„Videoüberwachung – biometrische Zugangssysteme – Chipkarten – Wie viel Kontrolle braucht der Arbeitgeber wirklich?“

Vortrag im Rahmen des Expertengesprächs „Arbeitnehmerdatenschutz“

am 28.6.2010

in Berlin

von Prof. Dr. Peter Wedde / Frankfurt

Inhalt

1. Allgemeines zum Referentenentwurf

- Ziele des Entwurfs – Schutz der Arbeitnehmer
  - Beschäftigte sollen vor der unrechtmäßigen Erhebung und Verwendung ihrer personenbezogenen Daten geschützt werden.
  - Für Zwecke des Beschäftigtenverhältnisses sollen nur solche Daten verarbeitet werden dürfen, die für diese Verhältnisse auch erforderlich sind.
  - Beschäftigten sollen wirksam vor Bespitzelungen geschützt werden.

Allgemeines zum Referentenentwurf

- **Ziele des Entwurfs - Schutz der Arbeitgeber**
  - Arbeitgebern soll eine verlässliche Grundlage für die Durchsetzung von Compliance-Anforderungen und den Kampf gegen Korruption an die Hand gegeben werden.

- **„Ausgleichsfunktion" der Regelung**
  - **Beschäftigte** sollen vor der unrechtmäßigen Erhebung und Verwendung ihrer personenbezogenen Daten **geschützt werden, gleichzeitig** soll das **Informationsinteresse des Arbeitgebers** Beachtung finden, um so ein **vertrauensvolles Arbeitsklima** zwischen Arbeitgebern und Beschäftigten am Arbeitsplatz zu **unterstützen**.

Der erste Eindruck

- Der Gesetzesentwurf
  - legt als Maßstab der Zulässigkeit nicht den Beschäftigtendatenschutz an,
  - sondern den Schutz vor (schwerwiegenden) Vertragsverletzungen zu Lasten des Arbeitgebers.

Die Umsetzung der Schutzziele in Zahlen

- Der Referentenentwurf enthält in Gesetzestext und Begründung wichtige Begriffe in unterschiedlicher Zahl
  - **6 x** „Beschäftigtendatenschutz"
  - **11 x** „Schutzwürdige Interessen der Beschäftigten"
  - **3 x** „Korruption"
  - **4 x** „Compliance"
  - **14 x** „Vertragsverletzungen / schwerwiegende Vertragsverletzungen zu Lasten des Arbeitgebers"

Das Problem

- Einen wirklich wirksamen Beschäftigtendatenschutz erzeugt der Entwurf nicht.
- Viele Probleme bleiben unerwähnt.
- Erwähnte Probleme werden aus Sicht von Beschäftigten nicht zufriedenstellend gelöst.
- Dies wiegt vor dem Hintergrund der Tatsache schwer, dass die bekannt gewordenen Datenschutzskandale nur ein Teil des Problems sind.

2. Wie viel Kontrolle braucht der Arbeitgeber ?

- Kontrollmöglichkeiten unter Zugriff bzw. Verwendung personenbezogener sind in einigen Bereichen aus objektiver Sicht notwendig.
- Etwa
  - Banken
  - Sensible oder kritische Produktionsprozesse
  - Verkehrseinrichtungen usw.

Gründe für Kontrollen ...

... sind vielfältig

☞ Etwa

- Diebstahlschutz
- Absicherung von Beschäftigten
- Absicherung von Eigentum
- Notwendige Dokumentation usw.

Grenzen für Kontrollen ...

... leiten nach der Rechtsprechung von BAG und BVerfG insbesondere aus dem Persönlichkeitsrecht der Beschäftigten ab.

☞ Die Rechtsprechung verlangt beispielsweise

- den Ausschluss von Totalkontrollen bzw.
- von heimlichen Kontrollen sowie
- eine Begrenzung auf das mildeste Kontrollmittel.

☞ Diesen Vorgaben müsste auch ein Arbeitnehmer-datenschutzgesetz gerecht werden, wenn es seinen Namen berechtigt tragen wollte.

2.a. Wie viel Kontrolle braucht der Arbeitgeber durch Videoüberwachung?

Der „Schutz" vor unzulässiger Videoüberwachung ist geregelt in § 32f RefEntwBDSG

- **Abs. 1: Zulässigkeit**
  - Videoüberwachung ist **beispielsweise** zulässig zur Wahrung wichtiger betrieblicher Interessen wie etwa
    - Schutz des Eigentums (Nr. 3),
    - Sicherheit der Beschäftigten (Nr. 4) oder
    - Abwehr von Gefahren für die Sicherheit des Betriebs (Nr. 6).
  - **Grenze:** Überwiegen des schutzwürdigen Interesses der Betroffenen

Zulässige Videoüberwachung nach § 32f

- **Abs. 2: Heimliche Videoüberwachung**

  Voraussetzung:
  - Tatsächlicher Anhaltspunkte
  - begründen einen konkreten Verdacht
  - einer Straftat oder einer schwerwiegenden Vertragsverletzung zu Lasten des Arbeitgebers (Wichtiger Grund § 626 BGB).
  - Erhebung muss verhältnismäßig sein und
  - unterliegt der Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten

Unzulässige Videoüberwachung / Löschung der Daten

- **§ 32f Abs. 3: Unzulässige Videoüberwachung**
  - Betriebsstätten, die der privaten Lebensgestaltung dienen sowie
  - Sanitär-, Umkleide- und Schlafräume **bleiben ausgenommen**.
- **§ 32f Abs. 4: Löschung**
  - Daten sind **unverzüglich zu löschen**,
  - wenn der Zweck erreicht ist oder
  - wenn schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegen stehen.

Ist damit eine Verbesserung des Schutzes vor unzulässigen Videokontrollen erreicht?

- Wie wären Fälle der Videoüberwachung aus Vergangenheit und Gegenwart nach neuem Recht zu beurteilen?

1. **LIDL u.a.**

   Ein zentrales Argument für den heimlichen Kameraeinsatz bei LIDL war der Schutz vor Diebstählen. Ähnlich haben andere Firmen wie etwa IKEA oder Burger King argumentiert.

2. **Gebäudeüberwachung grenzenlos**

   In einem multinationalen IT-Konzern obliegt die umfassende Videoüberwachung aller Gebäude schon lange einem autonomen Konzernunternehmen. Bisher erfolgte die Überwachung in den Gebäuden. Seit einigen Monaten wird diese Aufgabe zentral aus Spanien wahrgenommen. Der Arbeitgeber vertritt die Auffassung, dass die Verlagerung der Technik nicht mitbestimmungspflichtig ist. Eine Information der Beschäftigten über das „Wie" und den Umfang der Kontrollen gibt es nicht.

Nach § 32f zulässig oder nicht?

- LIDL könnte etwa nach § 32 Abs. 1 Nr. 3 i.V.m. Abs. 2 Satz 1
  - zumindest für Filialen mit hohen Schwundquoten
  - tatsächliche Anhaltspunkte darlegen,
  - die den Verdacht begründen,
  - dass möglichweise auch Beschäftigte Straftaten begehen,
  - die zur fristlosen Kündigung berechtigen.
- Damit wäre möglicherweise ein Teil der Überwachungen aus der Vergangenheit heute legal.

Nach § 32f zulässig oder nicht?

- Der multinationale IT-Konzern könnte nach § 32 Abs. 1 Nr. 3 und Nr. 6
  - in jedem Fall die Kameraüberwachung rechtfertigen und
  - beim Vorliegen von Verträgen gemäß § 11 BDSG die Verlagerung der Kontrollmaßnahmen ins Ausland legal durchführen.
- Ein Überwiegen der schutzwürdigen Interessen der Betroffenen ist nicht offenkundig.
- Damit wäre dieses Vorgehen möglicherweise sehr viel klarer zulässig als nach derzeitigem Recht.

2.b. Wie viel Kontrolle braucht der Arbeitgeber durch biometrischer Zugangssysteme?

Der „Schutz" vor unzulässigen biometrischer Verfahren ist geregelt in § 32h RefEntwBDSG

- **Abs. 1: Zulässigkeit**
  - Biometrische Merkmale dürfen vom Arbeitgeber genutzt werden,
    - soweit dies aus betrieblichen Gründen zu Autorisierungs- und Authentifikationszwecken erforderlich ist.
    - **Grenze:** Überwiegen des schutzwürdigen Interesses der Betroffenen.
    - Vorhandene Fotos dürfen mit Einwilligung für andere Zwecke verarbeitet werden.
- **Abs. 2: Löschung**
  - Biometrische Daten sind zu löschen,
    - wenn sie nicht mehr erforderlich sind oder
    - wenn schutzwürdige Interessen entgegenstehen

Ist damit eine Verbesserung des Schutzes vor unzulässige Verwendung biometrischer Daten erreicht?

- Wie wären Fälle der Verwendung biometrischer Daten aus Vergangenheit und Gegenwart nach neuem Recht zu beurteilen?

1. **Mehr Sicherheit durch Iris-Scan**

   In einem Hochsicherheitszentrum soll die seit mehr als zehn Jahren bewährte Tastatureingabe zur Türöffnung durch eine Fingerabdruck-Scan-Anlage ersetzt werden. Die Daten des Abdrucks werden „im Klartext" gespeichert und können ausgelesen werden. Der Betriebsrat hat einen unzulässigen Eingriff in Persönlichkeitsrechte gesehen und die Zustimmung erfolgreich verweigert. Es wurde eine neue Tastaturanlage eingeführt.

2. **Mehr Transparenz für Kunden**

   Ein großes Vertriebsunternehmen will transparenter für Kunden werden. Deshalb wird von allen Mitarbeitern mit Kundenkontakten verlangt, dass sie Fotos auf die im Internet zugänglichen Firmenseiten stellen. Dies funktioniert auf der Grundlage einer „freiwilligen Einwilligung". Beschäftigten, die die Einwilligung verweigert haben, wurde signalisiert, dass dann keine Weiterbeschäftigung im kundennahen Bereich mehr möglich sei.

Nach § 32h zulässig oder nicht?

- Der Iris-Scan wäre nunmehr nach § 32h Abs. 1 Satz 1
  - möglicherweise zulässig, wenn der Arbeitgeber betriebliche Gründe vorträgt und
  - Beschäftigte nicht darlegen können, warum ihre schutzwürdigen Belange überwiegen.
- Die neue Regelung beseitigt damit nicht die bestehenden Unklarheiten und stärkt keinesfalls die Rechte der Beschäftigten.
- Sie normiert aber die Zulässigkeit des Einsatzes entsprechender Verfahren im arbeitsrechtlichen Bereich und schafft damit eine grundsätzliche Erlaubnisnorm für Arbeitgeber.

Nach § 32h zulässig oder nicht?

- Das Vertriebskonzern könnte nach § 32h Abs. 1 Satz 2 von seinen Beschäftigten eine Einwilligung verlangen.
- Da der Schutz vor „erzwungenen Einwilligungen" im Entwurf nicht gesichert ist, kann von einer Schaffung eines Arbeitnehmerdatenschutzes in diesem Punkt nicht die Rede sein.
- Problematisch ist aber auch bezüglich der Fotos, dass Arbeitgebern mit dieser neuen Norm ausdrücklich die Befugnis auf der Basis einer Einwilligung zugestanden wird, ohne dass zugleich ein adäquater Schutz der Beschäftigten verankert wurde.

2.c. Wie viel Kontrolle braucht der Arbeitgeber durch Chipkarten und Ortungssystemen?

- Der Schutz vor einem unzulässigen Einsatz von Chipkarten ist im Entwurf nicht ausdrücklich normiert.
- Regelungen hierzu finden sich in § 6c BDSG und sind nach § 32 Abs. 2 RefEntwBDSG weiter anwendbar.
- Regelungen zum Schutz vor einem unzulässigem Einsatz von Ortungssystemen finden sich in § 32g

Chipkarteneinsatz - § 6c BDSG

- **Abs. 1: Informationspflichten**
  - Die verantwortliche Stelle muss Sachinformationen über verwendete Chipkarten geben.
- **Abs. 2: Auskunftsrecht**
  - Die verantwortliche Stelle muss Geräte zur Verfügung stellen, mit denen Auskunftsrechte wahrgenommen werden können.
- **Abs. 3: Transparenz**
  - Durch Chipkarten ausgelöste Kommunikationsvorgänge müssen für Betroffene erkennbar sein.

Ortungssysteme - § 32g RefEntwBDSG

- **Abs. 1: Zulässigkeit**
  - Ortungssysteme dürfen nur eingesetzt werden, wenn dies aus betrieblichen Gründen erforderlich ist zur
    - Sicherheit der Beschäftigten oder
    - zur Koordinierung des Einsatzes des Beschäftigten
- **Abs. 2: Schutz beweglicher Sachen**
  - Ortungssysteme dürfen auch zum Schutz beweglicher Sachen eingesetzt werden.
  - Die personenbezogene Ortung der Beschäftigten muss in diesen Fällen während der erlaubten Nutzung der Sache verhindert werden.
- **Abs. 3: Löschung**
  - Die Daten sind nach der Erreichung der Zwecke zu löschen.

Wird damit der Schutzes vor unzulässiger Verwendung von Chipkarten und Ortungssystemen verbessert?

- Wie wären Fälle der Verwendung von Daten aus Chipkarten und aus Ortungssystemen aus Vergangenheit und Gegenwart nach neuem Recht zu beurteilen?

1. **Chipkarten als Wegezeitenkontrolle**

   Bei einem Getränkehersteller wurden Chipkarten als Firmenausweise ausgegeben. In der Folge wurde festgestellt, dass die Ausweise vom automatischen Warenwirtschaftssystem, dass die Warenflüsse anhand von RFID-Tags auf den Paletten steuerte, erkannt wurden. Damit ließ sich exakt feststellen, wo Mitarbeiter sich wann befanden.

Wird damit der Schutzes vor unzulässiger Verwendung von Chipkarten und Ortungssystemen verbessert?

- Wie wären Fälle der Verwendung von Daten aus Chipkarten und aus Ortungssystemen aus Vergangenheit und Gegenwart nach neuem Recht zu beurteilen?

2. **Koordination von Pharmareferenten**

   Ein großes Vertriebsunternehmen hat einen Mitarbeiter damit beauftragt, die Android-Software von neuen Mobiltelefonen („Google-Handys") so zu programmieren, dass online festgestellt werden kann, wer wo ist.

3. **Zugriff auf individuelle Navigationsdaten**

   Hersteller von mobilen Navigationsgeräten bieten Arbeitgebern Systeme zur Koordination an, die neben dem Standort der Mitarbeiter automatisch auch die „Plausibilität" der eingeschlagenen Routen hinweisen und bei „Abweichungen" oder „ungeplanten Pausen" ebenso Alarm schlagen wie beim Unterschreiten von Normgeschwindigkeiten.

Nach neuem Recht zulässig oder nicht?

- Beispiel 1: Der beschriebene Einsatz von Chipkarten in Ausweisen wäre derzeit auf Basis von § 6c BDSG
  - grundsätzlich zulässig, wenn der Arbeitgeber betriebliche Gründe vorträgt.
  - Die „überraschende" Ortung der Beschäftigten wäre als unzulässiger Eingriff in Persönlichkeitsrechte und „Totalkontrolle" nach den Maßstäben der Rechtsprechung unzulässig.

Nach neuem Recht zulässig oder nicht?

- Beispiel 2: Der beschriebene Einsatz besonders programmierter Mobiltelefone wäre auf Basis des neuen § 32g Abs. 1 Nr. 2 BDSG
  - zulässig, wenn Arbeitgeber vortragen, dass auf Basis der so gewonnen Daten der Einsatz koordiniert werden kann.
  - Für andere Bereiche (etwa Taxis) ließe sich der Einsatz aus Nr. 2 ableiten.
  - **Grenzen** nach dem Entwurf: Überwiegen des schutzwürdigen Interesses der Betroffenen
  - **Grenzen** nach der Rechtsprechung: Eine „überraschende" oder „heimliche" Ortung der Beschäftigten wäre als unzulässiger Eingriff in Persönlichkeitsrechte und „Totalkontrolle" wohl unzulässig.

Nach § 32g zulässig oder nicht?

- Der Einsatz von „intelligenten Navigationssystemen" könnte nach § 32g Abs. 1 Nr. 2 RefEntwBDSG ggf.
  - mit der Begründung zulässig sein, dass die Daten zur Koordination benötigt werden.
- Beschäftigte könnten einwenden, dass gegen den Einsatz dieser Technik überwiegende schutzwürdigte Interessen bestehen.
- Bleibt die Frage, ob diese im Streitfall anerkannt werden, wenn Arbeitgeber sie pflichtgemäß durch geeignete Maßnahmen i.S. von Abs. 1 Satz 2 informieren.

Ortungssysteme mit Schutzcharakter - § 32g Abs. 2 RefEntwBDSG

- Die Regelung in Abs. 2 räumt Arbeitgeber die Befugnis ein, Sachen mit Ortungstechnik zu versehen.
- Die Regelung zielt auf den Diebstahlschutz und ist insoweit plausibel.
- Wirksame Schutzvorgaben bezüglich der Beschäftigten enthält die Regelung nicht.

Brauchen Arbeitgeber diese Kontrollen wirklich?

- Die im Entwurf normierten neuen Erhebungs- und Verarbeitungsmöglichkeiten sind in vielen Bereichen und für viele Anwendungen nicht zwingend.
- Die normativen Erlaubnis von neuen Kontrollmöglichkeiten erhöht die Spielräume zugunsten der Arbeitgeber erheblich.

Wären Arbeitnehmer vor negativen Auswirkungen nunmehr erlaubter Kontrollmechanismen ausreichend geschützt?

- Einen wirksamen Arbeitnehmerdatenschutz schafft der neue Entwurf nicht.
- Teilweise verschlechtert sich die Rechtssituation gegenüber der vorherigen Situation.
- Verbesserungen muss man hingegen lange suchen.

3. Fazit

- Der vorgelegte Entwurf
  - erfüllt seinen Anspruch nicht, Beschäftigte als Folge der zahlreichen Datenschutzskandale aus der Vergangenheit besser vor unzulässigen Erhebungen und Verwendungen ihrer Daten zu schützen;
  - schafft zugunsten von Arbeitgebern zahlreiche ausdrückliche Verarbeitungsbefugnisse;
  - bringt keine Rechtsklarheit für Arbeitgeber und Beschäftigte;
  - ist zur Sicherung der Persönlichkeitsrechte der Beschäftigten nicht geeignet.

AdA
EUROPÄISCHE AKADEMIE DER ARBEIT
IN DER UNIVERSITÄT FRANKFURT AM MAIN

Dr. Frank Wedde

Direktor der Europäischen Akademie der Arbeit
an der Universität Frankfurt

Professor für Arbeitsrecht und
Recht der Informationsgesellschaft

Isenburgstraße 30
60325 Frankfurt
Tel. 069 772021
wedde@em.uni-frankfurt.de