Ortstagung Rhein-Main am 10. März 2010 in Frankfurt am Main

Am 10. März 2010 begrüßte Herr Dr. Peter Bader im gut besetzten Audimax des Hessischen Landesarbeitsgerichts in Frankfurt am Main den Referenten, Herrn Prof. Dr. Peter Wedde, Direktor der Europäischen Akademie der Arbeit in der Universität Frankfurt am Mainz. Dieser sprach zum Thema „Arbeitnehmerdatenschutz - Anforderungen aus der Praxis und juristische Reaktionsmöglichkeiten“.

In einem espritvollen faktenreichen Vortrag stellte Prof. Wedde mit viel Verve dem technisch Machbaren das rechtlich Zulässige gegenüber und warb für ein Arbeitnehmerdatenschutzrecht, das diesen Namen verdient.

Prof. Wedde begann mit Beispielen, wie sie Arbeitgebern und -nehmern regelmäßig begegnen:

> Der Arbeitgeber, der Daten von dem PC eines plötzlich für längere Zeit erkrankten Arbeitnehmers benötigt, weist seinen Systemadministrator an, dessen Passwort aufzuheben. Neben den gesuchten geschäftlichen Dateien werden mp3-Musikfiles gefunden. Da die private Nutzung des PC verboten ist, wird der Arbeitnehmer abgemahnt.
>
> Der Arbeitgeber ordnet an, dass während des Urlaubs oder anderer Abwesenheitszeiten eingehende E-Mails standardmäßig auf Accounts von Vertretern umgeleitet werden. Bei unvorhergesehener Abwesenheit wird die Umleitung von dem Systemadministrator eingerichtet. Der Mitarbeiter wird hierüber nicht benachrichtigt.

Zielsicher führte Prof. Wedde von dort auf die Datenschutzproblematik in multinationalen Konzernen. An Beispielen illustrierte er die Dringlichkeit und Explosivität des Themas:

Die Zentrale eines multinationalen Konzerns wird über eine „Whistleblowing-Hotline“ über Bestechungsvorwürfe in ihrer deutschen Niederlassung informiert. Ein von der ausländischen Zentrale beauftragtes Anwaltsbüro führt Untersuchungen durch. In diesem Zusammenhang werden die E-Mails von mehreren Dutzend Beschäftigten ausgewertet. Diese waren zuvor per Download auf ein Notebook der Rechtsanwälte übertragen worden.

In einem deutschen Konzern verlangt der Arbeitgeber vom Konzernbetriebsrat die Zustimmung, dass E-Mail-Accounts von Mitarbeitern in Deutschland auf Anforderung aus den USA kopiert und dorthin übermittelt werden dürfen. Zur Begründung verweist der Arbeitgeber darauf, dass ein US-Gericht dies in Zusammenhang mit Ermittlungen in einem Zivilverfahren angeordnet habe.

In einem großen Konzern sollen die EU-Anti-Terror-Verordnungen Nr. 2580/2001 und Nr. 881/2002 dadurch umgesetzt werden, dass die dort enthaltenen Daten mit den Informationen im zentralen Personal-informationssystem verglichen werden. Soweit Übereinstimmungen bestehen, sollen intern weitere Ermittlungen erfolgen. Die Betroffenen sollen nicht informiert werden. Ein Mitbestimmungsrecht wird nicht gesehen, da es sich um die Umsetzung gesetzlicher Vorgaben handele.

Die deutschen Unternehmen eines großen europäischen Konzerns haben ihren Betriebsräten mitgeteilt, dass das Unternehmen Daten ihrer Beschäftigten in die USA übermitteln bzw. Zugriffe von Sicherheitsbehörden auf die entsprechenden Datenbanken freigeben müsse, weil dies im Rahmen eines Angebots für einen Milliardenauftrag verlangt werde und ein Handlungsspielraum nicht bestehe.

Prof. Wedde machte deutlich, dass dieses ungeheure Informationsbedürfnis mit technischen Möglichkeiten einhergeht, es zu befriedigen. Nach dem Vortrag

blieben keine Zweifel mehr offen, dass bei Faxgeräten und -kopierern ebenso wie bei Telefonaten über das Internet nicht nur die Verbindungsdaten, sondern die Inhalte des gesendeten, kopierten und gesprochenen Wortes gespeichert werden können, dass durch den Einsatz von sogenannter „Spyware“ die vollständige Kontrolle jedes PC-Nutzers möglich ist, dass Navigationsgeräte und Mobiltelefone für Bewegungsprofile und eine GSM-Ortung der Mitarbeiter hergenommen werden können.

Dieser Situation, so Prof. Wedde, müsse sich ein Arbeitnehmerdatenschutzrecht stellen. Bislang seien die rechtlichen Rahmenbedingungen im Bereich des Arbeitnehmerdatenschutzes schwer überschaubar. Von fast allen Parteien im Bundestag seit 1992 immer wieder versprochen, sei nach wie vor der Inhalt eines Arbeitnehmerdatenschutzgesetzes umstritten. Zentrale Vorschriften zum Arbeitnehmerdatenschutzgesetz finden sich vor allem im BDSG, etwa zur Allgemeinen Zulässigkeit der Datenverarbeitung im Beschäftigungsverhältnis, § 4 Abs. 1 BDSG, zur Erforderlichkeit der freiwilligen Einwilligung des Arbeitnehmers, § 4a Abs. 1 BDSG, zum Grundsatz der Datenvermeidung und -minimierung, § 3a BDSG, zur Videoüberwachung in öffentlichen Räumen, § 6b BDSG, zum technischen und organisatorischen Datenschutz, § 9 BDSG, sowie zur Auftragsdatenverarbeitung, § 11 BDSG.

Ein besonderes Augenmerk lenkte Prof. Wedde auf den seit 1. September 2009 neu eingeführten § 32 BDSG und insbesondere dessen Abs. 1 Satz 2. Hier heißt es: „Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffenen im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.“ Prof. Wedde plädierte für eine restriktive Auslegung des Begriffs der Erforderlichkeit. Regelmäßig nicht

erforderlich seien beispielsweise die Erhebung und Verarbeitung von Daten aus der Privatsphäre oder zum Konsumverhalten, allgemeine Gesundheitsdaten sowie umfassende Nutzungsdaten von IT-Systemen.

Die häufig fehlende Sensibilität im Umgang mit Arbeitnehmerdaten, so beklagte Prof. Wedde, habe nicht zuletzt im staatlichen Bereich Vorbilder. In diesem Zusammenhang wies er auf den Einsatz von Ganzkörperscannern auf Flughäfen oder „ELENA“ hin.

Angesichts teilweise fehlenden Schutzes durch das BDSG hob Prof. Wedde die Bedeutung der Rechtsprechung hervor. Von zentraler Bedeutung seien die Vorgaben des Bundesverfassungsgerichts und des Bundesarbeitsgerichts zur Zulässigkeit heimlicher Kontrollen, dem Einsatz von Videokameras und anderen Überwachungstechniken sowie zur Zulässigkeit von allgemeinen Leistungs- und Verhaltenskontrollen. Er nannte die Entscheidungen des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung (1983), das die Verfügungsgewalt über eigene Daten impliziert, zur Vertraulichkeit von Telefongesprächen im Arbeitsverhältnis (1991) sowie zum Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme (2008). Weiter erörterte Prof. Wedde die Entscheidungen des Bundesarbeitsgerichts zur Unzulässigkeit des heimlichen Abhörens von Telefongesprächen im Arbeitsverhältnis und zum Schutz vor heimlicher und ausufernder Videoüberwachung. Als Resümee fasste er zusammen, dass heimliche und verdeckte Kontrollen im Arbeitsverhältnis immer unzulässig seien, offene Kontrollen nur erfolgen dürften, wenn sie objektiv notwendig seien und mildere Mittel dem Arbeitgeber nicht zur Verfügung stünden. Ein Kernbereich persönlicher Daten müsse für den Arbeitgeber unantastbar sein.

Prof. Wedde griff abschließend drei besonders häufig diskutierte Einzelthemen heraus:

1. Kontrollbefugnisse des Arbeitgebers nach einem Verbot der privaten Internet-

Nutzung

Eindrucksvoll stellte Prof. Wedde klar, dass auch nach einem Verbot der Privatnutzung nicht alle Kommunikationsvorgänge dienstlicher Natur sind. Als Beispiele nannte er die Korrespondenz mit dem Betriebsarzt oder Betriebsrat sowie Zugriffe auf Web-Seiten mit vertraulichem Charakter, wie etwa Sucht-Hilfen oder Gewerkschaften. Wenn nach dem Verbot der Privatnutzung auf „rein dienstliche“ Kommunikationsinhalte zugegriffen werden solle, müsse, so Prof. Wedde, vom Arbeitgeber sichergestellt werden, dass „persönliche“ Daten, wie die beispielhaft herausgegriffenen von diesem Zugriff ausgenommen bleiben, weil es für einen Zugriff auf „dienstlich persönliche“ Daten an der rechtlichen Begründung gemäß § 4 Abs. 1 BDSG fehle. Arbeitnehmern verbleibe regelmäßig ein geschützter Bereich „persönlicher Kommunikation“, den der Arbeitgeber nicht kontrollieren dürfe. Soweit Arbeitgeber zu Kontrollen berechtigt seien, finde das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG Anwendung.

2. Umgang mit Arbeitnehmerdaten im Konzernbetriebsrat

Prof. Wedde führte aus, dass dem großen Interesse in Konzernen, Aufgaben zu zentralisieren, kein konzernweites Datenverarbeitungsprivileg gegenüberstehe. Vielmehr bedürfe es für übergreifende Datenverarbeitung entweder eines Auftrags nach § 11 BDSG oder einer Funktionsübertragung. Letztere sei im BDSG nicht enthalten. Sie führe - das der entscheidende Unterschied zur Auftragsverarbeitung - dazu, dass nach einer Funktionsübertragung die beauftragte Stelle allein für die datenschutzkonforme Durchführung der übernommenen Aufgaben verantwortlich ist. Ihre Zulässigkeit setze voraus, dass das Datenschutzniveau bei der neuen verantwortlichen Stelle dem im eigenen Betrieb entspreche. Der Betriebsrat des Daten abgebenden Unternehmens müsse umfassende Kontrollbefugnisse bei dem neuen Verarbeiter haben, Betriebsvereinbarungen des Daten abgebenden Betriebs könnten Verarbeitungsbefugnisse regeln.

3. Googeln von Bewerbern

Für das weit verbreitete „Googeln“ von Bewerbern fehle es an einem Rechtsgrund i. S. v. § 4 Abs. 1 BDSG. Es sei unzulässig. Erfolge es dennoch, müsse eine gesetzeskonforme Information der Bewerber erfolgen (§ 33 Abs. 1 BDSG), andernfalls ein Rechts- und Compliance-Verstoß vorliege.

Nach seinem fakten- und facettenreichen Vortrag zog Prof. Wedde den Schluss, dass sowohl das aktuelle Bundesdatenschutzgesetz als auch die Hinweise aus der Rechtsprechung nur einen begrenzten Arbeitnehmerdatenschutz schafften. Ein wirksamer Arbeitnehmerschutz bestehe derzeit nicht.

Dr. Silke Kohlschitter
Richterin am Arbeitsgericht, Frankfurt am Main