5. Ortstagung Kiel am 12. März 2014

I. Begrüßung

Der Einladung zur 5. Ortstagung des Deutschen Arbeitsgerichtsverbands e. V. in Kiel im Saal des Hauses des Sports folgten 55 Teilnehmerinnen und Teilnehmer. Rechtsanwalt Prof. Dr. Thomas Weiß eröffnete stellvertretend für die Präsidentin des Landesarbeitsgerichts Birgit Willikonsky sowie Peter Helbron (Vereinigung der Unternehmensverbände in Hamburg und Schleswig-Holstein e.V.) und Helmut Hüntling für (DGB-Rechtsschutz GmbH Region Nord) die Tagung und stellte den vortragenden **Prof. Dr. Matthias Jacobs**, Inhaber des Lehrstuhls ua. für Arbeitsrecht an der Bucerius Law School in Hamburg vor.

II. Vortrag: „Mitarbeiterüberwachung - rechtliche Grenzen unbegrenzte technische Möglichkeiten“

1. Formen der Mitarbeiterüberwachung

Formen der Mitarbeiterüberwachung sind die Überwachung der E-Mail-Kommunikation (direkter Zugriff auf E-Mail-Konten oder Speicherung von Verbindungsdaten), die offene oder verdeckte Videoüberwachung durch Monitoring bzw. Aufzeichnung, der automatisierte Datenabgleich (Überwachung durch kombinierte und automatisierte Untersuchung von Daten), die Verwendung von Ortungssystemen und schließlich der Einsatz biometrischer Verfahren (Überwachung durch Verifikation einer behaupteten Identität durch Überprüfung von physiologischen oder verhaltensbedingten Merkmalen).

2. Rechtsfolgen datenschutzrechtlicher Verstöße

Da das Datenschutzrecht „von hinten gedacht“ werden müsse, verweist Prof Jacobs insbesondere auf den Schmerzensgeldanspruch gemäß § 823 Abs. 1 BGB iVm. Art. 1, 2 GG/§§ 823 Abs. 2 BGB, 4 Abs. 1, 32 Abs. 1 Satz 2 BDSG (Hessisches LAG 25. Oktober 2010 - 7 Sa 1586/09 -, ArbG Frankfurt am Main 8. November 2013

- 22 Ca 9428/12 -), auf strafrechtliche Sanktionen gemäß § 44 Abs. 1 BDSG (BGH 4. Juni 2013 – 1 StR 32/10 -) und das gerichtliche Verwertungsverbot (BAG 20. Juni 2013 – 2 AZR 546/12 -; 16. Dezember 2010 - 2 AZR 485/08 –; 21. Juni 2012 - 2 AZR 153/11 -).

3. Verfassungsrechtlicher Grundkonflikt

Die rechtlichen Spielregeln für den Datenschutz beruhen auf dem verfassungsrechtlichen Grundkonflikt zwischen Arbeitnehmer- und Arbeitgeberrechten. Während sich Arbeitnehmer ua. auf das Recht der informationellen Selbstbestimmung (Art. 2 Abs. 1, 1 Abs. 1 GG) beziehen können, stehen dem auf Arbeitgeberseite ua. die Compliance-Anforderungen abgeleitet aus Art. 2 Abs. 1, 12 Abs. 1 und 14 Abs. 1 GG entgegen. Daraus folgt, dass das Recht der informationellen Selbstbestimmung nicht schrankenlos geschützt ist. Andererseits muss ein Eingriff hierein mittels Überwachung durch überwiegendes Arbeitgeberinteresse gerechtfertigt und damit gemessen an dessen Zweck verhältnismäßig sein. Er muss geeignet, erforderlich und angemessen sein. Als Erfahrungssatz kann gelten: Je intensiver der Eingriff, desto gewichtiger die rechtfertigenden Gründe.

Bei der Prüfung der Angemessenheit sind ua. die Nachteile des Eingriffs für den Mitarbeiter, der Nutzen des Eingriffs für den Arbeitgeber und die elektronische Verarbeitung der Daten zu berücksichtigen (vgl. BAG 21. Juni 2013 – 2 AZR 546/12 -).

4. Gesetzliche Lösung

Das Gesetz löst den Konflikt in § 4 Abs. 1 BDSG: Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist verboten, wenn kein Erlaubnistatbestand (Gesetz, Betriebsvereinbarung und Einwilligung) gegeben ist.

Gemäß § 32 Abs. 1 Satz 1 BDSG ist eine präventive Kontrolle zulässig, wenn die Kontrollmaßnahme für die Entscheidung, Begründung, für die Durchführung oder für die Beendigung des Beschäftigungsverhältnisses erforderlich ist. Entscheidender Maßstab ist ebenfalls die Verhältnismäßigkeit der Maßnahmen im konkreten Fall

(BAG 20. Juni 2013 – 2 AZR 546/12 -). Die Verhältnismäßigkeitsüberprüfung ist auch im Fall des § 32 Abs. 1 Satz 2 BDSG bei der Verfolgung von Straftaten maßgeblich.

Die Maßnahmen können auch durch Betriebsvereinbarung als Rechtsvorschrift iSd. § 4 Abs. 1 BDSG erlaubt sein. Allerdings ist der Gestaltungsspielraum durch § 75 Abs. 2 BetrVG begrenzt, die Wertungen des BDSG sind zu beachten und insbesondere auch der Verhältnismäßigkeitsgrundsatz (BAG 9. Juli 2013 – 1 ABR 2/13 (A)).

Die Einwilligung des Arbeitnehmers liegt vor, wenn sich dieser ohne Zwang und in Kenntnis der Sachlage frei entscheiden kann.

5. Die einzelnen Datenschutzkonstellationen

a) E-Mails

Die Überwachung der E-Mail-Kommunikation bei ausschließlich beruflicher Nutzung richtet sich nach § 32 Abs. 1 BDSG. Für die Angemessenheit gilt, dass grundsätzlich ein Interesse des Arbeitgebers an der geschäftlichen Korrespondenz besteht und das Persönlichkeitsrecht der Betroffenen mangels privater E-Mails vergleichsweise wenig tangiert ist.

Bei der Gestattung der E-Mail-Kommunikation auch zur privaten Nutzung richtet sich der Prüfungsmaßstab nach neuerer Instanzrechtsprechung ebenfalls nach § 32 Abs. 1 BDSG und nicht nach § 88 TKG (LAG Niedersachsen 31. Mai 2010 – 12 Sa 875/09 -).

b) Videoüberwachung

Bei der Videoüberwachung ist zwischen öffentlich zugänglichen und öffentlich nicht zugänglichen Räumen zu differenzieren.

Im ersteren Fall gilt § 6b BDSG. Bei offener Videoüberwachung ist eine Verhältnismäßigkeitsprüfung vorzunehmen. Dabei sind Aspekte wie Aufnahme oder Monito-

ring, Blickfeld der Kamera, Zoomfunktion, Häufigkeit der Aufnahmen, permanente oder zeitweilige Aufnahmen sowie Speicherung zu berücksichtigen.

Trotz des Wortlauts von § 6 b Abs. 2 BDSG ist eine verdeckte Videoüberwachung zulässig, wenn konkreter Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung bestehe und weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft worden seien. Die Überwachung darf insgesamt nicht unverhältnismäßig sein (BAG 21. Juni 2012 – 2 Sa 153/11 -).

Für die Überwachung in nicht öffentlich zugänglichen Räumen gilt wiederum § 32 Abs. 1 BDSG mit seiner Verhältnismäßigkeitsüberprüfung (BAG 26. August 2008 – 1 ABR 16/07 -; LAG Schl.-Holst. 29. August 2013 – 5 TaBV 6/13 -; LAG Köln 28. Dezember 2005 – 9 Ta 361/05 -).

c) Automatisierter Datenabgleich

Es gilt ebenfalls § 32 Abs. 1 BDSG. Die Angemessenheit erfordert einen konkreten Verdacht, andernfalls kommen allenfalls Stichproben in Betracht. Ferner sind die Zahl der Betroffenen, die Quellen, die Pseudonymisierung bzw. Anonymisierung der Daten, die Art der Informationen und die möglichen Folgen von Bedeutung.

d) Ortungssysteme

Im Rahmen der Angemessenheit gemäß § 32 Abs. 1 BDSG kommen wohl verdeckte Überwachung oder Dauerüberwachung nicht in Betracht, es sei denn dass ein konkreter Anhaltspunkt für Straftaten besteht (BGH 15. Mai 2013 – XII ZB 107/08 – und 4. Juni 2013 – 1 StR 32/13 -). Dagegen sind angekündigte, stichprobenartige, personenbezogene Kontrollen wohl zulässig.

e) Biometrische Verfahren

Bei der Angemessenheitskontrolle anhand § 32 Abs. 1 BDSG ist zu berücksichtigen, dass biometrische Daten datenschutzrechtlich besonders gefährlich sind. Eine ano-

nyme Speicherung von Vergleichsdaten kommt lediglich in Betracht zur Zuordnung zur zugangsberechtigten Gruppe. Eine verdeckte Erhebung ist unzulässig.

6. Schlussbemerkung

Aus Sicht von Prof. Jacobs sei das Datenschutzrecht gar nicht so schwierig, wenn man die Problemlage unter Berücksichtigung der verfassungsrechtlichen Grundkonstellation löse. Neue gesetzliche Regelungen seien angesichts der bestehenden Dogmatik nicht notwendig.

III. Abschließende Diskussion

Die Präsidentin des Landesarbeitsgerichts Willikonsky dankte Prof. Jacobs für den Vortrag und leitete über zu einer lebhaften Diskussion, wobei die Teilnehmer insbesondere datenschutzrechtliche Probleme aus der Praxis vorstellten und diskutierten.