profil

Arbeitnehmerdatenschutz

DGB Bundesvorstand | Bereich Arbeits- und Sozialrecht | August 2009

Impressum

Herausgeber
DGB-Bundesvorstand
Bereich Arbeits- und Sozialrecht
Henriette-Herz-Platz 2
10178 Berlin

verantwortlich:
VB 02, Ingrid Sehrbrock

Redaktion:
Martina Perreng
Isabel Eder

Satz und Druck:
PrintNetwork pn GmbH, Berlin

Stand:
August 2009

Bestellung von Broschüren und Materialien des DGB bitte über das
DGB-Online-Bestellsystem:
Link: https://www.dgb-bestellservice.de

Schriftliche Bestellungen NUR für
Bestellerinnen/Besteller ohne Zugang zum Internet:
PrintNetwork pn GmbH · Stralauer Platz 33 – 34 · 10243 Berlin

Inhalt

Vorwort

Internet und E-Mail sind aus dem täglichen Leben kaum mehr wegzudenken. Online-Banking, die Verwendung von Kreditkarten und Bonuskarten sind für die meisten zur Selbstverständlichkeit geworden. Ebenso ist die Nutzung moderner Kommunikationsmittel und technischer Einrichtungen im Arbeitsverhältnis allgemeiner Standard. Es scheint aber auch Standard geworden zu sein, Beschäftigte auszuspionieren, sie zu überwachen und ihre Interessenvertreter zu bespitzeln. Datenskandale der letzten Monate haben gezeigt, dass das Grundrecht (informationelle Selbstbestimmung), über die Verwendung persönlicher Daten selbst zu entscheiden, eklatant missachtet wird.

Beschäftigte können sich dagegen nur bedingt wehren, denn wer riskiert schon wegen des Schutzes seiner persönlichen Daten seinen Arbeitsplatz. Arbeitnehmerinnen und Arbeitnehmer sind gegenüber dem Arbeitgeber keine gleichberechtigten Vertragspartner, die alleine in der Lage wären, gegen den Datenmissbrauch vorzugehen.

Es ist deshalb dringend notwendig, durch gesetzliche Veränderungen und die Entwicklung eines eigenständigen Arbeitnehmerdatenschutzgesetzes endlich einen wirksamen Grundrechtsschutz im Arbeitsleben zu schaffen. Durch die fortschreitend technische Entwicklung reichen die bestehenden gesetzlichen Regelungen nicht aus. Mit der vorliegenden Broschüre wollen wir über die bestehende Rechtslage informieren, die Erfahrungen aus Wissenschaft und Praxis darstellen und notwendige Neuregelungen begründen.

Zielgruppe:
Vor allem politische Parteien aber auch Datenschutzbeauftragte des Bundes und der Länder sowie betriebliche Datenschutzbeauftragte; die Broschüre wird auch an die Bezirke und Regionen versandt.

Mit freundlichen Grüßen

Ingrid Sehrbrock
Stellvertretende Vorsitzende

A. Gesetzlich geregelter Arbeitnehmerdatenschutz – dringender denn je

Peter Schaar
Bundesbeauftragter für den Datenschutz und Informationsfreiheit

I. Einleitung

Das im Grundgesetz verankerte allgemeine Persönlichkeitsrecht ist die Grundlage des Datenschutzes. Er soll die Würde, Privatsphäre und Handlungsfreiheit der Individuen gewährleisten. Ohne einen geschützten Raum, in dem man unbeobachtet reflektieren und sich mit anderen austauschen kann, kann es keine freie demokratische Gesellschaft geben. Dies gilt auch für die Arbeitswelt. Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis in vielfältiger Weise bedroht: Während eines Berufslebens sammelt sich über jeden Berufstätigen umfangreiches Datenmaterial bei Arbeitgebern an. Sie erhalten bei der Bewerbung Angaben über Schulbildung, berufliche Ausbildung, bisherige Tätigkeiten etc.. Diese Angaben werden mit der Zeit immer weiter ergänzt, zum Beispiel durch Leistungsbewertungen und Beurteilungen, Gehaltsdaten, Fehlzeiten, Krankmeldungen und Urlaubsdaten. Zudem werden mittels Arbeitszeiterfassungssystemen Daten über die An- bzw. Abwesenheit erhoben und in Arbeitszeitkonten erfasst. Digitale Telefonanlagen registrieren die Telefonate, und bei der Nutzung des Internets fallen Daten über E-Mails und das Surfverhalten an. Computer und Kassensysteme ermöglichen die direkte Erfassung von Leistungsparametern – zum Beispiel zu den von einer Schreibkraft eingegebenen Zeichen und zur Fehlerhäufigkeit. Immer mehr Arbeitsplätze werden durch Videokameras überwacht. Außerdem können Controllingverfahren die Leistung und das Verhalten überwachen und bewerten.

Die Gefahr liegt darin, dass informationstechnische Systeme, die eine immer größere Überwachungsdichte ermöglichen, schleichend Besitz von unserem beruflichen und privaten Alltag ergriffen haben. Wir sind dabei, uns an immer umfassendere Kontrollen und an permanente Überwachung zu gewöhnen.

Die bislang zielgerichtete Überwachung von Arbeitnehmern wird zunehmend entgrenzt und zeitlich und räumlich allgegenwärtig. Hintergrund dieser Überwachung ist nicht immer der böse Wille der Arbeitgeber, vielmehr stecken dahinter in der Regel vielfältige andere Zwecke und – ganz banal – die technische Entwicklung. Der Einsatz von IT für Kontrollzwecke wird immer billiger, einfacher in der Anwendung, komplexer, intelligenter und immer stärker vernetzt. Das technologisch bedingt immer umfangreichere Datenaufkommen trifft auf die Begehrlichkeit nach immer umfassenderer Überwachung.

II. Gefahren für die Persönlichkeitsrechte am einzelnen Arbeitsplatz

Auf dem Weg zum gläsernen Mitarbeiter:
Ein Beispiel aus den USA zeigt, wohin die Entwicklung bei der Überwachung des Arbeitsalltags im Betrieb führen kann, wenn man nicht rechtzeitig die Notbremse zieht.

Ein großes Softwareunternehmen entwickelt ein System zur Erfassung der Leistungsfähigkeit von Arbeitnehmern. Dabei sollen Körperfunktionen permanent gemessen und dauerhaft gespeichert werden.

Körperfunktionen eines Menschen verändern sich unter Stress. Beispielsweise bei der stressbeladenen Arbeit am PC. Sensoren, die am Körper des Mitarbeiters befestigt werden und permanent eine Vielzahl von Körperfunktionen messen, sollen künftig für eine bessere Kommunikation zwischen Mensch und Maschine sorgen.

Weichen die gemessenen Werte von den Durchschnittswerten ab, „weiß" der zentrale Rechner: „Hier gibt es ein Problem!" Dann fragt er nach und bietet dem gestressten Arbeitnehmer automatisch seine Hilfe an. Lässt sich das Problem auf diesem Weg nicht lösen, kann der Überwachungsrechner in seiner Datenbank nach einem anderen Mitarbeiter suchen, der eine ähnliche Aufgabe irgendwann bereits erledigt hat, und bittet ihn um Hilfe. Die Mitarbeiter sollen durch permanente Überwachung entlastet werden und im Ergebnis stressfreier arbeiten. Doch das ist nur die eine Seite der Medaille. Die andere Seite ist, dass alle Überwachungsdaten in einer zentralen Datenbank gespeichert werden und zu persönlichen Gesundheits- und Leistungsprofilen verarbeitet werden können. Das Kontrollsystem produziert ganz nebenbei, was sich viele Arbeitgeber wünschen: den gläsernen Mitarbeiter.

In Deutschland darf ein Unternehmen nicht nach eigenem Belieben Software zur Überwachung seiner Arbeitnehmer einführen. Schon das Betriebsverfassungsgesetz verleiht dem Betriebsrat ein zwingendes Mitbestimmungsrecht bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung von Arbeitnehmern zu überwachen". Und der Betriebsrat wird es sich genau überlegen, ob er der totalen Überwachung aller Arbeitnehmer wirklich zustimmt. Aber auch das Grundrecht auf informationelle Selbstbestimmung, abgeleitet aus dem allgemeinen Persönlichkeitsrecht, setzt der Überwachung im Arbeitsleben rechtliche Grenzen, wie die Gerichte wiederholt festgestellt haben. Trotzdem verbleiben Unklarheiten, wo diese Grenzen verlaufen. Ein Arbeitnehmerdatenschutzgesetz könnte hier mehr Klarheit bringen.

Gesundheitsdaten im Arbeitsleben:
Das Beispiel des verkabelten Mitarbeiters hat ja – Gott sei Dank – noch keinen Einzug in unseren Arbeitsalltag gefunden und dazu wird es hoffentlich auch nie kommen. Doch ist das Interesse von Arbeitgebern am Gesundheitszustand ihrer Mitarbeiter ungebrochen. Dabei ist die Verarbeitung von Gesundheitsdaten datenschutzrechtlich besonders kritisch; für diese Daten gelten rechtlich strengere Maßstäbe als für sonstige personenbezogene Daten. Entgegen der gängigen Rechtsprechung durch die Arbeitsgerichte werden allerdings zum Beispiel Bewerberinnen nach wie vor gefragt, ob eine Schwangerschaft vorliege.

Die Entwicklung in der Gesundheitsforschung beeinflusst auch den Arbeitnehmerdatenschutz. Neue Diagnosemöglichkeiten und molekulargenetische Untersuchungsmethoden gewinnen zunehmend an Bedeutung für das Arbeitsverhältnis. Prädikative Gentests zielen darauf ab, genetische Faktoren zu identifizieren, die zu einem späteren Zeitpunkt mit erhöhter Wahrscheinlichkeit zu einer Erkrankung führen können. Die genetischen Untersuchungen werden heute überwiegend nicht mehr als aufwändige individuelle Labortests durchgeführt, sondern mittels sogenannten Biochips, die mehrere hundert Gensequenzen in Minutenschnelle auswerten können. Praktische und finanzielle Schranken verlieren so mehr und mehr an Bedeutung für solche Tests. Arbeitgeber sind verständlicherweise daran interessiert,

vorzugsweise leistungsfähige und gesunde Arbeitnehmer einzustellen. Schon deshalb wird sich der Druck zur Durchführung genetischer Untersuchungen auf Bewerber verstärken.

Der Arbeitgeber könnte seine Bewerber auf bestimmte Gendefekte testen und so ihre Anfälligkeiten für bestimmte Krankheiten herausfinden, auch wenn dies nach der Rechtsprechung unzulässig ist.

Generell ist es dem Arbeitgeber lediglich gestattet, dem Bewerber Fragen zu stellen, die für den jeweiligen konkreten Arbeitsplatz relevant sind. Soweit dabei der Gesundheitszustand berührt ist, muss sich der Arbeitgeber allerdings auf Fragen nach wesentlichen Beeinträchtigungen der Leistungsfähigkeit oder des Einsatzes des Arbeitnehmers durch akute oder ansteckende Krankheiten oder nach geplanten Operationen beschränken. Das Fragerecht umfasst regelmäßig nicht Angaben zu genetischen Dispositionen. Die Frage eines Betriebsarztes etwa im Rahmen einer Einstellungsuntersuchung nach „schweren Krankheiten bei Familienmitgliedern" stellt eine simple Form von genetischer Diagnostik dar und braucht nicht beantwortet zu werden.

Internet- und E-Mail-Nutzung am Arbeitsplatz:
Die meisten Beschäftigten haben heute Zugang zum Internet am Arbeitsplatz. Jede E-Mail und jeder Aufruf einer Webseite am Arbeitsplatz hinterlässt Spuren in den betrieblichen IT-Systemen. Während diese Daten bei der häuslichen Nutzung nur beim Anbieter des entsprechenden Dienstes anfallen, erhält beim dienstlichen Surfen zusätzlich der Arbeitgeber Kenntnis vom Surfverhalten – bisweilen mit erheblichen Konsequenzen für den Arbeitnehmer.

Da Unternehmens- und Verwaltungsnetze üblicherweise stärker abgesichert sind als private Systeme, werden hier sogar mehr Daten erfasst und automatisiert ausgewertet. Die Auswertung umfasst bisweilen sogar die Inhalte der Kommunikation. Immer wieder wenden sich Betroffene – häufig zu Recht – an die Datenschutzaufsichtsbehörden, weil sie befürchten, der Chef lese die E-Mails mit. Manchen Arbeitgebern scheint nicht klar zu sein, dass selbst bei rein dienstlicher Nutzung des Internets eine lückenlose Überwachung von E-Mails oder dem Surfverhalten nicht zulässig ist, weil damit die ständige Kontrolle des Arbeitnehmers verbunden wäre und eine derartige automatisierte Vollkontrolle als schwerwiegender Eingriff in das Persönlichkeitsrecht der Beschäftigten nicht zulässig ist. Der Arbeitgeber darf aber eine stichprobenhafte und zeitnahe Auswertung der Protokolldaten vornehmen, wobei das Verfahren möglichst transparent zu gestalten ist.

Soweit Beschäftigten die private Nutzung von Internet und E-Mail erlaubt ist, sind zudem die Vorgaben des Telekommunikationsrechts zu beachten. So hat der Arbeitgeber das Fernmeldegeheimnis zu wahren, wenn er dem Arbeitnehmer die private Nutzung des betrieblichen E-Mail-Systems oder auch des Dienstte-lefons gestattet hat. Die Überwachung wäre dann sogar eine Straftat.

Da der Arbeitgeber ein berechtigtes Interesse daran hat, Missbrauch oder gar strafbare Handlungen nicht nur im dienstlichen Bereich, sondern auch bei der privaten Nutzung des dienstlichen Internetzugangs zu unterbinden, kann er die private Nutzung an bestimmte Bedingungen hinsichtlich des Zeitrahmens, der

zugelassenen Bereiche und regelmäßig durchzuführende Kontrollen knüpfen. Entsprechende Regelungen sollten in einer Betriebs- bzw. Dienstvereinbarung – am besten mit der Personalvertretung – verbindlich festgelegt werden. Die Beschäftigten sollten die Kenntnisnahme schriftlich bestätigen. Wenn ein Mitarbeiter die erforderlichen und festgelegten Kontrollmaßnahmen nicht akzeptiert, muss er die private Nutzung unterlassen. Es gibt keinen Anspruch, das Internet und die E-Mail privat am Arbeitsplatz nutzen zu können.

Eine Protokollierung darf ohne Einwilligung nur erfolgen, wenn sie zu Zwecken der Datenschutzkontrolle, der Datensicherung, zur Sicherung des ordnungsgemäßen Betriebs oder zu Abrechnungszwecken erforderlich ist. Die Verwendung der Protokolldaten zu anderen Zwecken ist unzulässig.

Videoüberwachung am Arbeitsplatz:
Videoüberwachung des öffentlichen Raumes oder aber auch in Firmen ist heute weit verbreitet. Sie soll dem Schutz von Objekten vor Vandalismus, Diebstahl oder anderen Eigentumsdelikten oder aber dem Schutz von Personen dienen. Es muss nicht Sinn und Zweck der Videoüberwachung sein, die Beschäftigten zu beobachten und zu kontrollieren. Doch ist beides oftmals deckungsgleich. So werden in Kreditinstituten oder Parkhäusern, in Kassenbereichen von Warenhäusern oder Museen – quasi nebenbei – auch die Mitarbeiter überwacht. Ob beiläufig oder zielgerichtet bezweckt, für beides gilt, dass die Videoaufzeichnung des Arbeitnehmerverhaltens nur in engen Grenzen zulässig ist.

Unabhängig davon, nach welchen Regeln des Bundesdatenschutzgesetzes (BDSG) die Zulässigkeit einer Videoüberwachung zu beurteilen ist, ob nach § 6b BDSG, der die Überwachung öffentlich zugänglicher Räume, also Räumen mit Publikumsverkehr, regelt oder nach den generellen Erhebungs-, Verarbeitungs- und Nutzungstatbeständen des § 28 BDSG: Der zentrale Wertungsmaßstab bei der Beurteilung der Zulässigkeit einer Videoüberwachung ist immer die Verhältnismäßigkeit. Die Überwachung muss sich als erforderlich darstellen, d.h. es dürfen keine objektiv zumutbaren Alternativen zur Videoüberwachung gegeben sein. Daneben muss auch die Mittel-Zweck-Relation gewahrt sein, d.h. Videoüberwachung darf nicht im Zusammenhang mit geringfügigen Verstößen eingesetzt werden, zum Beispiel um ein bestehendes Rauchverbot zu überprüfen.

Wenn eine Videoüberwachung von öffentlich zugänglichen Räumen aus Sicherheitsbedürfnissen nach § 6b BDSG zulässig ist und dieser Bereich gleichzeitig Arbeitsplätze von Mitarbeitern umfasst – wie zum Beispiel der Bereich einer Bank –, so werden die Mitarbeiter die Videoüberwachung als arbeitsplatzimmanent hinnehmen müssen. In diesen Fällen, in denen die Mitarbeiter nicht der eigentliche Beobachtungsgegenstand sind, ist eine Auswertung der Beobachtungsergebnisse zum Zweck einer mitarbeiterbezogenen Leistungs- und Verhaltenskontrolle allerdings unzulässig. So würde die Auswertung der zum Schutz gegen Überfälle gerechtfertigten Videoüberwachung einer Bank zwecks Kontrolle des Mitarbeiterverhaltens mit der Datenerhebung und -speicherung unvereinbar sein.

Die Zwecke der Überwachung müssen im Vorhinein konkret festgelegt werden, d.h. dokumentiert und in einem Verfahrensverzeichnis jedem Interessierten offengelegt werden (§ 4g Abs. 2 BDSG).

Im Allgemeinen wird Arbeit jedoch nicht in öffentlich zugänglichen Räumen verrichtet, sodass die gesetzlichen Regelungen zur Videoüberwachung für den Arbeitsplatz im Allgemeinen nicht gelten. Hier darf die Videoüberwachung nur eingesetzt werden, wenn sie zur Gewährleistung der Sicherheit erforderlich ist, wobei das Verhältnismäßigkeitsprinzip und die Persönlichkeitsrechte der Beschäftigten berücksichtigt werden müssen. Dabei hat das Bundesarbeitsgericht anerkannt, dass schon die Möglichkeit der jederzeitigen Überwachung einen Druck auf den Arbeitnehmer erzeugt, der mit seinem Anspruch auf Wahrung seiner Persönlichkeitsrechte regelmäßig nicht zu vereinbaren ist. Das Bundesarbeitsgericht zieht daraus den Schluss, dass die Videoüberwachung von Arbeitsplätzen nur durch besondere Sicherheitsinteressen des Arbeitgebers ausnahmsweise gerechtfertigt ist. Generell ist von den folgenden Grundsätzen auszugehen, die sich in der Rechtsprechung entwickelt haben:

- Das einen Eingriff in das Persönlichkeitsrecht rechtfertigende schutzwürdige Interesse des Arbeitgebers, etwa zum Schutz vor Verlust von Firmeneigentum durch Diebstahl etc., muss vor Beginn der Videoüberwachung durch konkrete Anhaltspunkte und Verdachtsmomente belegt sein. Eine vage Vermutung oder ein pauschaler Verdacht gegen alle Beschäftigte reicht nicht aus.
- Eine an sich zulässige Videoüberwachung ist grundsätzlich offen mittels einer sichtbaren Anlage nach vorheriger Information der Belegschaft durchzuführen.
- Eine Überwachung durch verdeckte Kameras ist als „ultima ratio" nur zulässig, wenn das die einzige Möglichkeit darstellt, berechtigte schutzwürdige Interessen des Arbeitgebers zu wahren.
- Die Videoüberwachung unterliegt der Mitbestimmung des Betriebsrates oder der Personalvertretung. Zu beachten ist hier jedoch, dass eine an sich unzulässige Videoüberwachung durch die Zustimmung des Betriebs- oder Personalrats nicht legitimiert wird.
- Die durch eine rechtswidrige Überwachung gewonnenen Erkenntnisse unterliegen einem Verwertungsverbot.

Chipausweise im Arbeitsalltag:
In fast allen Bereichen des Arbeitslebens sind heutzutage mit Chips ausgestattete kontaktlose Betriebs- oder Dienstausweise im Einsatz. Sie dienen der Zeiterfassung und oftmals auch als Zutrittsschlüssel. Ganz nebenbei lassen sich so nicht nur das Kommen und Gehen protokollieren, sondern auch das Betreten und Verlassen einzelner Räume. Dann können dabei leicht betriebsinterne Bewegungsprofile der einzelnen Mitarbeiter entstehen. In manchen Unternehmen dient der Ausweis auch als Zahlungsmittel in der Kantine, als Karte für das digitale Signieren elektronischer Dokumente oder als Berechtigungskarte für Serviceangebote des Arbeitgebers. Dadurch entstehen möglicherweise in der Kantine Konsumprofile, in Freizeiteinrichtungen Interessenprofile und im Intranet Tätigkeitsprofile.

Gegen die Einführung chipbasierter Ausweise ist grundsätzlich nichts einzuwenden, soweit dabei die datenschutzrechtlichen Vorgaben – auch im Hinblick auf die Datensicherheit – gewährleistet sind. So ist das zweckfremde Nutzen und Zusammenführen all dieser Daten nicht zulässig. Bei der Einführung von Chipausweisen sollte daher unbedingt darauf geachtet werden, dass in einer Betriebsvereinbarung/Dienstvereinbarung die dezentrale Speicherung der Daten festgelegt und detaillierte Nutzungs- und Zugriffskonzepte geregelt werden.

Biometrie am Arbeitsplatz:
Noch weitergehende Konsequenzen hat der Einsatz von Biometrie am Arbeitsplatz. Mit Fingerabdruck-, Iris-, Stimm- oder Gesichtserkennung wird – jedenfalls bei zentraler Speicherung der biometrischen Merkmale – das lästige Zücken des Betriebsausweises überflüssig. Zugleich erfolgt eine sichere Identifizierung des Beschäftigten beim Betreten des Arbeitsplatzes, beim Einloggen ins Firmennetz oder beim Betreten eines Sicherheitsbereiches. Auch bei der Bezahlung in Kantinen findet man heute schon Biometriesysteme.

Der Einsatz von Biometrie birgt ähnliche Gefahren wie der kontaktlose Chip. Verstärkt werden diese noch durch eine in der Regel lebenslange Bindung des biometrischen Merkmals an die Person. Es besteht die Gefahr der – evtl. heimlichen – dauerhaften Überwachung, der Ansammlung umfangreicher Datenbestände und der Bildung von Verhaltensprofilen. Des Weiteren können aus den biometrischen Merkmalsdaten so genannte Überschussinformationen gewonnen werden, das sind zum Beispiel Informationen über Krankheiten, die entweder direkt aus dem biometrischen Merkmal, also zum Beispiel der Iris des Auges, erkannt werden können oder nach der Statistik aller Wahrscheinlichkeit nach auftreten werden.

Aus Datenschutzgesichtspunkten sollte darauf geachtet werden, dass biometrische Merkmale nicht in Datenbanken gespeichert werden, sondern nur auf der Chipkarte.

Weitere datenschutzrechtliche Gefahren ergeben sich aus der Verknüpfung von Biometrie und Videotechnik. Der Weg eines Mitarbeiters kann bei entsprechender Kameradichte vom Erreichen des Geländes bis zum Verlassen automatisiert und lückenlos verfolgt werden. Personen werden dabei anhand hinterlegter Fotos automatisch identifiziert. Beispiel für die Absicherung durch modernste Zugangstechnik ist eine Großbank in der Schweiz: Der Zugang zum Gebäude einschließlich Tiefgarage sowie die Hauptgänge in der Bank sind videoüberwacht. Bei der Zufahrt in die Tiefgarage werden die Autokennzeichen automatisch gescannt und nach automatisierter Überprüfung wird die Zufahrt freigegeben. Fahrstuhlbenutzung, Etagen- und Bürotüren sowie Zugang zum PC sind biometrisch abgesichert. Die Beschäftigten benötigen weder Schlüssel noch PIN oder Passwort.

Man kann sich hier so einiges an Datenmissbrauchsmöglichkeiten vorstellen. In diesem Fall war Grundlage für die Installation allerdings ein detailliertes Datenschutz- und Datensicherheitskonzept und eine direkte Einbindung der Mitarbeitervertretung bei allen Entscheidungen die Technik betreffend. Ohne eine derartige technische und verfahrensmäßige Absicherung halte ich ein derartiges System nicht für vertretbar.

Datenflüsse in Unternehmen durch Personalinformationssysteme
Beispiel Skill - Datenbank:
Fast alle Unternehmen benutzen heute automatisierte Systeme für die Verwaltung ihrer Personaldaten. Durch derartige Systeme wird das Verhalten der Beschäftigten immer lückenloser registriert, bisweilen sogar, ohne dass die Betroffenen dies merken.

In sogenannten Skill-Datenbanken werden Kenntnisse, Erfahrungen und Kompetenzen von Mitarbeitern, zum Teil konzernweit, verwaltet. Sie werden zu unterschiedlichen Zwecken erstellt. Teilweise dienen sie der optimalen Rekrutierung von Führungskräften oder generell der Vergabe von Beförderungsstellen im Konzern. Sie dienen auch dazu, mit wenig zeitlichem und finanziellem Aufwand den richtigen Mitarbeiter an für den Konzern optimaler Stelle zu platzieren oder geeignete Projektteams zu bilden. Die Anliegen sind aus Sicht der Unternehmen verständlich, doch darf es nicht dazu kommen, dass hierdurch gläserne Mitarbeiter geschaffen werden und anhand der Skill-Profile interne und externe Leistungsbeurteilungen getroffen werden.

Es ist immer im Auge zu behalten, dass Mitarbeiterqualifikationen, insbesondere wenn sie in sehr detaillierter Form vorliegen, hochsensible Informationen sind und daher einen besonderen Schutz erfordern. Am datenschutzfreundlichsten sind Systeme, die auf Freiwilligkeit beruhen. Besonders zu begrüßen sind dabei Datenbanken, in denen die Mitarbeiter sich selber ein Profil anlegen unter Nutzung von Parametern, die vom Unternehmen vorgegeben werden. Sie verwalten ihre Profile selber, aktualisieren, berichtigen, löschen oder sperren ihre Profildaten mit der Konsequenz, dass sie beim Sperren ihres Profils bei der weiteren Suche nach geeigneten Personen für die Besetzung von Stellen oder Projekten nicht mehr berücksichtigt werden.

Bei der verpflichtenden Teilnahme der Beschäftigten an derartigen Verfahren müssen besondere Schutzvorkehrungen getroffen werden. Sollen Skill-Datenbanken verwendet werden, um potentiellen Kunden die Qualifikation der Mitarbeiter nachzuweisen, kommt grundsätzlich nur die Übermittlung solcher Daten in Betracht, aus denen der Kunde keine Rückschlüsse auf die Identität des Mitarbeiters ziehen kann. Besondere Vorsicht ist auch geboten, wenn bei derartigen Systemen personenbezogene Daten ins Ausland übermittelt werden.

III. Regelungen zum Arbeitnehmerdatenschutz

Es gibt bis heute bedauerlicherweise keine speziellen gesetzlichen Regelungen zum Arbeitnehmerdatenschutz. Arbeitnehmer und Arbeitgeber sind daher im Wesentlichen darauf angewiesen, sich an der lückenhaften und im Einzelfall für die Betroffenen nur schwer zu erschließenden einschlägigen Rechtsprechung zu orientieren.

Auch der Ansatz der Einwilligung – ein ansonsten durchaus sinnvoller Ansatz, der die Datenverarbeitung außerhalb gesetzlicher Regelungen nur zulässt, wenn der Betroffene eingewilligt hat – ist im Arbeitsverhältnis nur sehr eingeschränkt sinnvoll. Eine Einwilligung nach dem Bundesdatenschutzgesetz setzt eine freie Entscheidung voraus. Wegen seiner Abhängigkeit kann der Arbeitnehmer jedoch im Regelfall nicht wirklich frei von Zwang entscheiden. Welcher Arbeitnehmer wird sich in der heutigen Zeit angesichts der hohen Arbeitslosenzahlen schon seinem Chef entgegenstellen, um seine Privatsphäre zu schützen. Im Regelfall wird die Furcht vor Repressalien hier größer sein. Ein anderer Aspekt ist der, dass der Arbeitnehmer die Tragweite seiner Einwilligung zur Nutzung eines neuen informationstechnischen Systems, einer

Software oder eines neuen Verfahrens oftmals gar nicht erkennt. Ihm ist gar nicht bewusst, dass hier sein informationelles Selbstbestimmungsrecht tangiert wird. Welcher Beschäftigte weiß schon Bescheid über die genauen Datenflüsse bei der Einführung und dem Betrieb von Personalverwaltungssystemen oder Personalinformationssystemen oder beim Einsatz von Videotechnik am Arbeitsplatz und die damit verbundenen Risiken für die Persönlichkeitsrechte.

Hier sind vor allem die Interessenvertretungen – aber auch die betrieblichen Datenschutzbeauftragten – eines Unternehmens gefragt. Die Einführung automatisierter Systeme unterliegt in weiten Bereichen der Mitbestimmung des Betriebs- oder Personalrats. Das Betriebsverfassungsgesetz verpflichtet Arbeitgeber und Betriebsrat, „die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern". Hierzu gehört auch das Recht auf informationelle Selbstbestimmung.

Mitbestimmungsrechte bestehen etwa, wenn eine Einrichtung eingeführt wird, mit der sich das Verhalten oder die Leistung der Mitarbeiter kontrollieren oder messen lässt. Die Möglichkeit der Verhaltens- oder Leistungskontrolle muss dabei nicht der eigentliche Sinn und Zweck der Einführung des Verfahrens sein; es reicht aus, dass – sozusagen als Nebenprodukt – eine solche Verhaltens- oder Leistungskontrolle ermöglicht wird. So müssen Betriebs- oder Personalräte zustimmen, wenn Arbeitnehmer das Internet nutzen sollen und wenn ein System zur Kommunikation mittels E-Mail oder ein Controllingsystem eingeführt wird. Für die Einführung solcher Systeme sind Regelwerke zu erstellen, die ausführlich beschreiben, wie die Systeme zu nutzen sind und welche Konsequenzen ein Missbrauch zur Folge hat.

In vielen Unternehmen achten die Arbeitnehmervertretungen mit Argusaugen auf die Gewährleistung des Arbeitnehmerdatenschutzes. Diese Kontrolle entfällt aber regelmäßig, wenn ein Betrieb wegen seiner geringen Größe oder aus anderen Gründen keinen Betriebsrat hat. Auch betriebliche Datenschutzbeauftragte leisten wertvolle Hilfestellung. In manchen Unternehmen fehlt allerdings auch diese unternehmensinterne Kontrollinstanz, sei es, weil die Voraussetzungen für die Bestellung eines Datenschutzbeauftragten nicht gegeben sind (§ 4f BDSG), sei es, weil ein solcher entgegen den gesetzlichen Vorgaben nicht ernannt worden ist. In diesen Fällen sind die Beschäftigten darauf angewiesen, den Beteuerungen der Unternehmensleitung zu glauben. Zwar kann sich jedermann an die zuständige Datenschutzaufsichtsbehörde wenden, falls er vermutet, dass gegen Datenschutzbestimmungen verstoßen wird. Im betrieblichen Alltag sind allerdings – wohl aus der verständlichen Angst vor Repressalien – nur wenige Mitarbeiter zu diesem Schritt bereit.

Um den Schutz der informationellen Selbstbestimmung und damit der Persönlichkeit der Beschäftigten nicht von all diesen Unwägbarkeiten abhängig zu machen, fordern Datenschützer und Gewerkschaften seit vielen Jahren gesetzliche Regelungen zum Arbeitnehmerdatenschutz. Angesichts stetig wachsender technischer Möglichkeiten muss klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit auch für die Unternehmen einen nicht zu unterschätzenden Standortvorteil.

Obwohl der Deutsche Bundestag entsprechende Forderungen wiederholt mit großen, fraktionsübergreifenden Mehrheiten unterstützt hat, hatten die verschiedenen Bundesregierungen bislang keine konkreten Aktivitäten auf diesem Gebiet entwickelt. In ihrer Stellungnahme zu dem letzten Tätigkeitsbericht hat sich die Bundesregierung dahingehend geäußert, dass sie die Auffassung des BfDI, ein Gesetz zum Schutze der Arbeitnehmerdaten sei notwendig, teile. Das vom Bundesinnenminister im Februar 2009 initiierte Spitzengespräch mit den Bundesministern für Arbeit und Wirtschaft, den Arbeitgeberverbänden, den Gewerkschaften und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ist ein hoffnungsvoller Schritt auf dem Weg zu den dringend benötigten gesetzlichen Regelungen zum Schutze der Daten von Arbeitnehmern.

Darüber hinaus muss eine Stärkung des betrieblichen Datenschutzbeauftragten erfolgen. Dazu gehört, dass er vor der Umsetzung betrieblicher Maßnahmen umfassend beteiligt wird und einen wirksamen Kündigungsschutz genießt. Zu überlegen wäre auch, ob künftig dem Betriebsrat ein Mitwirkungsrecht bei der Bestellung des betrieblichen Datenschutzbeauftragten zugestanden wird. Schon heute müsste der Betriebsrat eine enge Zusammenarbeit mit dem betrieblichen Datenschutzbeauftragten einfordern. Auch dies sollte auf eine gesetzliche Grundlage gestellt werden.

Da die technologische Entwicklung und deren Einzug in die Arbeitswelt mit all ihren Risiken und Gefahren für den Datenschutz des Einzelnen nicht halt machen wird, ist es umso wichtiger, dass die Interessenvertretungen hier für die Arbeitnehmer ihre Stimme erheben und im Rahmen ihrer Möglichkeiten aktiv werden. Der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz und die Informationsfreiheit werden sie hierin nach Kräften unterstützen.

B. Arbeitnehmerdatenschutz auf der Grundlage des geltenden Datenschutzrechts

Prof. Dr. Peter Wedde
Universität Frankfurt

Das Thema Arbeitnehmerdatenschutz findet seit Februar 2008 in der breiten Öffentlichkeit und in der rechtspolitischen Diskussion eine ungeahnt intensive Beachtung. Der Grund hierfür ist allerdings nicht eine höhere Einsicht in die Notwendigkeit, in diesem lange vernachlässigten rechtlichen Bereich nunmehr etwas tun zu müssen. Ausgelöst wurde die Debatte vielmehr durch eine nicht enden wollende Reihe von Skandalen, die ihren Beginn im Frühjahr 2008 beim Lebensmitteldiscounter Lidl nahm und ihren letzten fragwürdigen Höhepunkt Anfang 2009 bei der Bahn AG fand. Dass die Reihe fortgesetzt wird, zeigte Anfang April 2009 wiederum die Firma Lidl, bei der offenkundig unter Verstoß gegen das geltende Datenschutzrecht Gesundheitsdaten und Krankheitsinformationen von Mitarbeitern gesammelt und verwendet worden sind.

Die zahlreichen datenschutzrechtlichen Skandale haben das Eine deutlich gemacht: In der Bundesrepublik Deutschland fehlt eine einheitliche Datenschutzregelung, die den besonderen Gegebenheiten in Arbeitsverhältnissen gerecht wird. Das Fehlen eines Gesetzes zum Arbeitnehmer- oder Beschäftigtendatenschutz wird insbesondere von Gewerkschaften und Wissenschaftlern seit längerer Zeit bemängelt. Inzwischen scheint Bewegung in dieses Thema zu kommen. Die Schaffung eines Arbeitnehmerdatenschutzgesetzes wurde im März 2009 nach einem Spitzentreffen von den zuständigen Ministern zugesagt. Im Juli 2009 wurde in das Bundesdatenschutzgesetz mit § 32 eine besondere Regelung für die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses eingefügt. Vor diesem Hintergrund soll dargelegt werden, welchen gesetzlichen Rahmen es schon heute für den Umgang mit Arbeitnehmerdaten gibt und wie die Rechtsprechung auf dieser Grundlage konkrete Problemfälle bisher gelöst hat.

1. Arbeitnehmerdatenschutz nach geltendem Recht

Solange es kein spezielles Arbeitnehmerdatenschutzgesetz gibt, bleibt zur juristischen Aufarbeitung von datenschutzrechtlichen Problemen im Arbeitsleben nur der Rückgriff auf allgemeine Rechtsregeln, wie sie insbesondere das Bundesdatenschutzgesetz (BDSG) zur Verfügung stellt. Die Anwendung dieses allgemeinen Gesetzes auf die Besonderheiten des Arbeitslebens ist allerdings mit dem Problem behaftet, dass zahlreiche Regelungslücken und Anwendungsprobleme bestehen. In der Praxis trifft die Wahrnehmung der nach dem BDSG bestehenden Rechte beispielsweise auf das Problem, dass Beschäftigte Datenschutzverstöße individualrechtlich gegenüber ihren Arbeitgebern geltend machen müssen und dass sie sich damit möglichen Sanktionen aussetzen. Auch Betriebsräte haben kein direktes Mitbestimmungsrecht, mit dem sie anstelle der Beschäftigten im individuellen Bereich tätig werden könnten. Keine Hilfe sind in dieser Situation die betrieblichen Datenschutzbeauftragten. Einerseits sind diese Personen nach der Feststellung des Bundesarbeitsgerichts aus dem Jahr 1997 vom Arbeitgeber nicht wirklich unabhängig. Andererseits verfügen sie nicht über wirksame gesetzliche Durchsetzungsmöglichkeiten, um ein unzulässiges Handeln des Arbeitgebers zu unterbinden. Und auch die Einflussmöglichkeiten der staatlichen Aufsichtsbehörden sind schon deshalb gering, weil die personelle Ausstattung es in der Praxis schwer bis unmöglich macht, konkrete Rechtsverstöße der Arbeitgeber flächendeckend zu identifizieren und zu beenden.

a) Der Schutzrahmen des Bundesdatenschutzgesetzes

Trotz der vorstehend angesprochenen individuellen Durchsetzungsprobleme gewährt das BDSG auf der normativen Ebene ein Mindestmaß an Schutz für die Persönlichkeitsrechte der Beschäftigten. Dieser leitet sich aus den allgemeinen Normen ab, die zur Regelung des Umgangs mit personenbezogenen Daten im nicht-öffentlichen Bereich zur Verfügung stehen.

Die zentrale Erlaubnisnorm ist § 4 Abs. 1 BDSG. Nach dieser Vorschrift ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet. Darüber hinaus kann die Verwendung von Daten im Arbeitsverhältnis erlaubt sein, wenn Arbeitnehmer dieser im Rahmen einer Einwilligung zugestimmt haben. Bedeutsam ist, dass die nach § 4a Abs. 1 BDSG erforderliche Einwilligung freiwillig sein muss (vgl. hierzu unter 1.b.).

Als einschlägige Rechtsnorm, auf deren Grundlage eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Arbeitsverhältnis gemäß § 4 Abs. 1 BDSG zulässig ist, kommt nunmehr an Stelle von § 28 Abs. 1 Satz 1 Nr. 1 BDSG der ab dem 01. September 2009 geltende neue § 32 BDSG in Betracht. Nach dieser neuen Rechtsnorm ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten zulässig, wenn dies zu Zwecken der Begründung oder Durchführung des Beschäftigungsverhältnisses erforderlich ist. Die Feststellung der Erforderlichkeit muss unter Berücksichtigung der gegenseitigen Interessen erfolgen.

Im Rahmen eines Bewerbungsverfahrens führt diese normative Situation dazu, dass Arbeitgeber bei Bewerbern die Informationen abfragen dürfen, die sie aus objektiver Sicht benötigen, um eine Auswahl treffen zu können. Dabei müssen sie allerdings mit Blick auf das in § 3a BDSG enthaltene allgemeine Gebot der Datenreduzierung auf die Informationen beschränken, die für die Bewerberauswahl unbedingt benötigt werden. In diesem Rahmen dürfen beispielsweise Auskünfte zur beruflichen Qualifikation oder zur Berufserfahrung abgefragt werden, nicht aber aus objektiver Sicht nicht erforderliche Informationen zu Erkrankungen, zu Kinderwünschen oder zu Schwangerschaften.

Scheitert eine Bewerbung, müssen Arbeitgeber die erhobenen Daten mit Blick auf § 35 Abs. 2 Nr. 1 BDSG unverzüglich vollständig löschen. Ausnahmen sind nur zulässig, wenn Beschäftigte einer längerfristigen Speicherung mit dem Ziel einer späteren Einstellung ausdrücklich freiwillig zugestimmt haben.

Weitergehende Informationen benötigen Arbeitgeber für die Durchführung laufender Arbeitsverhältnisse. Auch die Berechtigung hierfür leitet sich ab dem 01. September 2009 nicht mehr aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG, sondern aus dem neuen § 32 BDSG ab. Soweit es sich um personenbezogene Daten handelt, die eindeutig für die Durchführung des Beschäftigungsverhältnisses erforderlich sind, wie etwa Name, Anschrift oder Ausbildungsverlauf, darf der Arbeitgeber diese als Bestandteil der Vertragsbeziehung erheben und verarbeiten. Der zweckbezogene Umgang mit diesen Daten ist aus datenschutzrechtlicher Sicht im Regelfall unproblematisch.

Schwierigkeiten treten hingegen auf, wenn Arbeitgeber als Grundlage der Verarbeitung nicht den unmittelbaren Vertragszweck anführen, sondern auf die Notwendigkeit der Wahrung ihrer berechtigten Interessen hinweisen. Dies ist oft im Zusammenhang mit sog. Compliance-Verfahren oder im Bereich der Korruptionsbekämpfung der Fall. Grundsätzlich ist die Erhebung, Speicherung oder Übermittlung personenbezogener Daten zur Wahrung berechtigter Interessen von Arbeitgebern nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG weiterhin möglich. Allerdings darf die Verarbeitung von Beschäftigtendaten nach dem klaren Wortlaut im zweiten Halbsatz von § 28 Abs. 1 Satz 1 Abs. 1 Nr. 2 nur erfolgen, wenn kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegen. Gerade dieser zweite Halbsatz ist offenkundig von den meisten Arbeitgebern übersehen worden, die in den letzten Monaten durch Datenschutzskandale von sich Reden gemacht haben. Seine Beachtung hätte beispielsweise im Falle der Bahn AG unmittelbar zu der Erkenntnis führen müssen, dass die Weitergabe der Beschäftigtendaten an Dritte oder das Mitlesen von E-Mails durch interne Stellen des Konzerns aus datenschutzrechtlicher Sicht wegen des entgegenstehenden schutzwürdigen Interesses unzulässig war.

Zudem wird bei der Interessenabwägung im Rahmen der Nr. 2 zukünftig die generelle Beschränkung auf das Erforderliche zu berücksichtigen sein, die sich für Beschäftigungsverhältnisse aus § 32 Abs. 1 Satz 1 BDSG ableitet. Weiterhin muss beachtet werden, dass nach § 32 Abs. 1 Satz 2 BDSG die Erhebung, Verarbeitung und Nutzung mit dem Ziel der Aufklärung von Straftaten durch Arbeitgeber nur zulässig ist, wenn dokumentierende tatsächliche Anhaltspunkte einen entsprechenden Verdacht begründen und wenn die beabsichtigten Maßnahmen nicht unverhältnismäßig sind. Diese normative Anforderung ist bei der Verhältnismäßigkeitsprüfung im Rahmen von § 28 Abs. 1 Satz 1 Nr. 2 BDSG ebenfalls zu berücksichtigen.
Bei der Verwendung von Beschäftigtendaten müssen Arbeitgeber die Vorgaben zur Zweckbindung beachten, die in § 4 Abs. 3 Nr. 2 BDSG und in § 28 Abs. 1 Satz 2 BDSG verankert sind. Die Zwecke der Verarbeitung und Nutzung müssen damit bereits bei der Erhebung konkret festgelegt werden. Zweckänderungen sind nur unter sehr engen normativen Voraussetzungen möglich.

Die eindeutigen Vorgaben des BDSG stehen freien Auswertungen von personenbezogenen Daten mit dem Ziel der Verhaltens- und Leistungskontrolle ebenso entgegen wie der Einführung von Konzepten des Datamining oder Screening. Damit ist es im Regelfall beispielsweise unzulässig, dass Anwesenheitsdaten, die zu Abrechnungszwecken erfasst worden sind, im Nachhinein daraufhin ausgewertet werden, wie viele Krankheitstage pro Mitarbeiter vorliegen. Auch die spätere Verwendung dieser Daten für Krankenrückkehrgespräche ist im Regelfall datenschutzrechtlich unzulässig. Ein klarer Verstoß gegen geltendes Datenschutzrecht liegt zudem vor, wenn Arbeitgeber gezielt Informationen zu Erkrankungen von Beschäftigten sammeln, da diese als besondere Art personenbezogener Daten gemäß § 3 Abs. 9 BDSG unter einem spezifischen gesetzlichen Schutz stehen.

b) Freiwillige Einwilligungen im Arbeitsleben

In der arbeitsrechtlichen Praxis stellt sich immer wieder der Umgang mit freiwilligen Einwilligungen der Betroffenen zu Datenverarbeitungen des Arbeitgebers, die aufgrund des Fehlens einschlägiger gesetzlicher Erlaubnisnormen ansonsten unzulässig wären, als problematisch heraus. Nach § 4a Abs. 1 Satz 1 BDSG sind Einwilligungen von Beschäftigten nur wirksam, wenn sie auf deren freier Entscheidung beruhen. Bezogen auf ein Arbeitsverhältnis bestehen am Vorliegen der notwendigen Freiwilligkeit immer grundlegende Zweifel. Diese lassen sich aus den Ausführungen zur Freiwilligkeit ableiten, die sich im Beschluss des Bundesverfassungsgerichts in seiner „Lügendetektorentscheidung" vom 18.08.1981 finden. Hier hat das Gericht ausgeführt, dass Freiwilligkeit nur gegeben ist, wenn eine Entscheidung nicht unter Druck oder in einer Zwangslage getroffen wird.

Gerade diese Voraussetzungen werden aber bei den meisten Arbeitnehmern nicht erfüllt sein, wenn der Arbeitgeber einseitig entsprechende Zustimmungen verlangt. Ursache hierfür ist die im Arbeitsverhältnis immer bestehende Disparität zwischen Arbeitnehmern und Arbeitgebern. Insbesondere bei Vertragsabschluss wird ein Arbeitnehmer sich im Regelfall gar nicht weigern können, „freiwillig" in bestimmte Kontrollmaßnahmen einzuwilligen. Erteilt er eine Einwilligung unter Hinweis auf die Vorgaben in § 4a Abs. 1 BDSG nicht, führt dies nämlich in der Bewerbungsphase mit hoher Wahrscheinlichkeit zum Scheitern der Vertragsverhandlungen und in der Probezeit zur schnellen Kündigung. Wird eine Einwilligung nach der Probezeit verlangt, ist es nicht karrierefördernd, wenn Arbeitnehmer sich entsprechenden Forderungen widersetzen.

Gesteigerte Anforderungen an eine wirksame Einwilligung bestehen, wenn es sich um besondere Arten personenbezogener Daten handelt. Dieses sind nach der gesetzlichen Definition in § 3 Abs. 9 BDSG Informationen über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Diesbezüglich ist im Arbeitsverhältnis davon auszugehen, dass Arbeitnehmer kein Interesse daran haben können, diese Daten ihrem Arbeitgeber freiwillig zu offenbaren. Dies gilt besonders bezogen auf Gesundheitsdaten, weil sich hiermit immer das Risiko verbindet, dass Arbeitgeber entsprechende Informationen zur Begründung krankheitsbedingter Kündigungen heranziehen. Bezogen auf den jüngst bekannt gewordenen Fall individueller Krankenberichte bei Lidl lässt sich insoweit bereits auf den ersten Blick feststellen, dass derartige Aufzeichnungen des Arbeitgebers datenschutzrechtlich absolut unzulässig sind.

c) Videoüberwachung im Arbeitsleben

Begrenzt sind die Regeln, die das BDSG bezüglich der Videoüberwachung von Beschäftigten enthält. In § 6b BDSG finden sich nur Vorgaben, die sich auf öffentlich zugängliche Räume beziehen. Damit stehen gesetzliche Regelungen beispielsweise für Arbeitsplätze in Kaufhäusern zur Verfügung. Nicht normativ geregelt ist hingegen der Einsatz von Kameras in nicht-öffentlichen Räumen wie beispielsweise in Produktionshallen oder in Bürogebäuden. Die damit bestehende Gesetzeslücke hat der Gesetzgeber bei

Verabschiedung der derzeit geltenden Fassung des BDSG im Jahre 2001 durchaus gesehen. In den Gesetzesmaterialien wird darauf verwiesen, dass eine entsprechende Regelung für nicht-öffentliche Räume im Rahmen eines besonderen Gesetzes zum Arbeitnehmerdatenschutz erfolgen soll. Damit ist das Thema nach wie vor normativ ungeregelt.

Die Rechtsprechung hat die bestehende Regelungslücke inzwischen teilweise gefüllt. Insbesondere der 1. Senat des Bundesarbeitsgerichts hat in Entscheidungen aus den Jahren 2004 und 2008 ausgeführt, dass die Videoüberwachung von Arbeitnehmern ausnahmsweise zulässig sein kann, wenn im Rahmen einer Verhältnismäßigkeitsprüfung die Interessen des Arbeitgebers überwiegen (vgl. unter 2.b). Dies kann beispielsweise im Wertbriefbereich eines Postverteilzentrums der Fall sein. Ausgeschlossen sind nach der Rechtsprechung des Bundesarbeitsgerichts aber Totalkontrollen, die Arbeitnehmern keinen kontrollfreien Raum lassen.

d) Vorgaben zur Datensicherheit und Arbeitnehmerdatenschutz

Weitere normative Vorgaben mit Auswirkungen auf den arbeitsrechtlichen Bereich lassen sich aus § 9 BDSG ableiten. Diese Vorschrift listet technische und organisatorische Maßnahmen auf, die die Ausführung des Gesetzes gewährleisten sollen. Aus dem Katalog der Schutzmaßnahmen lässt sich beispielsweise folgern, dass der Zugriff auf die personenbezogenen Daten von Beschäftigten durch Kollegen oder Vorgesetzte auch im Arbeitsverhältnis im Regelfall nicht zulässig ist. Dies folgt aus den Grundsätzen zur Zugangs- und Zugriffskontrolle, die in den Nrn. 2 und 3 der Anlage zu § 9 Satz 1 BDSG enthalten sind.

Die Zugangskontrolle steht zusammen mit der Weitergabekontrolle in Nr. 4 und der Eingabekontrolle in Nr. 5 dieser Vorschrift auch der Weitergabe oder gemeinsamen Nutzung von individuellen Passwörtern entgegen. Aus den einschlägigen Vorgaben zum technischen und organisatorischen Datenschutz leitet sich zudem die Konsequenz ab, dass die Durchführung von heimlichen „Zwangsabfragen" durch Vorgesetzte im Regelfall ebenso unzulässig ist wie der Zugriff auf persönliche Daten der Beschäftigten.

Aus der Regelung in Nr. 8 der Anlage zu § 9 Satz 1 BDSG lässt sich darüber hinaus folgern, dass gemäß dem ursprünglichen Verarbeitungszweck eine Trennung der Daten erfolgen muss. Diese Vorgabe steht beispielsweise dem Verlangen einer Konzernspitze entgegen, personenbezogene Daten unternehmensübergreifend auswerten zu wollen. Datenverarbeitung darf vor diesem Hintergrund im Regelfall nur unternehmensbezogen, nicht aber konzernweit erfolgen.

e) Auftragsdatenverarbeitung

Die Liste der datenschutzrechtlichen Problemfelder, die sich im Bereich eines Arbeitsverhältnisses ergeben, setzt sich im Bereich der Auftragsdatenverarbeitung fort. Sollen Daten beispielsweise unternehmensübergreifend erhoben, verarbeitet oder genutzt werden, muss zwischen den beteiligten Unterneh-

men immer ein Auftrag nach § 11 BDSG vorliegen. Diese normative Voraussetzung muss auch zwischen Unternehmen desselben Konzerns immer erfüllt sein, da das BDSG insoweit keine Privilegierung für die konzernweite Datenverarbeitung enthält.

In der Praxis wird diese zwingende gesetzliche Vorgabe gerade in multinationalen Konzernen oft nicht ausreichend berücksichtigt. Dies bestätigen Betriebsräte aus diesem Bereich, die der Einführung entsprechender Verarbeitungen beziehungsweise entsprechender Systeme wegen des Fehlens einer ausreichenden datenschutzrechtlichen Fundierung unter Hinweis auf ihr Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) erfolgreich widersprochen haben.

Werden Aufträge auf der Basis von § 11 BDSG erteilt, muss nach dem insoweit eindeutigen Wortlaut in Abs. 2 Satz 2 der Vorschrift die Schriftform gewahrt werden. Damit stellt die nur mündliche Erteilung von Aufträgen zum Datenabgleich, wie sie nach Presseberichten im Fall der Bahn AG gegenüber der externen Firma Network Deutschland GmbH erfolgt sein soll, einen klaren Verstoß gegen eine zwingende Norm des BDSG dar.

Darüber hinaus verlangt § 11 Abs. 2 Satz 1 BDSG von Auftraggebern, dass die Auftragnehmer unter besonderer Berücksichtigung der Eignung und der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt werden müssen. Ob diese Vorgabe bei den bekannt gewordenen Fällen datenschutzrechtlich unzulässiger oder fragwürdiger Beauftragungen jeweils eingehalten wurde, wird sich noch zeigen.

Werden Bereiche, in denen personenbezogene Daten verarbeitet werden, vollständig an andere Stellen übertragen, liegt keine Auftragsverarbeitung vor, sondern eine sogenannte Funktionsübertragung. Aus datenschutzrechtlicher Sicht handelt es sich hierbei um eine Übermittlung von Daten an Dritte. Diese kann unter den Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG ebenfalls zur Wahrung berechtigter Interessen von Arbeitgebern zulässig sein, wenn kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Übermittlung überwiegen. Diese normative Voraussetzung kann dann erfüllt sein, wenn beim Datenempfänger mindestens das gleiche datenschutzrechtliche Schutzniveau besteht wie bei der abgebenden Stelle. Im arbeitsrechtlichen Bereich beinhaltet dieses Schutzniveau auch die Vorgaben, die sich zur Wahrung von Persönlichkeitsrechten aus Betriebsvereinbarungen ableiten. Darüber hinaus muss die Erforderlichkeit im Sinne von § 32 Satz 1 BDSG gegeben sein.

f) Grenzüberschreitende Datenverarbeitung

Der Schutzrahmen des BDSG hat trotz seiner geographischen Begrenzung auf das Hoheitsgebiet der Bundesrepublik Deutschland Auswirkungen auf die Übermittlung ins Ausland. Diese ist nur zulässig, wenn im Empfängerland ein vergleichbarer datenschutzrechtlicher Schutzstandard wie in der BRD gegeben ist und wenn die Daten dort mindestens gleichgut geschützt sind. Dies ist innerhalb der Europäischen Union grundsätzlich der Fall, weil alle Mitgliedstaaten gemäß der EU-Datenschutzrichtlinie vom 24.10.1995 inzwischen über ein einheitliches Datenschutzniveau verfügen.

Ein entsprechendes Schutzniveau muss auch garantiert sein, wenn personenbezogene Daten in andere Staaten außerhalb der Europäischen Union übermittelt werden sollen. Dies gilt insbesondere für Übermittlungen in die Vereinigten Staaten von Amerika, die über keine vergleichbaren gesetzlichen Regeln zum Datenschutz verfügen. Vor diesem Hintergrund wird beispielsweise die Übermittlung von personenbezogenen Daten aus einem deutschen Konzernunternehmen an die amerikanische Konzernmutter datenschutzrechtlich selbst dann unzulässig sein, wenn US-amerikanisches Recht entsprechende Übermittlungen zwingend einfordert. Dies hat das Bundesarbeitsgericht in einer Entscheidung des 1. Senats zur Anwendung von US-amerikanischen Ethik-Richtlinien in der Bundesrepublik Deutschland vom 22.07.2008 im Ergebnis ebenso gesehen.

Maßgeblich für die Bewertung der Zulässigkeit der Datenübermittlung ins Ausland ist in derartigen Fällen allein das nationale Datenschutzrecht der Bundesrepublik Deutschland. Bei der vorzunehmenden Rechtsgüterabwägung ist davon auszugehen, dass schutzwürdige Interessen der Betroffenen immer überwiegen und der Übermittlung entgegen stehen, wenn Daten an Stellen oder Länder übermittelt werden sollen, in denen der Standard des nationalen beziehungsweise des europäischen Datenschutzrechts nicht garantiert werden kann. Für die Datenübermittlung müssen in diesen Fällen flankierende Vorkehrungen getroffen werden, wie etwa der Abschluss sogenannter EU-Standardverträge und die ergänzende vertragliche Festlegung der Verarbeitungsgründe und Zwecke.

g) Schutzrahmen des BDSG

Fasst man die angesprochenen Regelungsspielräume und Normen des BDSG zusammen, wird deutlich, dass der Arbeitnehmerdatenschutz nach diesem allgemeinen Gesetz nicht umfassend und eindeutig garantiert wird. Das Gesetz trifft insbesondere dort auf seine Grenzen, wo es von gleichrangigen Vertragspartnern ausgeht, die es im Arbeitsverhältnis im Regelfall nicht gibt. Darüber hinaus stellt es sich aber problematisch dar, dass Betroffene aus dem BDSG zwar umfangreiche Auskunfts- und Löschungsrechte ableiten können, ihre Ansprüche aber im Streitfall vor dem Arbeitsgericht gegen den Arbeitgeber durchgesetzt werden müssen. Viele Arbeitnehmer verzichten hierauf aus Angst vor Karrierenachteilen oder Arbeitsplatzverlust.

Ein großes Defizit leitet sich unmittelbar daraus ab, dass im BDSG, bezogen auf die Besonderheiten im Arbeitsleben, klare Ge- und Verbotsregeln fehlen. Besonders deutlich wird dies bezogen auf heimliche oder verdeckte Datenerhebungen und -verarbeitungen, die Gegenstand der meisten Datenschutzskandale der letzten Monate waren. Aber auch die Abwesenheit klarer und zwingender Pflichten etwa im Bereich der Datenlöschung macht sich im Arbeitsverhältnis als besonders problematisch bemerkbar.

Die bestehenden Probleme werden noch dadurch verschärft, dass sich die gesetzlichen Sanktionen, die verantwortliche Stellen als Folge von Verstößen gegen das geltende Datenschutzrecht befürchten müssen, in engen Grenzen halten. So wird beispielsweise das unbefugte Erheben oder Verarbeiten personenbezogener Daten nach § 43 Abs. 2 Nr. 1 BDSG lediglich als Ordnungswidrigkeit geahndet. Strafbar ist ein

solches Handeln nach § 44 BDSG hingegen nur, wenn es vorsätzlich gegen Entgelt erfolgt oder mit der Absicht, sich oder einen anderen zu bereichern oder zu schädigen. Bezogen auf die Datenschutzskandale der letzten zwölf Monate lässt sich insbesondere das Vorliegen eines Vorsatzes wohl zumeist nicht nachweisen.

2. Rechtsprechung zum Arbeitnehmerdatenschutz

Aus der Rechtsprechung des Bundesverfassungsgerichts und des Bundesarbeitsgerichts lassen sich Anhaltspunkte dafür ableiten, welche Formen der Datenverarbeitung im Arbeitsverhältnis zulässig sind und welche nicht. Einschlägige Entscheidungen gibt es zu Themen wie „Zulässigkeit heimlicher Kontrolle", „Einsatz von Videokameras im Betrieb" und „Zulässigkeit von allgemeinen Verhaltens- und Leistungskontrollen mittels technischer Einrichtungen".

a) Rechtsprechung des Bundesverfassungsgerichts

Für den arbeitsrechtlichen Bereich von grundlegender Bedeutung ist die Entscheidung des Bundesverfassungsgerichts vom 15.12.1983 zur Rechtmäßigkeit der damals geplanten Volkszählung. Mit dieser Entscheidung wurde ein neues „Grundrecht auf informationelle Selbstbestimmung" begründet, das auch das aktuelle BDSG entscheidend geprägt hat. Das Recht auf informationelle Selbstbestimmung sichert dem Einzelnen die Verfügungsgewalt über seine persönlichen Daten. In dieses Grundrecht darf nur nach Durchführung einer Verhältnismäßigkeitsprüfung eingegriffen werden, wenn höherrangige staatliche Interessen dies zwingend erfordern.

Bezieht man diese allgemeinen Verfassungsgrundsätze auf das Arbeitsrecht, wo das Recht auf informationelle Selbstbestimmung per Drittwirkung ebenfalls zur Anwendung kommt, wird deutlich, dass dem Umgang mit personenbezogenen Daten der Beschäftigten allgemeine Grenzen gesetzt sind. Arbeitgeber sind aus verfassungsrechtlichen Erwägungen gehindert, beliebige Bearbeitungsvorgänge mit personenbezogenen Daten durchzuführen, weil dies gegen das Recht auf informationelle Selbstbestimmung verstoßen würde. Entsprechendes gilt für das durch das allgemeine Persönlichkeitsrecht ebenfalls geschützte „Recht am eigenen Bild". Auf dieses könnten Arbeitnehmer sich beispielsweise berufen, wenn ein Arbeitgeber die Fotos aller Mitarbeiter auf seiner Firmenwebsite präsentieren möchte. Einer besonderen Begründung bedarf die Wahrung des Rechts am eigenen Bild nicht. Höherrangige Interessen des Arbeitgebers, die eine Veröffentlichung zulässig machen würden, können ausnahmsweise gegeben sein, wenn etwa Beschäftigte in einem Unternehmen herausragende Funktionen wahrnehmen, die einen klaren Bezug zur Öffentlichkeit haben.

Berücksichtigung finden muss im Arbeitsverhältnis schließlich nunmehr das neue Grundrecht auf „Vertraulichkeit und Integrität informationstechnischer Systeme", das am 27.02.2008, bezogen auf ein neues Gesetz zur Onlineüberwachung in Nordrhein-Westfalen, vom Bundesverfassungsgericht begründet wurde. Das Gericht hat hierzu ausgeführt, dass aus technischer Sicht in komplexen IT-Systemen neue und

weitgehende Überwachungsmöglichkeiten bestehen. Es hat die Zulässigkeit der heimlichen Erfassung von in IT-Systemen vorhandenen Daten davon abhängig gemacht, dass eine massive Gefährdung für das Gemeinwesen oder für das Leben von Menschen besteht. Auch für diese Fälle hält das Bundesverfassungsgericht elektronische Ausforschung jedoch nur für zulässig, wenn vorher eine richterliche Anordnung erfolgt ist.

Überträgt man diese Vorgaben des Bundesverfassungsgerichts zur Vertraulichkeit und Integrität informationstechnischer Systeme auf das arbeitsrechtliche Gebiet, lässt sich hieraus zunächst ein grundsätzliches Verbot heimlicher Überwachungsmaßnahmen im Betrieb ableiten, wenn hierzu die Informationen aus vernetzten Datenverarbeitungssystemen verwendet werden sollen. Auch die offene Ausforschung und Verwendung der in Datenverarbeitungssystemen oder in Kommunikationsnetzen vorhandenen Daten zur Verhaltens- und Leistungskontrolle kann unter Beachtung der Vorgaben des Bundesverfassungsgerichts unzulässig sein, wenn Beschäftigte im Arbeitsverhältnis darauf angewiesen sind, bestimmte IT-Anwendungen intensiv für ihre Arbeit zu nutzen. Das Grundrecht soll für diese Fälle garantieren, dass die zwingend anfallenden Daten nicht dazu verwendet werden dürfen, umfassende Persönlichkeitsprofile zu erstellen. Die Beachtung dieser verfassungsrechtlichen Vorgaben macht für die Bewertung zulässiger Auswertungen im Arbeitsverhältnis eine grundlegende Neuausrichtung erforderlich.

b) Rechtsprechung des Bundesarbeitsgerichts

Die Rechtsprechung des Bundesarbeitsgerichts hat sich der vom Bundesverfassungsgericht verfolgten Linie, die heimliche und verdeckte Überwachungsmaßnahmen für unzulässig hält, in einer Reihe von Entscheidungen angeschlossen. Besonders deutlich wird dies bei der Bewertung von Fällen, in denen Arbeitgeber (oder auch Arbeitnehmer) Telefongespräche heimlich aufgezeichnet haben. Hierzu hat das Bundesarbeitsgericht regelmäßig ein Beweisverwertungsverbot angenommen. Die Nutzung der heimlich gewonnenen Informationen für Kündigungen oder Forderungen war somit nicht möglich.

Entsprechendes gilt für den Bereich heimlicher oder umfassender Videoüberwachung. Heimliche und dauerhafte Kontrollen hält der 1. Senat des Bundesarbeitsgerichts in Entscheidungen vom 29.06.2004 und vom 14.12.2004 für unzulässig, weil sie unangemessen tief in Persönlichkeitsrechte der Beschäftigten eingreifen. Der 1. Senat setzt sich mit dieser Positionierung in einen begrüßenswerten Widerspruch zur Rechtsprechung des 2. Senats. Dieser hatte nämlich in einer Entscheidung vom 27.03.2003 die heimliche Videoüberwachung ausdrücklich für den Fall zugelassen, dass nur so ein Diebstahlsverdacht des Arbeitgebers bestätigt werden kann.

Ergebnis dieser widersprüchlichen Entscheidungen ist eine große Unklarheit über das Maß des Zulässigen im Bereich der heimlichen Überwachung. Diese Unklarheit wird noch gesteigert durch eine Entscheidung des 2. Senats des Bundesarbeitsgerichts vom 13.12.2007, mit der das sogenannte Beweisverwertungsverbot und damit die Zulässigkeit der Berufung auf unzulässig erlangte Informationen in Frage gestellt wird.

Auf der Grundlage dieser Entscheidung ist es unklar, ob Arbeitgebern die Nutzung heimlich oder sonst wie unzulässig erlangter Informationen auch in Zukunft verwehrt bleibt.
Der 2. Senat hat in dieser Entscheidung festgestellt, dass es Arbeitgebern nicht verwehrt ist, für die Kündigung auf Informationen zurückzugreifen, die unter Verstoß gegen eine geltende Betriebsvereinbarung erlangt wurden. Die Annahme eines „Sachvortragsverwertungsverbots" steht nach Auffassung des Senats in deutlichem Widerspruch zu den Grundprinzipien des deutschen Zivil- und Arbeitsgerichtsverfahrens und kann deshalb die Verwendung von Informationen nicht verhindern, die Arbeitgebern vorliegen. Die Entscheidung überzeugt zwar weder in der Begründung noch im Ergebnis, erzeugt aber bezüglich der Verwendung von heimlich oder sonst wie fragwürdig erlangten Beweismitteln ein hohes Maß an Rechtsunsicherheit. Für Betriebsräte leitet sich aus ihr die zwingende Notwendigkeit ab, in Betriebsvereinbarungen klare und abschließende Verwendungsregeln einzufügen. Für Beschäftigte, die in Betrieben ohne Betriebsrat tätig sind, erhöht sich das Risiko, dass Arbeitgeber unzulässig erlangte Beweismittel zur Begründung einer Kündigung nutzen.

Erfolgen Kontrollen nicht heimlich, sondern offen und für die Beschäftigten sicht- oder wahrnehmbar, können sie nach der Rechtsprechung des Bundesarbeitsgerichts ausnahmsweise zulässig sein, wenn Arbeitgebern keine anderen Kontrollmöglichkeiten zur Verfügung stehen. Insoweit hat der 1. Senat in seinen angesprochenen Entscheidungen aus dem Jahr 2004 die Zulässigkeit einer komplexen Videoanlage in einem Postverteilzentrum unter Hinweis darauf verneint, dass dem Arbeitgeber gegebenenfalls andere Kontrollmöglichkeiten, wie etwa die Einstellung zusätzlichen Personals, zur Verfügung stehen würden. Durch die restriktive Zulassung soll vermieden werden, dass Arbeitnehmer während ihrer Tätigkeit einem umfassenden Überwachungsdruck ausgesetzt werden. Allerdings hat der 1. Senat diese restriktive Position in einer aktuelleren Entscheidung vom 26.08.2008 relativiert und dem Arbeitgeber zugestanden, dass er vorhandene Videokameras beim Vorliegen eines Diebstahlsverdachts, bezogen auf konkret abgegrenzte Bereiche, einschalten darf. Die Zulässigkeit einer Generalüberwachung hat der Senat allerdings auch für diese Fälle verneint.

3. Fazit

Fasst man die einschlägigen normativen Vorgaben des BDSG und die Aussagen der Rechtsprechung von Bundesverfassungsgericht und Bundesarbeitsgericht zusammen, leiten sich hieraus überschaubare Vorgaben bezüglich der Zulässigkeit von Überwachungsmaßnahmen ab. Sind im Einzelfall Kontrollen unumgänglich, weil es aus objektiver Sicht keine zumutbaren Überwachungsalternativen für den Arbeitgeber gibt, muss sichergestellt werden, dass die damit verbundenen Eingriffe in Persönlichkeitsrechte der Beschäftigten so gering wie möglich sind und sich im erforderlichen Rahmen gemäß § 32 Abs. 1 Satz 1 BDSG bewegen. Erfolgt beispielsweise in Bankfilialen aus Sicherheitsgründen eine permanente Kameraüberwachung, ist durch entsprechende organisatorische Vorkehrungen sicherzustellen, dass eine Auswertung nur durchgeführt wird, wenn es zu Straftaten gekommen ist und dass so die personenbezogenen Daten der Beschäftigten maximal geschützt bleiben.

Entsprechendes gilt für die Kontrolle von dienstlichen E-Mails mit geschäftlichem Inhalt, die aus Sicht von Arbeitgebern erforderlich und berechtigt sind. Hierbei muss mit Blick auf die schutzwürdigen Interessen gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG sichergestellt werden, dass persönliche E-Mails, die ein Beschäftigter etwa an einen Betriebsrat oder an den Betriebsarzt schreibt, kontrollfrei bleiben. Entsprechendes muss für die „soziale Kommunikation" unter den Beschäftigten gelten. Es besteht beispielsweise kein überwiegendes rechtliches Interesse des Arbeitgebers, eine E-Mail mitlesen zu können, in der sich zwei Kollegen zum Mittagessen in der Kantine verabreden.

Die Regelungen des BDSG und die Feststellungen der Rechtsprechung sind jedoch nicht ausreichend, um alle bekannten Probleme zu bewältigen. Hieran ändert auch die neue Regelung des § 32 BDSG nichts Grundlegendes. So stellt es sich beispielsweise als problematisch dar, dass Arbeitnehmer, die von unzulässigen Kontrollen betroffen sind, den Arbeitgeber nur auf individualrechtlichem Weg zur Rechtskonformität zwingen können. Ein solches Vorgehen unterbleibt in den meisten Fällen aus Angst vor dem dann drohenden Arbeitsplatzverlust oder vor arbeitsrechtlichen Sanktionen. Auch auf die theoretisch mögliche Einschaltung staatlicher Aufsichtsbehörden wird in diesen Fällen zumeist verzichtet.

Problematisch ist weiterhin das Fehlen absoluter Verbotsnormen, durch die beispielsweise der Zugriff auf besondere Arten von personenbezogenen Daten (etwa der Zugriff des Betriebsarztes auf die vor der Einführung stehenden Gesundheitskarte der Beschäftigten auf der Grundlage einer freiwilligen Einwilligung) für bestimmte Fälle ebenso ausgeschlossen wird wie die heimliche Überwachung mit technischen Einrichtungen. Darüber hinaus sollte es im Arbeitsverhältnis grundsätzlich ausgeschlossen werden, dass Verarbeitungskompetenzen durch freiwillige Einwilligungen der Beschäftigten ausgeweitet werden können.

Nicht hilfreich bei den erkennbaren Problemen können die betrieblichen Datenschutzbeauftragten sein, solange ihnen keine wirksamen Handlungsmöglichkeiten zur Verfügung stehen, um einen Datenmissbrauch im konkreten Fall verhindern zu können. Eine Lösung würde darin bestehen, ihre Handlungsmöglichkeiten massiv auszubauen. Hilfreich ist, dass sie aufgrund der aktuellen Novelle des BDSG zukünftig

einen besonderen Kündigungsschutz genießen und über eigenständige Weiterbildungsansprüche verfügen werden.

Sind Arbeitnehmer in Konzernunternehmen tätig, führt dies in vielen Fällen zu einer Erhöhung der Datenschutzprobleme. Einer der Hauptgründe hierfür ist die umfassenden Datenübermittlungen, die in diesen Fällen stattfinden. Von Arbeitgebern wird hier oft mit den Zwängen des Marktes und den anderenorts getroffenen Verarbeitungsentscheidungen argumentiert. Ergebnis ist, dass Arbeitnehmer und deren Betriebsräte oft nicht mehr wissen, wo welche Daten zu welchen Zwecken verarbeitet werden. Dies führt faktisch zur Aushöhlung bestehender Rechtspositionen der Beschäftigten. Allerdings werden Arbeitgeber auch in diesem Punkt zukünftig die Erforderlichkeit von Übermittlungen im Lichte des § 32 Abs. 1 Satz 1 BDSG begründen müssen.

Die vorstehenden Beispiele verdeutlichen das Eine: Um klare Grenzen für den Umgang von Arbeitgebern mit den persönlichen Daten ihrer Mitarbeiter zu setzen, reicht es nicht, auf bestehenden Normen im Bundesdatenschutzgesetz zu setzen. Notwendig sind vielmehr Datenschutzregelungen, die die spezifische Situation von abhängig beschäftigten Menschen in der Arbeitswelt angemessen berücksichtigen und die detaillierte Regelungen enthalten, als sie nunmehr in § 32 BDSG zu finden sind. Die Situation von Beschäftigten ist nämlich gerade nicht durch die Möglichkeit der freien Entscheidung über die Preisgabe von personenbezogenen Daten gekennzeichnet, sondern durch das Problem, dass Arbeitgeber am längeren Hebel sitzen. Hier für eine echte Parität zu sorgen, ist Aufgabe des längst überfälligen Gesetzes zum Arbeitnehmerdatenschutz. Ein solches Gesetz würde sich in andere Schutznormen einreihen wie etwa solche für Verbraucher oder Mieter und ist damit nicht systemfremd.

Im Ergebnis würde ein Arbeitnehmerdatenschutzgesetz zwar das Problem vorsätzlicher Datenschutzverstöße auch für die Zukunft nicht völlig aus der Welt schaffen. Es könnte aber durch klare Ge- und Verbotsnormen für alle Beteiligten deutlich machen, wann Arbeitgeber im Einzelfall unzulässig handeln und damit Rechtsklarheit schaffen.

C. Log as Log can – was Protokolle über unsere elektronische Kommunikation aussagen

Gerrit Wiegand
Geschäftsführer, mainis IT-Service GmbH

„Eine Unternehmenskultur, die von starkem Misstrauen gegenüber allen Mitarbeitern geprägt ist, dürfe es nicht geben". So lautete die einhellige Meinung von Unternehmensführung und Interessenvertretern, als Anfang diesen Jahres der erste Teil der Datenaffäre bei der Deutschen Bahn AG in den Jahren 2002 und 2003 öffentlich bekannt wurde.[1]

[1] Quelle: ARD Tagesschau vom 28.01.2009

Dieser markigen Aussage schließen sich die Pressestellen großer Konzerne vermutlich nur zu gerne an. Insbesondere in solchen Unternehmen, die wegen ihrer Größe, Geschichte oder Tätigkeit ohnehin im Licht der Öffentlichkeit stehen und auf ein gutes Image angewiesen sind.

Aber gerade diese Unternehmen haben uns in den vergangenen anderthalb Jahren gezeigt, dass es offensichtlich eine große Diskrepanz zwischen dem öffentlichen Image-Anspruch und den konkreten unternehmerischen Interessen gibt.

Den durch die Presse dankbar aufgegriffenen Anfang dieser Datenskandal-Kette machte der Einzelhandel, ausgerechnet vertreten durch die zweitgrößte Einzelhandelskette Deutschlands, die Schwarz-Gruppe mit ihrer Discounter-Kette Lidl[2]. Diese Branche kann sich im anhaltenden Einzelhandels-Preiskrieg, der nur wenig Platz für Alleinstellungsmerkmale bietet, ihren Status nur durch zwei gegenläufige Ziele sichern: immer effektivere Arbeit und Expansion. Effektivere Arbeit bedeutet als Ziel ein hundertprozentig funktionierendes System – und damit praktisch den Ausschluss des Kosten- und Fehlerfaktors Mensch. Expansion benötigt als Basis ein gutes Image, um Käufer in die eigenen Läden zu ziehen. Doch beides zusammen geht langfristig oftmals nicht gut, wie der deutliche Image-Verlust nach Bekanntwerden der Optimierung der Arbeitnehmer-Effektivität durch Überwachung gezeigt hat.

[2] Quelle: Spiegel Online vom 14.01.2008, „Lidl-Mutter weltweit unter den Top Ten"

Und dabei hat sich Lidl in den bekannt gewordenen Überwachungs-Fällen aus technologischer Sicht noch mit Möglichkeiten aus der Steinzeit zufrieden gegeben: Ganz klassisch mit Videokameras und menschlichen Detektiven wurden die Arbeitnehmerinnen und Arbeitnehmer überwacht. Das ist aufwändig, teuer und auffällig. Ein Vorgehen also, das so manch anderem mit dem Stand der Technik überwachenden Unternehmen geradezu lächerlich vorkommen muss.

Deutlich weiter war da offensichtlich die Deutsche Telekom AG: Anstatt ihre Aufsichtsrats-Mitglieder aufwändig von Detektiven beschatten zu lassen, hat sie kurzerhand die ohnehin anfallenden Verbindungsdaten der Handys genutzt, um herauszufinden, wer wann mit wem wie lange gesprochen hat. Und vielleicht auch, über was gesprochen wurde? Aber das werden wir wohl nicht erfahren, da das Netz offiziell als „nahezu abhörsicher" gilt – zumindest von Dritten, die keinen Zugang zur Netz-Infrastruktur haben.

Wie eingangs gesagt, handelt es sich bei den meisten der in den letzten anderthalb Jahren bekannt gewordenen Datenschutz-Skandale um solche in Unternehmen, die auf ein gutes Image in der breiten Bevölkerung angewiesen sind und denen aus der Aufdeckung auch merkliche finanzielle Schäden entstanden sind. Aber wie sieht es aus, wenn ein Unternehmen nicht unter den Argusaugen der Presse arbeitet? Wenn es zu klein oder zu unbekannt ist, um es auch nicht mit einem Skandal in die überregionalen

Nachrichten zu schaffen, oder gar keinen relevanten Endkunden-Markt besitzt, und somit nur auf ein partiell gutes Image angewiesen ist? In diesen Unternehmen wird weitaus mehr, intensiver und technisch hochgerüsteter überwacht, da ein potentieller Schaden nicht so groß wäre.

Ein Beispiel dafür ist Tönnies-Fleisch, Europas größter Fleischverarbeiter. Zeitgleich zur Aufdeckung der Lidl-Skandale im März 2008 wurde bei Tönnies-Fleisch genau das gleiche Vorgehen der Mitarbeiterüberwachung bekannt, schaffte es jedoch nur in die ausgewählte Presse und nicht in das Bewusstsein der Öffentlichkeit[3]. Oder schon zwei Jahre zuvor die Bayer AG, die eine Rundum-Internet-Überwachung im Unternehmen einführte und die Arbeitnehmer mit dem unmissverständlichen Satz „wer Unfug treibt, dem kommen wir auf die Schliche" einschüchterte[4]. Oder im Januar 2008 ein zum Medion-Konzern gehörendes Call-Center, das Mitarbeitern kündigte, die einer Rundum-Überwachung nicht zustimmten[5].

[3] Quelle: ARD „Report aus Mainz" vom 29.03.2008
[4] Quelle: Ziff-Davis-Verlag, 1/2006
[5] Quelle: Spiegel Online vom 21.04.2008, „Aldi-Zulieferer feuert renitente Mitarbeiter"

Diese Beispiele – und viele mehr – lassen erahnen, dass heute das Überwachen des Arbeitsplatzes in vielen Unternehmen zur Tagesordnung gehört.

Während die Überwachung durch Kameras und Detektive auch schon vor vielen Jahren möglich war und sich im betrieblichen Umfeld inzwischen nur etabliert hat, bietet der Einsatz von elektronischen Hilfsmitteln fast jeder Art weitaus mehr, günstigeres und umfassenderes Überwachungspotenzial. Die vollständige Überwachung des PC-Arbeitsplatzes passiert heute nahezu automatisch und selbst ohne jeden Vorsatz, da sie zum Betrieb der technischen Systeme unbedingt notwendig ist. Aber auch die Überwachung der Telefonie und das Erstellen von Bewegungsprofilen sind heute schon möglich und in vielen Fällen ist zumindest das Entstehen der Daten gar nicht mehr zu verhindern – sondern nur deren Auswertung. Und genau da steckt das Risiko: Daten, die erst einmal da sind, bieten sich früher oder später dazu an, ausgewertet zu werden. Oftmals fallen sie auch bei Systemen an, die eigentlich aus einem ganz anderen Grund eingeführt wurden. Aber es ist nur eine Frage der Zeit, bis die dabei anfallenden, zum Teil hochgradig kritischen Daten missbräuchlich verwendet werden: Gerade erst ist die „teuerste Marke der Welt[6]" – Google – mit einer neuen Anwendung an die Öffentlichkeit gegangen, die erkennen soll, wann Mitarbeiter mit ihrem Arbeitsplatz unzufrieden und damit potentiell wechselwillig sind. Googles Personalchef Laszlo Bock beschreibt es sogar so: „Der Algorithmus helfe Google über Wechselwillige Bescheid zu wissen, bevor die Betroffenen selbst wüssten, dass sie wechseln wollen[7]". Oder die Technologiefirma Honeywell, die auf allen PCs ihrer weltweit 130.000 Mitarbeiter – und damit auch denen der 6.000 deutschen Mitarbeiter – ohne Wissen der Betroffenen die Software „EnCase" installierte. Nach Angaben von Honeywell dient die Software ausschließlich dem „Schutz von Firmennetzwerken vor Angriffen durch Hacker, Viren und andere Schadsoftware[8]", faktisch jedoch ermöglicht sie eine zentrale heimliche Rundum-Überwachung aller PCs. Zwei Beispiele, in denen die Möglichkeit der vollständigen Überwachung – willentlich oder nicht willentlich – durch die Hintertür eingeführt wurde.

[6] Quelle: Spiegel Online vom 21.04.2008, „Die teuersten Marken der Welt"
[7] Quelle: heise.de vom 19.05.2009, „Google will mit Software Mitarbeiter-Abwanderung stoppen"
[8] Quelle: Süddeutsche Zeitung vom 17.04.2009, „Zoff um Überwachungssystem"

Aber wo fallen überhaupt welche Daten an?

Auf dem PC…

Beginnen wir mit dem Allereinfachsten: jedem PC oder Notebook. Egal, ob eine – in der Regel illegale – gesonderte Spionagesoftware auf einem PC installiert ist oder nicht, jedes Gerät verrät von sich aus schon eine Menge über das Verhalten seiner Benutzerinnen und Benutzer. Die Schlagworte dazu sind den Meisten bekannt, ihre Auswirkungen aber nicht unbedingt:

Der so genannte Browser Cache wird von praktisch jedem Internet-Browser geschrieben. Er „kopiert" die von Benutzern angesehenen Internet-Seiten auf die lokale Festplatte. Der technische Hintergrund ist, dass diese bei einem erneuten Aufruf der Seite nicht erst wieder vergleichsweise aufwändig und teuer aus dem Internet heruntergeladen werden müssen, sondern um ein Vielfaches schneller von der Festplatte geholt werden können. Damit bringt der Browser-Cache für Benutzer einen großen Komfort- und gegebenenfalls sogar Kostenvorteil. Riskant jedoch ist, dass dieser Zwischenspeicher, wenn er nicht regelmäßig gelöscht wird, die Daten über einen sehr langen Zeitraum vorhält – über Tage, Wochen oder sogar Monate. Da der Browser bei Standard-Installationen einfach einen gewissen Prozentsatz der Festplatte für diesen Cache reserviert und Festplatten heute extrem groß sind, gibt es aus technischer Sicht keinen Grund, ihn zeitnah zu löschen. Das bedeutet, das jedes Bild, jede Seite und jeder angesehene Inhalt zusammen mit den Informationen, wann und von wem er zuletzt angesehen wurde, auf der Festplatte verweilt. Ein nahezu perfektes Surf-Profil.

Ganz ähnlich wie mit dem Browser-Cache verhält es sich mit den Cookies: Jeder Internet-Browser speichert auch Informationen ab, die ihm von einer Internet-Seite übermittelt werden können. Das sind in der Regel kleine, inhaltlich eher nichtssagende Datenpakete, die aber dazu geeignet sind, dass Benutzer von Internet-Seiten „wiedererkannt" werden. Also sind auch diese Cookies technisch sinnvoll und notwendig. Nur liefern auch sie ein genaues Bild davon, wer wann auf welche Internet-Seite zugegriffen hat, werden sie heute doch von praktisch jeder Internet-Seite geschrieben. Gegenüber dem Browser-Cache kommt erschwerend hinzu, dass sie beim Löschen der „temporären Dateien" nicht immer mitgelöscht werden und damit zum Teil eine wesentlich längere Verweildauer auf der Festplatte haben.

Ein leicht anderes Ziel verfolgt der Browser-Verlauf: Der Verlauf, den jeder Browser beim Besuch von Internet-Seiten abspeichert, ist den meisten wohl nur als großer Komfortgewinn ein Begriff: Wenn eine Adresse in den Browser eingegeben wird, wird sie automatisch aus der Liste der bisher aufgerufenen Seiten heraus vervollständigt. Man muss also nicht die ganze Adresse tippen, sondern meist reichen schon die Anfangsbuchstaben, um die gewünschte Seite zu finden. So komfortabel diese Funktion ist, so genau listet sie jedoch alle in der Vergangenheit besuchten Internet-Seiten auf und gibt damit ein hervorragendes Surf-Profil ab.

Ganz ähnlich, nur umfassender, arbeitet der Windows-Verlauf: Auch MS-Windows merkt sich detailliert, welche Dateien zuletzt von den Benutzern geöffnet wurden. Der Komfortgewinn ist, dass über das

Start-Menü ein sehr schneller Zugriff auf die zuletzt bearbeiteten „Dokumente" und damit eine Wiederaufnahme der Arbeit möglich ist. In dieser Liste werden jedoch im Allgemeinen nur die letzten 10 oder 15 Dateien angezeigt, die daher nur selten bedrohlich wirken. Intern jedoch speichert Windows die Liste wesentlich länger und umfangreicher: Jeder Brief, jedes Video, jedes PDF-Dokument, jedes Bild und jede Präsentation, die geöffnet wurden, werden zusammen mit der Information, wann sie zum letzten Mal geöffnet wurde, für etwa vier Wochen akribisch protokolliert. Diese Liste kann sehr einfach von jedem, der Zugriff auf die Festplatte hat, eingesehen werden. Insgeheim speichert Windows jedoch viel mehr und viel länger: Mit entsprechender Software[9] lässt sich die Liste aller(!) in der Vergangenheit aufgerufenen Programme und Internet-Seiten seit der Erstinstallation des PCs – mitunter also über Jahre – einsehen. Und dieses Protokoll ist so gut versteckt, dass es faktisch nicht gelöscht werden kann.

[9] Beispielsweise der Software „FreshDiagnose", www.freshdevices.com

Als letztes bieten die temporären E-Mail-Dateien einen tiefen Einblick in die E-Mail-Aktivitäten: Wenn ein Anhang einer E-Mail geöffnet wird, beispielsweise ein PDF-Dokument oder ein Bild, muss dieses vom Betriebssystem vor der Anzeige aus technischen Gründen auf der Festplatte zwischengespeichert werden. Wenn jetzt das Dokument länger geöffnet bleibt als die E-Mail, verlieren die meisten E-Mail-Programme diese „Verbindung" und löschen das Dokument nicht mehr automatisch. Das kann beispielsweise die zugeschickte MP3-Datei sein, die noch gehört wird, als die E-Mail schon wieder geschlossen wurde. Das bedeutet, dass sich in diesem temporären Verzeichnis unabsichtlich E-Mail-Anhänge anhäufen. Es gibt in den meisten Fällen keinen vollautomatischen Mechanismus, der dieses Verzeichnis bereinigt, so dass sich E-Mail-Reste teils jahrelang zurückverfolgen lassen – und im Zweifelsfall bei genauem Hinsehen Grund zum Misstrauen geben können.

Insgesamt bietet damit jeder PC auch ohne jede Spionagesoftware die Möglichkeit, ein ziemlich umfassendes Aktivitäts-Protokoll zu erstellen. Dazu ist natürlich der Zugriff auf den PC notwendig, aber der ist leicht möglich: Entweder durch spezielle Software für Fernwartungs-Zugriffe[10] und mit betriebssystemeigenen Funktionen wie der administrativen Laufwerksfreigabe[11], oder aber durch heimliche oder offensichtliche Konfiszierung des PCs – wie jüngst bei der Deutschen Bahn AG „nach konkreten Verdachtsmomenten" geschehen[12].

[10] Dazu gehört beispielsweise Diagnose- und Management-Software, die in den meisten größeren Unternehmen eingesetzt wird, um den Überblick über die IT zu behalten und nicht wegen jedem „Fehlerchen" einen Administrator zum PC schicken zu müssen, sondern diesen aus der Ferne „übernehmen" zu können.

[11] Die administrative Laufwerksfreigabe ermöglicht berechtigten Administratoren in einem Netzwerk den vollen Zugriff auf die lokalen Festplatten mit allen(!) Daten des PCs, insbesondere also auch allen oben genannten Protokollen.

[12] Quelle: Süddeutsche Zeitung vom 19.04.2009, „Bahn gesteht Kontrolle von Festplatten"

…im Netzwerk…

Mit einem anderen Ansatz – und damit im Sinne der unternehmensweiten Überwachung deutlich effektiver – gehen Filter- und Monitoring-Software ans Werk. Filter-Software überwacht nicht alle Aktivitäten auf einem PC, sondern „nur" alle Internet-Aktivitäten wie Surfen, E-Mail, Chatten etc. Sie wird im Allgemeinen am in jedem Netzwerk vorhandenen zentralen Übergabepunkt zwischen dem Unternehmensnetzwerk und dem Internet installiert – dem „Gateway", das technisch gesehen ein Router, eine Firewall, ein Proxy-Server oder ähnliches sein kann –, und hat damit Zugriff auf alle Daten, die diesen Flaschenhals passieren müssen. Für diese Software ist es ein Leichtes, jede E-Mail zu öffnen und den Text zu analysieren, jede angeforderte Internet-Seite auf Schlagworte zu durchsuchen und jeden Satz, der in einen Chat-Room geschrieben wird, auf seine „inhaltliche Korrektheit" zu prüfen. Wie leistungsfähig

diese Software heute ist, kann man sich am Beispiel eines normalen Spam-Filters, den praktisch jedes Unternehmen im Einsatz hat, klar machen: Spam-Filter sortieren E-Mails heute nicht mehr nur alleine aufgrund von Schlagwörtern, wie das früher der Fall war. Dazu ist Spam heutzutage zu komplex und „gut", und das Risiko versehentlich aussortierter Mails viel zu groß. Daher versuchen heutige Spam-Filter, den Inhalt von E-Mails zu „verstehen", sie analysieren sie also semantisch und erfassen ihren Sinn. Diese millionenfach eingesetzte Technologie kann mit Leichtigkeit dazu verwendet werden, auch andere Informationen zu gewinnen und entsprechend zu verwenden. Beispielsweise persönliche Briefe, solche mit potenziell korruptem Inhalt oder schlicht nicht tätigkeitsbezogene Mails. Wie gut das funktioniert, weiß jeder Benutzer des E-Mail-Dienstes von Google, Google-Mail: Das kostenlose Angebot von Google wird darüber finanziert, dass die Mails inhaltlich analysiert und möglichst gut zum Inhalt passende Werbung eingeblendet wird – mit Erfolg!

Kurz gesagt bedeutet das, dass jede Aktivität, die eine Internet-Verbindung benötigt, detailliert protokolliert wird. Auf jeden Fall immer die Meta-Daten der Kommunikation wie das „wer", „wann" und „mit wem", immer häufiger aber auch das „was" – ohne dass sich die Benutzer dagegen wehren könnten oder überhaupt genau wissen, welche Daten anfallen.

Die Krux dabei ist, dass viele der Programme eigentlich sinnvolle Tätigkeiten verrichten. Filter-Software beispielsweise ist erst einmal nicht Schlimmes und auch nicht pauschal zu verurteilen. Sie ist dafür konzipiert, Regeln bei der Nutzung des Internets durch Mitarbeiterinnen und Mitarbeiter technisch zu unterstützen und gegebenenfalls einzuschränken. Das kann beispielsweise durch eine Beschränkung der Online-Zeit geschehen (entweder der tatsächlich genutzten Zeit oder aber beispielsweise der Zeitkorridore), durch das Verbieten von Internet-Diensten, die keinen direkten Bezug zur Arbeit haben (Tauschbörsen, Chat-Foren etc.), oder durch die Einschränkung der Internet-Seiten, die angesehen werden dürfen. Ob diese Art der Zensur als richtig empfunden wird oder nicht, mag jeder selbst entscheiden und eine Bewertung hängt letztendlich von den Gepflogenheiten im Unternehmen ab. Spannend wird es jedoch dann, wie die anfallenden Daten ausgewertet werden. Filter-Software beispielsweise kann Zugänge nicht einfach nur sperren, sondern darauf reagieren. Von der simplen Erstellung eines Log-Protokolls bis hin zu umfangreichen Alarmfunktionen gibt es alles, was technisch möglich ist. Und dabei werden nicht nur Klartext-Nachrichten wie E-Mails oder Chats ausgewertet, auch Dateianhänge oder gar Bilder können mit in die Suche nach Schlagworten für Alarmfunktionen einbezogen werden – und kopiert, gespeichert oder aber nur gesperrt werden.

…beim Telefonieren…

Nicht nur der PC und das Netzwerk liefern viele Informationen über unser Tun. Auch schon das simple Telefonieren über Festnetz, Handy oder neuerdings VoIP[13]. Dass die Meta-Daten von jedem einzelnen Telefonat („wer wann mit wem") heute an mehreren Stellen gespeichert werden, ist spätestens seit der Diskussion um die Vorratsdatenspeicherung hinlänglich bekannt. Aber die Technik kann noch viel mehr – und tut es auch: Bei jedem Handy-Telefonat wird unter anderem auch der Standort der mobilen

[13] VoIP steht für „Voice over IP" und damit das Telefonieren über das Internet und nicht mehr eine eigene, parallele Telefonie-Netzwerkstruktur.

Teilnehmer protokolliert. Dieser ist dem Anbieter bekannt, da sich jedes Handy in seiner nächstgelegenen Funkzelle anmeldet, die einen Radius von etwa 200 Metern bis hin zu wenigen Kilometern hat – je nach Besiedelungsdichte. Recht präzise Standort-Angaben, die zumindest seitens der Mobilfunk-Betreiber sehr genaue Bewegungsprofile zulassen. Diese sind dort eigentlich erst einmal gut aufgehoben und werden nicht herausgegeben, weshalb findige Entwickler inzwischen andere Lösungen gefunden haben: Ein neuer Spross der Google-Innovationen ist der Dienst „Latitude"[14]. Die einfache Installation einer Software auf dem Handy genügt, um Google ständig die aktuellen Standortdaten mitzuteilen, und das je nach Handy weitaus präziser als nur über die entsprechende Funkzelle, sondern beispielsweise auch über die aktuellen GPS-Koordinaten des Handys, also auf wenige Meter genau. Diese Daten können dann von Freundinnen und Freunden abgerufen werden – und sind erschreckend präzise. Zwar können die Benutzer einstellen, welcher Freund wie genaue Angaben über den Standort sehen darf (nur die Stadt oder detaillierter in verschiedenen Abstufungen), die exakten Daten selbst aber fallen bei Google auf jeden Fall erst einmal an. Außerdem ist es nur eine Frage der Zeit, bis diese Informationen beispielsweise bei Dienst-Handys auch an den „Freund" Arbeitgeber weitergegeben werden. Derzeit sucht Goggle zwar nach Lösungen, Missbrauch wenigstens einigermaßen auszuschließen – beispielsweise durch die SMS-Benachrichtigung des Betroffenen bei jedem fünften Ortungsversuch –, letztenendes wurde durch die Einführung dieser Technik jedoch die Büchse der Pandora geöffnet, die nur schwerlich wieder geschlossen werden kann.

[14] http://www.google.com/intl/de_de/latitude/intro.html

Aber in der Telefonie steckt noch mehr: Zunehmend verbreitet sich das Telefonieren über das Internet, kurz „VoIP". Privatanwender können heute praktisch keinen Breitband-Internet-Vertrag mehr abschließen, ohne VoIP kostenlos mit dazu zu bekommen – und sie nehmen dieses Angebot dankbar an, da es im Allgemeinen mit niedrigeren Gesprächsgebühren verbunden ist. Auch in Unternehmen verbreitet sich VoIP zunehmend, da bei den Verbindungskosten großes Einsparpotenzial besteht. Die Sprachdaten des Telefonats werden dazu digitalisiert und – wie beispielsweise eine Internet-Seite auch – über das Netzwerk und das Internet übertragen. Aber VoIP hat einen Haken: Es basiert auf den Protokollen „SIP" und „RTP"[15]. Erstgenanntes ist für den Verbindungsaufbau zuständig, letzteres für das eigentliche Gespräch. Das Problem ist, dass dieser weit verbreitete Standard keine Verschlüsselung des Gesprächs vorsieht. Damit können alle Datenpakete „belauscht" und die Telefonate inhaltlich rekonstruiert werden. Das, was jetzt so aufwändig klingt, ist in Wirklichkeit sehr einfach: Den Netzwerkverkehr mitzuprotokollieren ist leicht, und viele ohnehin in einem Netzwerk vorhandene Geräte stellen dazu sogar spezielle Funktionen bereit, die nahezu keinerlei Sachkenntnis des Benutzers erfordern[16]. Zur Auswertung dieser Protokolle benötigt man dann spezielle – legale! – Software, die die Pakete wieder chronologisch zusammenfügt – und damit auch das unverschlüsselte Telefonat wieder hörbar macht[17].

[15] SIP steht für „Session Initiation Protocol" und regelt den Verbindungs-Auf- und Abbau, während RTP, das Real-Time Transport Protocol, das eigentliche Gespräch überträgt.

[16] Dazu werden einfach alle Datenpakete, die übertragen werden, „kopiert" und auf die Festplatte geschrieben. Die Funktionen zum Speichern dieser Protokolle sind in vielen Routern, und Switches für die Fehleranalyse vorgesehen und können einfach über die Verwaltungsoberfläche eingeschaltet werden.

Auch hier gibt es Ansätze, im Nachhinein das Problem wieder in den Griff zu bekommen (beispielsweise „SRTP", wobei das S für Secure steht, oder den Alternativdienst Skype, dessen Gespräche standardmäßig verschlüsselt sind), im Normalfall aber können alle VoIP-Telefonate erst einmal von jedem, der Zugriff auf das Netzwerk hat – und sei es nur der heimische Router – im Nachhinein abgehört werden.

[17] Ein sehr bekanntes und kostenloses Programm zur Protokollanalyse ist beispielsweise „wireshark", www.wireshark.org

…und an vielen anderen Stellen

In unserem (beruflichen) Alltag fallen noch eine Vielzahl mehr von Protokollen an, die auch weit über die elektronische Kommunikation hinausgehen. Beispielsweise RFID-Chips[18] in Transpondern von schlüssellosen Zugangssystemen oder Unternehmensausweisen. Diese ermöglichen ein lückenloses Bewegungsprofil innerhalb der Räume des Unternehmens und natürlich auch Auswertungen wie die Häufigkeit des Toilettengangs oder den Zeitbedarf vom Büroeingang zum Arbeitsplatz. Oder auch echte, in der Regel illegale Spionage-Software, die alle PC-Aktivitäten nicht nur rundum überwacht, sondern neuerdings neben Bildschirmfotos auch heimlich Webcam-Fotos der Personen vor dem PC macht oder das Mikrofon in Notebooks einschaltet – mit allen daraus resultierenden Konsequenzen für das Ziel eines hundertprozentig funktionierenden Systems.

[18] RFID steht für „Radio Frequency Identification" und bezeichnet eine berührungslose Technik zum Auslesen eines weltweit eindeutigen Chips.

D. Anonymitätsinteressen und Arbeitnehmerdatenschutz

Prof. Dr. Marie-Theres Tinnefeld
Hochschule München

I. Einführung

Das Recht auf Anonymität ist als Teil des Grundrechts auf informationelle Selbstbestimmung (Datenschutz) gewährleistet. Schon der Gesetzgeber hat in unterschiedlichem Kontext ausdrücklich Anonymität vorgesehen. Die bekannteste Regelung findet sich im Allgemeinen Teil des BDSG (§ 3a). Darin ist der Grundsatz der Datenvermeidung und Datensparsamkeit festgelegt, wonach die Gestaltung und Auswahl der Datenverarbeitungssysteme nach Möglichkeit an Anonymisierungs- und Pseudonymisierungs-Lösungen auszurichten sind. Da es bis heute keinen Arbeitnehmerdatenschutz gibt, gilt die Regelung des § 3a auch für Arbeitsverhältnisse. Sie soll auch hier die „Autonomie des Einzelnen" stärken. Festzuhalten ist aber, dass die Vorschrift keine durchsetzbaren, verbindlichen Vorgaben macht, obwohl der Einzelne nirgends so nachhaltigen Informationsansprüchen ausgesetzt ist wie im Arbeitsverhältnis.

Arbeitnehmerdaten dürfen allerdings „zwangsweise" nur aufgrund bereichsspezifischer Regelungen (zum Beispiel für die Gewährung von Sozialleistungen) und ausschließlich für Zwecke des Arbeitsverhältnisses nach dem BDSG (§ 28 Abs. 1 Satz 1 Nr. 1) oder für andere Zwecke aufgrund einer ausdrücklichen Einwilligung (§ 4a Abs. 1 und 3) verwendet werden. Die Einwilligung ist allerdings im arbeitsrechtlichen Abhängigkeitsverhältnis eine problematische Legitimationsgrundlage. Umso mehr dürfen dem Arbeitnehmer keinerlei Nachteile angedroht werden, wenn er sich etwa der zweckentfremdeten Weitergabe seiner Daten beispielsweise im Konzern widersetzt.

Prinzipiell darf der Arbeitgeber keine besonderen Daten im Sinne von § 3 Abs. 9 BDSG erheben. Das gilt insbesondere für sensible Attribute, welche Informationen über eine Person darstellen, die nicht mit ihr verbunden werden sollen. Beispiele sind Religion, politische Haltung und Gesundheitszustand. Hervorzuheben sind Informationen aus einem prädikativen Gentest, bei denen Wahrscheinlichkeiten vorhergesagt werden, an einem bestimmten Leiden zu erkranken. Für diese Informationen gilt grundsätzlich ein Erhebungsverbot. Der Arbeitgeber darf sich die äußerst sensiblen Angaben auch nicht im Rahmen der Einstellungsverhandlungen von einem „genetisch gesunden" Arbeitnehmer aufdrängen lassen,[1] sie müssen von Anfang an anonym bleiben. Im Vergleich zu anderen Ländern fehlt in Deutschland bis heute eine ausdrückliche gesetzliche Regelung, sei es in einem Gendiagnostik- oder in einem Arbeitnehmerdatenschutzgesetz.

[1] Tinnefeld/Viethen, Arbeitnehmerdatenschutz und Internet-Ökonomie, NZA 2000, 978f.

Den Arbeitgeber geht es aus Gründen des Datenschutzes beispielsweise auch nichts an, welche Freizeitaktivitäten der Arbeitnehmer wahrnimmt, solange dieser sich an die gesetzlichen und vertraglichen Pflichten hält, seine Arbeitsleistung erbringt und die Interessen des Arbeitgeber nach dem (moralischen) Grundsatz von Treu und Glauben wahrnimmt, also den Vertrauensschutz im Unternehmen respektiert. Anders liegt der Fall, wenn der Arbeitnehmer vermeintliche oder bestehende Missstände in der Firma an die Öffentlichkeit bringt.[2] Hier ist zu prüfen, ob er als sogenannter Whistleblower anonym handeln darf, um vor einer potenziellen fristlosen Kündigung des Arbeitsverhältnisses oder vor einem Mobbing durch betroffene Mitarbeiter geschützt zu sein.

[2] Vgl. Tinnefeld/Rauhofer, DuD 11/2008, 720f.

Im Folgenden soll zuerst untersucht werden, was unter Anonymität zu verstehen ist und welche Bedeutung sie im Arbeitsverhältnis hat. Das führt zu der Frage, welche Interessen nach Anonymität und welche im Gegenteil nach Offenlegung der Identität verlangen. Danach sollen die Gefahren im Arbeitsverhältnis näher betrachtet werden, die sich aus der Anonymität beziehungsweise Identitätsoffenlegung für den Whistleblower ergeben.

II. Anonymität

Der Begriff „Anonym" kommt aus dem Griechischen und bedeutet namenlos. Der Name dient seit alters der Identifizierung einer Person. Anonym meint daher im Kern das Nicht-Offenlegen der Identität. Die Identität einer Person kann zwar in der Realität häufig immer wieder herausgefunden werden, unter Umständen aber erst mit einem sehr hohen Aufwand an Zeit, Kosten und Arbeitskraft. Ein absolutes Verständnis von Anonymität kann es in der Realität nicht geben. Man spricht daher im Datenschutzrecht von faktischer Anonymität.

1. Faktische Anonymität und Datenschutz

Im datenschutzrechtlichen Zusammenhang wird Anonymität relativ verstanden. Anonym bedeutet danach, dass die Offenlegung der Identität ohne unverhältnismäßigen Aufwand nicht möglich ist (vgl. auch § 3 Abs. 6 BDSG). Wie viele anonyme Informationen sind erforderlich, um etwa durch ihren Abgleich mit einer Vergleichsdatenbasis mehr oder weniger bestimmte personenbezogene Übereinstimmungen zu erreichen? Kann der Arbeitgeber anonyme genetische Daten aus einer Datenbank im Internet über die Datenbasis des Betriebsarztes personenbezogen erschließen? Er kann möglicherweise, aber er darf nicht. Die Vergleichsdatenbasis mit den Krankengeschichten der Arbeitnehmer muss technisch so sicher wie möglich vor dem Zugriff des Arbeitgebers abgeschottet sein.

2. De-Anonymisierung mit Data-Mining-Technologien

Anonymität kann in Zeiten des Internets allerdings relativ einfach überwunden werden. Mit Hilfe moderner Data-Mining-Technologien ist es in vielen Fällen möglich, anonymisierte Daten wieder einem Klarnamen zuzuordnen. Einzige Voraussetzung ist in der Regel, dass man Zugriff auf Datensätze ähnlichen Inhalts mit vorhandenen Klarnamen hat. Dies lässt sich häufig mit Hilfe frei zugänglicher Datenbanken im Internet oder den eigenen Unternehmensaufzeichnungen realisieren.

Ende 2007 ist es beispielsweise Informatikern der University of Texas in Austin gelungen, die von einem US-amerikanischen Online-DVD-Verleiher anonymisiert für einen Programmierwettbewerb zur Verfügung gestellten Filmbewertungen der Kunden, durch Verknüpfung mit frei zugänglichen Datenbanken im Internet teilweise wieder Klarnamen zuzuordnen. Das die vom Veranstalter zur Verfügung gestellten

Daten nicht nur Filmkritiken, sondern auch andere persönliche Informationen enthielten, war es möglich, umfangreiche Profile über die „enttarnten" Personen zu erstellen.[3]

Man kann davon ausgehen, dass Deutsche Bahn und Telekom ähnlich vorgegangen sind, um die von ihnen gesuchten „undichten Stellen" aufzuspüren. Da die Konzerne üblicherweise Zugang auf die Einzelverbindungsnachweise von dienstlichen Telefonen und Handys ihrer Mitarbeiter haben, kann ohne Weiteres nachvollzogen werden, welche Mitarbeiter mit bekannten Telefonnummern etwa von Journalisten telefoniert haben.

Richtigerweise stellt der Informatiker Tim Fickert fest: „Es ist nicht zwingend notwendig, dass unmittelbar ähnliche Datensätze vorhanden sein müssen. Auch eine Verkettung über mehrere Datenbanken ist möglich. So muss man beispielsweise zum Nachweis einer Verbindung zwischen einem eigenen Mitarbeiter und einem Journalisten und seinen Telefonanschlüssen zunächst eine Verknüpfung zwischen dem Namen des Journalisten und seinen Telefonanschlüssen vornehmen, anschließend kann man die der eigenen Firma vorliegenden Einzelverbindungsnachweise nach diesen Telefonnummern durchsuchen. Im Falle eines Treffers muss man letztendlich nur noch den Einzelverbindungsnachweis wieder einem Mitarbeiter zuordnen. Diese Ketten können prinzipiell beliebig lang werden, solange man Zugriff auf die benötigten Daten hat. Moderne Data-Mining-Technologien sind in der Lage, auch aus einer großen Anzahl von Daten und Datenbanken umfangreiche Querverbindungen zu ziehen."[4]

3. Das Recht auf Anonymität

Ein grundsätzliches Problem aus Sicht des Datenschutzes ist die Frage, mit welchen anderen Datensätzen geheimzuhaltende oder anonymisierte Daten abgeglichen werden dürfen. TK-Inhaltsdaten und grundsätzlich auch TK-Verkehrsdaten fallen unter den Schutz des Telekommunikationsgeheimnisses.[5] Letztere dürfen nur nach den Regeln des TK-Datenschutzes verarbeitet werden. Zur Ausübung des Grundrechts auf informationelle Selbstbestimmung des Mitarbeiters gehört es, dass diese Daten zu ganz bestimmten Zwecken genutzt werden dürfen, gegebenenfalls zu Abrechnungszwecken oder für die Verfolgung von schwerer Korruption und Wirtschaftskriminalität.[6] Der Kontakt eines Mitarbeiters zu einem Journalisten ist noch kein Indiz für einen „Geheimnisverrat"[7] oder für die Verletzung von Loyalitätspflichten und somit auch kein Grund für die Überwachung eines E-Mailaustausches.[8]

Der Mitarbeiter darf nur im gesetzlich zulässigen Rahmen vom Arbeitsgeber überwacht, nicht aber „bespitzelt" werden. Diese Wertung besagt, dass Anonymität als Teil des Grundrechtsschutzes der Normalfall und die Einschränkung der rechtfertigungsbedürftige Ausnahmefall ist. Der Vorwurf zur Beihilfe des „Geheimnisverrats" wird auch benutzt, um gegen Journalisten zu ermitteln und bei der Durchsuchung festzustellen, wer ihnen Informationen weitergegeben hat, wie es beim Magazin Cicero 2005 der Fall war.[9] Mit anderen Worten: Die Offenlegung einer Identität ist dem Staat nur dann erlaubt, wenn eine gesetzliche Grundlage vorhanden ist. Die Einschränkung muss durch ein überwiegendes öffentliches Interesse oder durch den Schutz von Grundrechten Dritter gerechtfertigt und verhältnismäßig sein.

[3] http://arxiv.org/abs/cs/0610105; s.a. Sweeney, Uniqueness of Simple Demographics in The U.S. Population, LIDAPWP4, Carnegie Mellon University , Laboratory for International Data Privacy , Pittsburgh, PA, 2000, der basierend auf den statischen Daten des Jahres 1990 gezeigt hat, dass 87 Prozent der amerikanischen Bevölkerung (248 Millionen Menschen) durch drei einfache demografische Merkmale: Geschlecht, 5-stellige Postleitzahl und exaktes Geburtsdatum eindeutig gekennzeichnet sind.

[4] Mail-Auskunft Fickert vom 24.03. 2009.

[5] LG Köln, Urteil vom 28.05.2008 - 28 O 157/08 unter: http://www.aufrecht.de/urteile/delikt-strafr/unzulaessigkeit-der-veroeffentlichung-privater-emails-im-internet-lg-koeln-urteil-vom-28052008-az-28-o-15708.html: "Der Absender einer Email wird in seinem allgemeine Persönlichkeitsrecht in Form der Geheimsphäre verletzt, wenn der Empfänger die Email auf einer öffentlich zugänglichen Homepage veröffentlicht. Die Geheimsphäre betrifft den Bereich menschlichen Lebens, der der Öffentlichkeit bei verständiger Würdigung nichtpreisgegeben werden soll. In diesen Bereich fallen schriftliche sowie Tonbandaufzeichnungen, per-

Bei privatem Handeln etwa des Arbeitgebers muss die Einschränkung durch ein Gesetz oder durch die Einwilligung des Mitarbeiters (die eine umstrittene Legitimationsgrundlage bildet) gerechtfertigt sein. Unter dem Stichwort strukturelle Unterlegenheit plant der Gesetzgeber bei einer Interessenabwägung eine stärkere Berücksichtigung der Besonderheiten im Arbeitsverhältnis (§ 28 Abs. 1 Nr. 2 BDSG). Es ist allerdings zu fragen, ob nicht unter den ausgefeilten neuen Technologien, durch die digitale personenbezogene und -beziehbare Informationen im Internet potenziell allgegenwärtig sind, ein umfassendes Arbeitnehmerdatenschutzgesetz erforderlich ist.

Jeder Eingriff durch den Staat oder jede Einschränkung durch die Wirtschaft in den Datenschutz ist an das Prinzip der Verhältnismäßigkeit gebunden. Es muss immer geprüft werden, ob es keine mildere Maßnahme gibt, mit welcher der Zweck einer zulässigen Maßnahme im Arbeitsverhältnis noch erreicht werden kann, ob gegebenenfalls auch pseudonyme Lösungen im Unternehmen in Frage kommen. Gerade die nahezu unbegrenzten technischen Möglichkeiten, sensible Arbeitnehmerdaten zu de-anonymisieren sind eine Herausforderung für den Gesetzgeber. Es gilt Techniken zu entwickeln beziehungsweise einzusetzen, die einen Identifikationsschutz vorsehen.

Gut designte Software und Computeranwendungen können dabei helfen, die Qualität von Informationen zu beurteilen. Das IT-System könnte etwa Regelungen treffen, wonach es eine zutreffende Antwort verweigert, falls dadurch eine zu schützende Information offen gelegt wird. Solche Regelungen gehören auch zu den kollektiven Aufgaben. Der Betriebsrat muss solchen Maßnahme zustimmen. Er kann sie auch im Rahmen einer Betriebsvereinbarung (§ 87 Abs. 1 Nr. 6 BetrVG) grundrechtskonform lösen.

III. Anonymitätsgefahren und Datenschutz

Die anonyme Weitergabe von personenbezogenen Daten ist nach Ansicht der „Art.-29-Datenschutzgruppe" (Datenschutzbeauftragte der Mitgliedstaaten in der EU) und der Arbeitsgruppe „Beschäftigtendatenschutz" des sogenannten Düsseldorfer Kreises (informationelle Vereinigung der obersten Aufsichtsbehörden) äußerst bedenklich. Die französische Datenschutzgruppe CNIL hat sie für datenschutzwidrig, also für illegal erklärt.[10] In Deutschland soll eine Bestimmung zum Informantenschutz in das BGB (§ 621a) eingeführt werden, um den Whistleblower, der etwa einen Wirtschafts- oder Datenschutzskandal aufdeckt, vor Sanktionen, insbesondere vor einer fristlosen Kündigung zu schützen.[11]

Anonymität kann dazu führen, dass die Qualität der anonymen Handlung leidet. Das ist etwa dann der Fall, wenn der Whisleblower als Denunziant agiert und seine anonyme Anzeige aus niedrigen Beweggründen tätigt oder völlig falsche Anschuldigungen vorbringt.[12] Es handelt sich also um die Gefahr, dass er die Möglichkeit der Anonymität nützt, damit ihm etwaiges kriminelles Handeln nicht zugerechnet werden kann und der Angezeigte sich nicht angemessen wehren kann. Zu den Perspektiven des europäischen Datenschutzes gehört grundsätzlich aber die Forderung des betroffenen Bürgers nach „Durchsichtigkeit der Verarbeitung seiner Daten".

sönliche Briefe, aber auch solche Aufzeichnungen und Briefe, die berufliche oder geschäftliche Fragen betreffen, insbesondere persönliche Aufzeichnungen zu beruflichen oder geschäftlichen Erlebnissen oder Planungen.

[6] Vgl. auch die Diskussion um die Vorratsdatenspeicherung bei Petri, DuD 11/2009, 729ff.

[7] Geheimnisverrat betrifft nach. § 353b StGB nur Staatsbedienstete, nicht Angestellte etwa der Bundesbahn.

[8] Aktuell zur „Bespitzelung" von E-Mails bei der Deutschen Bahn, Kuhr, Surfen auf dünnstem Eis, SZ v. 28./29. März, 2009, 2.

[9] Zur Verletzung der Pressefreiheit vgl. BVerfG, (Cicero)Urteil vom 27. Februar 2007 – 1 BvR 538/06; 1 BvR 2045/06 –.

[10] Siehe unter: www.theworld-lawgroup.com/newsletter/details.asp?ID=12436712205; siehe auch Tinnefeld/Rauhofer, DuD a.a.O, 2008, m.w.N.

[11] Zum Entwurf http://www.bundestag.de/ausschuesse/a10/anhoerungen/a10_81/16_10_849.pdf [30.06.2008]; s. auch die Zusammenstellung der in der Anhörung abgegebenen Stellungnahmen unter http://www.bundestag.de/ausschuesse/a10/anhoerungen/a10_81/index.html [30.06.2008].

[12] Zur dunklen Seite des Whistelblowings im Dritten Reich und der DDR vgl. Tinnefeld/Rauhofer, DuD, 2008, 721.

1. Anonymous Hotlines for Whistleblower?

Die Strafverfolgungsbehörden in Deutschland hätten es zwar ohne Hinweise von Mitarbeitern sehr viel schwerer gehabt, an deliktische Handlungen (Bespitzelungen etwa durch Ausspähen der Mails von Mitarbeitern) oder an Tatverdächtige heranzukommen. Trotzdem birgt ein anonymes System ein erhebliches datenschutzrechtliches Konfliktpotenzial. Nicht nur die anzeigende, sondern auch die angezeigte Person kann schutzwürdig sein. Dementsprechend muss beim Wistleblowing im besonderen Maß Wert auf festgelegte Verfahren gelegt werden, die das schutzwürdige Interesse beider betroffenen Personengruppen wahren.

In den USA hat die Verbreitung von Whistleblower-Systemen – anonyme elektronische Hotlines für Whistleblower – eine beachtliche Quote erreicht.[13] Der Sarbanes-Oxley Act (SOX) hatte bereits im Jahre 2002 alle an den US-Börsen gelisteten Unternehmen einschließlich ihrer Unternehmenseinheiten außerhalb der USA verpflichtet, weltweit einheitliche Codes of Conduct zum Zwecke der Förderung von ehrlichem und moralischem Verhalten einzurichten. Danach sind börsennotierte Unternehmen sowie Unternehmen mit Berichtspflichten gegenüber der Börsenaufsichtsbehörde SEC verpflichtet, Verfahren zur Entgegennahme, Speicherung und Verarbeitung für anonyme Anzeigen von Mitarbeitern einzurichten, die fragwürdige Methoden bei der Rechnungslegung, bei internen Rechnungslegungskontrollen und bei den internen Wirtschaftsprüfungsfragen betreffen.

[13] Bussmann/Matschke, wistra 2008, 88, 94.

In Deutschland werden inzwischen entsprechende Systeme bei der Strafverfolgung verwendet. So setzt das LKA Niedersachsen das „Business Keeper Monitoring System (BKMS) ein. Hier kann der Whistleblower unter technisch abgesicherter Geheimhaltung seiner Identität Angaben zu Sachverhalten machen, die seiner Meinung nach jeweils von dem Verwender näher zu bezeichneten Verstößen zuzuordnen sind, insbesondere von Wirtschaftsstraftaten.[14] Die Ausgestaltung der Verfahren ist nicht datenschutzkonform. Das gilt vor allem, wenn private Unternehmen eingesetzt werden, die keine Verfahrensregeln zum Schutz der Betroffenen vorsehen.

[14] Siehe unter: http://www.business-keeper.com/ger_DE/100/grundprinzip.html [30.06.2008] sowie Lindemann, ZRP 2006, 127; derzeit verwenden fünf Organisationen das BKMS: das LKA Niedersachsen, die kenianische Antikorruptionsbehörde, die Deutsche Telekom AG, die Kaufmännische Krankenkasse KKH und die AOK Bayern zusammen mit der Kassenärztlichen Vereinigung Bayerns; s. http://www.business-keeper.com/ger_DE/100/einsatzbereiche.html [30.06.2008].

2. Identitätstreuhänder als Ausweg?

Aus Datenschutzsicht bestehen Interessen an der Offenlegung der Identität des Whistleblowers. Der Gesetzgeber könnte offene Anzeigen einfordern. Die Offenlegung kann allerdings auch dazu führen, dass sich der Mitarbeiter aus Angst vor Drohungen, Einschüchterungen, Schikanen und einer potenziellen Kündigung „konform" verhält und eine Anzeige unterlässt, die ihm zurechenbar ist. Eine mögliche Lösung wäre die Installierung eines „Identitätstreuhänders".[15] Bei ihm müsste in besonderer Weise seine Neutralität sichergestellt sein. Jedenfalls genügt die Stellung als Rechtsanwalt oder Notar allein nicht als Gewähr für eine neutrale Amtsausübung. Man muss auch hier durch geeignete Verfahren eine Neutralität und Vertraulichkeit herstellen. Dies legen nicht zuletzt die Bahndatenaffäre und die Probleme mit einem Ombudsmann nahe.

[15] Zur Idee des Treuhänders in Fällen, wo ein Recht auf Anonymisierung zur Debatte steht vgl. Rudin, Das Recht auf Anonymität, digma 2008, 12.

Die neutrale Instanz muss die Identität des Anzeigenden kennen, um als Treuhänder wirken zu können. Bei dem Verfahren geht es um eine reversible Anonymisierung beziehungsweise um eine Pseudonymisierung, bei welcher der direkte Personenbezug entfernt, aber mit einem Schlüssel (Code) wieder hergestellt werden kann, um Anzeigen überprüfen zu können (Transparenzgebot). Dabei ist die Frage zu klären, unter welchen Voraussetzungen eine Re-Identifizierung des Whistleblowers datenschutzrechtlich geboten ist. Hier sind geregelte Anwendungsfälle in einem Arbeitnehmerdatenschutzgesetz erforderlich.

IV. Fazit

Schon jetzt versucht das deutsche Datenschutzgesetz, Anonymitätsinteressen der Bürger zu schützen. Ein eigens geregelter Schutz im Arbeitsverhältnis fehlt jedoch bis heute, obwohl die technischen Möglichkeiten einer De-Anonymisierung auch von sensiblen Arbeitnehmern im Arbeitsverhältnis enorm sind. Um betriebsnahe technische Anonymisierungslösungen zu erzielen, ist gegebenenfalls die Mitwirkung des Betriebsrates unverzichtbar.

Ein besonderer gesetzlicher Handlungsbedarf besteht im Bereich des globalen anonymen Whistleblowings. Interessen an der Offenlegung der Identität des Whistleblowers gibt es auch aus datenschutzrechtlichen Gründen. Andererseits bestehen Offenlegungsgefahren, die seine berufliche Existenz bedrohen. In solchen Fällen könnte die irreversible Anonymität durch eine reversible Anonymität über einen „Identitätstreuhänder" eingerichtet werden. Dazu müssten zur Gewährleistung der Grundrechte von betroffenen Arbeitnehmern technische und organisatorische Pseudonomysierungslösungen erarbeitet werden. Ein Arbeitnehmerdatenschutzgesetz sollte hier für alle Beteiligten Rechtssicherheit schaffen.

E. Impulsreferat: Strictly confidential vs. Die Gedanken sind frei

Anonym

Sehr geehrte Damen und Herren,

streng genommen dürfte ich hier und heute nicht sein, und auch zu Ihnen nicht sprechen. Laut einer im Konzern angewandten Information Protection Policy hätte ich mich mit dem Eingang zur heutigen Anhörung unverzüglich mit einem zentralen Koordinator für Kommunikation (Corporate Affairs) in England in Verbindung setzen müssen. Dort wäre dann abzustimmen, was über den Konzern, wie und durch wen, in die Öffentlichkeit darf.

Ich bin mit dem privaten PKW in meiner Freizeit angereist. Über eine Corporate Kreditkarte des Unternehmens wäre diese Reise, der Anlass, das was ich unterwegs verzehre und über die Karte ausgebe, registriert. Meine Abrechnung ginge (Einzelbelege eingescannt) an den Server in den USA sowie an das europäische Reisebuchungssystem nach England. Meine Reiseprofile sind also nicht nur im Konzern bestens bekannt, es ist über die Corporate Card auch eine Schufa-Auskunft über meine private Bonität vorhanden.

Anreisen über die Bahn tätige ich gar nicht mehr, da mit der Beantragung und dem Erhalt einer Bahncard (korrekte Zahlung über die Corporate Card, Fehlbuchung bei der Bahn) einige Mahnungen an mich persönlich, sowie ein Inkassoverfahren über ein durch die Bahn beauftragtes Inkassounternehmen ausgelöst wurden.

Sensible oder vertrauliche Kommunikation zwischen Arbeitnehmern und Arbeitnehmervertretern (und nicht nur diese) erfolgt immer häufiger nicht mehr über das Firmen-Telefon, -Handy, -Fax oder den Computer. Der Konzern behält sich nämlich das Recht vor, jederzeit und ohne Vorankündigung alle Informationsressourcen zu überwachen, auf sie zuzugreifen und sie zu nutzen, einschließlich der Inhalte von Firmencomputern. Mit dem Starten eines Rechners erreicht Sie zunächst folgende „Legal Notice": „Mit dem Drücken einer Taste greifen Sie auf das Eigentum des Konzerns zu. Die Nutzung dieses Eigentums wird durch Vorschriften und Verfahren des Konzerns geregelt, die auch das Recht auf Zugriff, Überprüfung, Lesen, Vervielfältigung und Druck von E-Mails und anderen Computerinhalten einschließen." Ohne diesen Tastendruck können Sie keine Arbeit beginnen! Weiterhin behält sich der Konzern das Recht vor, alle nicht dem Konzern gehörenden elektronischen Geräte zu überwachen und auf sie zuzugreifen, sofern darauf dem Konzern gehörende Informationen enthalten sein könnten.

Information Protection Regeln wie die Asset Classification (Dokumentklassifizierung – öffentlich, vertraulich, streng vertraulich) erleichtern ungemein einen zielsicheren Zugriff auf alle relevanten Dokumente weltweit.

Aus über 50 weiteren US-amerikanischen Information Protection Policies, Arbeitsanweisungen und Verpflichtungserklärungen des Konzerns gehen weitere Regelungen, Aktivitäten und Transaktionen hervor.

Viele globale Systeme sind in der Anwendung: Satisfaction Surveys & Rates (Service-Zufriedenheitsumfragen und Ergebnisse) werden regelmäßig erhoben, Job-Banding-Systeme erfassen und verarbeiten Daten zu Arbeitsbedingungen und machen diese weltweit vergleichbar. Performance-Zielvereinbarungselemente ergänzen und schließen den Kreis. Personalentwicklungsplattformen sind weltweit zugänglich und halten den Beschäftigten Profile von Arbeitnehmern vor. Seine Innovationsfähigkeit kann jeder Arbeitnehmer weltweit durch die innovative Ideeneingabe unter Beweis stellen.

Nicht nur oder seit dem 11. September 2001 bereisen Sicherheitsfachleute des Konzerns die Standorte, erfassen, sammeln, werten aus. Niemand weiß oder gibt Auskunft darüber, was mit Daten wie – wer gehört welcher Nichtregistrierungsorganisation, Gewerkschaft, Partei oder welchem Verein an – wo geschieht.

Sie sehen also, der Konzern meint es ernst, ernst mit seinem Eigentum, dem Schutz des Eigentums auch und insbesondere mit dem geistigen Eigentum. Natürlich sollen dabei die nationalen Gesetze eingehalten werden. Sich den Safe-Harbour-Regeln zu unterwerfen ist allerdings mit den Konzernzielen nicht vereinbar beziehungsweise konform.

Fazit

Arbeitnehmer und Arbeitnehmervertreter sind im Konzern überfordert. Betrachten Unternehmen grundsätzlich alle Arbeitnehmer als potentielle Kriminelle? Die Frage, was zulässig oder unzulässig ist, bleibt häufig ein Fragezeichen. Datenflüsse, deren Verwertung gerade in Konzernen, die weltweit eine aktive Rolle spielen, nicht transparent genug sind, um festzustellen, ob auch alles mit rechten Dingen zugeht. Shared Service Center, externe Auftragsbearbeiter und das gezielte Aufstellen der Server an unterschiedlichen Standorten der Welt tragen zu Ping-Pong-Effekten bei: Wer ist zuständig, wer ist verantwortlich, wer ist Ansprechpartner, wer hat Entscheidungskompetenzen? Arbeitnehmer sowie Arbeitnehmervertreter decken andere Profile beziehungsweise Prioritäten ab. Sie sind in aller Regel keine Informatiker, keine IT-Spezialisten, Techniker oder Juristen. Es kommen eher durch Zufall Vorgänge ans Licht. Ein Informationsschutz besteht nicht. Meldungen münden in Aussagen wie: Das eigene Nest beschmutzen ist nicht erwünscht oder es stehen viele Arbeitsplätze auf dem Spiel. Die juristische Auseinandersetzung zur Sache ist ebenfalls eher die Ausnahme.

Ein kodifiziertes Arbeitnehmerdatenschutzgesetz ist längst überfällig. Anbei einige Ansätze zu einem kodifizierten Arbeitnehmerdatenschutzgesetz:

- Neuformulierung relevanter Arbeitnehmerdaten zur Nutzung im Arbeitsverhältnis
- Ungeminderte Auskunftsrechte für Arbeitnehmer / Auskunftspflichten für Arbeitgeber (auch länderübergreifend)
- Neue Definition / Besonderer Schutz / Stärkung des geistigen Eigentums der Arbeitnehmer
- Freie Expertenwahl und Nutzung durch Arbeitnehmervertreter
- Informantenschutz / Kündigungs- und Maßregelungsverbot für alle Arbeitnehmer
- Arbeitnehmerschutz bei Schäden / Haftungspflicht des Verursachers
- Meldepflichten gegenüber Behörden
- Nachweispflichten der Arbeitgeber
- Gesetzlich versicherte Auftragsverfahren
- Regelmäßige behördliche Überprüfungen in den Unternehmen

F. Rechtsprechung

Wichtige Rechtsprechung zum Arbeitnehmerdatenschutz

Gegen ein eigenständiges Arbeitnehmerdatenschutzgesetz wird teilweise eingewandt, dass die differenzierte Rechtsprechung des Bundesverfassungsgerichts und der Arbeitsgerichte im Bereich des Arbeitnehmerdatenschutzes ausreicht. Allerdings spricht Einiges dagegen, die Rechtsfortbildung allein in die Hände der Gerichte zu geben:

Problematisch an der Rechtsprechung als Instrument der Rechtsetzung ist insbesondere die Einzelfallbezogenheit. Der Wortlaut ist punktuell auf einen speziellen Sachverhalt bezogen und die Entscheidung kann deshalb nicht verallgemeinert werden. Eine kleine Änderung des Sachverhalts führt möglicherweise zu einer vollkommen anderen Entscheidung. Diese Feinheiten sind für Beschäftigte schwer nachzuvollziehen. Diese Rechtsunsicherheit führt letztendlich auch dazu, dass bei einer nur geringfügigen Abweichung von der Rechtsprechung zum Mittel der Klage gegriffen wird.

Die Entscheidung eines höchsten Gerichts ist für den Einzelnen aber auch immer ein langer, schwieriger Prozess. Wenn die Rechtsfortbildung den Gerichten überlassen wird, bedeutet das aber auch, dass viele Sachverhaltsvariationen gar nicht zur Entscheidung kommen. Ein Arbeitsgerichtsprozess zerstört häufig das Vertrauensverhältnis und die Ungezwungenheit, die am Arbeitsplatz für eine angenehme und effiziente Arbeitsatmosphäre unverzichtbar ist, und macht so eine weitere Zusammenarbeit zumindest schwierig, wenn nicht sogar unmöglich. Verständlicherweise wagen nur wenige diesen Schritt in einem Beschäftigungsverhältnis, weil sie Ausgrenzung und Kündigung fürchten. Dementsprechend kann man trotz der vielen zum Arbeitnehmerdatenschutz ergangenen Entscheidungen von einer weit größeren Dunkelziffer an Datenmissbräuchen ausgehen, die bislang nicht geregelt werden können.

In Vorbereitung dieser Broschüre haben wir eine Datenbank zu den Entscheidungen im Bereich des Arbeitnehmerdatenschutzes angelegt. Darin sind nunmehr über 190 Entscheidungen verschiedenster Gerichte dokumentiert. Angesichts dieser Fülle von Entscheidungen wird besonders deutlich, dass der Bereich des Arbeitnehmerdatenschutzes für den einzelnen Beschäftigten, aber auch für den Arbeitgeber undurchschaubar ist. Unterinstanzliche aber auch höchstrichterliche Urteile sind teilweise widersprüchlich und für den Einzelnen schwer einschätzbar. Die unteren Instanzen warten oft auf eine Entscheidung des Bundesarbeitsgerichts, des Bundesverfassungsgerichts oder auch des Europäischen Gerichtshofs.

Ein eigenständiges Arbeitnehmerdatenschutzgesetz mit klaren und differenzierten Regelungen, die der Eigenart des Beschäftigungsverhältnisses Rechnung tragen und auch mit Blick auf die Zukunft entwickelt werden, kann dazu beitragen, dass der Einzelne sich nicht mit 190 Entscheidungen auseinandersetzen muss. Die Beschäftigten, die Arbeitgeberinnen und Arbeitgeber hätten ein Instrument zur Hand, um ihre Vertragsbeziehungen gemeinsam zu gestalten, mit dem Wissen, welche Grenzen dabei einzuhalten sind.

Hier finden Sie eine kleine Auswahl der wichtigsten Entscheidungen zum Arbeitnehmerdatenschutz:

Gericht, Az, Datum	Schwerpunkt der Entscheidung	Fundstellen/Kommentare
BAG, 1 ABR 20/74, 09.09.1975	Eine technische Einrichtung i.S.d. § 87 Abs. 1 Nr. 6 BetrVG ist dann dazu bestimmt, das Verhalten oder die Leistung der AN **zu überwachen**, wenn die Einrichtung zur Überwachung **objektiv** und **unmittelbar geeignet** ist, **ohne Rücksicht darauf, ob der AG dieses Ziel verfolgt und die durch die Überwachung gewonnenen Daten auch auswertet**. Die Möglichkeit, dass erst durch zusätzliche anderweitige Anordnungen oder bestimmte Gestaltungen zukünftig AN überwacht werden könnten, genügt andererseits nicht. Der Tatbestand des § 87 Abs. 1 Nr. 6 BetrVG greift auch, wenn aufgrund der Einrichtung unmittelbar Rückschlüsse auf das Verhalten oder die Leistung bestimmter anderer AN gezogen werden können, die nicht die mit der Einrichtung versehene Maschine bedienen.	

Gericht, Az, Datum	Schwerpunkt der Entscheidung	Fundstellen/Kommentare
BVerfG, 1 BvR 209/83 unter anderem, 15.12.1983	Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art. 2 Abs. 1 in Verbindung mit GG Art. 1 Abs. 1 umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf **„informationelle Selbstbestimmung"** sind nur im überwiegenden Allgemeininteresse zulässig.	Volkszählungsurteil: Meilenstein des Datenschutzes
BAG, 5 AZR 116/86, 07.10.1987	Eine **Verletzung des Persönlichkeitsrechts** eines ANs kann vorliegen, wenn er einem **ständigen lückenlosen Überwachungsdruck** dadurch unterworfen wird, dass der AG sich vorbehält, **jederzeit ohne konkreten Hinweis** den Arbeitsplatz durch versteckt aufgestellte Videokameras zu **beobachten**. Eine Maßnahme der vorbezeichneten Art kann allerdings gerechtfertigt sein, wenn überwiegend schutzwürdige Interessen des AGs sie erfordern. Hierzu bedarf es eines substantiierten Sachvortrages.	
BAG, 2 AZR 467/93, 11.11.1993	An der bisherigen Rechtsprechung des Bundesarbeitsgerichts zur Anfechtung wegen arglistiger Täuschung bei wahrheitswidriger Beantwortung der **Frage** nach der **Schwerbehinderteneigenschaft** ist jedenfalls in den Fällen weiter festzuhalten, in denen die Schwerbehinderungserkrankung für die auszuübende Tätigkeit **von Bedeutung** ist.	vgl. BAG U.v. 07.06.1984 - 2 AZR 270/83; BAG U.v. 28.02.1991 - 2 AZR 515/90

Gericht, Az, Datum	Schwerpunkt der Entscheidung	Fundstellen/Kommentare
BAG, 5 AZR 508/96, 29.10.1997	Das **heimliche Mithörenlassen von Telefongesprächen** zwischen AN und AG ist im Allgemeinen unzulässig. Es **verletzt** das **Persönlichkeitsrecht** des Gesprächspartners. Auf diese Weise erlangte Beweismittel **dürfen nicht verwertet werden**. Will der AG Dritte an einem Gespräch mit dem AN mithören lassen, muss er dies dem AN offenbaren.	
LAG BaWü, 12 Sa 115/97, 06.05.1998	Ein **Video-Spähangriff** eines AGs gegen eine Kassiererin eines Einzelhandelsbetriebes **verstößt gegen das allgemeine Persönlichkeitsrecht**, wenn vor Beginn des Angriffs kein durch Tatsachen begründeter Tatverdacht einer vorsätzlichen schweren Vertragsverletzung oder Straftat gerade gegen diese, sondern nur ein **pauschaler Verdacht gegen die gesamte Belegschaft** bestanden hat. Die hieraus gewonnenen Erkenntnisse dürfen – zumal wenn durch Missachtung des Mitbestimmungsrechts zustande gekommen – **als „Früchte vom verbotenen Baum" im Prozess nicht verwertet werden**; dies gilt auch für ein unter dem Druck der so gewonnenen Beweise abgegebenes unspezifisches Geständnis (Fernwirkung). Die ANin kann den aufgrund einer Drohung mit Strafanzeige abgeschlossenen Aufhebungsvertrag anfechten, weil die Drohung ein rechtswidriges, da inadäquates Mittel zur Abgabe der Willenserklärung i.S.v. § 123 BGB ist.	

Gericht, Az, Datum	Schwerpunkt der Entscheidung	Fundstellen/Kommentare
BAG, 2 AZR 55/99, 12.08.1999	Die Pflicht des ANs, beim Vorliegen eines berechtigten Interesses des AGs eine ärztliche Untersuchung seines Gesundheitszustandes zu dulden, ist im Übrigen auch ohne zum Beispiel tarifliche Regelung anzunehmen und resultiert aus der allgemeinen Treuepflicht des ANs. Das Interesse des AGs an der geforderten Untersuchung ist vielmehr abzuwägen gegen das Interesse des ANs an der Wahrung seiner Intimsphäre und körperlichen Unversehrtheit. Ein **AN ist** regelmäßig **nicht verpflichtet, im laufenden Arbeitsverhältnis routinemäßigen Blutuntersuchungen** zur Klärung, ob er alkohol- oder drogenabhängig ist, **zuzustimmen**.	vorgehend: LAG Hamm 19. Kammer, 02.11.1998, Az: 19 Sa 853/98, vorgehend: ArbG Bielefeld, 25.03.1998, Az: 3 (7) Ca 3176/97
BAG, 2 AZR 621/01, 06.02.2003	Die **Frage** des AGs nach einer **Schwangerschaft** vor der geplanten unbefristeten Einstellung einer Frau **verstößt regelmäßig gegen § 611a BGB**. Das gilt **auch** dann, **wenn** die Frau die vereinbarte Tätigkeit **wegen eines mutterschutzrechtlichen Beschäftigungsverbotes zunächst nicht aufnehmen kann**.	Teilweise Aufgabe der bisherigen Rechtsprechung vom 01.07.1993 - 2 AZR 25/93 - AP BGB § 123 Nr. 36 = EzA BGB § 123 Nr. 39" (Juris: AP Nr. 36 zu § 123 BGB = EzA Nr. 39 zu § 123 BGB).

Gericht, Az, Datum	Schwerpunkt der Entscheidung	Fundstellen/Kommentare
BAG, 2 AZR 51/02, 27.03.2003	1.) Die heimliche Videoüberwachung von AN greift in deren Allgemeines Persönlichkeitsrecht (Art. 2 Abs. 1 GG) ein und ist nur dann gerechtfertigt, wenn - **konkreter Verdacht einer strafbaren Handlung / schweren Verfehlung** des AN - **weniger einschneidende Mittel zur Aufklärung ausgeschöpft** - heimliche Videoüberwachung quasi **einzig verbleibendes Mittel** - insgesamt **nicht unverhältnismäßig**. Mildere Aufklärungsmaßnahmen bei Warenfehlbeständen (Diebstahlverdacht gegenüber AN): stichprobenartige Kontrolle des Lieferumfangs/Überprüfung im Warenwirtschaftssystem, oder Ähnliches 2.) Videoüberwachung unterliegt zwingender Mitbestimmung des BR (§ 87 Abs. 1 Nr. 6 BetrVG) Ist die Videoüberwachung entgegen § 87 Abs. 1 Nr. 6 BetrVG ohne vorherige Zustimmung des BR durchgeführt worden, ergibt sich aus diesem Verstoß jedenfalls dann **kein eigenständiges Beweisverwertungsverbot, wenn der BR** der Verwendung des Beweismittels und **der darauf gestützten Kündigung zustimmt** und die Beweisverwertung nach den allgemeinen Grundsätzen gerechtfertigt ist.	NZA 2003, 1193 NZA 2004, 1280: "schutzw. Belange des AG" hier hat das BAG im konkreten Einzelfall auch die verdeckte Videoüberwachung für zulässig gehalten

Gericht, Az, Datum	Schwerpunkt der Entscheidung	Fundstellen/Kommentare
BAG, 1 ABR 34/03, 14.12.2004	Eine vorgesehene **offene Videoüberwachung** (hier: in einem Postverteilzentrum) stellt einen **schwerwiegenden Eingriff** in das **Persönlichkeitsrecht** der hier beschäftigten AN dar. Die Videoüberwachung ist der AGin nicht allein auf Grund ihres Hausrechts gestattet. Postgeheimnis, Eigentum der Postkunden und eigene wirtschaftliche Interessen der AG sind hohe Rechtsgüter, reichen im vorliegenden Fall aber nicht aus, um den Eingriff in das Persönlichkeitsrecht der AN zu rechtfertigen. Es **reicht nicht, dass für einen Vorfall irgendein AN verantwortlich ist. Es muss ein eingrenzbarer Personenkreis verdächtig sein**. Wenn ein BR besteht, muss eine BV geschlossen werden, bei deren Ausgestaltung besonders das Allgemeine Persönlichkeitsrecht unschuldiger, nicht betroffener AN berücksichtigt werden muss.	Hans Decruppe, RA und FA für Arbeitsrecht, jurisPR-ArbR 29/2005 Anm. 3 (Anmerkung zum Urteil)
LAG Rheinland-Pfalz, 7 Sa 272/07, 29.08.2007	Die nach Begründung des Arbeitsverhältnisses durchgeführte **Eignungsuntersuchung** muss auf der Grundlage eines Vergleiches zwischen dem konkreten Gesundheitszustand des ANs und der konkreten arbeitsvertraglichen Tätigkeit, die er verrichten soll, erfolgen. Es fehlt an einem **konkreten Bezug zwischen dem Gesundheitszustand des ANs und der geschuldeten Arbeitstätigkeit**, wenn der untersuchende Arzt die negative Feststellung der gesundheitlichen Eignung darauf stützt, dass dieser an **Fettleibigkeit** leide und aufgrund des gegebenen Body-Mass-Indexes von 44,70 generell für eine Tätigkeit im öffentlichen Dienst ungeeignet sei.	

Gericht, Az, Datum	Schwerpunkt der Entscheidung	Fundstellen/Kommentare
BAG, 2 AZR 537/06, 13.12.2007	Allein die Verletzung eines Mitbestimmungstatbestands oder die Nichteinhaltung einer Betriebsvereinbarung und deren Verfahrensregelungen können es grundsätzlich nicht rechtfertigen, einen entscheidungserheblichen, unstreitigen Sachvortrag der Parteien nicht zu berücksichtigen und im Ergebnis ein „**Sachverhaltsverwertungsverbot**" anzuerkennen. Jedenfalls rechtfertigen die möglichen Verstöße der Mitarbeiter der Beklagten gegen die Regelungen der BV-Personalkontrolle bei der Durchführung der Spätkontrolle am 8. Februar 2005 es nicht, die daraus gewonnenen, unstreitigen Erkenntnisse, nämlich die Auffindung des Lippenstifts in der Tasche der Klägerin, bei der Bewertung des wichtigen Grundes außer Acht zu lassen.	vorgehend ArbG Rheine, 25.10.2005, Az: 3 Ca 349/05, Urteil vorgehend LAG Hamm (Westfalen) 3. Kammer, 05.04.2006, Az: 3 Sa 1376/05, Urteil
BAG, 1 ABR 16/07, 26.08.2008	AG und BR **sind grundsätzlich befugt, eine Videoüberwachung** im Betrieb einzuführen. Die Zulässigkeit des damit verbundenen Eingriffs in die Persönlichkeitsrechte der AN richtet sich nach dem Grundsatz der **Verhältnismäßigkeit**.	

Legende:
AG = Arbeitgeber
AN = Arbeitnehmer
Bekl. = Beklagte
BR = Betriebsrat
BV = Betriebsvereinbarung
Kl. = Kläger

G. Position des DGB zum Arbeitnehmerdatenschutz

(Beschluss des DGB-Bundesvorstandes vom 02.12.2008)

Allgemeine Bemerkungen

Der Umgang mit Internet, E-Mail und Mobiltelefonen, Online-Banking und Internethandel sowie Kreditkarten und elektronischen Bonus-Systemen ist in den letzten Jahren für die meisten zur Selbstverständlichkeit geworden. Bequem und schnell wird kommuniziert und gehandelt. Dabei fallen persönliche Daten an, die oft nur unzureichend gegen unrechtmäßige Nutzung und Weitergabe an Dritte gesichert sind.

Im Arbeitsverhältnis werden Chipkarten eingesetzt, die den Zugang der Beschäftigten aufzeichnen, bei der Verwendung von RFID (radio frequency identification) können Tätigkeitsprofile erstellt werden und Handys ermöglichen über GPS (global positioning system) jederzeit die Feststellung, wo sich Beschäftigte befinden. Leistungskontrollen sind über die Benutzerprofile am Computer auch ohne besondere Software möglich. Und nicht zuletzt werden unter dem Stichwort Terrorbekämpfung von staatlichen Stellen über den Arbeitgeber im Rahmen der Sicherheitsüberprüfung Daten zum Beispiel über religiöse Präferenzen oder ethnische Herkunft ermittelt und weitergegeben – sogar an ausländische Stellen und für Daten, die eigentlich dem Persönlichkeitsschutz unterliegen. Zusätzlich entstehen mit Vorhaben wie der elektronischen Gesundheitskarte und dem Verfahren des elektronischen Einkommensnachweises (ELENA) riesige Datensätze, deren Verwendung zwar gesetzlich geregelt ist, die aber durchaus neue Begehrlichkeiten wecken können.

Durch all dies entstehen erhebliche Gefahren. So wurden von Seiten der Landesbeauftragten für den Datenschutz erhebliche verfassungsrechtliche Bedenken gegen den ELENA geäußert. Denn unter staatlicher Verantwortung und Verfügungsmacht werde eine riesige Datensammlung entstehen. Die betroffenen ArbeitnehmerInnen hätten keine Einflussmöglichkeiten. Diese riesige Datensammlung verstieße gegen das verfassungsrechtliche Verbot einer Datenspeicherung auf Vorrat. Es wäre ein unverhältnismäßiger Eingriff in das Grundrecht auf informationelle Selbstbestimmung.

Im Übrigen hat sich gezeigt, dass die persönlichen Daten insbesondere von Beschäftigten, aber auch im allgemeinen Geschäftsverkehr außerordentlich missbrauchsanfällig sind. Die Vorfälle bei Lidl und anderen Discountern, die die Überwachung von Mitarbeitern bis hin zur Videobeobachtung in Umkleideräumen angeordnet haben, die Telefonbespitzelung bei der Telekom und die Weitergabe der Gewerkschaftsmitgliedschaft im Rahmen des Abkommens zur Datenübermittlung zwischen Deutschland und den USA haben gezeigt, dass die Hemmschwelle, das Persönlichkeitsrecht von Beschäftigten und Bürgern zu verletzen, soweit überhaupt noch vorhanden, zumindest außerordentlich niedrig ist.

Der DGB und seine Mitgliedsgewerkschaften fordern seit Jahren wirksame gesetzliche Regelungen in einem eigenständigen Arbeitnehmerdatenschutzgesetz, die sicherstellen, dass dem Persönlichkeitsrecht der Beschäftigten im Arbeitsverhältnis endlich Rechnung getragen wird. Dabei bedeutet Datenschutz den Schutz personenbezogener und -beziehbarer Daten von Beschäftigten vor Missbrauch.

Notwendigkeit klarer gesetzlicher Regelungen

Zweck des Datenschutzes muss es sein, den Einzelnen davor zu schützen, dass durch Missbrauch seiner Daten eine Beeinträchtigung seines grundrechtlich geschützten Persönlichkeitsrechts erfolgt. Obwohl der Koalitionsvertrag der ersten rot-grünen Regierung ein solches gesetzgeberisches Vorhaben vorsah, ist dieses Vorhaben weder auf nationaler Ebene noch auf europäischer Ebene bislang auch nur ansatzweise verwirklicht worden. Gerade auf Grund der aktuellen Vorfälle ist es deshalb notwendig, die bisherigen Forderungen zu bekräftigen und die Politik aufzufordern, ihrer Verpflichtung, die Grundrechte zu schützen, durch wirksame Gesetze nachzukommen und deren Einhaltung durch wirksame Sanktionen zu gewährleisten.

Die Regelung dieses wichtigen Bereiches darf nicht der Rechtsprechung allein überlassen werden, die nur in der Lage ist, in Einzelfällen zu entscheiden. Zudem kann die Rechtsprechung keine unmittelbare Bindungswirkung im Allgemeinen entfalten. Das informationelle Selbstbestimmungsrecht und das allgemeine Persönlichkeitsrecht müssen im Arbeitsverhältnis geschützt werden.

Insgesamt ist die Forderung nach einem Arbeitnehmerdatenschutzgesetz nach wie vor dringlich. Zurzeit stellt sich die Rechtslage unübersichtlich und unklar dar. Ziel einer eigenständigen gesetzlichen Regelung muss daher auch sein, für Arbeitgeber und Arbeitnehmer klare und möglichst verständliche Regelungen zu schaffen. Die Vorschriften müssen klar strukturiert sein. Der Schutz der Beschäftigten vor unzulässiger Datenerhebung, -verarbeitung, -speicherung und -nutzung könnte so besser in der Praxis durchgesetzt werden, und die Arbeitgeber bekämen den Rahmen aufgezeigt, in dem sie sich legal bewegen können. Dabei muss ebenfalls klargestellt werden, dass das Datenschutzgesetz einen Minimalstandard regelt, der auch durch Betriebsvereinbarungen nicht unterschritten werden darf.

Forderungen des DGB:

1.
Die gezielte Beobachtung und Überwachung von Beschäftigten am Arbeitsplatz, aber auch im privaten Umfeld muss ausdrücklich verboten werden. Es muss klargestellt werden, dass weder eine direkte Überwachung durch Beauftragte, Externe noch durch Mitarbeiter oder eine indirekte Überwachung durch Video- oder Tonaufnahmen gerechtfertigt ist. Soweit der Schutz von Anlagen eine Überwachung notwendig macht, ist dies durch Betriebsvereinbarung zu regeln. Ebenso wenig kann die Kontrolle der Beschäftigten durch Auswertung oder mit Hilfe computergesteuerter oder biometrischer Systeme erlaubt sein. Nur für den Fall, dass der begründete Verdacht einer strafbaren Handlung, eines Missbrauchs oder einer schwerwiegenden Schädigung des Arbeitgebers besteht, kann auf gesetzlicher Grundlage eine Überwachung im Einzelfall zulässig sein. Die Anordnung einer solchen Überwachung bedarf jedoch immer der Zustimmung der betrieblichen Interessenvertretung. Ebenso kann ausnahmsweise die Überwachung aufgrund höherrangiger Interessen wie der Sicherheit und der Gesundheit der Bevölkerung (zum Beispiel bei der Überwachung von Atomkraftwerken) gerechtfertigt sein. Dann muss der Eingriff in das Persönlichkeitsrecht der Beschäftigten so gering wie möglich gehalten werden.

2.
Bei elektronischer Datenverarbeitung ist eine besondere Schutzbedürftigkeit in Bezug auf das allgemeine Persönlichkeitsrecht gegeben, da im Hinblick auf die Vielzahl und die Qualität der verwendeten Daten, die Kombinations- und Auswertungsmöglichkeiten, den Kontextverlust und die zeitlich unbegrenzte Verfügbarkeit besondere Risiken bestehen. Um der strukturellen Unterlegenheit von Beschäftigten Rechnung zu tragen, kann deshalb das grundsätzliche Verbot des Zugriffs auf personenbezogene oder beziehbare Nutzerdaten bei der Verwendung moderner Kommunikationsmittel durch den Arbeitgeber auch nicht durch eine generelle Einwilligung des Arbeitnehmers ausgeschlossen werden. Durch gesetzliche Regelungen, die auch spezifisch erforderliche Abweichungen durch Tarifvertrag oder Betriebsvereinbarung vorsehen können, kann die Datenerfassung durch Arbeitgeber aus dringenden betrieblichen Gründen für bestimmte Fälle vorgesehen werden.

3.
Das Fragerecht des Arbeitgebers bei der Einstellung und die Möglichkeit der Anordnung von ärztlichen Untersuchungen muss gesetzlich auf die Fälle beschränkt werden, die die Rechtsprechung bislang vorsieht. Das bedeutet, dass nur die Fragen bei der Einstellung zulässig sind, die für die konkrete Tätigkeit von entscheidender Bedeutung sind. Ebenso darf nur dann eine ärztliche Untersuchung angeordnet werden, wenn dies ausdrücklich gesetzlich geregelt ist (zum Beispiel im Jugendarbeitsschutzgesetz). Verboten werden muss, dass der Arbeitgeber die Ergebnisse ärztlicher Untersuchungen entgegen-nimmt oder verwendet, insbesondere im Zusammenhang mit Pflichtverletzungen aus dem Arbeitsvertrag. Dies muss im besonderen Maße für Genomanalysen gelten. Für Drogen- und Alkoholtests muss gelten, dass ihre Durchführung weder angeordnet, noch die Ergebnisse entgegengenommen werden dürfen, es sei denn, es liegt ein begründeter Verdacht des Drogen- und Alkoholmissbrauchs vor und der Beschäftigte hat in den Test eingewilligt. Außerdem muss vor Anordnung aller Untersuchungen die Zustimmung des Betriebsrates vorliegen.

4.
Sofern Beschäftigte gleichzeitig auch Kunden ihres Arbeitgebers sind, wie dies zum Beispiel bei Banken, Versicherungen oder auch in Krankenhäusern häufig der Fall ist, muss sicher gestellt werden, dass die den Kundenbereich betreffenden Daten gesondert geführt und geschützt werden. Insbesondere muss gewährleistet sein, dass die personalverantwortliche Stelle auf die Daten nicht zugreifen kann.

5.
Sofern Arbeitnehmer interne Daten über schwerwiegende Rechtsverstöße des Arbeitgebers, die geeignet sind, Gesundheit oder Leben der Beschäftigten oder der Allgemeinheit zu gefährden, wie zum Beispiel bei den Fleisch- oder Schwarzgeldskandalen der jüngsten Vergangenheit an staatliche Stellen weiterleiten müssen sie vor Repressalien durch den Arbeitgeber geschützt werden. Dies kann dadurch erfolgen, dass das Recht zur Weitergabe ausdrücklich geregelt wird, mit der Folge, dass dieses Recht dann dem Maßregelungsverbot unterliegt.

6.
Erlaubte Datenerhebung muss diskriminierungsfrei erfolgen, unrechtmäßig erworbene Daten müssen einem Beweisverwertungsverbot unterliegen.

7.
Die Rechtsposition des betrieblichen Datenschutzbeauftragten muss verbessert werden. Dazu kommt in Betracht, dass er, wie Betriebsräte auch, vor Kündigungen geschützt wird. Zudem müssen die Mitbestimmungsrechte der Betriebsräte beim Datenschutz gestärkt werden.

8.
Die Einhaltung der gesetzlichen Bestimmungen kann nur dann gewährleistet werden, wenn die alleinige Last der Durchsetzung ihrer Rechte durch Klage von den betroffenen Beschäftigten genommen wird. Die Erfahrung zeigt, dass Arbeitnehmer im bestehenden Beschäftigungsverhältnis in der Regel nicht gegen den Arbeitgeber klagen können. Zu groß ist die Gefahr von Repressalien bis hin zur Kündigung. Deshalb reicht es nicht aus, dass gesetzlich ein so genanntes Maßregelungsverbot vorgesehen wird, das heißt, dass dem Arbeitgeber verboten wird, Beschäftigte wegen der Wahrnehmung ihrer Ansprüche aus einem Arbeitnehmerdatenschutzgesetz zu benachteiligen. Vielmehr muss ein Verbandsklagerecht vorgesehen werden.

9.
Um den gesetzlichen Regelungen auch tatsächlich Wirkung zu verleihen, sind angemessene und abschreckende Sanktionen vorzusehen. Zum einem muss demjenigen, dessen Persönlichkeitsrecht verletzt worden ist, ausdrücklich ein konkreter Anspruch auf Schmerzensgeld in Form einer Entschädigung, entsprechend der Entschädigungsregelung in § 15 AGG bei Verstoß gegen das Diskriminierungsverbot, zugebilligt werden. Dieser Entschädigungsanspruch kann entweder direkt für bestimmte Verstöße die Höhe der Entschädigung regeln oder die gesetzliche Regelung muss den abschreckenden Charakter einer solchen Entschädigungszahlung ausdrücklich hervorheben. Darüber hinaus muss die Verletzung des allgemeinen Persönlichkeitsrechts strafbewehrt werden. Die bloße Ordnungswidrigkeit reicht angesichts der rechtsverneinenden Praxis der Arbeitgeberseite nicht aus.

10.
Bei Verfahren wie der elektronischen Gesundheitskarte und ELENA muss zwingend sichergestellt werden, dass die persönlichen Daten der Betroffenen vor unbefugtem Zugriff geschützt sind und nur in Kenntnis und mit Zustimmung der Betroffenen verwendet werden können. Solange daran Zweifel bestehen, muss die Verwendung ausgeschlossen sein.

11.
Das Bundesdatenschutzgesetz muss den heutigen technischen Gegebenheiten des Internets angepasst werden. Im Falle einer Datenverarbeitung im Auftrag müsste im § 11 BDSG dahingehend präzisiert werden, dass für die in Auftrag gegebene Datenverarbeitung und die zu treffenden technisch-organisatorischen Maßnahmen ein Vertrag abzuschließen ist und welchen Mindestanforderungen er entsprechen

sollte. Die Nutzung muss dokumentiert werden. Außerdem wird der Sanktionsrahmen weder im Bereich des Ordnungswidrigkeitenrechts noch im Strafrecht vollständig ausgeschöpft. Deshalb sollten Verstöße gegen das Bundesdatenschutzgesetz Offizialdelikte statt Antragsdelikte sein.

12.
Beim europäischen Datenfluss im Zusammenhang mit Migration ist unbeschadet der Einführung angemessener Instrumente des Datenschutzes auf Behördenebene darauf zu achten, dass die dort gewonnenen Daten möglichst vor dem Zugriff durch Arbeitgeber geschützt sind.

H. Weiterführende Literatur

Däubler, Prof. Dr. Wolfgang	Gläserne Belegschaften?, 4. Aufl., 2002 Neuauflage im Herbst 2009
Wedde, Prof. Dr. Peter	Schutz von Beschäftigtendaten – weiterhin ein Problem, AiB 2009, S. 57
Wedde, Prof. Dr. Peter	Wenn der Arbeitgeber heimlich filmt, Der Betriebsrat 2008, Nr. 5, S. 16-17
Wedde, Prof. Dr. Peter	Für die Unternehmen muss es richtig teuer werden, Mitbestimmung (Magazin der Hans-Böckler-Stiftung) 5/2009, S. 24
Schaar, Peter	Bundesdatenschutzbeauftragte für den Datenschutz und die Informationsfreiheit, 22. Tätigkeitsbericht, 2007-2008

DGB Neuerscheinungen

DGB40342 Broschüre: Elterngeld und Elternzeit – Nutzen Sie die Chance für eine partnerschaftliche Teilung!

DGB41494 Broschüre: Ratgeber Ausgelernt – und nun? Studieren!

DGB23012 Broschüre: Forderungen an die künftige Regierungspolitik zu Migration, Integration und Antirassismus

DGB23013 Broschüre: Wahl- und Regierungsprogramme der Parteien im Vergleich

DGB40341 Broschüre: Frauen bestimmt. Gleichstellungspolitische Positionen des DGB im Wahljahr 2009

DGB10010 Broschüre: Politische Anforderungen des Deutschen Gewerkschaftsbundes im Jahr 2009

DGB60017 Broschüre: Der Deutsche Qualifikationsrahmen (DQR) – Chancen und Risiken aus gewerkschaftlicher Sicht

DGB24010 Broschüre: Für ein nachhaltiges Deutschland? Zum Fortschrittsbericht 2008 der nationalen Nachhaltigkeitsstrategie

DGB21345 Ratgeber: Hilfen für Beschäftigte mit geringem Einkommen – Wohngeld – Kinderzuschlag – Hartz IV

DGB25039 Broschüre: Rente mit 67. Erhöhtes Risiko von Einkommenseinbußen und Altersarmut

Bestellung von Broschüren und Materialien des DGB
bitte über das DGB-Online-Bestellsystem:
Link: https://www.dgb-bestellservice.de

Schriftliche Bestellungen NUR für
Bestellerinnen/Besteller ohne Zugang zum Internet:
PrintNetwork pn GmbH · Stralauer Platz 33 – 34 · 10243 Berlin