleich darauf hinweist, dass bei einer Abwicklung persönlicher Angelegenheiten auf elektronischen Geräten und über das Netzwerk

- der Arbeitnehmer keine Vertraulichkeit erwarten und
- der Arbeitgeber die Nutzung überwachen und bei gegebener Notwendigkeit die Daten einsehen kann, die der Arbeitnehmer anlegt oder mit anderen austauscht.

Ein Arbeitnehmer muss, wenn er illegale Aktivitäten gegen seinen Arbeitgeber entwickelt, bei einer derart eingeschränkten Vertraulichkeit der Privatnutzung damit rechnen, dass Spuren, die er durch die Nutzung von elektronischen Ressourcen des Arbeitgebers hinterlässt, in einem Prozess gegen ihn verwendet werden.

Dem Vortrag *Joussens* folgte eine intensive Diskussion unter anderem zu Fragen der betrieblichen Übung, zur Betriebsratsbeteiligung, zur - auch faktischen - Durchsetzbarkeit von Verboten betreffend die private Nutzung von Kommunikationsmitteln sowie zur Handhabung bei Außendienstmitarbeitern und Dienstwagen mit GPS-Ortung.

Die Ortstagung schloss mit einem entspannten Austausch der Teilnehmer im Foyer des Landesarbeitsgerichts Hamm.

Dr. Derk Strybny
Richter am Arbeitsgericht, Münster