# Vortrag Däubler

Liebe Kolleginnen und Kollegen,

Ich bin seit 1971 Mitglied der ÖTV, dann zu ver.di gekommen. Und ich habe eine Anschlussmitgliedschaft in der IG Metall.

Zweiter persönlicher Punkt. Ich bin seit einer Reihe von Jahren relativ intensiv mit China befasst. Einmal ist es ein gewisses Mittel gegen das Älterwerden, wenn man sich um neue Dinge kümmert und nicht nur das auf Sparflamme fortsetzt, was man immer gemacht hat. Ich bin zweimal im Jahr einen Monat dort und bin im Begriff eine Kultur zu entdecken, die mir viele neue Erkenntnisse und auch im Alltag viele interessante Erfahrungen bringt.

Das Problem des Datenschutzes gibt es übrigens auch in China. Bei meinem letzten Aufenthalt habe ich eine Lehrveranstaltung über „Datenschutz in Europa“ gemacht. Das Interesse für diesen Problembereich wächst auch dort, weil die Leute sich ärgern, wenn sie unaufgefordert irgendwelche Werbematerialien zugesendet bekommen oder von Unbekannten angerufen werden.

Ich selbst bin auf eher ungewöhnliche Art zum Datenschutz gekommen. Ein kluger und intelligenter Gewerkschaftskollege, damals bei der Böckler-Stiftung beschäftigt, hatte eigene Entscheidungsspielräume. Er wollte, dass ich in diesen Bereich einsteige. Zunächst musste ich mich erst mal in die Materie einlesen. In dem Böckler-Projekt wurde mir dann ein Beirat zur Seite gestellt, der mich immer wieder mit Fragen quälte. Mitte der achtziger Jahre kam dann aufgrund des Projekts ein Buch zustande, das es heute noch unter dem Titel "Gläserne Belegschaften?“ gibt.

Moderator: Einige Unterpunkte, AEO-Zertifizierung, Safe Harbor-Bestimmungen, Compliance-Richtlinien, GPS-Überwachung. Mindestens 3 von 4 Sachen waren mir vorher nicht so ganz klar. Ich hoffe, dass du uns ein bisschen Licht ins Dunkel bringen wirst.

Däubler: Zunächst ein paar einleitende Bemerkungen über den Datenschutz. Im Betrieb werden außerordentlich vielfältige Daten gespeichert und verarbeitet. Da gibt es einmal die Personalakte, in der etwas über den Lebenslauf steht, über die Qualifikation, über die Familienverhältnisse, über Fehlzeiten und anderes mehr. Daneben entstehen im Betrieb je nach Technisierung eine Menge arbeitsbezogener Daten. Da sind z. B. die Kommens- und Gehenszeiten, die heute normalerweise elektronisch erfasst werden. Auch wann der PC eingeschaltet oder ausgeschaltet wird, kann ohne weiteres festgehalten werden. Man kann auch überprüfen, wie weit ein bestimmtes Projekt gediehen ist. Wie schnell haben die Beteiligten gearbeitet und wie weit sind sie jetzt? Man kann auch feststellen, wie oft sich jemand vertippt hat.

Lange Zeit galt der Arbeitnehmerdatenschutz als eine exotische Materie. Man hatte gewisse Schwierigkeiten, Fälle zu belegen, bei denen man sagen konnte, unerhört, was da passiert ist, wir brauchen einen konsequenten Datenschutz.

In einer Kantine isst beispielsweise jemand regelmäßig das Diätessen. Dies lässt den Rückschluss zu, dass dieser Mensch offensichtlich einen empfindlichen Magen hat, also kommt er für Einsätze in Ländern mit robuster Küche wie z. B. in Russland nicht unbedingt in Betracht.

Ein anderes relativ harmloses Beispiel war das Abgleichen von Kindergeburtstagen mit den eintägigen Fehlzeiten von Frauen. Man stellte erhebliche Überschneidungen fest. Das legte natürlich einen Verdacht nahe.

Grundlegendes änderte sich erst durch die Datenschutzskandale bei der Bahn, bei

der Telecom und bei Lidl. Ich will dies nur an dem Fall Lidl etwas verdeutlichen. Es gab in keiner der dreißig Lidl-Vertriebsgesellschaften auch nur einen einzigen betrieblichen Datenschutzbeauftragten. Die Firma hatte einige versteckte Kameras installiert, Videokameras, von denen niemand etwas wusste, auch die Betriebsräte nicht. Außerdem hatte man zahllose Privatdetektive eingesetzt. Diese behaupteten, sie wären normale Mitarbeiter und sollten nur verhindern, dass Kunden bei Lidl klauten. Folglich sahen die Beschäftigten von Lidl diese quasi als ihre Kollegen an und behandelten sie entsprechend. Jeden Abend schrieben die Privatdetektive ein Protokoll über ihre Gespräche, die sie mit diesen Beschäftigten geführt hatten. Das kam auf etwas abenteuerliche Art und Weise heraus und wurde Gegenstand eines Fernsehberichts: Journalisten bekamen die Abrechnungen, die die Detektei an Lidl geschickt hatte. Da wurde stundengenau abgerechnet und auch die Abendstunden mit der Protokollierung erfasst. Auf diese Weise kam heraus, dass die Privatdetektive die Gespräche mit den Lidl-Beschäftigten im Einzelnen protokolliert hatten. Die Öffentlichkeit war schockiert. Aber es waren ein paar glückliche Zufälle, die dazu führten, dass die Lidl Geschichte überhaupt an die Öffentlichkeit gelangte. Seither hat man sehr viel mehr Sensibilität für diesen Bereich entwickelt und es dauert im Grunde keine vierzehn Tage, bis man nicht irgendwo wieder einen größeren oder kleineren Skandal entdeckt.

Im Moment beschäftige ich mich mit dem Fall des Steakhauses *Maredo* aus Frankfurt. Es hat auch eine Niederlassung in der Frankfurter Fressgass´. Die findet man ganz spontan sympathisch. Die Arbeitsbedingungen dort sind aber weniger schön. Man hatte dort seit vielen Jahren das Phänomen, dass hin und wieder Beschäftigte einzelne Dinge, die man nicht mehr an Kunden ausgab, mit nach Hause genommen haben, z. B. ein Anschnitt von Brot oder Reste, die übrig geblieben waren. Manchmal aß jemand auch im Betrieb selbst etwas. Das war jahrelang so üblich. Dann verkündete der Arbeitgeber, dass ab sofort nur noch das mitgenommen und gegessen werden darf, was bezahlt wird. Die Kollegen und Kolleginnen ignorierten das und machten so weiter wie bisher, weil der Arbeitgeber eine Betriebsübung nicht einfach abschaffen kann. Daraufhin installierte die Firma Maredo drei versteckte Kameras, ohne den Betriebsrat zu fragen. Außerdem engagierte sie zwei Privatdetektive, die als Kellner tätig waren.

Die gleiche Methode wie bei Lidl. Eine Woche lang erfolgte eine Überprüfung mit dem Ergebnis, dass da und dort wieder ein Stück Brot und Ähnliches mitgenommen wurde. Daraufhin ließ man an einem Abend plötzlich das Licht ausgehen bei Maredo. Es kam ein privater Sicherheitsdienst. Keiner durfte das Lokal verlassen. Den Beschäftigten wurde vorgeworfen, dass sie sich alle am Eigentum des Arbeitgebers vergangen hätten und das ist bekanntermaßen heilig und unantastbar. Sie wurden vor die Entscheidung gestellt, entweder selbst zu kündigten oder fristlos gekündigt zu werden. Es waren etwa vierzig Beschäftigte, vierzehn kündigten selbst, ungefähr zwanzig wurden fristlos gekündigt. Dann ließ sie der Sicherheitsdienst wieder raus.

Es gibt eine Strafanzeige wegen Freiheitsberaubung. Die Staatsanwaltschaft ermittelt. Im Moment befasst sich die hessische Arbeitsgerichtbarkeit mit den Kündigungsschutzklagen. Heute in einer Woche findet eine Solidaritätsveranstaltung für die Maredo-Beschäftigten im DGB-Haus in Frankfurt statt.

Ein Beispiel, was in unserem Lande so alles passiert, bietet auch ein Augsburger Fall. Der Arbeitgeber ließ im PC des Betriebsratsvorsitzenden eine sogenannte Spyware einbauen, ohne dass dieser etwas davon bemerken konnte. Niemand hatte das Zimmer betreten, um die Software zu installieren. Das hatte man aus der Ferne gemacht. Dieses eingebaute Programm zeichnete durch sog. Screenshots ganz genau auf, was der Einzelne macht. Voraussetzung war „Auslöser“, nämlich der Kontakt zum Zeiterfassungsprogramm, weil man dem Betriebsratsvorsitzenden Vorwürfe wegen der angeblichen Manipulation seiner Arbeitszeiten machte. Das wurde vom Arbeitsgericht Augsburg für unzulässig erklärt. Auch dies war ein Fall, wo man sich eindeutig wehren sollte.

Im Betrieb passiert heute eine ganze Menge, der Datenschutz wird zu einer dringenden Angelegenheit. Der Betrieb ist ein Ort, wo außerordentlich viele Daten über einzelne Beschäftigte gesammelt werden. Viel mehr Daten als sie beispielsweise die Polizei oder die Gemeindeverwaltung oder sonst irgendeine Instanz hat. Auch die Krankenkasse weiß nur etwas über Krankheiten, nicht über das sonstige Leben des Betroffenen.

Der Datenschutz hat eine Rechtsgrundlage. Das ist das Bundesdatenschutzgesetz, das insbesondere in seinem § 32 auch Arbeitnehmer erfasst. Daneben gibt es eine wachsende Zahl an Gerichtsentscheidungen. Wichtig sind weiter die Entscheidungen der Aufsichtsbehörde. In jedem Land gibt es eine Aufsichtsbehörde, die alle zwei Jahre einen Bericht über ihre Tätigkeit anfertigt. Da kommt sehr viel an Erfahrungen zusammen. Die Aufsichtsbehörden sind mittlerweile unabhängig vom Innenministerium. Es sind in der Regel engagierte Datenschützer, die dort tätig sind.

Dazu kann ich einen Fall erzählen. In der Gegend von Oldenburg gab es einen Streik in einem Metallbetrieb. Ziel war es, wieder Anschluss an den Flächentarif zu bekommen. Der Arbeitgeber war der Auffassung, dass der Streik eine schlechte Sache sei, gewissermaßen Revolution im Kleinformat. Er wollte herausfinden, wer sich bei der Revolution besonders hervortut. Am Abend vor dem Streik installierte er auf dem Dach drei Videokameras, die den Eingang und den Hof des Gebäudes abdeckten.
Am Morgen entdeckte der Betriebsrat die Überwachung und engagierte einen Anwalt, der einen Antrag auf einstweilige Verfügung stellte, die dem Arbeitgeber dieses Vorgehen untersagen sollte. Außerdem wurde die Aufsichtsbehörde für Datenschutz in Hannover über diese unerlaubte Überwachung informiert. Die zuständige Person setzte sich gleich in den Zug und fuhr nach Oldenburg. Sie drohte dem Vernehmen nach dem Unternehmen mit einem Bußgeld von über fünfzigtausend Euro, wenn er die Videokameras nicht abbaue und die schon gemachten Filme nicht vernichte. Daraufhin wurden die Geräte abgebaut und die Filme vernichtet. Das Arbeitsgericht entschied drei Tage später über den Antrag auf einstweilige Verfügung. Da war die Sache schon erledigt, weil die Geräte bereits weg waren. Es war nur noch über die Kosten zu entscheiden. In dem Zusammenhang befand das Arbeitsgericht auch darüber, dass eine solche Form der Videoüberwachung von Streikposten illegal ist. Dies war die erste Entscheidung dieser Art.

Neue Entwicklungen in der Technik schlagen sich häufig im Betrieb nieder. Ich nenne einmal die Geschichte mit den gentechnischen Untersuchungen. Bekannt ist die Speichelprobe aus der Kriminalistik. Folgender Fall: Bei einer Sparkasse in Baden-Württemberg hatte jemand einen anonymen Brief an den Vorstand geschrieben. In diesem Brief stand: Ein Vorstandsmitglied verfüge über bescheidene charakterliche und geistige Fähigkeiten, insbesondere verstehe er nicht viel von Geld. Dies ist für einen Sparkassenvorstand der schwerste denkbare Vorwurf. Daraufhin überlegten sie Im Vorstand, wer das wohl geschrieben habe. Sie hatten einen Tipp bekommen, dass es ein Personalratsmitglied gewesen sein könnte. Aber das konnten sie nicht beweisen. Was tun? Da der Brief ja mit Speichel zugeklebt war, hatten sie eine Idee. Sie luden den verdächtigen Menschen zur Verabschiedung eines Kollegen ein. Als Personalratsmitglied kam er natürlich auch. Es gab Kaffee und Kuchen, anschließend ein Glas Wein. Als er fertig war, packten sie die Kaffeetasse, die Kuchengabel und das Glas zur Seite. Dann schickten sie diese drei Gegenstände und den Briefumschlag als Gegenstück an ein Institut, das sich normalerweise um die Feststellung von Vaterschaften kümmert. Die Gentechniker stellten fest, dass die Speichelproben übereinstimmten. Daraufhin wollte der Vorstand dem Personalratsmitglied kündigen. Im Gesetz „... aus wichtigem Grund mit Zustimmung des Personalrats“. Dieser verweigerte seine Zustimmung. Dann ging es zum Verwaltungsgericht, das in solchen Fällen zustimmen muss. Da der Richter fand, dass es eine schwierige Geschichte mit den Speichelproben sei, versuchte er

zu begründen, es käme gar nicht darauf an. So gemein sei der Brief auch wieder nicht gewesen. Es gibt ja Meinungsfreiheit in unserem Land, da könne man schon einmal Kritik äußern. Freundlich sei es nicht, aber für eine fristlose Kündigung reiche es auch nicht. Sie wiesen deshalb den Antrag des Arbeitsgebers zurück.

Die Sparkasse legt Beschwerde zum Verwaltungsgerichtshof in Mannheim ein. Die Richter waren etwas mutiger und sagten, dass solche Äußerungen schon ausreichten würden für einen wichtigen Grund. Aber die Speichelprobe kann nicht verwendet werden, da es sich um eine heimliche Ermittlungsmaßnahme des Arbeitgebers handelte. Die ist vorgesehen in der Strafprozessordnung, wenn ein Richter das anordnet und auch dann nur bei schwersten Delikten, nicht etwa bei Beleidigungen. Wenn der Staat nach dem Strafprozessrecht so etwas nur unter ganz engen Voraussetzungen machen kann, ist es unzulässig, dass gewissermaßen der Arbeitgeber das aus eigener Initiative macht, unter Berufung auf Notwehrrecht oder was auch immer. Also der Arbeitgeber darf sich nicht mehr rausnehmen, als sich der Staat selbst gestattet. Das hatte er hier aber getan und mit dieser Begründung wurde der Antrag zurückgewiesen.

Das war glücklicherweise ein vernünftiger Senat mit einer außerordentlich wichtigen Aussage: „Was der Staat nicht darf, darf der Arbeitgeber erst recht nicht!“ Es gibt viele Fälle, wo es anders gehandhabt wurde und wird.

Wie die Gentechnik tauchen im Betrieb auch andere technischen Neuerungen auf. Dazu zählt z. B. auch RFID („radio-frequency identification“). In der Ware befindet sich ein sehr kleiner Chip (z. B. in Kleidungsstücken). Wenn man damit an einem Lesegerät vorbeikommt, wird dies automatisch erfasst. So kann man Waren physisch steuern. Man könnte theoretisch aber auch die Bewegungsabläufe einzelner Menschen kontrollieren, indem man beispielsweise Chips in der Kleidung anbringt.

Dann gibt es GPS, dazu kommen wir noch. Dann gibt es Facebook und andere soziale Netzwerke. Das ist nicht unter den speziellen Themen, die ich hier behandeln soll. Deshalb nur ein paar kleine Bemerkungen.

Zunächst einmal eins: Wenn ich zu Hause am Computer sitze und da irgendetwas eingebe, dann fehlt mir die kritische Rückmeldung, die ich im Gespräch normalerweise habe. Wenn ich z. B. E-Mails schreibe, ist mein Ton ein anderer, vielleicht auch schärfer und verletzender, als wenn ich jemandem direkt gegenüberstehe. Das heißt die unmittelbare menschliche Korrektur fehlt, ich merke nicht, wie das Gesicht des Anderen auf das reagiert, was ich sage. Und deshalb ist die Gefahr sehr groß, dass man etwas schreibt, das man unter Anwesenden normalerweise nie öffentlich sagen würde.

Es gibt ein kleines Beispiel aus der Rechtsprechung. Eine Azubi ärgert sich über ihren Chef und schreibt in Facebook: "Dieser Widerling. Aber, da gibt es Gegenmaßnahmen, nichts als ab zum Arzt und nach Mallorca!" Sie lässt sich tatsächlich krankschreiben und fliegt nach Mallorca. Das war eindeutig eine vorgetäuschte Krankheit. Sie wurde dann fristlos gekündigt. Das zeigt, dass man allein vor dem Computer Sätze in die Welt setzt, die man normalerweise nie öffentlich sagen würde.

Weiter gibt es das Problem, dass man seine eigenen Eintragungen zwar löschen kann, aber man nie weiß, ob diese nicht von anderen Menschen kopiert wurden. Dann bleiben sie bestehen, und es kann weiter noch irgendjemand auf sie zurückgreifen, der diese dann für seine Zwecke verwenden kann. D. h., das, was ich eingebe, hat in gewissem Umfang, auch wenn ich es wieder zurücknehme, Ewigkeitswert. Und das ist besonders gefährlich.

Eine weitere Geschichte zu Facebook. Es gibt ein sehr aktives und von klugen Leuten besetztes unabhängiges Landes-Datenschutz-Zentrum in Schleswig-Holstein

(ULD). Sie entdeckten dort Folgendes: Wenn man ein Bild in Facebook eingibt, dann wird dieses Bild, ohne dass man vorher gefragt wird, automatisch vermessen. D. h., die Gesichtszüge werden im Einzelnen sehr genau wie für Fahndungen biometrisch erfasst. Dies bedeutet dann, dass andere Leute, die beispielsweise ein Bild von jemandem aus früheren Jahren haben, feststellen können, ob er oder sie es ist oder nicht. Man ist dann sehr viel leichter erkennbar, weil der Vergleich mit anderen Bildern der Person möglich ist. Verharmlosend ausgedrückt: Der Einzelne wird zu einem kleinen Kriminalkommissar.

So etwas kann man machen, wenn der Betroffene damit einverstanden ist. Ohne Einverständnis geht es nicht. Das Problem ist nur, dass Facebook hier keine Niederlassung hat, sondern in Irland. Diese hat aber zu allem Überfluss nichts zu sagen. Das unabhängige Landeszentrum für Datenschutz hat deshalb einen Brief an den Sitz der Konzernspitze nach Kalifornien geschickt, mit der Forderung diese Form der Vermessung von Gesichtern doch bitte zu unterlassen. Dem hat Facebook inzwischen entsprochen.

Soziale Medien sind sehr mit Vorsicht zu genießen. Sie sind ein wichtiges Thema auch im Betrieb. Wenn z. B. einzelne Beschäftigte moralisch vom Arbeitgeber verpflichtet werden, sich bei Facebook oder Twitter anzumelden und dafür zu sorgen, wenn der Betrieb kritisiert wird, eine gute Gegenposition einzunehmen, im Sinne, dass die Produkte ihres Betriebes die besten sind. Man hat das Phänomen, dass der Arbeitnehmer gewissermaßen in diesen sozialen Netzwerken eingesetzt wird als Propagandist des Arbeitgebers. Daraus ergeben sich eine ganze Reihe von Folgefragen. Ist man wirklich dazu gezwungen? Ist das im Arbeitsvertrag festgelegt oder kann man nein sagen? Was passiert, wenn man nein sagt? Und ähnliches mehr.

Als nächstes erläutere ich einmal die AEO-Zertifizierung. Was heißt AEO? AEO heißt: Acknowledged Economic Operator, also anerkannter Wirtschaftsteilnehmer. Dies wird man nur aufgrund eines Zertifikats, das man vom Bundesfinanzministerium bekommt. Das Zertifikat und die Überprüfung zu verlangen, ist von der Rechtsgrundlage her aus folgendem Grund höchst zweifelhaft: Es gibt zwei EU-Verordnungen zur Bekämpfung des Terrorismus. In diesen Verordnungen steht, dass es eine bestimmte Anzahl von verdächtigen Menschen gibt, die im Anhang aufgeführt sind. Das sind jeweils ungefähr 300 Personen – das kann man im Amtsblatt der Europäischen Union und auch im Internet nachlesen. Es handelt sich um jeweils 300 vorwiegend arabische Namen auf diesen Listen.

Anerkannt wird nur derjenige, der beweisen kann, dass in seiner Belegschaft niemand auf dieser Liste steht. Denn die Liste erfasst Personen, die in Verdacht stehen, den Terrorismus zu unterstützen. Das sind alles keine Personen, die als Terroristen unmittelbar gesucht werden oder Beihilfe leisteten, denn dann wäre das kein Problem. Wenn man sie hätte, würden sie ins Gefängnis kommen. Sondern hier geht es um einen Personenkreis, dem man nicht nachweisen kann, den Terrorismus, Al Kaida, die Taliban oder wen auch immer zu unterstützen. Es besteht nur ein Verdacht; vermutlich denkt der CIA, dass die fraglichen Personen den Terrorismus unterstützen.

Wenn davon eine Person auf der Liste steht, hat das für sie erhebliche existentielle Konsequenzen. Es gilt dann ein so genanntes Bereitstellungsverbot. Das klingt ganz harmlos. Das heißt der Sache nach aber sehr viel mehr. Es ist mit Strafe untersagt, mit solchen Personen noch irgendwelche Verträge zu schließen, ihnen irgendwelche wirtschaftlichen Werte bereitzustellen. Selbst der Verkauf von drei Brötchen wäre ein Verstoß gegen das Bereitstellungsverbot. Man nimmt also gewissermaßen diese Leute aus dem wirtschaftlichen Leben heraus, man entzieht ihnen die Rechte als Marktbürger. Wenn diese Personen Arbeitnehmer sind, darf man ihnen nicht einmal für die Zeit, die sie schon gearbeitet haben, das Gehalt auszahlen. Auch das wäre eine wirtschaftliche Unterstützung.

Dieses Zertifikat als anerkannter Wirtschaftsbeteiligter bekommt man also nur, wenn man vorher die eigene Belegschaft mit der Antiterrorliste abgeglichen hat. Zum Glück gibt es in der Bundesrepublik niemanden, der ernsthaft versucht, den Terrorismus zu unterstützen. Aber das Problem ist, dass es Namensgleichheiten geben kann. Wenn man sich die Liste einmal anschaut, stellt man fest, dass die Leute nur mit Namen und potentiellem Geburtsort aufgeführt sind; oft steht da auch gleich ein Fragezeichen dahinter. Auch im arabischen Raum gibt es wie in Deutschland Sammelnamen wie Fritz Müller. Wenn jemand einen solchen Namen hat – z. B. Abu Alabd –, dann kann es ihm passieren, dass er erst einmal nicht mehr beschäftigt werden kann und aus dem Betrieb ausgegliedert wird. Was macht man in einer solchen Situation? Zunächst einmal ist klar, dass der Betriebsrat ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG hat, so weit es um die Abgleichung geht. Es ist eine Maßnahme von Kontrolle und vor allem um die Leistung der Arbeitnehmer.

Eine andere Frage ist, inwieweit Unternehmer den Betriebsrat wirklich fragen oder einfach die Abgleichung so vornehmen. Das ist schwierig zu beantworten. Vermutlich gibt es eine ganze Reihe von illegalen Abgleichungen, weil die Unternehmer davon ausgehen, dass keiner davon auf der Liste steht und deshalb keine Probleme entstehen. Das ist unkorrekt. Es verletzt die Rechte des Betriebsrats. Wenn nun der Betriebsrat Mitbestimmungsrechte ausübt, dann sollte er dafür sorgen, dass Menschen, die wegen Namensgleichheit in Verdacht geraten, ausreichend geschützt sind. Indem, z. B. der Arbeitgeber dafür sorgt, dass ihnen ein sachkundiger Anwalt zur Verfügung gestellt wird, der sich in dieser sehr spezifischen Materie auskennt. Der Arbeitgeber ist in Gefahr, sich strafbar zu machen, wenn er ihm Geld zahlt. Zunächst gilt dieser Mensch als Bösewicht, weil er anscheinend mit einem identisch ist, der auf der Liste steht. Dann muss man sich erst einmal wieder dagegen wehren und muss klarstellen, dass man mit diesem überhaupt nichts zu tun hat. Das geht sinnvollerweise nur mit anwaltlicher Hilfe. Man muss sehen, dass man dann auch Familienangehörige und andere unterstützt. Es gibt auch ein paar Modelle, die aufzeigen, was in solchen Fällen zu machen ist.

Frage: Ist das eine reine Namensliste. Stehen da keine anderen Daten, die noch irgendwelche Herleitungen machen?

Däubler: Das ist unterschiedlich. Bei einzelnen Personen ist nur der Vor- und Zuname vermerkt. Dann gibt es solche mit genauer Angabe des Geburtstags und Geburtsortes, was es leichter macht. Und solche, bei denen ein Name vermerkt ist und ein Pseudonym. Manchmal ist vermerkt, dass sich hinter dem Pseudonym wahrscheinlich der oder jener verbirgt. Weil die Angaben sehr unterschiedlich sind, ist die Gefahr, dass jemand mit arabischen Namen drunter fällt, nicht von der Hand zu weisen, auch wenn er überhaupt nichts mit Terrorismus zu tun hat. Es gibt einen Fall, bei dem jemand dagegen geklagt hat, dass er auf der Liste steht.

Dabei ging es allerdings nicht darum, welcher und wer der Richtige ist. Er war der Richtige. Das Problem war, dass er mit dem Terrorismus nichts zu tun hatte und deshalb von der Liste gestrichen werden wollte. Die EU-Kommission erhält die Listen anscheinend vom CIA, bekommt aber keine Fakten mitgeliefert, auf die sie einen Verdacht stützen könnte. Deshalb konnte sie im gerichtlichen Verfahren nur auf Zeit spielen. Die Kommission verlor vor dem Europäischen Gericht erster Instanz, und auch der Europäische Gerichtshof verlangte, dass der Kläger namens Kadi von der Liste gestrichen wird. Das Verfahren dauerte aber insgesamt sieben Jahre, eine lange Zeit, in der der Betroffene als „Ausgebürgerter“ zu leben hatte,

Wenn ein Betriebsrat in der Lage ist, über eine solche Situation eine Betriebsvereinbarung zu schließen, so sollte er dies unbedingt tun. Wer ohne Verschulden in Verdacht gerät, verdient Schutz.

Das war die AEO-Zertifizierung, ein modernes Problem des Datenschutzes.

Es gibt ähnliche Fälle aus dem Flugverkehr, für den er Sonderregelungen im Luftsicherheitsgesetz gibt. Auch hier wird die Problematik wieder an einem konkreten Fall deutlich. Jeder, der auf dem Flughafen oder bei einer Airline beschäftigt ist, musste (und muss) sicherheitsüberprüft werden. Zur Sicherheitsprüfung gibt es ein Spezialgesetz. Sie erstreckt sich auf alle denkbaren verfassungsfeindlichen Aktivitäten und Straftaten. Auch wer häufig in die Moschee geht, könnte als verdächtig gelten.

Nun gab es schon im Jahr 2002 das Problem, dass die öffentliche Hand gespart hat. Deshalb standen dem Verfassungsschutz, der die Überprüfung machen sollte, nur drei Leute für etwa 100.000 zu überprüfende Personen pro Jahr zur Verfügung. Was machten diese armen Menschen?

Sie hatten ersichtlich keine Möglichkeit zu überprüfen, ob jemand andauernd in die Moschee geht, um dort einem bösen Prediger zuzuhören. Das einfachste für sie war, beim Strafregister anzufragen, ob sich der Betreffende strafbar gemacht hat. War dies der Fall, dann war er nach den Richtlinien ein Sicherheitsrisiko und deshalb ungeeignet. Nun gab es einen Fall, von dem ich bei einem Seminar von Betriebsräten aus Flughafengesellschaften erfuhr. Es ging um Beschäftigten aus München, der sich von seiner Frau hatte scheiden lassen. Im Rahmen des Scheidungsprozesses beschimpfte er seine Verflossene ziemlich heftig. Sie war beleidigt und strengte einen Strafprozess an, ein sog. Privatklageverfahren. Es kam zu einer Verurteilung wegen Beleidigung, die auch ins Strafregister eingetragen wurde. Das wiederum veranlasste die Sicherheitsüberprüfer, ihn als Sicherheitsrisiko einzustufen. Verrückt an der Geschichte war, dass der Flughafen München insgesamt eine sicherheitsempfindliche Zone war. Für diesen Menschen gab es also keine Beschäftigung mehr. Der Arbeitgeber wollte ihm zwar nicht kündigen, da er ein guter und loyaler Mitarbeiter war. Die Aufsichtsbehörde erklärte, wenn er ihm nicht kündige, verliere er seine Betriebserlaubnis und dürfe keinen Flughafen mehr betreiben. Also wurde dem Mitarbeiter wegen dieser läppischen Geschichte gekündigt. Dieser reichte Klage ein. Es gibt keine veröffentlichte Entscheidung des Arbeitsgerichts München über diesen Fall. Man kann als Optimist vermuten, dass man eine vernünftige Lösung in Form einer anderen Beschäftigung gefunden hat.

Frage: Was ist denn die oberste Instanz von diesem AEO? Bestimmt die CIA oder wer?

Däubler: Die CIA liefert der EU die Daten. Diese übernimmt sie in ihre Verordnungen. Ob sie im Einzelfall auch mal abweicht, kann ich nicht beurteilen. Dazu habe ich keinen Zugang. Ich vermute: nein. Das Material kommt aus den USA und von der EU-Kommission, und das legen wir zugrunde. Im Bereich des Flugverkehrs überprüfen wir dann nicht nur, ob jemand mit dem Menschen auf der Liste identisch ist, sondern auch, ob er ein Sicherheitsrisiko darstellt. Das ist Aufgabe des zuständigen Landesamts für Verfassungsschutz in Kooperation mit dem Flughafenbetreiber oder in Kooperation mit anderen privaten Arbeitgebern. Die verfahrensmäßigen Einzelheiten sind im Sicherheitsüberprüfungsgesetz von 1994 festgelegt.

Klar ist: wenn der Große Bruder jenseits des Atlantiks sagt, man müsse etwas gegen Terrorismus tun, so wirkt sich das auch hierzulande aus.

Teilnehmer: Die EU ist sehr großzügig, solche Listen zu übernehmen. Diese Liste von den Arbeitnehmern ist eine kleine Mini-Liste. Wenn man sich z. B. mit dem Zoll beschäftigen muss und ein zertifizierter Betrieb ist, gibt es eine Liste, was man direkt verzollen darf, eine Liste wem man und wo man weltweit nichts hinschicken darf, weil der Verdacht besteht, die könnten das für Bomben oder sonst etwas gebrauchen.

Däubler: Sie sprechen das Problem der Datenübermittlung ins Ausland an. Im Rahmen einer ins Ausland verkauften Maschine gibt es immer ein paar Leute, die mitgehen, um den Käufern zu vermitteln, wie die Maschine funktioniert. Da werden in dem Zusammenhang neben den Zutaten auch ein paar Daten übermittelt.

Dann gibt es, und das ist viel gravierender, die Verlagerung von Datenverarbeitungsvorgängen ins Ausland. Das können Lohnabrechnungen sein, das kann die gesamte Buchhaltung sein. Warum? Weil es billiger ist. Man spart Kosten, wenn man die Dinge nach Rumänien oder nach Bulgarien oder nach Tschechien verlagert. Da wird eine Menge von Daten ins Ausland übermittelt. Und schließlich gibt es die multinationalen Konzerne mit ausländischer, z. B. amerikanischer, kanadischer oder australischer Spitze. Dort will man natürlich sehr genau wissen, was in den europäischen Niederlassungen passiert. Deshalb gibt es da auch eine Notwendigkeit zur Datenübermittlung über die Grenzen.

Die rechtliche Regelung ist Folgende. Innerhalb der EU gilt im Prinzip überall dasselbe Datenschutz-Niveau, weil alle Mitgliedstaaten die EU-Datenschutzrichtlinie umgesetzt haben. Deshalb bestimmen sich Übermittlungen in ein anderes EU-Mitgliedsland nach den gleichen Grundsätzen wie die Übermittlung innerhalb der Bundesrepublik. Rechtlich macht es keinen Unterschied, ob Daten von Hamburg nach München übermittelt werden oder von Hamburg nach Barcelona oder nach Sofia. Bei Drittstaaten wird differenziert. Es gibt Drittstaaten mit vergleichbarem Datenschutz-Niveau. Dazu gehören die Schweiz, Kanada, Argentinien. Dann gibt es die Drittstaaten ohne ausreichenden Datenschutz wie z. B. Indien, China und die USA. Auch die letzteren haben keinen ausreichenden Datenschutz, was allgemein anerkannt ist. Ein solches Werturteil können wir uns gerade noch erlauben. Wenn man dorthin Daten übermitteln will, muss man einen Mustervertrag der EU-Kommission zugrunde zu legen. Dann ist die Datenübermittlung nämlich zulässig, und zwar auch dann, wenn der fragliche Staat überhaupt keinen Datenschutz hat.

Weiter gibt es sogenannte bindende Verpflichtungen multinationaler Konzerne, die das europäische Datenschutzniveau verbindlich festschreiben müssen und die dann ebenfalls eine ausreichende Basis für die Übermittlung sind. Eine Sonderregelung gibt es für die USA unter dem Stichwort: "safe harbor („Sicherer Hafen“). Diese Grundsätze beruhen auf einer Abmachung aus dem Jahr 2000, die zwischen der EU-Kommission und dem Außenhandelsministerium der USA getroffen wurde. Darin sind bestimmte Prinzipien niedergelegt, zu denen sich amerikanische Unternehmen bekennen können. Machen sie davon Gebrauch, wird die Übermittlung an sie wie ein innereuropäischer Vorgang behandelt. Voraussetzung ist, dass sie sich der recht milden Kontrolle des US-Außenhandelsministeriums unterwerfen. Machen US-Unternehmen davon keinen Gebrauch, hilft nur der Abschluss eines Mustervertrags oder ein den ganzen Konzern bindendes Regelwerk.

In jüngerer Zeit sind gegen die Safe-Harbor-Grundsätze Bedenken aufgekommen. Es gab Fälle, in denen ein amerikanisches Partnerunternehmen erklärte, es unterstelle sich den Safe Harbor Grundsätzen, dies aber in Wirklichkeit gar nicht tat. Dies beanstandeten die Aufsichtsbehörden für den Datenschutz. Außerdem wurde die in die Grundsätze aufgenommene Verpflichtung, Personen zu informieren, wenn zum ersten Mal Daten über sie gespeichert wurden, häufig nicht eingehalten. In solchen Fällen entfällt die Gleichwertigkeit des Safe-Harbor-Modells. Dazu kommt noch Folgendes. In der USA ist seit dem elften September nach dem Patriot Act jedes Unternehmen verpflichtet, Daten den amerikanischen Sicherheitscontrollern („Heimatschutzministerium“) zur Verfügung zu stellen. Voraussetzung ist nur, dass die Sicherheitsinteressen der Vereinigten Staaten dies erfordern. Das ist ein weit gefasster Begriff, dessen Vorliegen man fast immer bejahen kann. Hier entstehen gewichtige Probleme für deutsche Unternehmen, die verhindern wollen, dass auf diesem Wege ihre Betriebsgeheimnisse der amerikanischen Konkurrenz bekannt werden. Wer Näheres darüber wissen möchte, findet auf der Website des ULD, des unabhängigen Landeszentrums für Datenschutz in Schleswig-Holstein ein Fülle von

Material.

Dritter Punkt, *Compliance-Richtlinien*. „Compliance“ bedeutet eigentlich, dass man sich fügt, dass man sich normkonform verhält. „To comply with“ heißt, sich entsprechend der Vorgabe verhalten. Im Unternehmen beachtet man alle Rechtsnormen und darüber hinaus auch Dinge, die rechtlich nicht unbedingt verbindlich, die aber ethisch positiv besetzt sind.

Hintergrund ist auch hier ein gewisser US-Einfluss. Nachdem dort in den Bilanzen einiges schiefgelaufen war, verfügte die Börsenaufsicht in New York, dass prinzipiell jedes Unternehmen Compliance-Regeln haben muss und einen Compliance-Beauftragten, der die Einhaltung überwacht. Die Unternehmen sind verpflichtet mitzuteilen, ob alles in Ordnung ist oder ob es aus irgendwelchen Gründen Abweichungen gibt („comply or explain“). Das sind Voraussetzungen für die Börsenzulassung. Sehr viele Unternehmen führten deshalb Compliance-Regeln ein, ernannten einen Compliance-Beauftragten und hatten in vielen Fällen regelmäßig das Problem, ob ein bestimmtes Verhalten compliancekonform ist oder nicht. Ein Beispiel: Eine öffentlich-rechtliche Bank, die übrigens nicht spekuliert hat, hat eine Loge im Bremer Weserstadion, Darf sie auch ihre Aufsichtsratsmitglieder dorthin einladen? Dies ist jetzt ein riesiges Compliance-Problem. Darf die Bank ihr Vermögen in dieser Weise mindern und vielleicht sogar den scharfen Blick der Aufsichtsräte etwas verdunkeln?

Auf einer Tagung in Shanghai erlebte ich Leute von Siemens. Einer bekam ein Vortragshonorar von 200 Euro. Für ihn war es ein Problem, ob er diese Summe annehmen durfte oder nicht. Glücklicherweise war ein Compliance-Beauftragter von Siemens vor Ort, an der er sich vernünftigerweise wandte. Dieser reagierte mit einem „Mmh“ und ging weg. Offensichtlich traute er sich nicht, eine eindeutige Entscheidung zu treffen. Gleichzeitig bedeutete das auch: „Wenn du es nimmst, passiert nichts“. Eigentlich sollte man sich auf andere Dinge konzentrieren.

Immer wieder wird behauptet, dass Compliance Dinge erlaubt, die aus anderen Anlässen nicht möglich wären, z. B. Daten zu erheben, die man sonst nicht erheben könnte. Das trifft nicht zu. Compliance ist auch dazu da, für die korrekte Befolgung des Datenschutzrechts zu sorgen. Weiter lässt sich sagen, dass zum rechtmäßigen Verhalten eines Unternehmens auch die vollständige Einhaltung des Arbeitsrechts gehört. Werden z. B. Betriebsräte schlecht behandelt, so ist das ein Compliance-Problem und sie können beim Compliance-Beauftragten beschweren. Das könnte möglicherweise zu einer erheblichen Verunsicherung führen.

Doch es gibt auch schwierige Fälle ohne eindeutige Lösung. Der Arbeitnehmer ist grundsätzlich verpflichtet, wahrheitsgemäß zu antworten, wenn der Arbeitgeber wissen will, was er zu einem bestimmten Zeitpunkt gemacht hat und wie er mit einem bestimmten Problem umgegangen ist. War nun sein Verhalten nicht ganz in Ordnung, so ist er verpflichtet, sich selbst zu belasten. Belügt er den Arbeitgeber, liegt eine Verletzung der arbeitsvertraglichen Pflichten und damit eine Erschütterung des Vertrauensverhältnisses vor. Auf der anderen Seite hat nach § 55 der Strafprozessordnung jedermann das Recht, die Aussage zu verweigern, wenn er sich belasten würde. Müsste man das nicht auf Compliance-Ermittlungen übertragen?

In einem bestimmten Lebensbereich ergeben sich besonders große Schwierigkeiten. Auf dem Rückflug von Südamerika saß ich neben einem Vertreter einer schwäbischen Firma, die Textilmaschinen baute. Er erzählte mir Folgendes. Die Hauptniederlassung für Lateinamerika lag in Sao Paulo. Nun hatten sie das Problem, dass trotz schwäbischer Wertarbeit hin und wieder so eine Textilmaschine kaputt ging und man Ersatzteile brauchte. Diese waren in Sao Paulo nicht immer vorrätig, sondern mussten aus Deutschland eingeflogen werden. Normalerweise kommen sie per Luftfracht innerhalb von eineinhalb Tagen dort hin. Diese Form des Transports ist

nicht gerade billig, aber die Ersatzteile sind da. Der Zeitfaktor spielt eine große Rolle, weil die Kunden möglichst schnell weiterproduzieren wollen. Nun kam aber höchstens die Hälfte aller Pakete in Sao Paulo an. Die andere Hälfte blieb verschwunden. Daraufhin ging er zum Leiter der Post in Sao Paulo und klagte ihm sein Leid. Dieser bedauerte das sehr. Doch bei guten Kunden gebe es eine Sonderreglung. Man bekomme eine Extraadresse, die in Wirklichkeit gar nicht existiere, also eine Deckadresse. Die komme auf eine Liste. Wenn nun die Ersatzteile mit einem Frachtflugzeug aus Europa kommen, wählt man als erstes immer die aus, die an jemanden auf der Deckadressen-Liste gerichtet sind. Sie kommen dann in ein Extra-Lager. Anhand einer weiteren Liste, auf der die wahren Adressen stehen, werden die Pakete dann umgehend zugestellt. Der Leiter der Post wies allerdings darauf hin, dass damit Arbeit verbunden sei und eine Aufwandentschädigung von 1.000 Euro monatlich üblich sei. Was täte jemand, der loyal zu seiner Firma steht, in so einer Situation? Natürlich würde bezahlt. Die Compliance-Controller würden ihn nun dazu zwingen, sich selbst zu beschuldigen und dafür sorgen, dass er zugibt, dass er den Leiter der Post in Sao Paulo bestochen hat.

Deshalb ist es wichtig, dass man ähnlich wie im Strafprozess Regeln schafft, die den Einzelnen davor bewahren, sich selbst belasten zu müssen.

Das kann man erreichen, weil der Betriebsrat nach § 87 Absatz 1 Nr.1 BetrVG ein Mitbestimmungsrecht hat, und zwar über das Verfahren, wie man die Einhaltung von Compliance-Grundsätzen überprüft. In diesem Rahmen könnte man auch festlegen, dass niemand verpflichtet ist, sich selbst zu belasten, und dass er keine Nachteile erleiden darf, wenn er davon Gebrauch macht und sich nicht belastet, die Aussage verweigert oder etwas Unrichtiges sagt.

Der letzte Punkt: GPS. Mit diesem System kann man nicht nur sein Ziel finden. Man kann es auch für die Steuerung und Kontrolle von Fernfahrern und Außendienstmitarbeitern einsetzen. Dabei kann man sehr genau feststellen, wo sich die fragliche Person zu einem bestimmten Zeitpunkt aufhielt. Man kann nachfragen, weshalb ihr Auto eine halbe Stunde ungenutzt herumstand und was sie da gemacht hat. Für Außendienstmitarbeiter ist das deshalb besonders gravierend, weil der Außendienst ein höheres Maß an freier Arbeitsgestaltung gewährt, insbesondere in zeitlicher Hinsicht, als sie der normale Arbeitnehmer im Büro oder in der Fabrik hat. Man kann selbst entscheiden, welchen Weg man wählt, in welcher Reihenfolge man die Kunden besucht und ob man auch mal eine halbe Stunde in ein Cafe geht. Wegen dieser Spielräume akzeptieren Außendienstmitarbeiter häufig, dass sie mehr als vierzig Stunden in der Woche unterwegs sind. Das wird hingenommen, weil man auf der anderen Seite ein freier Mensch ist.

An meinem dörflichen Wohnsitz ist mir deutlich geworden, dass diese Freiheit sehr viel wert ist. Als wir dorthin gezogen sind, bekam ich nach etwa drei Wochen eine Grippe. Die Dorfärztin diagnostizierte diese zutreffend und verordnete Medikamente. Meine Frau sollte sie in der Apotheke besorgen. Vorher machte sie noch Halt beim Bäcker. Dort wussten sie bereits, dass ich krank sei und eine Grippe habe. Soviel zu Datenschutz und ärztlicher Schweigepflicht. Fern von aller modernen Technik gab es innerhalb des Dorfes einen Kommunikationszusammenhang, wonach fast alles über andere bekannt wird. Das bezieht sich auch auf Bankdaten; ob jemand sein Konto überzogen hat oder es öfter überzieht, wie viel Schulden er hat, das bleibt auch nicht unbedingt geheim. Ich habe einmal irrtümlich den Vermögenssteuerbescheid eines Händlers in meinem Briefkasten gefunden und habe ihn gelesen. Da erfährt man im Prinzip alles. Wenn man aber Auto fährt und sich von der örtlichen Gemeinschaft entfernt, können andere in meinem Fall nur noch feststellen, ob man Richtung Tübingen oder Richtung Hechingen gefahren ist. Mehr wissen sie nicht. Was ich in Tübingen oder in Hechingen mache, entzieht sich der Kontrollkompetenz der Nachbarschaft und des ganzen Dorfes.

Diese Freiheit, die man immer hatte, wird durch GPS entscheidend eingeschränkt. GPS führt im Grunde dazu, dass man eine Art Videokamera über sich im Weltall hat, die genau aufzeichnet, wo man sich wann befindet. Dabei kann man genau kontrollieren, wo und wann man was gemacht hat. Vernünftige Arbeitgeber würden das nicht tun. Sie wollen ihre Arbeitnehmer nicht demotivieren, aber es gibt auch andere. Nach dem Entwurf des Beschäftigten-Datenschutzgesetzes, der in dieser Legislaturperiode hoffentlich nicht mehr kommen wird, wäre es für Arbeitgeber prinzipiell möglich, die GPS-Daten zu erfassen. Begründung dafür ist, dass es möglich sein soll, vor Katastrophen zu warnen oder den Einsatz einer Fahrzeugflotte zu koordinieren.

Auch hier ist wieder ein Blick in die Strafprozessordnung nützlich. Da kann man seit einiger Zeit auch GPS als Mittel einsetzen, um Gangster genauer verfolgen zu können. Die Schwelle ist aber sehr hoch. Erstens braucht man einen Richter, der das anordnet. Nur bei Gefahr im Verzug kann es die Staatsanwaltschaft anordnen. Anlas sind außerdem nur relativ schwere Delikte. Wegen einer kleinen Geschichte darf nicht ein so weitgehender Eingriff in die Persönlichkeitssphäre des Einzelnen angeordnet werden. Vielmehr geht dies wie beim Speicheltest nur im Zusammenhang mit gravierenden Delikten. Das gibt gute Argumentationsmöglichkeiten. Der Arbeitgeber, der in eigener Person Richter und Kripobeamter wäre, darf nicht mehr Eingriffsmöglichkeiten als der Staat haben.