

## Der „lichtgeschwinde Zugriff“ auf Arbeitnehmerdaten

Wolfgang Däubler über die wachsende Informationsmacht der Unternehmer  
und die Gefahr gläserner Belegschaften

Frankfurter Rundschau, 08.02.1988

Das mittlerweile zehn Jahre alte Bundesdatenschutzgesetz soll nach den Plänen von Bundesinnenminister Friedrich Zimmermann (CSU) novelliert werden. Noch im Frühjahr soll, wie bereits berichtet, der Entwurf eines Gesetzes „zum Schutz personenbezogener Daten in Dateien“ vom Kabinett gebilligt werden. Als „Rückschritt“ bezeichnete der Bundesbeauftragte für den Datenschutz, Reinhold Baumann, den Entwurf im Vergleich zum derzeit geltenden Gesetz. Nichts Neues enthält die Vorlage zum Thema Arbeitnehmerdatenschutz. Das Volkszählungsurteil des Bundesverfassungsgerichts hat mit seiner Anerkennung des „informationellen Selbstbestimmungsrechts“ den Datenschutz für Arbeitnehmer und Beamte auf eine neue Grundlage gestellt. Welche rechtlichen Handhabungsmöglichkeiten es als Schutz vor einer Totalüberwachung durch Personalinformationssysteme und Betriebsdatenerfassung gibt, das hat Wolfgang Däubler in seinem jüngsten Buch „Gläserne Belegschaften“, das vor kurzem im Bund-Verlag Köln erschienen ist, zusammengetragen. Wir dokumentieren die abschließenden Thesen des an der Universität Bremen lehrenden Arbeitsrechtlers, die er um eine Einleitung ergänzt hat.

Arbeitnehmer sind bevorzugte Informationsobjekte. Nirgends wird über den einzelnen so viel gespeichert wie im Arbeitsverhältnis – höchstens das Finanzamt oder die Sozialhilfebehörde können im Einzelfall mithalten. Dies hat wenig oder gar nichts mit „Neugierde“ und bewußter Ausforschung zu tun, sondern ist Ausdruck handfester Entwicklungen in der Personalverwaltung wie im Arbeitsprozeß selbst.

Seit Beginn der siebziger Jahre ist ein großer Teil der Personalakten „computerisiert“ worden. Ein Grund liegt darin, daß die Arbeitgeber zahlreiche Daten über ihre Beschäftigten erheben und an die staatliche Verwaltung weiterleiten müssen. Wichtigste Beispiele sind die Abführung der Lohnsteuer und der Beiträge zur Sozialversicherung. In der juristischen Literatur ist von 75 verschiedenen (staatlichen) Datenempfängern und 239 Bescheinigungsarten bzw. Auskunftspflichten die Rede. Die Arbeitgeber versuchen verständlicherweise, die ihnen auferlegte Tätigkeit möglichst kostengünstig zu erledigen. Hier tut die EDV gute Dienste.

Ein anderer Grund liegt in der Rationalisierung des Personaleinsatzes. Dieser setzt nicht nur präzise Informationen über die jeweiligen Arbeitsplätze und die dort vorhandenen Anforderungen voraus, sondern verlangt auch umfassende Informationen über alle irgendwie arbeitsrelevanten Eigenschaften der in Frage stehenden Arbeitnehmer. Der Gedanke liegt nahe, nicht nur ein „Qualifikationsprofil“, sondern auch ein „Persönlichkeitsprofil“ zu erstellen, das alle Stärken und Schwächen des einzelnen wiedergibt. Dazu können Gesundheitsdaten, Fehlzeiten, Mahnungen und andere Maßnahmen mit disziplinarischem Charakter, aber auch Angaben zu so unterschiedlichen Dingen wie Rentenversicherungsnummer, Parteizugehörigkeit sowie Lärm-, Staub- und Gasverträglichkeit gehören. Insgesamt sollen normalerweise über 2000 Einzeldaten pro Beschäftigten gespeichert sein. Die Quantität ist freilich nicht allein entscheidend: Auch wenn der Vorrat sehr viel geringer ist, können durch Verknüpfung jederzeit neue Informationen über den einzelnen erzeugt werden. Sind etwa die Fehlzeiten aller

Mitarbeiter der Abteilung gespeichert, läßt sich unschwer bestimmen, ob X oder Y überdurchschnittlich oft gefehlt haben.

Zu diesen „offenen“ sind in den vergangenen Jahren verstärkt „verdeckte“ Personalinformationssysteme hinzugekommen: Im Zusammenhang mit dem Arbeitsprozeß selbst fallen zahlreiche Daten an, die zumindest personenbeziehbar, wenn nicht unmittelbar personenbezogen sind.

Diese sogenannte Betriebsdatenerfassung beginnt etwa mit einer automatisierten Zugangskontrolle: Das Werkstor oder die Türe zu einem bestimmten Arbeitsbereich öffnet sich nur, wenn ein mit entsprechender Nummer kodierter Ausweis in einen Schlitz gesteckt wird. Ist der „Ausweisleser“ mit dem zentralen Rechner verbunden, lassen sich sehr genau die „Kommens- und Gehenszeiten“ erfassen. Um eine mißbräuchliche Benutzung von Ausweisen zu verhindern, wird bisweilen erwogen, die Zugangsberechtigung des einzelnen über „Fingerprint“ zu überprüfen: Die beim Zutritt auf eine bestimmte Stelle gemachten Fingerabdrücke werden in Sekundenschnelle mit ihrem digitalisierten Abbild verglichen, das sich im Speicher der Rechenanlage befindet. Dasselbe läßt sich mit Hilfe einer Fernsehkamera bewerkstelligen, die die Gesichtszüge des Einlaß Begehenden mit dem vorhandenen Lichtbild vergleicht.

Ein weiterer Bereich betrifft das Telefonverhalten: Aufgezeichnet wird nicht nur der Apparat, von dem aus ein Gespräch geführt wird, sondern auch die angerufene Zielnummer, Beginn und Ende des Gesprächs sowie die angefallenen Gebühren. Erstreckt man dies auch auf (zugelassene) Privatgespräche, läßt sich unschwer kontrollieren, in welchem Umfang beispielsweise Kundenkontakte gepflegt bzw. die Arbeit für private Zwecke unterbrochen wurde.

Während Zugangs- und Abgangskontrolle sowie Telefondatenerfassung nur einzelne Teile des Arbeitnehmerverhaltens betreffen, ist dies bei der Computerisierung von Produktionsvorgängen anders. Auftragsverfolgungssysteme sind in der Lage, den jeweiligen Bearbeitungszustand sekundengenau auszuweisen – was Rückschlüsse auf das Arbeitsverhalten der Beteiligten in puncto Schnelligkeit, Materialverbrauch usw. zuläßt. Bei der Textverarbeitung am Terminal kann jede Betätigung der Korrekturtaste gespeichert und auf diese Weise festgehalten werden, wie oft sich die dort tätige Person vertippt hat. Bei einem Anschluß an einen zentralen Rechner wird üblicherweise die Nutzungszeit erfaßt und der jeweiligen Kostenstelle zugeordnet. Auch hier sind Rückfragen denkbar, weshalb sich ein oder mehrere Benutzer ungewöhnlich viel oder ungewöhnlich wenig in das Informationssystem eingeschaltet haben.

Die Rede ist schließlich von bereits funktionierenden Systemen, in denen für jeden Arbeitnehmer sogenannte elektronische Zeitstrahlen gebildet werden, auf denen jedes irgendwie relevante Ereignis während des Arbeitstags festgehalten wird. Weitere Beispiele ließen sich unschwer finden: Betriebsdatenerfassung ist ersichtlich nicht weniger wichtig als Personalinformationssysteme.

Auch die Möglichkeiten zur Ausweitung der gespeicherten Daten wurden in den vergangenen Jahren perfektioniert. Immer häufiger kommen sogenannte Abfragesprachen zur Anwendung, die den Benutzern eine fast beliebige Verknüpfung der gespeicherten Daten erlauben. Daß sich das Kontrollpotential dadurch vergrößert, bedarf keiner näheren Begründung. Dasselbe gilt für den Einsatz von Personalcomputern (PC): Das Kopieren von Programmen oder Daten auf Diskette läßt sich insbesondere dann nicht kontrollieren, wenn der Benutzer ein mitgebrachtes Betriebssystem laden kann, das keinerlei Kontrollen wie Protokollierung usw. enthält und dessen „Arbeit“ keinerlei Spuren hinterläßt. Erst recht kann jede „Übersicht“ über das Schicksal der eigenen Daten verlorengehen, wenn sie in vernetzten Systemen gespeichert sind, die sich insbesondere im Rahmen multinationaler Konzerne auch über Staatsgrenzen hinweg entwickeln.

## Technikspezifische Risiken

Die Existenz eines immensen „Datenvorrats“ über den einzelnen besitzt eine andere Qualität als das Vorhandensein einer besonders dicken Akte. Mit der Speicherung personenbezogener Daten in der Rechenanlage ist notwendigerweise eine „Endindividualisierung“, ein Absehen von zahlreichen Umständen des Einzelfalls verbunden. Dieser sogenannte Kontextverlust kann zu Irrtümern und Fehlentscheidungen führen. Sieht sich der einzelne dann einem Computerausdruck gegenüber, wird es ihm sehr schwerfallen, im nachhinein atypische Umstände zu belegen und so die „Sachautorität“ des Computers zu erschüttern. Dies ist schon bei Fehlbuchungen „schwierig genug“, besteht doch bei vielen Mitbürgern ein unerschütterliches Vertrauen, technische Apparaturen würden exakt (oder gar nicht) funktionieren. Polizeifotos bei Geschwindigkeitsüberschreitungen im Straßenverkehr mögen als Beispiel stehen.

Neben Kontextverlust und Irrtumsrisiko besteht das Problem einer „Durchleuchtung“ des einzelnen samt seiner persönlichen Beziehungen bzw. eine Totalkontrolle seines Arbeitsverhaltens. Die genannten Fälle der Betriebsdatenverarbeitung machen dies hinreichend deutlich. Die „Maschine“ weiß mehr über den einzelnen, als dieser über sich selbst. Die zu verschiedenen Zwecken wie z. B. Zugangskontrolle, Kantinenabrechnung, Gesundheitsschutz, Kontrolle der Vertragserfüllung usw. gespeicherten Daten können fast beliebig miteinander verknüpft werden. Anstelle langwieriger, mit unzumutbarem Aufwand verbundener Recherchen tritt der „lichtgeschwinde Zugriff“. Die Informationsmacht des Arbeitgebers wird um vieles größer – auch gegenüber dem Betriebsrat, dem vergleichbare Möglichkeiten nicht zur Verfügung stehen.

Nicht nur in der Vorstellung, sondern auch in der Realität gilt schließlich der Grundsatz „Computer können nicht vergessen“. Daten können unschwer so lange aufbewahrt werden, daß sie auch dann noch verfügbar sind, wenn weder der Betroffene noch ein mit gutem Gedächtnis versehener Personalleiter sich an den in Frage stehenden Vorgang erinnern könnte. Computer müssen insoweit auf „menschliches Maß zurückgeschraubt werden“ (Bull), unbefangenes Miteinander bleibt nur möglich, wenn Fehler und Mißgriffe nicht gleich Ewigkeitscharakter besitzen.

## Reaktion der Rechtsordnung

Der Schutz des Arbeitnehmers gegen übermäßige Verdattung hat bislang nur eine unvollständige Regelung erfahren. Im Arbeitsrecht haben sich Grundsätze über das „Informationserhebungsrecht“ des Arbeitgebers entwickelt, doch finden sich kaum präzise Vorgaben über die „Datennutzung“ durch den Arbeitgeber. Auch die Einschaltung des Betriebsrats ist erst teilweise geklärt. Der dritte Abschnitt des Bundesdatenschutzgesetzes findet zwar auch im Arbeitsverhältnis Anwendung, doch besitzen seine Normen wenig scharfe Konturen: So darf vom Wortlaut des § 23 Bundesdatenschutzgesetz her gesehen alles gespeichert werden, was sich im Rahmen des „Zwecks des Arbeitsverhältnisses“ bewegt. Ebenso pauschal ist die Datenübermittlung und die Datenveränderung geregelt – wobei unklar ist, ob und unter welchen Voraussetzungen eine Auswertung überhaupt unter den Tatbestand der „Datenveränderung“ fällt.

Der wenig konsolidierte Zustand des Arbeitnehmer-Datenschutzes läßt die Frage besonders dringend werden, ob die im Volkszählungsurteil des Bundesverfassungsgerichts entwickelten Grundsätze auf das Arbeitsverhältnis angewandt werden können. Besitzt der Arbeitnehmer auch gegenüber dem argb ein „informationelles Selbstbestimmungsrecht“, in das nur aufgrund präziser und bereichsspezifischer gesetzlicher Regelung eingegriffen werden darf? Gibt es auch im Arbeitsverhältnis ein „Zweckentfremdungsverbot“? Dürfen Daten, die zu Abrechnungszwecken erhoben wurden, nicht in anderem Zusammenhang verwendet werden? Muß man im Unternehmen eine „informationelle Gewaltenteilung“ praktizieren, wie sie das Bundesverfassungsgericht für die öffentliche Verwaltung vorgeschrieben hat?

Benötigt man auch im Betrieb einen unabhängigen, von keiner der beiden Seiten beeinflussbaren Datenschutzbeauftragten? Im folgenden sollen in Thesenform Antworten versucht werden.

1. Nach der inzwischen mehrfach bestätigten Rechtsprechung des Bundesverfassungsgerichts ist aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG das Recht des einzelnen abzuleiten, selbst über die Preisgabe „seiner“ Daten zu entscheiden. Die Anerkennung dieses „informationellen Selbstbestimmungsrechts“ hat zur Folge, daß jede Erhebung und Verwendung fremder Daten als „Eingriff“ zu qualifizieren ist, der einer besonderen Rechtsgrundlage bedarf.

2. Eingriffe in das informationelle Selbstbestimmungsrecht sind nur unter Wahrung bestimmter enger Voraussetzungen zulässig. Die öffentliche Hand benötigt eine gesetzliche Grundlage, außerdem muß sie sich auf ein „überwiegendes Allgemeininteresse“ stützen können. Ausgeschlossen ist u. a. eine Registrierung und Katalogisierung der Bürger sowie die Erhebung von Daten ohne Sozialbezug. Der Verwendungszweck der erhobenen Daten muß „bereichsspezifisch und präzise“ festgelegt sein. Eine „Zweckentfremdung“ ist auch nicht unter Berufung auf den Grundsatz der Amtshilfe zulässig. Für die Verwaltung läuft dies auf ein Gebot informationeller Gewaltenteilung hinaus. Die Einhaltung dieser Regeln ist durch unabhängige Datenschutzbeauftragte sicherzustellen. Weiter muß für den Betroffenen Datentransparenz in dem Sinne bestehen, daß er sich über den Verbleib seiner Daten informieren und die Löschung unrichtiger Angaben verlangen kann.

Der Existenz dieser „Eingriffsschranken“ kommt mindestens ebenso große wie dem informationellen Selbstbestimmungsrecht als solchem zu.

3. Die vom Bundesverfassungsgericht entwickelten Grundsätze haben in der arbeitsgerichtlichen Rechtsprechung bisher nur bescheidene Resonanz gefunden. Das BAG hat zwar die Risikoanalyse des Bundesverfassungsgerichts übernommen und das informationelle Selbstbestimmungsrecht einem abgelehnten Bewerber wie einem Arbeitnehmer zuerkannt, doch soll dieses unter dem Pauschalvorbehalt berechtigter Interessen des Arbeitgebers stehen. Die „Eingriffsschranken“, wie sie sich etwa im Gebot informationeller Gewaltenteilung und in der Installierung einer unabhängigen Kontrollinstanz niederschlagen, fanden keine Berücksichtigung. Auch die Literatur ist in diesem Punkte äußerst zurückhaltend. Aussagen darüber, ob zu Abrechnungszwecken erhobene Dateien auch für Disziplinarmaßnahmen herangezogen werden dürfen, finden sich nur selten. Erst recht hat das wenig an Innovation ausgerichtete Beamtenrecht die Rechtsprechung des Bundesverfassungsgerichts noch nicht wahrgenommen.

4. Die Anwendung des informationellen Selbstbestimmungsrechts im Arbeitsverhältnis ist eine Frage der Drittwirkung der Grundrechte. Diese sind unbestrittenermaßen beim Abschluß von Tarifverträgen und Betriebsvereinbarungen sowie im Beamtenverhältnis zu beachten. Auch im Arbeitsverhältnis gilt gerade für Grundrechte mit Persönlichkeitsbezug nichts anderes. Zwar bekennt sich das BAG in neuerer Zeit dazu, Grundrechte könnten nur über die Auslegung von Generalklauseln Eingang ins Arbeitsverhältnis finden, doch führt dies nach der bisherigen Praxis nicht zu einer Reduzierung ihrer Geltungskraft. Auch einige Formulierungen der Volkszählungsentscheidung sprechen für eine Beachtung im Verkehr zwischen Privaten, wenn etwa vor einer „Gesellschaftsordnung“ gewarnt wird, in der der Bürger nicht wissen kann, „wer, was, wann und bei welcher Gelegenheit“ über ihn weiß.

5. Einschränkungen des informationellen Selbstbestimmungsrechts im Arbeitgeberinteresse stellen sich als Problem der Grundrechtskollision dar. Würde man den Arbeitgeber darauf beschränken, nur aufgrund überwiegenden Allgemeininteresses Daten seiner Arbeitnehmer erheben und verarbeiten zu dürfen, wäre er in seiner durch Art. 12 Abs. 1 GG garantierten Berufungsfreiheit übermäßig eingeschränkt. Ein Eingriff in das informationelle Selbstbestimmungsrecht ist daher auch dann möglich, wenn andernfalls die Funktionsfähigkeit des Unternehmens gefährdet wäre. Diese vergleichsweise hohe Schwelle erklärt sich damit, daß nur dann das Arbeitgeberinteresse „überwiegt“, stellt doch das

informationelle Selbstbestimmungsrecht nach Auffassung des Bundesverfassungsgerichts nicht nur ein individuelles Rechtsgut, sondern auch eine Funktionsvoraussetzung einer freiheitlichen Kommunikationsordnung dar.

6. Persönlichkeitsprofile sind unzulässig. Sie liegen dann vor, wenn die Informationsdichte über den einzelnen Arbeitnehmer so groß ist, daß künftiges Verhalten prognostizierbar und so ein persönliches Gespräch mit dem Betroffenen überflüssig wird.

7. Auch im Arbeitsverhältnis gilt das Gebot der Zweckbindung. Der Verwendungszweck von Daten ist dabei möglichst eng zu bestimmen: Je weiter der Zweck, um so größer sind Datenmenge und Verknüpfungsmöglichkeiten und um so tiefer dann auch die Eingriffe in die Persönlichkeitssphäre. (...)

14. Das auch im Arbeitsverhältnis geltende Verbot der Zweckentfremdung muß durch Separierung der Datenbestände abgesichert werden. Dies gilt etwa für arbeitsmedizinische Daten, die nur dem Betriebsarzt zur Verfügung stehen dürfen. Die aus ihnen abgeleiteten Schlußfolgerungen für die Eignung eines Arbeitnehmers dürfen nicht als Begründung für eine Kündigung herangezogen werden. Daten, die im Hinblick auf die soziale Auswahl bei betriebsbedingten Kündigungen erhoben werden, dürfen nur in diesem Kontext eine Rolle spielen. Was zu Abrechnungszwecken erfaßt wurde, darf nicht im Rahmen der Nachwuchsförderung, was bei Betriebsdatenerfassung anfällt, darf nicht für Disziplinarmaßnahmen verwendet werden. Dem Arbeitgeber steht es frei, daneben Daten zu Zwecken der Abrechnung oder der (zulässigen) Kontrolle des Arbeitsverhaltens zu speichern. Die Separierung der Datenbestände ist zumindest durch die Zuteilung von beschränkten Zugriffsrechten sicherzustellen. Die in größeren Unternehmen schon aus Zweckmäßigkeitsgründen praktizierte funktionale Differenzierung wird so zum rechtlichen Gebot.

15. Auch unter Wahrung der Zweckbestimmung sind nicht beliebige Auswertungen zulässig. Sie dürfen nicht die Grenze zum Persönlichkeitsprofil und zur Totalüberwachung des Arbeitsverhaltens überschreiten. Werden durch Auswertungen neue Aussagen erzeugt, liegt eine „Datenveränderung“ im Sinne des § 25 BDSG vor. Auch sie ist nur zulässig, soweit sie für die Funktionsfähigkeit des Unternehmens erforderlich ist. Statistische Berechnungen, die im Rahmen der Personalplanung einen legitimen Platz haben, sind möglichst umgehend zu anonymisieren, Auswertungen ohne aktuellen Anlaß sind unzulässig. Wird wie beim reinen Datenabruf keine neue Aussage erzeugt, gelten dieselben Grundsätze, da das informationelle Selbstbestimmungsrecht auch gegen manuelle Auswertungen dieser Art schützt.

16. Übermittlung ist die gefährlichste Form der Datenverarbeitung. Auch ist sie nur bei überwiegendem Interesse des Arbeitgebers, Dritter oder der Allgemeinheit zulässig. Die Zweckbindung muß beim Datenempfänger gesichert bleiben.

17. Zulässig ist die Weitergabe von Betriebsdaten bei fremdgesteuerter Produktion. Bei der Überlassung von Arbeitskräften können auch die dafür notwendigen Informationen mitgeliefert werden. Die Übermittlung von Arbeitnehmerdaten an ein anderes Konzernunternehmen ist nur dann zulässig, wenn auch das Arbeitsverhältnis für den Gesamtkonzern besteht. Die konzerninterne Auftragsdatenverarbeitung ist allein dann rechtlich unbedenklich, wenn das Arbeitgeberunternehmen personalpolitische Autonomie besitzt und besondere Vorkehrungen gegen einen Datenabgleich getroffen werden. Die Weitergabe von Arbeitnehmerdaten an einen Branchenauskunftsdienst ist unzulässig. Einen neuen Arbeitgeber zu informieren, ist in engem Rahmen zulässig.

18. Übermittlungen ins Ausland sind nur bei konzerndimensionalem Arbeitsverhältnis mit einem multinationalen Unternehmen zulässig. Dabei verbietet es der deutsche „ordre public“, eine freie Datennutzung in Staaten ohne Datenschutzgesetzgebung zuzulassen.

Kontrollrechte

19. Die Informationspflicht des Arbeitgebers nach § 26 Abs. 1 BDSG und der Auskunftsanspruch des Arbeitnehmers nach § 26 Abs. 1 BDSG werden den Vorgaben des Bundesverfassungsgerichts nicht gerecht und können die gebotene Datentransparenz nicht sicherstellen. Der Arbeitnehmer muß soweit informiert werden, daß er sinnvolle Nachfragen stellen kann. Sein Auskunftsanspruch muß sich auch auf die Herkunft der Daten, die Rechtsgrundlage der Speicherung und alle (nicht nur die regelmäßigen) Empfänger von Übermittlungen erstrecken.

20. Die Verwendung von Abfragesprachen beim Umgang mit Echtdaten ist unzulässig, da der Betroffene nicht mehr wissen kann, welche konkreten, seine Person betreffenden Informationen mit Hilfe von Verknüpfungen hergestellt werden. Auch unterlaufen Abfragesprachen das Gebot der Zweckbindung. Zulässig sind sie nur beim Umgang mit Testdaten.

21. Unzutreffende Tatsachen müssen nach § 27 Abs. 1 BDSG berichtigt werden. Im Prozeß hat die speichernde Stelle die Richtigkeit zu beweisen.

22. Der Arbeitgeber hat Daten zu sperren, die er nicht mehr benötigt. Dies gilt auch für Vorstrafen, die in einem polizeilichen Führungszeugnis nicht mehr in Erscheinung treten würden, sowie für Betriebsbußen und Abmahnungen, die länger als zwei bis drei Jahre zurückliegen.

23. Bestimmte besonders sensible Datensind nach § 27 Abs. IV. Satz 3 BDSG bereits dann zu löschen, wenn der Betroffene ihre Richtigkeit bestreitet. Gleichzustellen sind Abmahnungen oder gewerkschaftliche Aktivitäten.

24. Das Recht zur Gegendarstellung aus § 83 Abs. 2 BetrVG hat keine datenschutzrechtliche Parallele und besteht daher neben den Rechten aus § 27 BDSG.

25. Der sog. betriebliche Datenschutzbeauftragte besitzt nur eine sachliche, jedoch keine persönliche Unabhängigkeit gegenüber dem Arbeitgeber. Bestimmte besonders arbeitgebernahe Personen sind als Datenschutzbeauftragte ungeeignet.

26. Die Stellung der Aufsichtsbehörde ist schwach und entspricht nicht den Vorgaben des Bundesverfassungsgerichts für eine unabhängige Kontrollinstanz.

### Interessenvertretung

27. Der Betriebsrat hat die Einhaltung des BDSG und anderer datenschutzrechtlicher Normen zu überwachen. Zu diesem Zweck steht ihm gegenüber dem Arbeitgeber ein umfassendes Informationsrecht zu. Soweit dieses auch personenbezogene Daten einzelner Arbeitnehmer erfaßt, ist das informationelle Selbstbestimmungsrecht nicht verletzt. Der Betriebsrat ist auch zur Hinzuziehung eines Sachverständigen berechtigt, dessen Kosten der Arbeitgeber tragen muß.

28. Die Beteiligungsrechte des Betriebsrats nach §§ 92, 94, 95 und 87 Abs. 1 Ziffer 6 BetrVG stellen eine kollektivrechtliche Ergänzung des individualrechtlichen Persönlichkeitsschutzes dar. Sie erfüllen die Funktion eines Verfahrens zur Realisierung des informationellen Selbstbestimmungsrechts.

29. Das Mitbestimmungsrecht des Betriebsrats aus § 94 BetrVG bezieht sich auf alle standardisierten Erhebungsmittel einschließlich einer Bildschirmmaske sowie auf die weitere Verwendung der erhobenen Daten. Unter Verstoß gegen § 94 BetrVG erlangte Informationen dürfen nicht gespeichert werden.

30. Werden Eignungs- und Fähigkeitsprofile von Arbeitnehmern und Anforderungsprofile von Arbeitsplätzen abgeglichen, so greift die Mitbestimmung nach § 95 Abs. 1 BetrVG ein.

31. Aufgrund seiner Unabhängigkeit vom Arbeitgeber erfüllt der Betriebsrat die Anforderungen des Bundesverfassungsgerichts an ein Überwachungsorgan. Er darf daher nicht der Kontrolle des potentiell vom Arbeitgeber abhängigen „betrieblichen“ Datenschutzbeauftragten unterstellt werden.

32. § 87 Abs. 1 Ziffer 6 BetrVG greift bei allen EDV-Systemen ein, die personenbezogene Daten speichern. Im Extremfall genügt ein einzelnes personenbezogenes Datum, da durch Verknüpfung mit anderen gespeicherten Daten und durch Verwendung von Zusatzwissen Aussagen zu Verhalten und Leistung des Arbeitnehmers möglich sind. Im einzelnen gilt folgendes:

- EDV-Systeme sind „technische Einrichtungen“ im Sinne des § 87 Abs. 1 Ziffer 6. Der Mitbestimmung unterliegt dabei das gesamte System. Es ist nicht möglich, sie auf einzelne Komponenten wie Überwachungsprogramme zu beschränken.

- „Überwachung“ erfaßt nicht nur das „Beobachten“, d. h. die Erhebung von Daten, sondern auch ihre Auswertung. Auch einzelne Datenläufe sind daher mitbestimmungspflichtig.

- Die Überwachung kann sich auch auf nichtarbeitsbezogenes Verhalten des Arbeitnehmers erstrecken. Fehlzeiten sind ebenfalls erfaßt.

- Ohne Bedeutung ist die Qualität der gespeicherten Daten. Entscheidend kommt es allein darauf an, ob sie ein Element für die Erarbeitung einer Aussage über Verhalten und Leistung sind.

- Die technische Einrichtung muß die Aussage über Verhalten und Leistung nicht selbst erarbeiten. Es reicht aus, daß diese mit Hilfe von Zusatzwissen des „Systemherrn“ herstellbar ist.

- Ob der Arbeitgeber überwachen will oder nicht, ist ohne Bedeutung. Es reicht, daß das System unter Berücksichtigung der obigen Grundsätze zur Überwachung geeignet ist. Eine „unmittelbare“ Eignung ist nicht mehr erforderlich.

- Gruppenüberwachung ist dann mitbestimmungspflichtig, wenn der Überwachungsdruck auf den einzelnen durchschlägt. Dies muß nicht notwendigerweise von einer bestimmten Gruppengröße oder der Arbeit im Akkord abhängen.

33. Bei der Ausfüllung des durch § 87 Abs. 1 Ziffer 6 eröffneten Regelungsspielraums sind die Betriebsparteien an zwingendes Recht, insbesondere an Grundrechte gebunden. Durch Betriebsvereinbarung kann zwar eine Datenverarbeitung zugelassen werden, die nach dem BDSG nicht möglich wäre, doch ist das informationelle Selbstbestimmungsrecht der Arbeitnehmer zu beachten. Die aus der Rechtsprechung des Bundesverfassungsgerichts folgenden Anforderungen – insbesondere die Eingriffsvoraussetzungen eines überwiegenden Arbeitgeberinteresses und der Zweckbindung – sind auch für die Betriebsparteien maßgebend. Weiter scheidet die Aufzeichnung von Telefondaten einschließlich der angewählten Zielnummer entgegen der Auffassung des BAG an Art. 10 GG.

34. Die Betriebsparteien sind nicht darauf beschränkt, nur solche Regelungen zu treffen, die unmittelbar durch den von § 87 Abs. 1 Ziffer 6 verfolgten Zweck des Persönlichkeitsschutzes geboten sind. Es geht vielmehr um einen „billigen Ausgleich“ zwischen den Belangen der betroffenen Arbeitnehmer und den wirtschaftlichen Interessen des Arbeitgebers. Die „Billigkeit“ ist dann nicht gewahrt, wenn dem Arbeitgeber Verwertungsmöglichkeiten außerhalb des vorgesehenen Zwecks bleiben oder ein Überwachungsdruck nicht durch intensive Einschaltung des Betriebsrats kompensiert wird.

35. Das Mitbestimmungsrecht des Betriebsrats umschließt ein Initiativrecht; es kann auch im Wege einer Regelungsabrede ausgeübt werden. Eine Durchsetzung ist im Wege der einstweiligen Verfügung, aber auch dadurch möglich, daß die von einer mitbestimmungswidrigen Maßnahme betroffenen Arbeitnehmer ihre Arbeitsleistung so lange zurückhalten, bis der Rechtsverstoß beseitigt ist.

36. Änderungen eines Informationssystems sind mitbestimmungspflichtig, soweit sie die Überwachungskapazität gegenüber den Arbeitnehmern erhöhen.

37. Die Einführung und Veränderung von Abfragesprachen unterliegt – unbeschadet datenschutzrechtlicher Bedenken – der Mitbestimmung.

38. Die Verarbeitung von Arbeitnehmerdaten auf PC ist unzulässig. Eine Ausnahme gilt dann, wenn die Datensicherung nach § 6 BDSG im selben Umfang wie bei einem Rechenzentrum verwirklicht wird, was nicht ohne außergewöhnlichen Aufwand möglich ist.

39. Innerbetriebliche Vernetzung bedeutet Einführung einer neuen technischen Einrichtung und löst deshalb das Mitbestimmungsrecht nach § 87 Abs. 1 Ziffer 6 aus. Die auf einzelne Komponenten des Systems bezogenen Regelungen bleiben zunächst wirksam.

40. Bei Einführung überbetrieblicher Vernetzung kann nur der im Betrieb oder Unternehmen befindliche Systemteil mitbestimmt werden. Die Einbeziehung von Arbeitnehmerdaten wird häufig schon datenschutzrechtlich unzulässig sein. Auch wird es wegen der mangelnden Kontrollmöglichkeiten des Betriebsrats meist an einem billigen Interessenausgleich fehlen.

41. Das Personalvertretungsrecht bleibt wegen seiner Handhabung durch die Verwaltungsgerichte häufig auch dann hinter dem Betriebsverfassungsrecht zurück, wenn der Gesetzestext voll oder weitgehend übereinstimmt. Hinzu kommt, daß die Diskussion über die Einführung neuer Technologien in der personalvertretungsrechtlichen Literatur noch wenig entwickelt ist.

42. Der Personalrat hat grundsätzlich dieselben Informationsrechte wie der Betriebsrat (§ 15, II). Die einschlägigen Beteiligungsrechte nach BPersVG weisen keine wesentlichen Abweichungen vom Betriebsverfassungsrecht auf.

**D/R/S**