

EDV Tage 2009

SAP im Einsatz - Neue Perspektiven für die betriebliche Interessenvertretung
im Wilhelm-Gefeller-Bildungszentrum der IG BCE in Bad Mündel

Friedrich-Karl Matten

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit
Ref. III Sozialwesen, Mitarbeiterdatenschutz, Bonn

Gesetzlich geregelter Arbeitnehmerdatenschutz – dringender denn je

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 Urlaubdaten. 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 – z.B. 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 ungezielt 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. Die Zwecke liegen vor allem in der Rationalisierung der Betriebsabläufe durch Automation sowie in der Erhöhung der Produktionssicherheit wie allgemein der Sicherheit angesichts neuer Risiken.

Der Einsatz von IT für Kontrollzwecke wird immer billiger, einfacher in der Anwendung, komplexer, intelligenter und vernetzter.

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 geplante Kontrollsystem produziert ganz nebenbei, was sich ein jeder Arbeitgeber wünscht: Den gläsernen Mitarbeiter.

In Deutschland kann ein Arbeitgeber nicht nach eigenem Belieben Software zur Überwachung seiner Arbeitnehmer einführen. Unser 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.

Gesundheitsdaten im Arbeitsleben:

Das genannte 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 sind die Begehrlichkeiten von Arbeitgebern, möglichst viel über den Gesundheitszustand ihrer Mitarbeiter zu wissen, groß. 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 z.B. 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 sog. 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 Diensttelefons 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 Internet-Zugangs zu unterbinden, kann er die private Nutzung an bestimmte Bedingungen hinsichtlich des Zeitrahmens, der zugelassenen Bereiche und regelmäßig durchzuführender 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 anderer 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 Arbeitnehmersverhaltens 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, z.B. 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 z.B. 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, während die Videoüberwachung in einem Kaufhaus ggf. auch legitimerweise zum Schutz vor Diebstählen durch den Mitarbeiter eingesetzt wird.

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 „ultimo ratio“ nur zulässig, wenn das die einzige Möglichkeit darstellt, berechnigte 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 kontaktlose Betriebs- oder Chipausweise im Einsatz. Sie dienen zum einen der Zeiterfassung, aber oftmals auch zugleich als Zutrittsschlüssel. Ganz nebenbei lassen sich so nicht nur das Kommen und Gehen protokollieren, sondern auch das Betreten und Verlassen einzelner Räume. Über den Karteneinsatz 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 von elektronischen Dokumenten oder als Berechnigungskarte für Serviceangebote des Arbeitgebers. Dadurch entstehen in der Kantine Konsumprofile, in Freizeiteinrichtungen Interessenprofile und im Intranet Tätigkeitsprofile.

Gegen die Einführung dieser Systeme ist grundsätzlich nichts einzuwenden. Allerdings ist das zweckfremde Nutzen und Zusammenführen all dieser Daten nicht zulässig – aber möglich. Und der Reiz, diese vorhandenen Daten auch zu nutzen, ist für manch einen Arbeitgeber groß. Bei der Einführung von Chipausweisen sollte daher unbedingt darauf geachtet werden, dass in einer Betriebsvereinbarung/ Dienstvereinbarung die dezentrale Speicherung der Daten festgelegt und detaillierte Zugriffskonzepte geregelt werden.

Biometrie am Arbeitsplatz:

Einen ähnlichen Effekt wie der kontaktlose Chip hat der Einsatz von Biometrie am Arbeitsplatz. Mit Fingerabdruck-, Iris-, Stimm- oder Gesichtserkennung wird 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 z.B. Informationen über Krankheiten, die entweder direkt aus dem biometrischen Merkmal, also z.B. 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.

Eine weitere Anwendung findet sich in 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 Auto-kennzeichen 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's oder Passwörter.

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.

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 sog. Skill – Datenbanken werden Kenntnisse, Erfahrungen und Kompetenzen von Mitarbeitern, z.T. 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 nicht freiwilliger Aufnahme in derartige Tools hängt es vom Einzelfall ab, was zulässig ist und was nicht. 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.

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 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 die Interessenvertretungen 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 Controllingssystem 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 eines jeden Beschäftigten im Arbeitsleben 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, haben 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 gefordert werden. 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.