BTQ Kassel

Technologieforum 2004

Die Zukunft im Handel hat schon begonnen!

RFID, PEP, Loss Prevention & Co

Dokumentation der Fachtagung,
15. – 17. November 2004

Hrsg. BTQ-Kassel und
ver.di Fachbereich Handel

BTQ KASSEL

ver.di

Handel

Vereinte Dienstleistungs-gewerkschaft

Vortrag Prof. Dr. Wolfgang Däubler

Computersysteme im Handel – rechtliche Rahmenbedingungen für den Betriebsrat

Liebe Kolleginnen und Kollegen,

ich komme gerade noch im letzten Moment: Die ICE-Technik hat mal wieder versagt, aber ein erfindungsreicher Taxifahrer hat mich auf vielen Schleichwegen vom Bahnhof Duisburg in Rekordzeit hierher gebracht. Ohne kluge Menschen – so könnte man schließen – ist der technische Fortschritt eine recht uninteressante Angelegenheit.

Ich habe mein Thema „Computersysteme im Handel – rechtliche Rahmenbedingungen für den Betriebsrat" so verstanden, dass es schwerpunktmäßig um „Loss Prevention" und RFID gehen soll. Auf diese beiden Phänomene will ich mich konzentrieren, was nicht ausschließt, dass man in der Diskussion dann auch andere Systeme in die Betrachtung mit einbezieht.

Loss Prevention

Wie sehen die Handlungsmöglichkeiten des Betriebsrats bei „Loss Prevention" aus, also bei einem System, dessen Funktionsweise eben im Referat von Thilo Weichert, aber auch schon vorher im Einzelnen beschrieben wurde?

Unproblematisch ist zunächst eine Feststellung: Wenn dieses System mit personenbezogenen Daten betrieben wird, verstößt es eindeutig gegen geltendes Recht. Der Grund ist einfach: Wenn ich das Arbeitsverhalten einer konkreten Person total, in allen Einzelheiten erfasse, verstößt dies nach herkömmlicher Auffassung gegen die Menschenwürde und stellt einen inakzeptablen Eingriff in die Persönlichkeitssphäre dar. Die Rechtsprechung hat dies bisher am Fall der Video-Überwachung verdeutlicht – wenn diese nur zu dem Zweck erfolgt, die Arbeit und deren Qualität zu überwachen. Bei Loss Prevention kann nichts anderes gelten. Ein Übermaß an Kontrolle liegt aber auch deshalb vor, weil ein partielles Persönlichkeitsprofil erstellt wird – man weiß alles über das Verhalten des Einzelnen an seinem Arbeitsplatz: Man kennt den Rhythmus seiner Arbeitsvorgänge, die kleinen Unterbrechungen, die Korrekturen, weil er ein wenig unkonzentrierter als sonst war usw. Das Verhalten des Einzelnen wäre gewissermaßen aus einem digitalisierten Katalog abrufbar, er würde zum vollständig erfassten Objekt. Das lässt sich mit der grundgesetzlichen Sicht vom Menschen nach der Rechtsprechung des Bundesverfassungsgerichts nicht vereinbaren.

Ist Rasterfahndung im Betrieb erlaubt?

In der Literatur hat man weiter zu Recht die Parallele zur Rasterfahndung gezogen, was auf den ersten Blick ein wenig zur Beruhigung beitragen könnte: Nur wer ganz spezifische Voraussetzungen erfüllt, also von seinem Normalverhalten abweicht, sieht sich ja einer gezielten Kontrolle ausgesetzt. Um was geht es bei der Rasterfahndung?

Die Besonderheit dieser polizeilichen Ermittlungsform besteht darin, dass man zunächst nach eigentlich ganz harmlosen Angaben fragt. Nehmen wir das berühmte Beispiel, das zur Ergreifung eines RAF-Terroristen geführt hat: Die Ermittler waren der nahe liegenden

Auffassung, dass ein Terrorist wenig Neigung empfinden wird, sich beim Einwohnermeldeamt mit seinem Namen anzumelden; auch gefälschte Dokumente können als Fälschungen entlarvt werden, ein Risiko, das dazu führt, dass man besser den Kontakt mit dieser Behörde meidet. Nun brauchen aber auch Terroristen in ihrer Wohnung Strom. Die Rechnung von einem Konto abbuchen zu lassen, ist ihrerseits mit Schwierigkeiten und Risiken verbunden, denn am Ende kann ja auch die Bank Verdacht schöpfen. Also ist es besser, den Strom in bar zu bezahlen; man lässt sich eine Rechnung schicken und geht dann pünktlich zu der zuständigen Stelle, um seine Schuld zu begleichen. Dabei geht es überdies um Beträge, bei denen man auch Geld verwenden kann, das aus – sagen wir höflich: etwas angreifbaren Quellen – stammt. Also kamen kluge Polizeibeamte auf die Idee, sich die Liste aller Barzahler bei den Energieunternehmen geben zu lassen. Das waren im Land Hessen ungefähr 6000 Personen, die aus irgendwelchen Gründen mit den Banküberweisungen oder Abbuchungen so ihre Schwierigkeiten hatten. Nun stellte man fest, wer aus dieser Gruppe nicht polizeilich gemeldet war – was eine kleine Gruppe von etwa 200 Personen ausmachte. Die schaute man sich der Reihe nach ganz genau an und entdeckte in der Tat darunter einen der Gesuchten. Das gleichzeitige Vorliegen der Merkmale „Barzahler beim Strom" und „polizeilich nicht gemeldet" schuf eine Situation des Verdachts, die die Ermittler durchaus ein Stück voranbrachte.

Bei den so genannten „Schläfern" war man weniger erfolgreich. Denn da hat man einfach danach gefragt, ob jemand eine Person männlichen Geschlechts zwischen 18 und 40 Jahren war, aus einem arabischen Land stammte, unauffällig geblieben war, keine finanziellen Probleme hatte und relativ viel auf Reisen war. Nun ja, solche Menschen lassen sich finden. (Nur ist dann die Polizei am Ende ihres Lateins: Soll sie fragen: „Sagen Sie mal, sind Sie nicht vielleicht ein Schläfer?" Der Kreis ist zu groß und die Merkmale viel zu unspezifisch, als dass man wirklich eine gezielte Observation einleiten könnte. Einige Gerichte haben deshalb auch diese Form der Rasterfahndung wegen fehlender Eignung beanstandet.

Das eigentliche Problem solcher Fahndungsmaßnahmen liegt darin, dass sie viele Menschen erfasst, die automatisch in einen „Verdacht" geraten, ohne das Geringste mit den fraglichen Vorgängen zu tun zu haben. Sie sehen sich als Unschuldige gezielten Ermittlungen ausgesetzt. Deshalb sind im Strafprozess und im Rahmen des Polizeirechts derartige Maßnahmen nur ganz ausnahmsweise zulässig, insbesondere bei sehr schweren Delikten.

Für uns stellt sich die Frage: Gilt dies alles genauso im normalen Arbeitsleben? Darf der Arbeitgeber eine Methode, die im öffentlichen Bereich nur unter ganz engen Voraussetzungen eingesetzt wird, wegen eines unspezifischen, nicht auf eine bestimmte Person bezogenen Verdachts – „hier kommt Ware abhanden" – anwenden, obwohl es ja nun nicht gerade um ein Kapitalverbrechen geht? Die Antwort muss meines Erachtens eindeutig negativ lauten: Der Arbeitgeber ist kein Chefermittler und kann deshalb keine polizeilichen oder staatsanwaltschaftlichen Befugnisse ausüben. Er darf auch nichts tun, was einen gleichartigen Effekt hätte. Und er darf es erst recht nicht, wenn weniger gewichtige Rechtsgüter als z.B. bei der Bekämpfung des Terrorismus auf dem Spiel stehen. Eine Ausnahme gilt allenfalls dann, wenn schon ein sehr konkreter Verdacht gegenüber einer bestimmten Person besteht, aber das ist dann nicht mehr unser Fall.

Automatisierte Entscheidung

Daneben gibt es noch ein weiteres Bedenken: Es gibt im Bundesdatenschutzgesetz einen Paragraphen 6a, der besagt, man dürfe auf Personen bezogene Entscheidungen nicht ausschließlich auf die Auswertung von elektronischen Dateien stützen. Genau das tut man aber hier: Die Entscheidung, jemanden gezielt zu beobachten, gewissermaßen unter genaueste Observation zu nehmen, wird bereits dann getroffen, wenn das System eine Abweichung vom Normalprofil des Kassierverhaltens anzeigt. Da diese Entscheidung die einzelne Person durchaus nachteilig betrifft, sind die Voraussetzungen des § 6a BDSG gegeben. Sobald mit personenbezogenen Daten gearbeitet wird, lässt sich „Loss prevention" nicht mehr mit dem BDSG in Einklang bringen.

Pseudonymisierung als Ausweg?

Nun scheint es einen Ausweg zu geben: Man verzichtet zunächst auf den Personenbezug und stellt ihn erst her, wenn sich ein dringender Verdacht von strafbaren Handlungen ergibt. Dies kann im Wege der Pseudonymisierung der Daten erfolgen: Statt des wahren Namens oder der realen Personalnummer wird eine „Deckbezeichnung" gewählt. Eine „Anonymisierung" kommt nicht in Betracht, da die ganze Prozedur ja nur dann Sinn macht, wenn sich das schwarze Schaf nachträglich ermitteln lässt – und das wäre bei anonymen Daten nicht mehr der Fall. Pseudonymisierte Daten bleiben aber personenbeziehbar; man kann mit zumutbarem Aufwand ermitteln und aufdecken, welche Person sich hinter einer bestimmten Bezeichnung verbirgt. Dies müsste sogar schon dann geschehen, wenn der Einzelne nach § 34 BDSG Auskunft darüber verlangen würde, welche Daten über ihn eigentlich gespeichert sind. Die Verwendung von Pseudonymen in einer ersten Stufe führt also nicht zur Unanwendbarkeit des BDSG; man kann ihm durch diese Vorkehrung nicht „entkommen". Meines Erachtens kann „Loss prevention" auch mit dieser Modifikation nicht eingesetzt werden; es gibt auch keine „gemäßigte" Rasterfahndung im Betrieb.

Nun könnte man vielleicht auf den Gedanken verfallen, es liege doch keine wirkliche Verletzung der Persönlichkeit und der Menschenwürde vor, wenn sicher sei, dass das dem Einzelnen zugeordnete Pseudonym nur in Situationen eines dringenden Verdachts aufgedeckt würde. Dies mag auf den ersten Blick plausibel sein, lässt sich jedoch mit dem Gesetz nicht vereinbaren: Die Überwachungsgrenzen gelten in gleicher Weise für alle personenbezogenen und personenbeziehbaren Daten, ohne dass zwischen diesen beiden Arten irgendwie unterschieden würde. Dies hängt mit dem Gedanken zusammen, dass Datenschutz weitgehend „Gefährdungsschutz" ist, der auch bei bloßer Personenbeziehbarkeit seine Berechtigung behält.

Für den Einzelnen stellt es im Übrigen durchaus eine Belastung dar, wenn er weiß, dass sein Verhalten genau aufgezeichnet wird und er – vielleicht durch ein paar Ungeschicklichkeiten – in den Kreis der „Verdächtigen" geraten kann. Außerdem bleibt das Bedenken, dass die Annahme eines „dringenden Verdachts" eine in ihren Voraussetzungen höchst ungenaue Eingriffsvoraussetzung ist. Staatliche Behörden entwickelten im Laufe der Jahre eine konkretisierende Praxis, die eine gewisse Orientierung ermöglicht; beim einzelnen Arbeitgeber kann Derartiges nicht erwartet werden. Es bleibt also dabei, dass das BDSG hier nicht überwindbare Schranken bereithält.

Rechte des Betriebsrats

Der Betriebsrat kann verlangen, über den eventuellen Einsatz von „Loss prevention" im Betrieb informiert zu werden. Nach § 80 Abs. 1 Nr. 1 BetrVG muss er über die Einhaltung der Gesetze wachen, soweit die die Arbeitnehmer schützen; dies ist nach allgemeiner Auffassung auch beim BDSG der Fall. Bei Verstößen kann er auf Beseitigung der Gesetzwidrigkeit dringen. Stattdessen kann er sich auch auf den Standpunkt stellen: „Ich habe ein Mitbestimmungsrecht in Bezug auf alle Formen der Überwachung durch Technik." Wird eine solche Technik ohne seine Zustimmung eingesetzt, kann er im Wege der einstweiligen Verfügung verlangen, dass die Überwachung nicht fortgeführt wird, bis mit seiner Zustimmung (oder der der Einigungsstelle) eine legale Form der Kontrolle eingerichtet ist (oder auf diese verzichtet wird). Dieses Mittel ist sehr viel wirksamer als das bloße „Dringen auf Abhilfe", das bei festgestellter Gesetzwidrigkeit besteht.

Daneben kann sich der Betriebsrat allerdings an die Aufsichtsbehörde für den Datenschutz wenden. Dort kann er mit einem beträchtlichen Fall an Interesse und Aufgeschlossenheit rechnen. Dies hängt mit der Haltung der zuständigen Personen, aber auch damit zusammen, dass schon mit Rücksicht auf die regelmäßig zu erstellenden Tätigkeitsberichte interessante Fälle durchaus willkommen sind. Der Betriebsrat riskiert also nicht, mit einem „da könnte ja jeder kommen" und „das haben wir noch nie gemacht und wo kämen wir da hin" abgespeist zu werden. Vielmehr ist mit einer eingehenden Aufklärung zu rechnen.

RFID

Wie sieht es nun beim zweiten hier interessierenden Bereich, bei RFID aus? Ähnlich wie einstens bei der Einführung von Bildschirmarbeitsplätzen werden hier zwei Bereiche der Betriebsratskompetenzen angesprochen. Einmal geht es um die Mitbestimmung bei technischen Überwachungsmaßnahmen nach § 87 Abs. 1 Nr. 6 BetrVG. Zum zweiten kommen Beteiligungsrechte bei Betriebsänderungen in Betracht – also Informationsrechte, Interessenausgleich und Sozialplan.

Mitbestimmung nach § 87 Abs.1 Nr. 6 BetrVG

§ 87 Abs. 1 Nr. 6 BetrVG gibt dem Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, Verhalten und Leistung der Arbeitnehmer zu überwachen. Ihrem Wortlaut nach könnte man diese Vorschrift theoretisch so auslegen, dass sie eine Überwachungsabsicht voraussetzt. Im konkreten Fall würde dies bedeuten, dass sie ausscheidet, wenn es nur darum geht, die Logistik-Prozesse zu optimieren. Eine solche Auslegung wird aber seit nunmehr 20 Jahren von der Rechtsprechung einheitlich abgelehnt. Zu Recht meint das BAG, wenn man auf die Überwachungsabsicht des Arbeitgebers abhebe, bestehe sie in der Praxis so gut wie nie. In der Tat könnte man ein Mitbestimmungsrecht weitgehend vergessen, das davon abhängt, dass derjenige, dem gegenüber es wirken würde, das Vorliegen einer bestimmten Absicht zugesteht oder dafür entscheidende Indizien setzt. Deshalb hat das Bundesarbeitsgericht in partieller Korrektur des Wortlauts die Vorschrift so gelesen als stünde dort: Die Mitbestimmung setzt die Einführung oder Anwendung einer technischen Einrichtung voraus, die dazu „geeignet" ist, Verhalten und Leistung der Arbeitnehmer zu überwachen. Die objektive Eignung reicht also für die Annahme des Bestimmungszwecks aus. Dahinter

steht weiter eine verfassungsrechtliche Überlegung, die auch vom Bundesarbeitsgericht aufgegriffen wurde. In der Volkszählungsentscheidung aus dem Jahre 1983 hat das Bundesverfassungsgericht dem Einzelnen ein Recht auf informationelle Selbstbestimmung zuerkannt. Er muss selbst Herr seiner Daten sein können, insbesondere erkennen, wer was über ihn weiß. Dieses Recht bedarf der vielfältigen Absicherung. Deshalb gibt es betriebliche Datenschutzbeauftragte, deshalb gibt es staatliche Datenschutzbeauftragte, deshalb gibt es das BDSG mit seinen Verarbeitungsschranken. Und diesem Zweck dient auch – so das Bundesarbeitsgericht – das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6, das gewissermaßen so eine Art von „Vorfeldschutz" für das informationelle Selbstbestimmungsrecht schafft. Dadurch, dass der Betriebsrat in einem Bereich mitbestimmt, wo der Einzelne Opfer unangemessener Überwachung werden kann, schafft man einen zusätzlichen Sicherungsmechanismus. Man kann deshalb von einem Stück präventiven Schutzes gegen Verletzungen des informationellen Selbstbestimmungsrechts sprechen. Das ist gewissermaßen der zweite Grund, weshalb das BAG dem § 87 Abs. 1 Nr. 6 eine weite Auslegung gegeben hat.

Wenn der einzelne Beschäftigte ein RFID-Etikett im Betriebsausweis oder in der Kleidung mit sich führt, so stellt sich kein Rechtsproblem, die Eignung zur Überwachung ist dann selbstredend gegeben. Das Gleiche gilt dann, wenn die Funk-Etiketten, die sich auf irgendwelchen Waren befinden, personenbezogene Daten enthalten. Interessant ist daher viel eher der Fall, dass solche Daten fehlen: Wie in der bisherigen Praxis üblich, sollen mit Hilfe von RFID-Chips nur die Warenströme besser gesteuert und verfolgt werden können: Man kann leichter feststellen, wo sich welche Ware befindet, welche Zeit sie braucht, bis sie ein bestimmtes Ziel erreicht hat, ob sie gestohlen wurde oder ob fast leere Regale aufgefüllt werden müssen. Auf dem Chip sind also nur Sachdaten gespeichert, die das Lesegerät wahrnimmt. Ein unmittelbarer Personenbezug fehlt. Im Regelfall ist es aber möglich, diesen dadurch herzustellen, dass man so genanntes Zusatzwissen einsetzt: Ergibt sich aus Listen oder anderen Dokumenten, wer wann mit der fraglichen Ware zu tun hatte, kann das Arbeitsverhalten sehr genau rekonstruiert werden. Wird beispielsweise festgehalten, wann und auf welchem Fahrzeug eine Ware ein bestimmtes Lager verlässt, so ist gleichzeitig eine Aussage über denjenigen möglich, der für das Lager verantwortlich war oder der am Steuer des Lkw saß. Dieses „Zusatzwissen" stellt den Personenbezug her. Damit ist zugleich auch eine Kontrolle möglich – was zur Folge hat, dass das Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG eingreift. Mit dessen Hilfe kann man dann sicherstellen, dass die Kontrolle unterbleibt oder jedenfalls auf das Unerlässliche beschränkt wird. So kann man etwa dafür sorgen, dass nur sehr grobe Zeitangaben gespeichert werden, so dass das konkrete Arbeitsverhalten des Einzelnen nicht rekonstruiert werden kann. Möglich ist weiter, den Zugriff auf die Daten auf ganz bestimmte Personen oder Funktionen zu beschränken: So kann man etwa alle Personalverantwortlichen ausschließen und die Zugriffsberechtigten auf das Datengeheimnis verpflichten. Man praktiziert so eine Art „informationeller Gewaltenteilung" im Betrieb: Es gibt bestimmte Leute, die alles über die Logistik und die betrieblichen Abläufe wissen, und es gibt andere, die für die Beurteilung und die Beförderung von Beschäftigten zuständig sind und die sich mit Personalverwaltung befassen.

Betriebsänderung nach § 111 Satz 3 BetrVG

Lassen Sie mich zum zweiten Problembereich kommen. RFID kann im Extremfall dazu führen, dass der Kunde eine Karte erhält, die er an ein Lesegerät halten muss; wird sie „erkannt", eröffnet sich die Möglichkeit, Waren durch eine Schleuse zu schieben, wo deren Preis erfasst und seinem Konto belastet wird. Die Funktion der Kassiererin wird so überflüssig. Theoretisch wäre es denkbar, dieses Verfahren auf einen großen Teil der Kunden auszudehnen. Dies hätte natürlich ganz gravierende personalpolitische Konsequenzen. Kann der Betriebsrat insoweit Einfluss nehmen?

Man wird zunächst einmal davon ausgehen können, dass eine Betriebsänderung schon insoweit vorliegt, als der Einsatz der RFID-Technologie zur Anwendung grundlegend neuer Arbeitsmethoden nach § 111 Satz 3 Nr. 5 BetrVG führt. Mittelbar wird dies dadurch bestätigt, dass die Einsparpotenziale mit 35 % sehr hoch veranschlagt werden – und das deutet auf einen „Sprung" in der technologischen Entwicklung hin. Auch von der Erscheinungsform her liegt eine beträchtliche Veränderung vor. Kommt es zu Personalabbau, so dürfte in der Regel zugleich eine Betriebseinschränkung nach § 111 Satz 3 Nr. 1 BetrVG vorliegen. Liegt das eine oder das andere vor, so hat der Betriebsrat die bekannten Rechte nach den §§ 111 und 112 (BetrVG). In einem ersten Schritt kann er umfassende Informationen verlangen und über die Einführung der Technik im Hinblick auf einen möglichen Interessenausgleich verhandeln. Solange diese Verhandlungen dauern, darf die Maßnahme nicht durchgeführt werden. Nach der Rechtsprechung zahlreicher Landesarbeitsgerichte könnte dem Arbeitgeber per einstweiliger Verfügung verboten werden, durch einseitige Maßnahmen vollendete Tatsachen zu schaffen.

Kommt der Interessenausgleich zustande oder scheitert er, so kann der Betriebsrat den Abschluss eines Sozialplans verlangen, sofern wirtschaftliche Nachteile nicht ausgeschlossen werden können. Insoweit können dann Ausgleichsmaßnahmen verlangt werden.

Wahrscheinlich wird man in der Zukunft damit konfrontiert werden, dass die Einführung nicht auf einen Schlag, sondern etappenweise erfolgt. Dies ändert jedoch nichts am Vorliegen einer Betriebsänderung. Dasselbe Problem trat bei der Einführung von Bildschirmgeräten auf, die in den 80er Jahren gleichfalls nicht von einem Tag auf den andern eingeführt wurden, sondern ja nach wahrgenommener Dringlichkeit an einzelnen Arbeitsplätzen oder in einzelnen Abteilungen installiert wurden. Die schrittweise Einführung änderte jedoch nichts daran, dass eine prinzipielle Entscheidung, sich der neuen Technologie zu bedienen zugrunde lag, die die Basis für die Annahme einer einheitlichen Betriebsänderung ist. Vertritt der Arbeitgeber einen anderen Standpunkt, müsste er im Einzelnen belegen, dass er nicht von Anfang an die Absicht hatte, seinen Betrieb flächendeckend umzustellen, ja dass er dies nicht einmal in Erwägung zog; dies wird ihm nur ausnahmsweise gelingen. Die §§ 111 ff. Betriebsverfassungsgesetz geben also durchaus gewisse Möglichkeiten, die Einführung von RFID aus Arbeitnehmersicht mitzugestalten.

Dies als schneller Überblick über die rechtlichen Handlungsmöglichkeiten des Betriebsrats. Ich hoffe, dass sich nützliche und praxisbezogene Diskussionen ergeben werden. Vielen Dank.