MATTHIAS WILKE

# Rasterfahndung an der Supermarktkasse

**Zugegeben: Unternehmen müssen etwas gegen Diebstähle und Unterschlagungen unternehmen können. Das neue Kassenauswertungssystem für den Einzelhandel, ›Loss Prevention‹, schießt jedoch weit über jedes vertretbare Ziel hinaus.**

Bis zu acht Milliarden Mark Verlust, so eine Studie aus dem Jahr 2000, macht der Handel jährlich wegen Diebstahls. Bis zu einem Viertel davon, sagen Experten, geht auf das Konto des Personals. Eine neue Software – dieses Jahr auf der CeBIT erstmals vorgestellt – verspricht jetzt Abhilfe, noch dazu für wenig Geld. Doch die Sache hat einen Haken: Die damit verbundene lückenlose Überwachung an der Kasse verstößt massiv gegen den Datenschutz.

Das Zauberwort zur Verhinderung von ›Inventurdifferenzen‹ – also unerklärbaren Minderungen des Warenbestands im Einzelhandel – heißt ›Loss Prevention‹ (loss = Verlust, Schwund; prevention = Verhinderung, Verhütung). Und im Kampf dagegen stellt die auf der CeBIT 2002 präsentierte neue Software ›LORD Loss Prevention‹ nun gar göttliche Hilfe (lord = Gott) in Aussicht. Das Programm verspricht den Nutzern einen nahezu lückenlosen Überblick über das Verhalten des Personals.

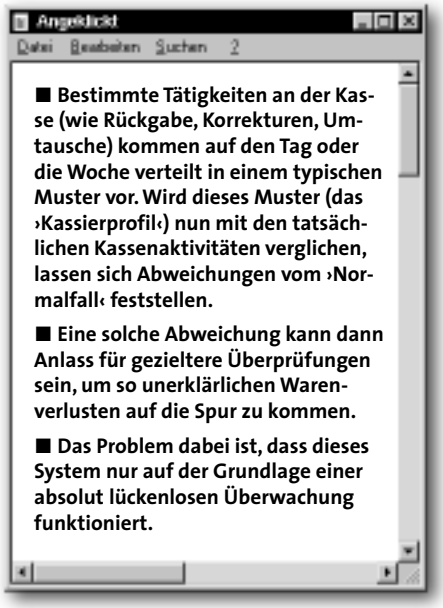
LORD bedeutet ›Logware Retail Data-Mining‹ und kann dem Vernehmen nach (fast) alles: »Es deckt schnell Unregelmäßigkeiten an den Kassen auf und ermöglicht es, geeignete Gegenmaßnahmen zu treffen. Das vermindert Verluste und steigert Erträge nachhaltig«, wirbt der Hersteller für sein Produkt. Und tatsächlich analysiert und lokalisiert die Software mögliche Verlustquellen, indem sie *sämtliche Transaktionen an der Kasse auf verdächtiges Verhalten hin überprüft*. Eine Methode, wie sie im Prinzip auch bei der Rasterfahndung nach Terroristen und ›Schläfern‹ eingesetzt wird.

## Wer klaut am meisten?

Wie es zu den hohen Verlusten im Einzelhandel kommt, ist nicht genau klar. Das Euro-Handelsinstitut (**www.ehi.org**) jedenfalls macht vier Verursachergruppen dafür verantwortlich: Kunden verursachen demnach angeblich knapp die Hälfte der Schäden, das Personal fast ein Viertel. Der Rest geht auf das Konto von Lieferanten und Service-Kräften sowie von organisatorischen Mängeln.

Um die durchaus erheblichen Verluste zu minimieren, hat der Einzelhandel in der Vergangenheit alle erdenklichen modernen Technologien entwickelt und eingesetzt – angefangen mit der Einführung computergestützter Kassensysteme über Video- und Kameraüberwachung bis hin zu hochintelligenten so genannten Cash-Management-Systemen (cash = Bargeld), von der Verkaufsrevision über elektronische Sicherungsetiketten bis zu In-Store-Sicherungssystemen (in store = innerhalb des Ladens).

Bis zu einem gewissen Grad waren alle diese Systeme – aufwändig und mit hohen Kosten verbunden – auch erfolgreich, wenn es darum ging, *Kunden* vom Stehlen abzuhalten. Unterschlagungen durch Beschäftigte an den Kassen hingegen haben sie nicht ausreichend aufdecken können. Dazu mussten Unternehmen bis jetzt eigene Detektive oder Security Firmen einschalten – die aber sind teuer, kosten viel Zeit und bringen oft nicht den gewünschten Erfolg.




## Suchraster an der Supermarktkasse

Den Erfolg könnte nun die neue Technik bringen. ›Loss Prevention‹ erstellt für die Kassiererinnen und Kassierer so genannte Kassier-Profile, die zunächst das ›gewöhnliche Verhalten‹ ermitteln, um auf dieser Grundlage dann ›ungewöhnliches Verhalten‹ im Einzelfall aufdecken zu können. Wird jemand nach diesem Raster auffällig, könnte das ein Hinweis auf Betrug oder Diebstahl sein – und verdient besondere Beobachtung.

Konnten auch vorher schon alle Aktivitäten an den Arbeitsplätzen lückenlos

erfasst, übermittelt und zentral gespeichert werden, so stellt ›Loss Prevention‹ nun den entscheidenden Schritt nach ›vorne‹ dar:

Denn jetzt haben Unternehmen erstmals ein ›intelligentes‹ Werkzeug zur Hand, das diese Datenmengen auch *analysieren* kann. Storniert eine Kassiererin zum Beispiel auffallend oft oder gibt sie, nachdem eine Kreditkarte automatisch gelesen wurde, anschließend deren Nummer mehrfach manuell ein, so ist dies nach ›Loss Prevention‹ bereits verdächtig. Auch das Öffnen der Kassenschublade ohne Verkauf nach einem Storno oder Leergutauszahlungen oder Leergutbuchungen, manuelle Preisüberschreibungen, Personaleinkäufe mit Rabattgewährungen, Warenrücknahmen ohne Kassenbon, Nullbons, Bon-Stornos, Bon-Abbrüche und dergleichen mehr werden als dubios identifiziert und ausgeworfen.

Kurz: Auf einen Blick wird deutlich, in welcher Filiale welche Kassiererin auffällig vom als ›normal‹ definierten Verhalten abweicht. Das Ergebnis bedeutet zwar nicht zwangsläufig, dass hinter jeder dieser Aktionen ein Betrug steht. Doch auf die Person an der Kasse, die deutlich mehr (oder weniger) als die durchschnittliche Anzahl dieser speziellen Aktivitäten ausführt, legt sich der Schatten des Verdachts.

## Die Rasterfahndung – ein Rückblick

Seit dem 11. September 2001 hat der Begriff ›Rasterfahndung‹ (wieder) Konjunktur. Man versteht darunter das computergestützte Durchsuchen von Datenbeständen nach bestimmten Merkmalen. Verglichen werden beispielsweise Daten aus den Einwohnermeldeämtern, aus dem Kraftfahrbundesamt sowie polizeiliche Daten wie etwa Täterprofile und Angaben über Tatverdächtige. Dazu kann noch gezielt nach bestimmten Eigenschaften der ins Visier Genommenen gesucht werden: Wohnen im Hochhaus, fehlende Anmeldung bei Energieunternehmen und so weiter.


Diese Fahndungsmethode, Mitte der 60-iger Jahre vom Bundeskriminalamt (BKA) entwickelt, dient bis heute vor allem der Terrorismus-Bekämpfung. Dabei werden Daten aus den verschiedensten Datenbanken, etwa von Schufa, Versicherungen, Krankenkassen und Energieversorgungsunternehmen, zusammengetragen und in einem aufwändigen Verfahren gegeneinander abgestimmt und ausgewertet.

So setzten die kriminalistischen Ermittler bei der Rasterfahndung in den 70-er Jahren voraus, dass Terroristen nicht polizeilich gemeldet sind und ihre Stromrechnungen immer bar bezahlen. Also wurden die Daten der Einwohnermeldeämter mit denen der bar zahlenden Stromkunden abgeglichen. Alle Barzahler, die nicht gemeldet waren, verfingen sich im Raster und wurden intensiv überprüft. Besonders erfolgreich war diese Fahndungsmethode bei der Suche nach den Terroristen, die die Lufthansa-Maschine ›Landshut‹ im Oktober 1977 gekapert und nach Mogadischu entführt hatten. Das BKA speicherte damals die Daten von 70 000 Hotelmeldezetteln im Abflugort Palma de Mallorca und verglich sie mit der PIOS-Terroristendatei – drei der vier Täter konnten auf diese Weise identifiziert werden (siehe: Telepolis, 13. 1. 2002, **www.heise.de**).

Trotz des Erfolgs gab es datenschutzrechtliche Bedenken gegen diese Fahndungsmethode.

Die Folge: Die Rasterfahndung wurde in Paragraf 98 a der Strafprozessordnung geregelt, der besagt, dass für den Einsatz einer Rasterfahndung *eine Straftat von erheblicher Bedeutung* vorliegen müsse. Und weiter heißt es dort: »Die Maßnahme darf nur angeordnet werden, wenn die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger Erfolg versprechend oder wesentlich erschwert wäre.«

## Der 11. September 2001 und die Schläfer

Drei der mutmasslichen Selbstmordattentäter vom 11. September 2001 lebten und studierten vor der Tat in Hamburg. Mit dem Abgleichsverfahren der Rasterfahndung werden seither bundesweit weitere ›unauffällige und unverdächtige‹ Menschen gesucht, die als potenzielle Al-Qaeda-Kämpfer in Frage kämen. Das BKA hat dazu folgendes ›Schläfer/Täter-Profil‹ erstellt:

- männliche Studenten und Ex-Studenten;
- zwischen 18 und 40 Jahren;
- mit (vermutlich) islamischer Religionszugehörigkeit;
- die aus (zwischen 15 und 30) islamischen Staaten stammen;
- einen legalen Aufenthaltsstatus haben;

**info**

**Analyse risikoreicher Vorgänge**

## Aus der Werbung für LORD Loss Prevention

**»Mit LORD Loss Prevention analysieren Sie unternehmensweit risikoreiche Vorgänge ... [Es] untersucht detailliert alle Transaktionen, bei denen Manipulationen möglich sind, z. B. Öffnung der Kassenschublade ohne Verkaufsvorgang. Auch Mitarbeiterkäufe, manuelle Eingaben und die Bezahlung mit elektronischen Zahlungsmitteln werden kontrolliert. Ebenso werden alle Handlungen der Kassenaufsicht, bei denen Differenzen in der Waren- und Geldwirtschaft entstehen können, auf fehlerhaftes Verhalten analysiert ...«**

**Auf was sich die Beschäftigten an den Kassen einstellen können, findet sich bunt bebildert auch auf der Website eines Anbieters:**

**www.logware.de/pdf/LORD_Loss_Prevention.pdf**

- in der Zeit von 1996 bis 2001 technisch-naturwissenschaftliche Fächer studier(t)en;
- finanziell unabhängig sind;
- rege Reisetätigkeit entfalten (teilweise Flugausbildung haben) und
- bislang kriminalpolizeilich noch nicht in Erscheinung getreten sind.

*(siehe.: FR vom 12. 4. 2002)*

## Wer ins Raster passt, könnte ein ›Schläfer‹ sein ...

Aber, wie gesagt: Diese Fahndungsmethode ist bei Datenschützern und Juristen umstritten: Mit drei Urteilen sind denn auch monatelange Rasterfahndungen nach so genannten Schläfern in Berlin, Hessen und in Nordrhein-Westfalen für rechtswidrig erklärt worden (siehe: FR vom 12. 4. 2002).

Der Bundesbeauftragte für den Datenschutz (BfD), Joachim Jacob, hat deshalb die Sicherheitsbehörden gemahnt, mit personenbezogenen Daten »noch sorgfältiger umzugehen«. Die Fahndung müsse »so präzise wie möglich beschrieben werden«. Denn auch unter dem Eindruck eines so schrecklichen Ereignisses wie des Terrorangriffs auf die USA könne es keine Massensammlungen von Daten nach dem Prinzip ›Suche nach der Stecknadel im Heuhaufen‹ geben. Dem Rechtsstaat, so Jacob weiter, seien Grenzen gesetzt, wenn er nach einer Gruppe von Menschen fahnde, die nur durch sehr wenige gemeinsame Merkmale zu beschreiben sei und deshalb bei der Suche in ungewöhnlich großem Ausmaß Verdachtsfälle produzieren würde.

## Auf Schatzsuche im PC-Bergwerk

Die auf der CeBIT dieses Jahres vorgestellte Software ›Loss Prevention‹ arbeitet nach dem Prinzip der Rasterfahndung auf der Basis des ›Data Mining‹-Verfahrens (= ›Daten-Bergbau‹).

So wie ein Minenarbeiter im Bergwerk nach verborgenen Schätzen sucht, so werden beim ›Data Mining‹ aus dem Wust der Verkaufs- und Personaldaten verborgene Informationen ans Tageslicht befördert. Damit können beispielsweise Prognosen, differenzierte Profile, Klassifizierungen und Bewertungen von Kassierern und Kassiererinnen erstellt werden (mehr zu Data Mining in: ›Bergleute im Daten-Lagerhaus‹ in cf 4/99 ab Seite 11).

Das ›Loss Prevention‹-System arbeitet dabei mit den Daten, die an jeder Kasse in jedem Markt über jeden Angestellten in jeder Stunde an jedem Tag gesammelt werden. Die Daten werden täglich in die zentrale Datenbank des ›Loss Prevention‹-Servers ›eingepflegt‹ und stehen für Analyse und Ermittlung zur Verfügung.

Im Marketing wird ›Data Mining‹ seit Langem eingesetzt. Dabei hat man, einer populären Anekdote zufolge, in den USA herausgefunden, dass Bier und Windeln auffällig oft zusammen gekauft werden. Eine mögliche Erklärung ist, dass die von ihren Ehefrauen beauftragten Ehemänner beim Gang in den Supermarkt schnell auch noch für flüssige Vorräte sorgen ...

Zahlreiche Unternehmen, gerade auch im Internet-Handel, haben bereits große Datenbanken mit detaillierten Informationen über ihre Kunden und Interessenten. Neben der bloßen Adresse und Informationen über Anfragen und Käufe liegen oftmals auch schon Daten über Alter, Geschlecht, Herkunft, Bildung und so weiter vor – Informationen, die in der Regel nur genutzt werden, um direkt mit dem einzelnen Kunden zu kommunizieren – wenn überhaupt.

Aus Sicht der Marketing-Experten werden Datenbanken dieser Art noch viel zu selten genutzt, um zum Beispiel strategisch wichtige Antworten auf Fragen wie diese zu finden:

- Welchen Kunden sollte wann welches Angebot unterbreitet werden?
- Bei welchem Kundenprofil lohnt ein Außendienstbesuch?
- Welche Kunden droht das Unternehmen zu verlieren?
- Wie hoch ist das ›Cross-Selling‹-Potenzial eines neuen Produkts (der Kunde kauft auch gleich noch weitere Produkte)?
- Wie lassen sich Interessenten mit hohen Lifetime-Values (›lebenslangen‹ Umsatzchancen) gewinnen?

*(Thomas Bittner, Jan Scholzen: ›Der lange Weg zum Customer Lifetime Value‹; in: Acquisa 9/2001)*

## Aber: Data Mining ist unzulässig, wenn ...

... personenbezogene Daten gespeichert und verarbeitet werden, dies ist die einhellige Meinung der Datenschützer. Die europäische Datenschutzrichtlinie spricht in ihrem Artikel 15 grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu sein (siehe: ›Personalentscheidung per Computer‹ in cf 7-8/02 ab Seite 44). Auch nach Meinung der Datenschutzbeauftragten des Bundes und der Länder ist ›Data Mining‹ ein Instrument, das für solche automatisierten Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hebt sogar ausdrücklich hervor, dass ›Data

Mining‹-Verfahren nicht zum Einsatz kommen dürfen, wenn personenbezogenen Daten gespeichert und verarbeitet werden – bei ›Loss-Prevention‹ mit Hilfe von ›Data Mining‹ aber ist genau das der Fall.

›Data Minig‹ ergänzt die bisher üblichen und eher einfachen statistischen Verfahren um neue Analysemethoden, die einen Großteil der Untersuchungsprozesse automatisieren und beschleunigen – Datenberge werden so gleichsam selbstständig durchforstet. Auch Mitarbeiterprofile sind damit möglich.

So können besondere Fragestellungen untersucht werden:

- Welche Filialen verhalten sich auffällig?
- Bei welchem Kassierprofil mit welchen Auffälligkeiten lohnt sich eine gezielte Überwachung (z. B. durch eine Detektei)?
- Gibt es bestimmte kritische Tageszeiten (Mittagspause, Tagesende)?
- Wo sind die besonders riskanten Kassen (z. B. im Getränkemarkt oder bei der Leergutannahme)?
- Welche Jahreszeiten sind besonders kritisch (Urlaub oder Weihnachtsgeschäft)?
- Gibt es prinzipiell ›riskante‹ Beschäftigtengruppen (Teilzeitbeschäftigte, Aushilfen, Alleinerziehende)?
- Gibt es Altersgruppen mit besonderen Auffälligkeiten bei den Beschäftigten?

Das Resultat kann in einem dreidimensionalen Schaubild betrachtet werden, so dass Unregelmäßigkeiten an der Kasse schnell zu erkennen und bis zum einzelnen Arbeitnehmer zurückverfolgt werden können.

## Loss Prevention? Ausgeschlossen!

Damit keine Missverständnisse aufkommen: Selbstverständlich dürfen sich die Unternehmen gegen Diebstahl durch das Personal absichern. Aber dafür müssen sie nicht mit Kanonen auf Spatzen schießen und vor allem dürfen sie nicht die Persönlichkeitsrechte der Beschäftigten missachten.

Und wehren können sich die Unternehmen durchaus schon jetzt: Das Selbsthilferecht zum Beispiel gibt dem Filialleiter oder dem Sicherheitsdienst das Recht, bei Straftaten des Personals die Eigentumsinteressen des Unternehmens zu wahren. Das geht so weit, dass sie auch das Recht zur vorläufigen Festnahme haben, wenn Beschäftigte auf frischer Tat beim Diebstahl ertappt werden und flüchten wollen. Außerdem sind Personen- und Taschenkontrollen am Personaleingang von Einzelhandelsgeschäften zur Aufdeckung und Abschreckung möglich und an der Tagesordnung (siehe: ›Die Zulässigkeit von Torkontrollen‹ in AiB 1999, Seite 428). Eine Totalüberwachung, wie mit ›Loss Prevention‹ möglich, wäre jedoch völlig überzogen. Die Rasterfahndung an der Supermarktkasse hat im Arbeitsleben nichts zu suchen.

Auch der Gesetzgeber geht davon aus, dass die freie Entfaltung der Persönlichkeit unter anderem durch Technisierung, Rationalisierung und zunehmende Verarbeitung personenbezogener Daten in einem besonderen Maß gefährdet ist. Kontrolle von Menschen soll demnach *nur durch Menschen*, nicht aber durch Maschinen erfolgen. Dieses Prinzip dient der grundgesetzlich garantierten, freien Entfaltung der Persönlichkeit. Gleichzeitig konkretisiert es den Auftrag des Betriebsverfassungsrechts an den Betriebsrat, die freie Entfaltung der Persönlichkeit der Beschäftigten im Betrieb zu schützen und zu fördern.

Bereits seit einem Urteil des Bundesarbeitsgerichts von 1985 ist klar, dass *alle* computergestützten Systeme auch mitbestimmungspflichtige ›technische Kontrolleinrichtungen‹ im Sinne des § 87 Abs. 1 Nr. 6 BetrVG sind. Dabei ist es, laut BAG, »nicht entscheidend, ob eine Überwachung auch tatsächlich stattfindet, es genügt, dass sie möglich ist.« Dessen ungeachtet versuchen Arbeitgeber immer wieder, die Mitbestimmung der Betriebsräte mit dem Argument zu bestreiten, eine Leistungs- und Verhaltenskontrolle sei ›gar nicht beabsichtigt‹, sondern lediglich eine ›unerwünschte Nebenwirkung‹ ...

Es ist also Ziel des Mitbestimmungsverfahrens, eine Vereinbarung mit dem Arbeitgeber zu treffen, die die Möglichkeit zur Überwachung Einzelner technisch und organisatorisch ausschließt. Denn Betriebsräte befürchten, wohl oft nicht ganz zu Unrecht, dass sich die Arbeitgeber die ›unerwünschte Nebenwirkung‹ gelegentlich doch zu Nutze machen und Kontrollauswertungen vornehmen, und wenn sie es nicht tun oder in Auftrag geben, dann macht es vielleicht ein übereifriger Abteilungsleiter.

Mit anderen Worten: Computertechnologie darf nur dann betrieblich genutzt werden, wenn der Arbeitnehmer-Datenschutz sichergestellt und die Entfaltung der Persönlichkeit gewährleistet ist und wenn Eingriffe in die Persönlichkeitssphäre der Beschäftigten ausgeschlossen sind. Eine Leistungs- und Verhaltenskontrolle, auch nur eine gelegentliche, wird deshalb in den einschlägigen Betriebsvereinbarungen so gut wie immer verboten. Spätestens bei ›Loss Prevention‹ aber ist die Leistungs- und Verhaltenskontrolle nicht mehr ›unerwünschte Nebenwirkung‹, sondern der eigentliche und einzige Sinn und Zweck des Systems!

Keine Aktion bleibt im Dunkeln, alles wird minutiös aufgelistet, ausgewertet und abgebildet. Das mag der Abschreckung dienen und Betrug aufdecken. Aber ganz nebenbei führen solche Programme auch zu einer verschärften Konkurrenz untereinander. Denn durch die Verhaltens- und Leistungskontrolle, die diese Programme möglich machen, kann der Filialleiter vergleichen: Wer erbringt die schnellste Arbeitsleistung an der Kasse? Wer ist besonders langsam beim Kassieren? Wer hat auffällig viele Stornierungen?

**Die ›Loss Prevention‹-Technik verletzt die Persönlichkeitsrechte der betroffenen Arbeitnehmer(innen) – dem kann und darf der Betriebsrat nicht zustimmen!**

Auch die Konkurrenz der Filialleiter untereinander wird gefördert nach dem Motto: Wer hat die geringsten Kassendifferenzen, wer die ›flottesten‹ Kassierer(innen) in seinem Markt?

Was daran problematisch ist, liegt auf der Hand: Die permanente, ununterbrochene Leistungs- und Verhaltenskontrolle, die diese Programme als zentrale Eigenschaft mit sich bringen, ist ein unzulässiger Eingriff in die Persönlichkeitsrechte der Beschäftigten. Das bringt eine wirklich neue Dimension der Datenverarbeitung in die Arbeitswelt. Und genau das disqualifiziert ›Loss Prevention‹ für den betrieblichen Einsatz. Denn Arbeitnehmern muss auch das Recht zugestanden werden, den einen oder anderen Fehler machen zu können, ohne dass dies gleich Konsequenzen nach sich zieht.

Noch gibt es wenige Handelsketten, die mit ›Loss Prevention‹ arbeiten. Die Betriebsräte der Branche stehen jedoch vor großen Herausforderungen, denn ab 2003 wollen die Software-Anbieter offensiv auf den deutschen Markt.

Die Begehrlichkeiten der Unternehmen für die Anwendung von ›Loss Prevention‹ werden vor allem auch mit Blick auf die relativ geringen Investitionen verständlich. Da die technische Infrastruktur in den meisten Einzelhandelsketten bereits weitgehend vorhanden ist, können bei vergleichsweise geringen Kosten hohe Erlöse erzielt werden. Große Handelsketten kalkulieren mit Anschaffungskosten von lediglich 200 000 bis 300 000 Euro, zuzüglich Wartungs- und Pflegekosten zwischen 30 000 und 40 000 Euro pro Jahr.

Unternehmen in der Schweiz, die Systeme dieser Art bereits anwenden, sprechen davon, dass sich die Investitionskosten bereits nach ein bis zwei Monaten (!) amortisiert hätten. Dort hat beispielsweise nach Angaben eines Firmensprechers eine Handelskette mit rund 700 Kassenarbeitsplätzen schon zwei Monate nach der Einführung von ›Loss Prevention‹ Unterschlagungen in Höhe von etwa 200 000 Franken ermittelt und über 50 verdächtige Kassiererinnen und Kassierer entlassen.

Aus Sicht der Unternehmen mag es also nur konsequent sein, bei ›Loss Prevention‹ einzusteigen. Dennoch müssen auch im Supermarkt mindestens die gleichen Schutzkriterien gelten wie bei der Fahndung nach Terroristen ...

Ein unzulässiger Eingriff in die Persönlichkeitsrechte, beispielsweise durch ›Loss Prevention‹, kann auch nicht etwa durch eine Betriebsvereinbarung ›geheiligt‹ werden (siehe: ›Personal-Informations-Systeme – die rechtlichen Rahmenbedingungen‹ in CF 8-9/00 ab Seite 22).

Für Betriebsräte gibt es also bei ›Loss Prevention‹-Systemen keinen Verhandlungsspielraum – diese Technologie verletzt die Persönlichkeitsrechte der Arbeitnehmer und Arbeitnehmerinnen, dem kann und darf der Betriebsrat nicht zustimmen!