

Wolfgang Däubler

Die kontrollierten Belegschaften

1 Die Ausgangssituation

Wer morgens das Betriebsgelände betritt, wird im 21. Jahrhundert nicht mehr von einem Pförtner begrüßt, der die »Zu-Spät-Kommenden« auf einer Liste vermerkt. Heute steckt man einen maschinenlesbaren Ausweis in einen Schlitz. Auf diese Weise wird sekundengenau erfasst, wann beispielsweise die Personalnummer 4713 den Eingangsbereich durchschritten hat.

Am Arbeitsplatz angekommen, wird der PC eingeschaltet. Dies wird genauso erfasst wie das weitere Tun: Mails abgerufen und beantwortet, ein Redemanuskript etwa für den Chef entworfen, im Internet nach einer Zugverbindung gesucht. Dazwischen wird telefoniert – mit welcher Nummer und wie lange wird im Rechner festgehalten. An allen modernen Computern lässt sich eine Kamera aktivieren, die das Gesicht der vor dem PC sitzenden Person zeigt: Ein freudiger Ausdruck spricht dafür, dass sie heute gut drauf ist, eine grimmige Miene eher fürs Gegenteil. Beim Mittagessen wird mit dem Firmenausweis bezahlt. Der Computer »weiß«, dass Person X immer nur das »Diätessen« nimmt, was für eine etwas empfindliche Verdauung spricht. Auch lässt sich unschwer feststellen, wer regelmäßig als nächste oder übernächste Person bezahlt. Auf diese Weise kann ermittelt werden, mit wem X normalerweise zu Mittag isst. Handelt es sich bei ihm etwa um den in der Direktionsetage wenig geschätzten Betriebsratsvorsitzenden, entstehen höchst »interessante« Informationen.

Datenverarbeitung durch die Personalabteilung

Die Personalabteilung verfügt über eine Menge anderer Daten. Das Bewerbungsschreiben ist dort noch vorhanden, gegebenenfalls auch das Abiturzeugnis und das Hochschuldiplom, aber auch jeder Urlaubsantrag befindet sich in der Akte und jede krankheitsbedingte Fehlzeit ist vermerkt. War jemand im Laufe eines Jahres länger als sechs Wochen krank, wird ihm ein »Eingliederungsmanagement« angeboten, das der Krankheit auf den Grund gehen und gegebenenfalls Abhilfe schaffen will. Lässt die betreffende Person sich darauf ein, werden viele Angaben über ihren

Gesundheitszustand, über ihre Lebensgewohnheiten – beispielsweise Rauchen und Trinken – sowie über ihren Ärger am Arbeitsplatz festgehalten. In vielen großen Firmen gibt es die »elektronische Personalakte«¹: Alle Urkunden werden eingescannt, die übrigen Angaben von vornherein nur elektronisch erfasst. Oft existiert auch ein Nebeneinander von traditioneller und elektronischer Personalakte.

Erkenntnisse aus der Kombination von Beschäftigtenaten

Werden die Daten über die Arbeitstage im Büro und die Daten aus der Personalabteilung zusammengeführt, so kennt man die Stärken und Schwächen der Beschäftigten, ihre Gewohnheiten und ihre Verhaltensweisen in höchst präziser und umfassender Weise. In vielen Betrieben wird das Bild noch sehr viel dichter, die Pixelzahl gewissermaßen noch um einiges höher. In der Produktion lässt sich nicht selten sekundengenau feststellen, wie weit bestimmte Arbeitsprozesse gediehen sind oder wo sich eine bestimmte anzuliefernde Ware gerade befindet. Natürlich ist auch bekannt, wer dafür verantwortlich ist, dass alles reibungslos läuft. Bisweilen werden Videokameras angebracht, die eigentlich vor Diebstahl schützen sollen, die aber ganz nebenbei auch das Arbeitsverhalten erfassen können. Für Außendienst-Mitarbeiterinnen und -Mitarbeiter gibt es »Ortungssysteme«; über → *Global-Positioning-System (GPS)* oder das mitgeführte Handy wird ermittelt, wo sich das Fahrzeug zu einem bestimmten Zeitpunkt befindet. Das lässt Rückfragen zu, an die bisher niemand gedacht hat: Weshalb stand Ihr Fahrzeug eine halbe Stunde lang auf dem Rastplatz rechts neben der Autobahn? Warum haben Sie nicht den direkten Weg zum Kunden gewählt? Was hatten Sie auf dem Supermarktparkplatz zu suchen? Die »Videokamera im Weltraum« macht's möglich.

Einen »gläsernen« Beschäftigten zu schaffen, ist technisch gesehen kein Problem mehr. Die Frage ist nur, ob von dieser Möglichkeit Gebrauch gemacht werden darf oder ob das geltende Recht solche Praktiken verbietet.

2 Rechtliche Grenzen der Überwachung von Beschäftigten

Ein kluger Arbeitgeber oder eine kluge Arbeitgeberin wird von den beschriebenen Möglichkeiten lediglich einen sehr sparsamen Gebrauch machen. Nur wer keinerlei Vertrauen zu seinen Beschäftigten hat, wird die Techniken umfassend einsetzen. Damit ist die Gefahr verbunden, nur

noch völlig »stromlinienförmige« Beschäftigte zu haben, die unter gar keinen Umständen negativ auffallen wollen. Auf Probleme hinzuweisen oder gar bessere Lösungen vorzuschlagen, wird ihnen allzu riskant erscheinen. In einem Callcenter, wo die geführten Telefongespräche an fünf Tagen in der Woche vollständig aufgezeichnet werden, kursierte der Spruch: »Heute ist wieder Stasi-Tag«, weil man per Indiskretion am Morgen erfahren hat, dass mal wieder alles auf Band festgehalten wird. Das schafft jedoch keine konstruktive Arbeitsatmosphäre.

Nun gibt es aber leider keine Sicherheit, dass alle Arbeitgeberinnen oder Arbeitgeber das tun, was eigentlich auch in ihrem eigenen langfristigen Interesse liegt. Vielmehr wird es immer Fälle geben, wo nach dem Motto gehandelt wird: je intensiver die Überwachung, umso stärker der Einsatz des Einzelnen bei der Arbeit. Diese Haltung findet sich insbesondere in Bereichen, wo nur Standardtätigkeiten verlangt werden, bei denen die Motivation der Beschäftigten eine relativ geringe Rolle spielt. Wer nicht »spurt«, kann unschwer durch einen anderen ersetzt werden.

Für die Überwachung im Betrieb gibt es zwei wesentliche rechtliche Grenzen.

Das Persönlichkeitsrecht der Beschäftigten

Zunächst muss das Persönlichkeitsrecht der Beschäftigten respektiert werden. Das Sammeln und Speichern von Informationen über den Einzelnen ist deshalb nicht beliebig zulässig. Vielmehr muss die Arbeitgeberseite das Bundesdatenschutzgesetz (BDSG) beachten, das nach einem Gesetzentwurf der Bundesregierung² durch eine Reihe von Sondervorschriften zum Beschäftigtendatenschutz ergänzt werden soll. Durch seinen heutigen § 32 Abs. 2 sind auch handschriftliche Notizen der Arbeitgeberseite und der von ihm Beauftragten erfasst. Dies kann bei Bewerbungs- und Weiterförderungsgesprächen erhebliche Bedeutung gewinnen, da die Betroffenen auf diese Weise auch unsachliche Randbemerkungen zur Kenntnis bekommen können. Der Arbeitsvertrag enthält im Übrigen nach der Rechtsprechung des Bundesarbeitsgerichts (BAG) die stillschweigende Verpflichtung der Arbeitgeberseite, auf die Persönlichkeitssphäre der Beschäftigten Rücksicht zu nehmen.

Darüber hinaus greift in fast allen Fällen der Erfassung und Verarbeitung von Daten ein Mitbestimmungsrecht des Betriebsrats (vgl. auch Abschnitt 4 dieses Beitrags). Dieser muss daher zustimmen, einseitige Handlungen der Arbeitgeberseite sind rechtswidrig und unwirksam. Nur wenn beide Voraussetzungen erfüllt sind – das Verhalten lässt sich nach

dem BDSG rechtfertigen und das Mitbestimmungsrecht des Betriebsrats ist gewahrt – liegt eine rechtmäßige Datenerhebung oder Datenverarbeitung vor.

3 Das Bundesdatenschutzgesetz als Schranke

Nach § 32 Absatz 1 Satz 1 BDSG dürfen Beschäftigtendaten nur dann erhoben, verarbeitet und genutzt werden, wenn dies für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses »erforderlich« ist. Andere Beschäftigte wie beispielsweise freie Mitarbeiterinnen und Mitarbeiter, Ein-Euro-Kräfte oder Auszubildende sind gleichgestellt. Es muss ein unmittelbarer Bezug zur Arbeit gegeben sein; was damit nicht in Zusammenhang steht, darf die Arbeitgeberseite nicht interessieren. Dies gilt beispielsweise für Freizeitbeschäftigungen und die familiäre Situation, aber auch für das in der Kantine gewählte Essen. Selbst wenn der Bezug zur übernommenen Tätigkeit da ist, wird verlangt, dass das Informationsinteresse der Arbeitgeberseite schwerer wiegt als der Eingriff in die Persönlichkeitssphäre der Beschäftigten – nur dann ist die Datenverarbeitung »erforderlich«. Daran fehlt es beispielsweise, wenn von Arbeitgeberseite mit Hilfe einer Kamera das Mienenspiel und die Stimmung der Beschäftigten »eingefangen« wird. Dies kann zwar für die Arbeitsorganisation irgendwie nützlich sein, aber die Dauerbeobachtung ist ein zu schwerer, übermäßiger Eingriff in die Sphäre des Einzelnen.

Daten von Bewerberinnen und Bewerbern

Was »erforderlich« ist, wurde im Verhältnis zu Bewerbern und Bewerberinnen bereits zu einer Zeit bestimmt, als es noch nicht einmal den Begriff des Datenschutzes gab. Das BAG entwickelte in den 1950er Jahren den folgenden Grundsatz: Die Arbeitgeberseite darf nur nach solchen Dingen fragen, an deren Kenntnis ein berechtigtes, billigeswertes und schutzwürdiges Interesse besteht. Dies wurde in Bezug auf Vorstrafen konkretisiert: Nur wenn sie sich auf dem in Aussicht genommenen Arbeitsplatz wiederholen können, war die Frage zulässig. Wer sich etwa als Fahrer bewirbt, kann nach Straßenverkehrsdelikten, wer sich als Jugendpfleger betätigen möchte, kann nach Sittlichkeitsdelikten gefragt werden. Ohne Bedeutung war es deshalb, als eine Bewerberin ihre Vorstrafe wegen eines politischen Delikts (konkret: Fortführung des verbotenen sozialistischen Jugendverbands Freie Deutsche Jugend,

FDJ) verschwiegen, weil sie lediglich eine völlig unpolitische Tätigkeit bei einer Bausparkasse ausüben wollte.

Schutz vor Diskriminierungen

Unzulässig sind insbesondere Fragen, die nach dem normalen Lauf der Dinge zu einer Diskriminierung führen. Dies gilt etwa für die Frage nach der Schwangerschaft (da sie Frauen benachteiligt), ebenso wie für die nach der Anerkennung als schwerbehinderte Person; die Antwort würde nichts über die tatsächlichen Fähigkeiten des Bewerbers oder der Bewerberin aussagen, aber eine Diskriminierung wegen Behinderung ermöglichen.

In beiden Fällen darf jemand die Unwahrheit sagen, ohne dass die Arbeitgeberseite später den Arbeitsvertrag anfechten kann, weil sie getäuscht worden sei oder sich geirrt habe. Manche sprechen insoweit von einem »Recht zur Lüge«.

Zulässig ist dagegen, die Eignung für den Arbeitsplatz zu ermitteln und dabei auch die gesundheitliche Verfassung des Bewerbers oder der Bewerberin einzubeziehen; selbst wenn sich dabei eine Behinderung herausstellt, könnte sie grundsätzlich berücksichtigt werden. Niemand darf außerdem wegen seiner ethnischen Zugehörigkeit benachteiligt werden; dass etwa jemand türkischer Herkunft ist, darf im Arbeitsleben keine Rolle spielen. In der Praxis dürfte dieser Grundsatz allerdings nicht immer beachtet werden, ist doch die nationale Herkunft häufig schon am Namen erkennbar. Ähnlich verhält es sich mit einem Rückgriff auf soziale Netzwerke wie beispielsweise *Facebook*. Folgt man einer verbreiteten Auffassung in der juristischen Literatur, ist dies nach geltendem Recht nicht erlaubt. Der aktuelle Gesetzentwurf des Bundesinnenministeriums will es jedoch grundsätzlich gestatten. Der praktische Unterschied ist allerdings nicht sehr groß, weil ein Verbot nicht wirklich kontrolliert werden kann: Wie will man beweisen, dass jemand gerade deshalb nicht eingestellt wurde, weil er im Netz etwas provokativ geschrieben hatte, er würde gerne mal eine Veröffentlichung von Bin Laden lesen? Die Personalabteilung wird offiziell nichts über die Recherche im Netz erzählen und einfach zu dem Ergebnis kommen, die Person habe im Vorstellungsgespräch den »weniger überzeugenden« Eindruck gemacht.

Beschäftigtendaten

Im Verhältnis zu Beschäftigten gelten dieselben Grundsätze, soweit ein vergleichbares Informationsbedürfnis besteht. Dies kann insbesondere bei Versetzungen und Beförderungen der Fall sein. Daneben ist die Arbeitge-

berseite verpflichtet, zahlreiche Daten über die Beschäftigten an die Sozialversicherung oder staatliche Stellen zu übermitteln.

Weiter taucht bisweilen das Problem auf, dass Arbeitgeber wissen möchten, ob jemand alkoholkrank oder drogenabhängig ist. Hat dies – was auf Dauer kaum in Betracht kommt – keinerlei Auswirkungen auf die Arbeit, gehört es zur Privatsphäre und bleibt schon deshalb außen vor. Können sich dagegen betriebliche Folgen einstellen, darf gleichwohl nicht jeder, sondern nur derjenige Beschäftigte untersucht werden, bei dem konkrete Verdachtsmomente wie eine »Fahne« oder eine offensichtlich geminderte Reaktionsfähigkeit bestehen.

Die Arbeit im Betrieb gibt die Möglichkeit, dass Beschäftigte nicht nur befragt, sondern dass besondere technische Mittel eingesetzt werden, um ihr Verhalten zu überwachen. Früher hat man beispielsweise sogenannte Einwegscheiben benutzt, die nur den Durchblick in einer Richtung gestatteten: Wer in einer Halle arbeitete, konnte so von einem Beobachtungsposten aus genau ins Visier genommen werden, ohne zu wissen, wann und ob dies gerade zu einem bestimmten Zeitpunkt geschah. Heute werden andere Methoden verwendet, die umfassendere Erkenntnisse ermöglichen.

Videouberwachung

Besondere Aufmerksamkeit hat die Videokamera gefunden, die sich nicht nur in Supermärkten und Tankstellen findet. Soweit es sich um öffentlich zugängliche Flächen oder Räume handelt, greift § 6b BDSG ein, wonach Daten im Grunde nur zur Abwehr von Straftaten erhoben werden dürfen. Auch müssen sie schnell wieder gelöscht werden. Bei anderen Räumen wie einem Büro oder einer Werkshalle fehlte bislang eine gesetzliche Regelung.

Das BAG hat schon frühzeitig entschieden, dass der Einsatz von Videogeräten nicht allein deshalb erfolgen darf, um »ordentliches Arbeiten« sicherzustellen; dies wäre ein übermäßiger Eingriff in die Persönlichkeitsphäre.

Anders verhält es sich, wenn es um Gefahrenabwehr geht, wenn beispielsweise das Lager durch Videokameras gegen Einbrüche gesichert wird. Dies ist unbestritten legal, wobei die »nebenbei« anfallenden Daten über das Arbeitnehmerverhalten ohne besonderen Grund nicht ausgewertet werden dürfen und auch rasch wieder zu löschen sind. § 32e des Regierungsentwurfs für einen Beschäftigtendatenschutz (BDSG-E) bestätigt dies mitteilbar und will gleichzeitig die heimliche Videouberwachung verbieten.

Überwachung der Kommunikation

Der heimliche Einbau eines Abhörgeräts am Arbeitsplatz ist unzulässig und strafbar, doch ergeben sich im Zusammenhang mit dem Telefonieren und anderen Formen der Telekommunikation (wie dem Versenden und Empfangen von E-Mails) zahlreiche Zweifelsfragen. Während das Erfassen der »äußeren Telefondaten« – das heißt mit welchem Anschluss wurde wann und wie lange telefoniert – in aller Regel bei Dienstgesprächen als unproblematisch angesehen wird, ist dies beim »Mithören« – also der direkten Kenntnisnahme des Inhalts – anders. Es ist nur ausnahmsweise im »überwiegenden Arbeitgeberinteresse« zulässig. Ein solches wurde vom BAG dann angenommen, wenn die ganze Arbeit am Telefon erfolgt und bei neu Eingestellten nur durch Mithören ermittelt werden kann, ob sie in angemessener Weise mit der Kundschaft umgehen und über die nötige Sachkunde verfügen.

Dies ist am Beispiel des Reservierungszentrums einer Fluggesellschaft entschieden worden, gilt aber für alle Callcenter. Eventuell könnte das »Mithören« auch dann erlaubt werden, wenn innerhalb eines kurzen Zeitraums mehrere Beschwerden eingehen und so eine »Qualitätskontrolle« naheliegt. Weiter zu gehen und das Mithören »stichprobenartig oder anlassbezogen« generell zuzulassen, wie dies § 32i Absatz 2 Satz 2 BDSG-E will, ist nicht zu rechtfertigen. Hier hilft auch der obligatorische Hinweis wenig, dass »irgendwann in nächster Zeit« eine Kontrolle stattfinden soll.

Kontrolle von E-Mails und Internetnutzung

Ob dieselben Grundsätze auch für die dienstliche Nutzung von E-Mail und Internet gelten, ist in der Rechtsprechung noch nicht geklärt. Das Telekommunikationsgesetz (TKG) geht von einem einheitlichen »Telekommunikationsgeheimnis« aus, so dass kein Grund für eine Differenzierung besteht. Beispielsweise darf der Chef also nicht einfach die E-Mails des Mitarbeiters lesen, es sei denn, er wäre selbst mit angeschrieben oder auf den Verteiler gesetzt worden. Nicht anders als bei Briefen kann er allerdings verlangen, dass ihm die Korrespondenz vollständig vorgelegt oder per E-Mail weitergeleitet wird.

Private Nutzung von Internet und Telefon am Arbeitsplatz

Soweit privates Telefonieren oder privates Surfen erlaubt ist, sind die dabei anfallenden Daten für den Arbeitgeber tabu. Eine Ausnahme gilt nur für Abrechnungszwecke. Muss der einzelne Beschäftigte die Privatgespräche

bezahlen, können die verbrauchten Gebühreneinheiten festgehalten werden, doch darf die Nummer des Angerufenen nicht vollständig, sondern nur in der Weise gespeichert werden, dass man die drei oder vier letzten Ziffern unterdrückt. Andernfalls wäre das Telekommunikationsgeheimnis verletzt.

Zulässigkeit des Einsatzes von Ortungssystemen

Ob und in welchem Umfang der Einsatz von Ortungssystemen zulässig ist, hat die Rechtsprechung noch nicht entschieden. § 32g BDSG-E will den Einsatz dann erlauben, wenn dies aus bestimmten Anlässen für den betrieblichen Ablauf erforderlich ist und schutzwürdige Interessen des Beschäftigten nicht entgegenstehen. Für Beschäftigte im Außendienst ist eine solche Überwachung mit einem Verlust jener Freiheit verbunden, die diese Tätigkeit für viele attraktiv macht: Bisher sind sie in zeitlicher Hinsicht selbstbestimmt und müssen niemandem Rechenschaft abgeben, weshalb sie etwa beim Kunden X erst nachmittags um halb vier aufkreuzten und außerdem eine etwas ungewöhnliche Route mit dem Auto gewählt haben. Ob es wirklich ein überwiegendes Arbeitgeberinteresse gibt, daran etwas zu ändern, wird man bezweifeln müssen: Wenn es darum geht, mehrere Fahrzeuge zu koordinieren oder kurzfristig umzuleiten, können etwa Handys ausgegeben werden, auf denen die Fahrerinnen und Fahrer jederzeit erreichbar sein müssen.

Diese Techniken stellen nur die wichtigsten Beispiele der Erhebung von Beschäftigtendaten dar. Daneben ist etwa bei der Zugangskontrolle an biometrische Methoden (*fingerprint* oder »Gesichtskontrolle«) zu denken (siehe zu Biometrie auch die Beiträge von Hansen, S. 78 ff. und von Bock, S. 310 ff. in diesem Band). Auch lässt sich der Warenfluss mit Hilfe von →RFID-Tags kontrollieren, wobei Lesegeräte festhalten, wann welcher Gegenstand welchen Punkt passiert. Mittelbar werden so auch die dort tätigen Beschäftigten überwacht.

Einwilligung der Betroffenen als Grundlage?

Können Beschäftigte wirksam einwilligen, dass ihre Daten in weiterem Umfang Verwendung finden als es Gesetze und Rechtsprechung zulassen? Können sie bei einer Einstellungsuntersuchung den Arzt oder die Ärztin von der Schweigepflicht entbinden? Kann der Beschäftigte das »Mithören« seiner Gespräche generell erlauben? Die Einwilligung des Betroffenen kann zwar grundsätzlich die Möglichkeiten der Datenverarbeitung

erweitern, doch muss sie nach § 4a BDSG »freiwillig« erfolgen (siehe auch den Beitrag von Hartge in diesem Band, S. 280 ff.). Für Arbeitnehmerinnen oder Arbeitnehmer ist es häufig schwierig, eine von der Arbeitgeberseite gewünschte Einwilligung abzulehnen, weil sie (zu Recht oder zu Unrecht) schlechtere Aufstiegschancen in der Zukunft oder Sanktionen wie Versetzungen befürchten. In aller Regel kann daher nur dann von »Freiwilligkeit« die Rede sein, wenn die Datenverarbeitung den Beschäftigten Vorteile bringt, wenn jemand beispielsweise in die »Nachwuchsförderungsdatei« aufgenommen wird.

Grenzüberschreitende Übermittlung

Besondere Probleme ergeben sich, wenn Daten von Beschäftigten ins Ausland übermittelt werden (siehe auch den Beitrag von Körner in diesem Band, S. 426 ff.). Dies ist insbesondere bei globalen Großkonzernen der Fall. Unproblematisch ist, wenn sich der Empfänger in einem anderen Mitgliedstaat der Europäischen Union (EU) befindet. Da aufgrund der EU-Datenschutzrichtlinie³ das Datenschutzrecht der einzelnen Länder weitestgehend übereinstimmt, wird nach denselben Grundsätzen wie im Inland verfahren. Es macht also rechtlich keinen Unterschied, ob Daten von Hamburg nach Stuttgart oder von Hamburg nach Lissabon übermittelt werden.

Bei Staaten, die nicht Mitglieder der EU sind (sogenannte Drittstaaten), ist die Sache komplizierter. Soweit ihr Datenschutzniveau von der EU-Kommission als gleichwertig anerkannt ist, gelten dieselben Grundsätze wie innerhalb der EU. Ist diese Voraussetzung nicht gegeben, muss die Aufsichtsbehörde den Datentransfer genehmigen. Davon wird aber eine Ausnahme gemacht, wenn die beteiligten Unternehmen einen Mustervertrag der EU übernehmen, der einen ausreichenden Datenschutz gewährleistet, oder wenn ein internationaler Konzern eine verbindliche Selbstverpflichtung abgibt, ein angemessenes Datenschutzniveau zu praktizieren. Im Verhältnis zu den Vereinigten Staaten von Amerika (USA) gilt die sogenannte → *Safe-Harbor*-Regelung: Hat das Empfängerunternehmen bestimmte Datenschutzgrundsätze anerkannt, wird es wie ein dem EU-Recht unterliegendes Unternehmen behandelt. Andernfalls wird auch hier eine Genehmigung oder eine Abmachung benötigt.

4 Mitbestimmungsrechte des Betriebsrates

Der Betriebsrat hat ein Mitbestimmungsrecht bei der »Einführung und Anwendung technischer Systeme, die dazu bestimmt sind, Verhalten und Leistung der Arbeitnehmer zu überwachen« (§ 87 Absatz 1 Nr. 6 BetrVG). Dabei kommt es nach der Rechtsprechung nicht auf die Kontrollabsicht der Arbeitgeberseite an, da bereits eine bloße »Eignung zur Überwachung« genügt. Soll eine Videoanlage beispielsweise nur gegen Einbruch schützen, ändert dies nichts an der Mitbestimmung, da ja auch das Verhalten von Beschäftigten im Bild festgehalten werden kann. Außerdem ist nicht erforderlich, dass der technische Vorgang selbst zu Aussagen über Verhalten und Leistung führt; es genügt, wenn diese mit Hilfe von sogenanntem Zusatzwissen möglich sind. Wird beispielsweise nur erfasst, dass eine Ware losgeschickt wurde, aber nicht angekommen ist, so genügt es, dass sich aus Schichtplänen, Listen etc. ergibt, wer für den Transport im konkreten Fall verantwortlich war.

Betriebsrat und Arbeitgeberseite müssen verhandeln. Lassen sich Meinungsverschiedenheiten nicht ausräumen, entscheidet eine Einigungsstelle mit einem unparteiischen Vorsitzenden. Handelt die Arbeitgeberseite ohne Zustimmung des Betriebsrats, kann dieser ihr durch einstweilige Verfügung des Arbeitsgerichts untersagen lassen, die fragliche Maßnahme aufrecht zu erhalten. Die Videokamera muss dann wieder abgebaut, das Mitanhören der Telefongespräche ausgesetzt werden. Um einen solchen Antrag bei Gericht zu stellen, muss der Betriebsrat aber zu einer gewissen Konfrontation mit der Arbeitgeberseite bereit sein. Diese Voraussetzung ist in der Praxis nicht immer gegeben. Auch wird nur etwa die Hälfte aller Beschäftigten durch einen Betriebsrat oder – im öffentlichen Dienst – durch einen Personalrat vertreten, der vergleichbare Befugnisse in diesem Bereich besitzt.

Viele Beschäftigte sind daher nur auf das BDSG verwiesen. Sie werden noch weniger als ein Betriebsrat bereit sein, sich mit der Arbeitgeberseite »anzulegen«. Sie können sich (wie übrigens auch der Betriebsrat) an die Person des oder der betrieblichen Datenschutzbeauftragten wenden, doch sind die Aussichten auf Abhilfe ungewiss: Diese Person ist letztlich von der Arbeitgeberseite eingesetzt, so dass sie vom BAG als dessen »Gewährsmann« bezeichnet wurde (die deshalb die Datenverarbeitung im Betriebsratsbüro nicht kontrollieren darf). Als wirklicher Ausweg steht lediglich die Möglichkeit zur Verfügung, die Aufsichtsbehörde für den Datenschutz einzuschalten (siehe auch den Beitrag von Kamp/Thomé in diesem Band, S. 298 ff.). Sie existiert in jedem Bundesland und muss plausibel darge-

legten Datenschutzverstößen nachgehen. Ihre Verantwortung ist groß: Je gründlicher sie arbeitet, umso stärker wird der Datenschutz in der Praxis an Bedeutung gewinnen.

Anmerkungen

- 1 Als elektronische Personalakte bezeichnet man Software, mit deren Hilfe Dokumente aus der Personalakte (beispielsweise Atteste) verwaltet werden können.
- 2 Bundesregierung, Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BR-Drs. 535/10 vom 3.9.2010. Der Gesetzentwurf (BDSG-E) differenziert zwischen Bewerbern und Beschäftigten sowie zwischen Erhebung und Verarbeitung einschließlich Nutzung von Daten. Seine Verabschiedung ist derzeit (Stand: Juli 2012) ungewiss, zumal das Bundesinnenministerium weitgehende Änderungsvorschläge gemacht hat.
- 3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995.

Roland Wolf

Beschäftigtendatenschutz ist Teil guter Unternehmensführung

Der Schutz persönlicher Daten von Beschäftigten gehört heute wie selbstverständlich zum Arbeitsrecht. Beschäftigtendatenschutz ist eine Notwendigkeit, ebenso wie die Einhaltung anderer nationaler und internationaler Vorschriften. Schon das bis zum 1. September 2009 geltende Bundesdatenschutzgesetz (BDSG) – ohne die entsprechenden Ergänzungen zum Beschäftigtendatenschutz¹ – bot hierfür eine Grundlage. Alle tatsächlichen oder vermeintlichen Datenskandale, die die Republik im Jahr 2009 bewegt haben, sind unter der Herrschaft des BDSG aufgeklärt worden. Dessen ungeachtet entschieden sich Regierung und Parlament im Sommer 2009 dafür, den Beschäftigtendatenschutz in einer eigenständigen Vorschrift klarzustellen.

Diese Regelung in § 32 BDSG ist jedoch missglückt. Sie bedarf der gesetzlichen Ergänzung und Änderung. Das Vorhaben, klare und rechts-sichere Regelungen durch eine Novelle des Bundesdatenschutzgesetzes zu schaffen, ist daher zu begrüßen. Der Gesetzentwurf der Bundesregierung² (BDSG-E) aus dem Jahr 2010 in seiner ursprünglichen Fassung verfehlte dieses Ziel.

1 Der geltende Beschäftigtendatenschutz

Die geltende Rechtslage ist für Arbeitgeber, Beschäftigte und Betriebsräte schwer verständlich. Weder Revisions- noch Rechtsabteilungen, weder Datenschutzbeauftragte der Betriebe noch die einzelnen Personalabteilungen können sicher sagen, nach welchen Kriterien sich der Datenschutz im Unternehmen richtet. Dies liegt vor allem an der unklaren Diktion von § 32 BDSG. An wenigen Beispielen sei dies im Folgenden verdeutlicht.

»Erforderlichkeit« der Datenerhebung ist zu unbestimmt

Nach § 32 Absatz 1 BDSG ist eine Datenerhebung, -verarbeitung und -nutzung zulässig, wenn sie erforderlich ist. Was der Gesetzgeber dadurch regeln wollte, ergibt sich nicht eindeutig aus der Norm, sondern aus der