Data Mining – Rasterfahndung im Betrieb

Lückenlose Leistungs- und Verhaltenskontrolle am Arbeitsplatz

Hier lesen Sie

- **wann die Einführung computergestützter Datenverarbeitungssysteme in Betrieben der Mitbestimmung des Betriebsrats unterliegt**
- **in welchen Fällen die Datenerhebung unzulässig ist**
- **wie Arbeitgeber genaue Leistungs- und Verhaltensprofile ihrer Mitarbeiter erstellen können**
- **was der Betriebsrat tun kann, damit unzulässige Einriffe in das Recht auf informationelle Selbstbestimmung unterbleiben**

Mit Data Mining wird wie im Bergwerk nach verborgenen »Schätzen« gesucht, dabei können riesige Datenmengen aus verschiedenen Datenbanken innerhalb kürzester Zeit ausgewertet werden, um verborgene Informationen ans Tageslicht zu befördern, beispielsweise zu besseren Klassifizierungen und Bewertungen von Kunden oder der Arbeitsproduktivität der Beschäftigten. Unter Data Mining wird gewöhnlich das computergestützte Entdecken und Herausfinden unbekannter Informationen aus großen Mengen von Daten verstanden.

Dazu durchsucht ein Programm die gesamten vorhandenen Informationen nach definierten Ereignissen und Auffälligkeiten. Auf der Basis aller täglich anfallenden Daten im Betrieb lässt sich bereits über einen recht kurzen Beobachtungszeitraum fast komplett das typische Arbeitsverhalten aller Beschäftigen ermitteln. Für die Arbeitnehmervertretung heißt das: Die Leistungs- und Verhaltenskontrolle ist nicht mehr »unerwünschte Nebenwirkung« eines Computerprogramms, sondern das zentrale Einsatzziel. Dadurch ist die absolute und kontinuierliche Analyse von personenbezogenen Daten am Arbeitsplatz zum eigentlichen Systemzweck geworden, die Datenverarbeitung in der Arbeitswelt hat eine neue Dimension erreicht. Ohne betriebliche Regelung verstößt Data Mining massiv gegen den Datenschutz und stellt einen unzulässigen Eingriff in das grundgesetzlich geschützte Persönlichkeitsrecht der Arbeitnehmer und Arbeitnehmerinnen dar.

Analyse von Sekundärdaten – nicht erlaubt!

Mit dem Einsatz von modernen Informations- und Kommunikationssystemen in der Arbeitswelt hat die Menge der gespeicherten Daten in den letzten Jahren dramatisch zugenommen. Die Nutzung und weitere Auswertung dieser Daten über den ursprünglichen Erhebungszweck hinaus – die so genannte Sekundärdatenanalyse – verspricht weitere interessante Erkenntnisse. Am Beispiel der großen Einzelhandelsunternehmen wird deutlich, wie weit fortgeschritten die Analyse von Sekundärdaten bereits ist. In der Regel sieht es dort heute folgendermaßen aus: In den örtlichen Filialen sammeln Computerkassen[1] alle Verkaufsdaten. So wird jede einzelne Bon-Zeile gespeichert. In der Zentrale laufen auf einem Server diese Verkaufsdaten aus allen Filialen über ein Kommunikationsnetz zusammen, wo sie für unterschiedliche Ziele, wie Rechnungsprüfung, Warenbewegung, Lagerkontrolle ausgewertet werden. Ein Unternehmen mit mehreren 100 Filialen erzeugt dabei jeden Tag leicht einen Bericht mit weit über drei Millionen Zeilen. Diese können nicht nur unter dem Aspekt der Warenwirtschaft analysiert werden, sondern auch »ganz nebenbei« von der Sicherheitsabteilung, die sich für die angefallenen Daten vor dem Hintergrund der Betrugsrecherche interessiert.

Nicht nur im Handel gibt es Daten, die über ihren eigentlichen Erhebungszweck ausgewertet werden könn(t)en. Bei jeder Maschinen- und Betriebsdatenerfassung (MDE/BDE) werden neben der unternehmensweiten Erfassung, Auswertung und Archivierung von Produktionsprozessen, Stückzahlen, Laufzeiten auch Daten erzeugt, die über die Beschäftigten Aussagen machen können. Ganz egal, ob beim Telefonieren oder beim Surfen im Internet, immer wenn Computer miteinander kommunizieren, beispielsweise in einem Firmennetzwerk, werden elektronische Protokolle erstellt, so genannte Logfiles. Dabei handelt es sich um die automatisch erstellte Aufzeichnung aller Aktionen von einem oder mehreren Nutzern an einem Rechner, ohne dass diese davon etwas mitbekommen oder ihre Arbeit beeinflusst wird.

Bis vor kurzem war das Problem, dass niemand solche riesigen Berichte analysieren oder bearbeiten konnte. Komprimierte Informationen lieferten nicht mehr die Details, die zur individuellen Beurteilung der Leistungsfähigkeit

1 So genannte Point-of-Sale-Systeme (PoS): Computerkassen mit Schnittstellen zu beliebigen Servern und Softwarepaketen, wie DFÜ-Kommunikationsprogramme, Kassenmanagement oder Warenwirtschaftssysteme.

oder zur Aufdeckung von Betrug erforderlich wären. In diesem Datenberg, so vermuten Personal- und Sicherheitsfachleute, könnten sich jedoch Informationen befinden, die

zu »Minderleistern« an den Maschinen oder unehrlichen Kassiererinnen und Kassierern führen. MDE/BDE, Daten aus dem SAP-System, und der Supermarktkasse, die für einen betriebswirtschaftlichen Zweck erhoben wurden oder Protokolldaten (Logfiles) des Firmennetzwerks, der Mailserver können mit Hilfe von Data Mining zu weiteren umfangreichen Analysen über den eigentlichen Erhebungszweck hinaus genutzt werden.
Die Auswertung von Personaldaten ist weder in Logfiles noch zur Aufdeckung von Betrug an der Kasse erlaubt.

Regelung im BDSG
Im Bundesdatenschutzgesetz wird klar geregelt, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zulässig ist, wenn ein Gesetz oder eine andere Rechtsvorschrift, beispielsweise eine Betriebsvereinbarung, dies erlaubt. Überdies muss den Beschäftigten der Zweck der Erhebung, Verarbeitung und Nutzung der Daten vorher mitgeteilt werden.[2]

Technische Informationen in den Logfiles, die übrigens meistens auch personenbezogene Daten enthalten, oder Bon-Zeilen, die von der Kasse gesammelt wurden, um damit den Umsatz von unterschiedlichen Warengruppen zu ermitteln, können nur für die erhobenen Zwecke ausgewertet werden, weitere sekundäre Analysen sind nur in Ausnahmefällen zulässig. Dennoch nutzen viele Unternehmen ihre Daten zu Sekundäranalysen. Mittlerweile werden von verschiedenen Systemanbietern Programme extra hierzu angeboten. Stellvertretend für viele andere Anwendungen soll an dieser Stelle ein »Werkzeug« zur Vermeidung von Inventurdifferenzen im Einzelhandel vorgestellt werden, das vermehrt seit dem Jahr 2000 in deutschen Einzelhandelskonzernen eingesetzt wird – oft ohne Wissen der Beschäftigten und Betriebsräte.

Suche nach Verdächtigen im »Datenberg« – wie geht das?

Unter dem harmlos klingenden Oberbegriff »Kassenmanagementsysteme« mit Produktnamen wie Loss Prevention von Fujitsu Services, Fraud Detection von Nixdorf, Sales-Audit von SAP, und besonders einfallsreich: McKillroy von Soft & Systems drängen Programme auf den Markt, die künftig, so versprechen es die Anbieter, im Einzelhandel Betrug und Unterschlagungen an den Kassenarbeitsplätzen aufdecken und verhindern sollen.
Loss Prevention und Co machen es sich zu Nutze, dass bereits eine Infrastruktur besteht, die riesige Mengen von Verkaufs- und Personaldaten zur Verfügung stellt. Alle Aktivitäten an den Arbeitsplätzen werden lückenlos erfasst, übermittelt und zentral gespeichert – das war auch vor Loss Prevention so. Aber erst jetzt haben die Unternehmen ein »intelligentes« Werkzeug, um diese Daten hinsichtlich des Vorgehens der Kassiererinnen und Kassierer zu analysieren; denn nach Aussagen der Experten gibt es gerade an Kassenarbeitsplätzen eine Vielzahl von Manipulations- und Betrugsmöglichkeiten. Mit den Managementsystemen scheint hier die Lösung gefunden worden zu sein, dem Betrug und Diebstahl an der Supermarktkasse ein endgültiges Ende zu setzen.
Loss Prevention, das frei übersetzt so viel bedeutet wie »Verlustvermeidung oder -verhinderung«, werden von den Herstellern nahezu »göttliche Fähigkeiten« zugeschrieben, dies deutet sich beim Anbieter schon im Namen an: In ihrer Werbung heißt es »LORD Loss Prevention untersucht detailliert alle Transaktionen, bei denen Manipulationen möglich sind (...) und deckt schnell Unregelmäßigkeiten an den Kassen auf. Das vermindert Verluste und steigert Erträge nachhaltig«.
Um diese Verluste zu minimieren – nach einer Studie des Eurohandelsinstitut (EHI) handelt es sich immerhin um vier Milliarden Euro für das Jahr 2003[3] – hat der Einzelhandel in der Vergangenheit alle erdenklichen modernen Technologien entwickelt und eingesetzt, um so genannte Inventurdifferenzen zu vermeiden. Angefangen bei der Einführung von Video- und Kameraüberwachung über hochintelligente Cashmanagementsysteme und Verkaufsrevision bis hin zu elektronischen Sicherungsetiketten und In-Store-Sicherungssystemen. All diese Systeme haben im Zusammenhang mit der Abwehr von Kundendiebstahl auch bis zu einem gewissen Grad ihre Aufgaben erfüllt. Sie sind jedoch häufig mit einem hohen organisatorischen Arbeits- und Kostenaufwand verbunden und haben im Hinblick auf die Unterschlagungen durch Mitarbeiter an den Kassen nie zufriedenstellend funktioniert.[4] Über die Ursachen an den zu verzeichnenden Verlusten, je nach Branche sind es etwa 0,7 bis 1,5 Prozent des Gesamtumsatzes, kann nur spekuliert werden. Grundsätzlich hält das EHI vier Verursachergruppen für Inventurdifferenzen verantwortlich: Kunden verursachen demnach knapp die Hälfte der Schäden, das Personal fast ein Viertel, also ca. eine Mrd. Euro.[5] Der Rest geht auf das Konto von Lieferanten und Servicekräften, sowie auf organisatorische Mängel. Die Annahme, dass ein erheblicher Anteil der Inventurdifferenzen durch Mitarbeiterdelikte entsteht, wird nicht nur vom EHI, sondern auch von Sicherheitsfachleuten[6] so eingeschätzt. Ebenso weisen

2 Vgl. § 4 BDSG, vgl. vertiefend zum Thema: Arbeitsrecht, Handbuch für die Praxis, 3. Aufl., § 113.
3 Vgl. EHI – The International Retail Network (Hrsg) 2004, Inventurdifferenzen 2004, Ergebnisse einer aktuellen Erhebung, S. 12 ff.
4 Vgl. Heide, Videobilder sagen mehr als tausend Worte, in: Criminal Digest 2/2000, 109 ff.
5 Vgl. EHI a. a. O., S. 20.
6 http://www.datapos-sicherheit.de oder http://www.sdg-sicherheit.de/ermitt.htm.

die Betriebsräte[7] im Einzelhandel in Gesprächen über dieses Thema auf diesen Sachverhalt hin.
Das Problem ist also unbestritten, der Einzelhandel muss etwas gegen die Inventurdifferenzen unternehmen. Um die Mitarbeiterdiebstähle an den Kassen zu beweisen, müssen die Unternehmen in der Regel umfangreiche Untersuchungen und Beobachtungen vor Ort durchführen, beispielsweise mit eigenen Detektiven oder durch externe Security Firmen. Dabei stellt sich häufig nicht der gewünschte Erfolg ein.
Hier setzten Loss Prevention und Co an, die Software verspricht Unregelmäßigkeiten an den einzelnen Kassen aufzudecken und so mögliche Hinweise auf potentielle Täter zu geben. Dies funktioniert folgendermaßen.

Suchraster für ungewöhnliches Verhalten

Für die Kassiererinnen und Kassierer werden »Kassier-Profile« erstellt, mit denen ungewöhnliches Verhalten aufgedeckt wird.

Das Suchraster an der Supermarktkasse könnte beispielsweise folgende Kriterien enthalten:

Anzahl von Stornierungen
Kartentransaktionen mit derselben manuell eingegebenen Kreditkartennummer
Öffnen der Kassenschublade ohne Verkauf nach einem Storno
Leergutauszahlungen bzw. Leergutbuchungen
manuelle Preisüberschreibungen
Personaleinkäufe mit Rabattgewährungen
Warenrücknahmen ohne Kassenbon
Bonstornos und Bonabbrüche

Dies ist nur eine kleine Zahl von Beispielen von echten oder vermeintlichen Betrugsmöglichkeiten, bestimmte Aktivitäten werden als »risikoreich« behandelt. Die zentral erfassten Daten sämtlicher Filialen können mit den Managementsystemen bearbeitet, ausgewertet und übersichtlich dargestellt werden. Auf einen Blick wird deutlich, in welcher Filiale, welche Kassiererin oder welcher Kassierer auffällig vom »normalen« Verhalten abweicht. Das Ergebnis bedeutet zwar nicht zwangsläufig, dass notwendigerweise hinter jeder dieser Aktionen ein Betrug steht, aber eine Kassiererin oder ein Kassierer, der deutlich mehr (oder weniger) als die durchschnittliche Anzahl dieser Aktivitäten ausführt, setzt sich damit dem Verdacht aus, eventuell auch zu betrügen. Sales-Audit, McKillroy, Loss Prevention und wie sie sonst noch heißen, ermitteln mit den Methoden der Rasterfahndung tagesaktuell die potentiellen Täter an den Kassen und leiten die Ergebnisse an die Kassenaufsicht oder den Sicherheitsdienst!

Rasterfahndung

Die Methode, mit der diese Systeme vorgehen, erinnert an jene polizeiliche Verfolgung und Verbrechersuche, die unter dem Begriff der Rasterfahndung bekannt geworden ist. Die Fahndungsmethode wurde bereits Mitte der 60er Jahre vom Bundeskriminalamt (BKA) entwickelt und vor allem zur Terrorismusbekämpfung eingesetzt.[8] Unter Rasterfahndung versteht man das computergestützte Durchsuchen von Datenbeständen nach bestimmten Merkmalen. Verglichen werden dabei beispielsweise Daten aus den Einwohnermeldeämtern und dem Kraftfahrbundesamt sowie polizeiliche Daten, etwa Täterprofile und Tatverdächtige. Dazu können noch gezielte Eigenschaften von Verdächtigen kommen, Wohnen im Hochhaus, fehlende Anmeldung bei Energieunternehmen. Diese Informationen werden aus den verschiedensten Datenbanken, z. B. von Schufa, Versicherungen, Krankenkassen und Energieversorgungsunternehmen zusammengetragen und in einem aufwendigen Verfahren aufeinander abgestimmt und ausgewertet.[9] Trotz einiger Erfolge bei der Terrorismusbekämpfung wurden damals gegen die Rasterfahndung erhebliche datenschutzrechtliche Bedenken laut,[10] die dazu führten, dass das Vorgehen bei dieser Fahndungsform durch die Strafprozessordnung geregelt wurde. Voraussetzung für die Anwendung der Rasterfahndung ist das Vorliegen einer Straftat von erheblicher Bedeutung.

§ 98 a StPO

»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«.

Ins Bewusstsein der Öffentlichkeit ist die Rasterfahndung bei der Suche nach weiteren Tatbeteiligten am Anschlag auf die Twin Towers am 11.9.2001 gerückt. Drei der mutmaßlichen Selbstmordattentäter lebten und studierten vor der Tat in Hamburg. Mit dem automatisierten Abgleichsverfahren der Rasterfahndung sollen bundesweit weitere »unauffällige und unverdächtige« Menschen gesucht werden, die als potentielle Al-Qaida-Kämpfer in Frage

7 1. Sicherheitstag des Einzelhandels Berlin/Brandenburg, 1.11.2001, Sicherheitsfachmesse SiTech Berlin 2001.
8 Schenk, Das wachsame Auge blickte stets nach links. Eine kritische Würdigung des Bundeskriminalamtes zum 50 Geburtstag, FR 22.3.2001.
9 Horst Herold, der ehemalige Chef des Bundeskriminalamts hat die Möglichkeiten der rasternden Täterfahndung bereits 1968 im »Taschenbuch für Kriminalisten« beschrieben: »Die elektronische Datenverarbeitung besitzt die Fähigkeit, riesige Datenmengen nach beliebigen Zusammenhängen zu verknüpfen und über diese Zusammenhänge quantitative Aussagen in kürzester Zeit nach dem allerneuesten Stand zu formulieren. Dem Gesetz der großen Zahl entsprechend ist die Treffgenauigkeit solcher Aussagen umso größer, je größer die Zahl der verarbeiteten Daten ist. (...) Damit wird die Kriminalpolizei erstmals in der Lage sein, auf Massenbasis und damit mit größter Genauigkeit rationale Einsichten in Ursache und auslösende Kräfte des Verbrechens zu gewinnen.«
10 Vgl. Koch/Oltmanns; SOS – Freiheit in Deutschland; Hamburg, 1978.

kämen.[11] Diese Fahndungsmethode ist auch heute bei Datenschützern und Juristen nicht unumstritten. Mit drei Urteilen sind die monatelangen Rasterfahndungen nach so genannten Schläfern in Berlin, Hessen und in Nordrhein-Westfalen teilweise für rechtswidrig erklärt worden.[12] Als Konsequenz hat der damalige Bundesbeauftragte für den Datenschutz (BfD), Joachim Jacob, einen »noch sorgfältigeren Umgang« mit personenbezogenen Daten durch die Sicherheitsbehörden angemahnt. Diese müssten »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 Motto der Suche nach der Stecknadel im Heuhaufen geben, erläuterte eine Sprecherin die Position des BfD. Dem Rechtsstaat 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 virtuellen Suche nach ihr in ungewöhnlich großem Ausmaß Verdachtsfälle produziert würden.[13] Trotz dieser Bedenken setzen die Unternehmen Programme wie Loss Prevention ein. Kassiererinnen und Kassierer werden mit den Methoden der Rasterfahndung permanent überwacht. Der Schritt ist aus der Perspektive der Unternehmen nur konsequent, dennoch müssen im Supermarkt die gleichen Kriterien gelten wie bei der Fahndung nach Terroristen.

Data Mining – im Datenbergwerk

Das Kassenmanagementsystem durchsucht und analysiert die gesamten vorhandenen Daten nach definierten kritischen Ereignissen und Auffälligkeiten, also beispielsweise nach dem bereits erwähnten häufigen Öffnen der Schublade ohne Verkauf oder häufigen Leergutauszahlungen oder Bonstornos. Das Managementsystem arbeitet also mit den Übertragungsdaten, 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 Kassenmanagement Servers eingepflegt und stehen zur Analyse und Ermittlung über vom Benutzer definierte Zeiträume zur Verfügung. Das Programm arbeitet im Wesentlichen auf der Basis von Data Mining-Algorithmen.[14] 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 Kassiererinnen und Kassierern gegeben werden.

Data Mining bezeichnet als Oberbegriff Techniken zum Finden von interessanten und nützlichen Mustern und Regeln (»Wissen«) in großen Datenbanken. Es wird oft auch als künstliche Intelligenz bezeichnet, weil das gefundene, maschinell erlernte Wissen nicht in Form von Abfragen existiert, sondern mit Hilfe von Algorithmen gefunden wird.[15] Algorithmen beschreiben einen methodischen Weg zur Lösung einer mathematischen Aufgabe, indem das Problem in endlich viele, eindeutig festgelegte Schritte aufgelöst wird. Seit langem wird Data Mining im Marketing eingesetzt. Dabei hat man, einer populären Data Mining-Anekdote zufolge, in den USA herausgefunden, dass Bier und Windeln auffällig oft zusammen gekauft werden, wohl, weil die von ihren Ehefrauen beauftragten Ehemänner beim Gang in den Supermarkt noch eben schnell für flüssige Vorräte sorgen ...

Wenn auch der Wahrheitsgehalt dieser Anekdote zweifelhaft ist, Data Mining-Techniken werden beispielsweise erfolgreich zur Sortimentsoptimierung eingesetzt. Zahlreiche Unternehmen, gerade auch beim Internethandel, haben große Datenbanken mit detaillierten Informationen über ihre Kunden und Interessenten. Neben der bloßen Adresse liegen oftmals soziodemographische Daten, Kaufinformationen, Potentialdaten sowie Kommunikationsdaten vor. Diese Informationen werden in der Regel genutzt, um direkt mit dem einzelnen Kunden zu kommunizieren. Auch einfache Managementfragen lassen sich mit Hilfe der Datenbank beantworten. So stellt es kein Problem dar, die Anzahl oder das Durchschnittsalter neuer Kunden oder Interessenten auszugeben. In den wenigsten Fällen wird jedoch die Datenbank zur Beantwortung folgender, für die Unternehmen entscheidungsrelevanter Fragen genutzt: Welchen Kunden sollte wann welches Angebot unterbreitet werden? Bei welchem Kundenprofil lohnt sich ein Außendienstbesuch? Welche Kunden droht das Unternehmen zu verlieren?

An dieser Stelle setzt das Data Mining an. Es ergänzt die einfachen statistischen Verfahren um neue Analysemethoden, die einen Großteil der Untersuchungsprozesse automatisieren und beschleunigen. Zum Beispiel durch Regression,[16] dabei handelt es sich um ein klassisches lineares Prognoseverfahren zur Erklärung von Verhaltensweisen mit Hilfe unabhängiger Variablen. Außerdem kommen regelbasierte Systeme, die zur Extraktion und Verifikation von Wenn-Dann-Regeln[17] dienen und Chi-squared Automatic Interaction Detection[18] als Methoden, die eine Menge von Datensätzen hinsichtlich einer abhängigen Variable segmentiert, zum Einsatz.

Bildlich gesprochen durchforsten Data Mining Algorithmen selbständig den Datenberg. Im Gegensatz zu den traditionellen Methoden wird nicht der gesamte Datenberg per Hand mühsam abgebaut und mikroskopisch untersucht,

11 Vgl. FR vom 12.4.2002.
12 Vgl. Gössner; Ausgerastert!? FR 12. 04 2002.
13 Vgl. Die Welt, 13.2.2002.
14 Vgl. Wrobel; Data Mining und Wissensentdeckung in Datenbanken, Künstliche Intelligenz 1/98, S. 6–10.
15 Vgl. Wrobel; a. a. O.
16 Vgl. Witten/Frank; Data Mining, Praktische Werkzeuge und Techniken für das maschinelle Lernen; München 2001, S. 227.
17 Vgl. Rieger, Entscheidungsunterstützung durch Data Mining, ExperPraxis 99/2000; S. 9.
18 Vgl. Rieger, a. a. O., S. 10.

sondern relevante Teile des Berges werden selbständig identifiziert und analysiert. Dabei bahnen sich die Methoden des Data Mining zielstrebig den Weg durch die Informationsflut, um schnell die bislang verborgenen Erkenntnisse und Zusammenhänge aufzuzeigen. Durch den Data Mining-Einsatz kann so ein Mitarbeiterprofil erstellt werden. Das Verfahren erlaubt verdächtige Verhaltensmuster zu entdecken und diese weiter zu detaillieren. Mit Loss Prevention und Co, also durch den Einsatz von Data Mining werden auffällige Kassiererinnen und Kassierer oder einzelne Filialen analysiert und können dann gezielt nach besonderen Fragestellungen untersucht werden.

Beispiel

Welche Filialen verhalten sich auffällig?
Bei welchem Kassierprofil lohnt sich eine gezielte Überwachung (z. B. Detektei)?
Gibt es bestimmte kritische Tageszeiten (Mittagspause, Tagesende)?
Wo sind riskante Kassen (z. B. im Getränkemarkt oder bei der Leergutannahme)
Wann sind besonders kritische Jahreszeiten (Urlaub, Weihnachtsgeschäft)?
Gibt es riskantes Personal (Teilzeitbeschäftigte, Aushilfen, Alleinerziehende)?
Gibt es auffällige Altersgruppen bei den Beschäftigten?
Wie lassen sich Transaktionen, die einen bestimmten Betrag übersteigen, erklären?

Das System ermöglicht dem Sicherheitsdienst, unregelmäßige Transaktionen an den Kassen schnell zu erkennen und bis hin zum einzelnen Kassenarbeitsplatz zu verfolgen.
Das bedeutet, in der Zentrale können ausgewählte Informationen zu Regionen, Städten, Ortsteilen und den jeweiligen Filialen durch anklicken weiter detailliert werden.

Neue Dimension: Leistungs- und Verhaltenskontrolle als Systemfunktion

Was hier für den Einzelhandel dargestellt worden ist, lässt sich fast nahtlos auf alle anderen Systeme und Branchen übertragen, bei denen ähnlich viele Daten über die Mitarbeiter erfasst werden, beispielsweise mit Maschinen- und Betriebsdatenerfassung, im Call Center, bei vielen SAP-Anwendungen oder bei der Auswertung von Logfiles.
Das wirklich neue an dieser Form von Managementsystemen ist die Tatsache, dass eine »Leistungs- und Verhaltenskontrolle« der Beschäftigten die eigentliche Zentralfunktion ist. Mit dieser Eigenschaft disqualifizieren sich diese Systeme jedoch für den betrieblichen Einsatz!

Die Einführung und Anwendung von Loss Prevention oder McKillroy mag für die Unternehmen verlockend sein, aus rechtlicher Hinsicht ist sie nicht zulässig und für die Betriebsräte nicht hinzunehmen!
Nach dem Betriebsverfassungsgesetz (BetrVG) haben die Betriebsräte bei der »Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen«,[19] mitzubestimmen. Dieses Mitbestimmungsrecht wurde geschaffen, weil technische Kontrolleinrichtungen stark in den persönlichen Bereich der Beschäftigten eingreifen. Der Gesetzgeber ging davon aus, dass die freie Entfaltung der Persönlichkeit unter anderem durch Technisierung, Rationalisierung und zunehmende Verarbeitung personenbezogener Daten in einem besonderen Maß gefährdet ist. Der Gesetzgeber wollte, dass eine Kontrolle von Menschen nur durch Menschen und nicht durch Maschinen erfolgt.[20] Dieses Prinzip dient der grundgesetzlich garantierten freien Entfaltung der Persönlichkeit und konkretisiert den im BetrVG enthaltenden Grundsatz,[21] die freie Entfaltung der Persönlichkeit der Beschäftigten im Betrieb zu schützen und zu fördern.
Der Betriebsrat soll mit Hilfe des Mitbestimmungsrechts eine präventive Schutzfunktion wahrnehmen, um potentielle Eingriffe in die Persönlichkeitssphäre der Beschäftigten zu verhindern.[22] Vor diesem rechtlichen Hintergrund haben sich Betriebsräte im Laufe der Zeit umfangreiche Mitbestimmungs- und Mitgestaltungsmöglichkeiten erstritten. Das BAG lässt seit 1985 keinen Zweifel mehr daran, dass alle computergestützten Systeme mitbestimmungspflichtige »technische Kontrolleinrichtungen« im Sinne des § 87 Abs. 1 Nr. 6 BetrVG sind, »wobei es nicht entscheidend ist, ob eine Überwachung auch tatsächlich stattfindet, es genügt, dass sie möglich ist.«[23] Bislang haben Arbeitgeber immer wieder versucht, die Mitbestimmung der Betriebsräte mit dem Argument zu bestreiten, »eine Leistungs- und Verhaltenskontrolle ist gar nicht beabsichtigt«, sondern lediglich eine »unerwünschte Nebenwirkung«.
Es ist also das Ziel des Mitbestimmungsverfahrens, eine überprüfbare Vereinbarung[24] 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 zu Nutze machen und doch Kontrollauswertungen vornehmen. Mit anderen Worten: Computertechnologie darf nur dann betrieblich genutzt werden, wenn der Arbeitnehmerdatenschutz sichergestellt und die Entfaltung der Persönlichkeit gewährleistet ist, sowie Eingriffe in die Persönlichkeitssphäre der Beschäftigten nicht möglich sind. Eine Leistungs- und Verhaltenskontrolle ist in Betriebsvereinbarungen eigentlich immer ausgeschlossen.
Bei Loss Prevention oder McKillroy ist die Leistungs- und Verhaltenskontrolle aber nicht mehr »unerwünschte Nebenwirkung«, sondern der eigentliche Sinn und Zweck. Das

19 § 87 Abs. 1, Nr. 6 BetrVG.
20 Vgl. BT-Druck S. VI/1786, S. 49.
21 § 75 BetrVG.
22 Vgl. Däubler, Gläserne Belegschaft? Datenschutz für Arbeiter, Angestellte und Beamte, Köln 1993.
23 Vgl. BAG v. 23.4.1985, v. 11.3.1986, AP Nrn. 12, 14 zu § 87 BetrVG.
24 Vgl. Wilke, EDV-Vereinbarungen überprüfen!, CF 2/2001, S. 17 ff.

ist eine neue Dimension der Datenverarbeitung in der Arbeitswelt!

Datenschutzrechtliche Problematik von Data Mining

Die absolute und kontinuierliche Analyse von personenbezogenen Leistungs- und Verhaltensdaten durch Loss Prevention kann den Arbeitnehmerinnen und Arbeitnehmern nicht zugemutet werden – auch nicht bei einer vermuteten Inventurdifferenz von 1 Milliarde Euro im Jahr durch das Personal.

Das BAG stellte bereits 1987 fest, dass die Verletzung des Persönlichkeitsrechts eines Arbeitnehmers dann vorliegt, wenn dieser sich einer ständigen lückenlosen Überwachung unterworfen sieht.[25] So ist beispielsweise eine akustische Überwachung der Arbeitnehmer durch Abhörgräte oder Tonbandaufnahmen immer unzulässig. Das gleiche gilt für das Abhören oder heimliche Mithören von Telefongesprächen oder für die Überwachung mit Videokameras.[26] Mit anderen Worten, das dauerhafte Screening des Kassierverhaltens mit Loss Prevention ist nach der herrschenden Rechtsprechung nicht erlaubt und stellt eine gravierende Verletzung der Persönlichkeitsrechte der Beschäftigten dar, und dies muss von ihnen nicht hingenommen werden!

Erstellen von Persönlichkeitsprofilen

Ebenso wie mit der Überwachung verhält es sich mit den Persönlichkeitsprofilen, die mit Loss Prevention angefertigt werden können. Ziel des Programms ist es, ein typisches Profil des Kassierverhaltens zu erstellen, um dann anhand des Verhaltens einzelner Kassiererinnen und Kassierer festzustellen, wer von diesem typischen Profil abweicht. Die datenschutzrechtliche Zulässigkeit zur Erstellung von Persönlichkeitsprofilen findet sich im Bundesdatenschutzgesetz (BDSG). § 4 BDSG statuiert für die Verarbeitung und Nutzung personenbezogener Daten ein Verbot mit so genanntem Erlaubnisvorbehalt, dem auch die Erstellung von Persönlichkeitsprofilen als Form der Datenverarbeitung unterliegt. Danach ist der Umgang mit personenbezogenen Daten nur zulässig, wenn dieser durch eine Rechtsvorschrift erlaubt ist oder der Betroffene eingewilligt hat. Da das BDSG ein generelles Verarbeitungsverbot verfügt, fällt darunter auch das Erstellen von Persönlichkeitsprofilen.[27]

Datenschutz als Grundrecht

Das Verbot zum Erstellen von Persönlichkeitsprofilen begründet sich in der Rechtsprechung des Bundesverfassungsgerichts (BVerfG) zum Grundrecht auf informationelle Selbstbestimmung. Dort ist bereits 1983 für den Bereich der elektronischen Datenverarbeitung das allgemeine Persönlichkeitsrecht konkretisiert worden. Das Verfassungsgericht stellte damals im Zusammenhang mit der Volkszählung fest, dass jeder Bürger ein Selbstbestimmungsrecht über seine Daten hat.

In der Entscheidung heißt es:

»Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit dem Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen«.[28]

In der Folge hat das BVerfG dies mehrfach präzisiert und aus dem »Grundrecht auf informationelle Selbstbestimmung« mit dem so genannten Quellensteuerurteil erstmals das »Grundrecht auf Datenschutz«[29] gemacht.

Die freie Entfaltung der Persönlichkeit setzt nach dem Verständnis des BVerfG unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Daraus folgt, dass der einzelne Bürger – auch in seiner Rolle als Arbeitnehmer – grundsätzlich über die Preisgabe und Verwendung seiner persönlichen Daten selbst bestimmt. Weiter führt das BVerfG im für den Datenschutz wesentlich wegweisenden Volkszählungsurteil aus, die informationelle Selbstbestimmung sei heute unter anderem deshalb besonders gefährdet, weil personenbezogene Daten mit anderen Datensammlungen zu einem teilweise oder vollständigen Persönlichkeitsbild zusammengefügt werden könnten, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren könnte. Außerdem sei es mit der Menschenwürde nicht vereinbar, »den Menschen in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren«.[30] Dies gilt übrigens nicht nur für die Beschäftigten, sondern auch für die Kunden. Auch deren Daten sind schützenswertes Gut.[31] Mit den Worten des BVerfG: »Eine umfassende Registrierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen ist auch in der Anonymität statistischer Erhebungen unzulässig«.[32] Mit dieser Entscheidung ist auch die Anfertigung von Teilabbildern von Persönlichkeiten verboten.

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnologie wächst die Menge gespeicherter personenbezogener Arbeitnehmerdaten

25 Vgl. BAG v. 7.10.1987 – 5 AZR 116/86.
26 Vgl. BAG v. 29.6.2004 – 1 ABR 21/03.
27 Vgl. Gola/Schomerus/BDSG, § 4 Rdnr. 1.4.
28 Vgl. BVerfGE 65, 1.
29 BVerfGE 84, 239 (279 f.).
30 Wittich, Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen, RDV 2/2000, S. 61.
31 Vgl. Baeriswyl, Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut? RDV 1/2000, S. 6–11.
32 BverfGE 65, 1 (53).

in der Arbeitswelt weiter an. Mit Data Mining werden alle personenbezogenen Daten in einem einheitlichen Datenpool – losgelöst von ihrer ursprünglichen Verwendung – zusammengeführt. Mit dem von Loss Prevention verwendeten Verfahren des Data Minings stehen den Unternehmen Werkzeuge zur Verfügung, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten wissenswerten Zusammenhängen durchsuchen.

Mit Kanonen auf Spatzen schießen

Damit an dieser Stelle keine Missverständnisse aufkommen: Es soll hier nicht dem Diebstahl und der Unterschlagung durch Mitarbeiterinnen und Mitarbeiter an der Kasse das Wort geredet werden. Selbstverständlich muss den Unternehmen die Möglichkeit eingeräumt werden, gegen schwarze Schafe vorzugehen. Der Einsatz von Data Mining und der damit verbundene Eingriff in das grundgesetzlich geschützte Persönlichkeitsrecht der Beschäftigten erscheint jedoch unverhältnismäßig, hier wird mit »Kanonen auf Spatzen geschossen«.

Ein Fehlbetrag von 1 Milliarde Euro durch Unterschlagungen an der Kasse ist kein Pappenstiel. Dass die Rasterfahndung bei dieser hohen Summe übertrieben ist, wird, angesichts einer Pressemeldung des Bundesverbandes der Verbraucherzentrale (vzbv) deutlich: »Fertigpackungen – Verbraucher zahlen bis zu 1 Milliarde Euro zu viel«. Weiter heißt es dort, dass durch zu gering gefüllte Packungen die Verbraucher bis zu 1 Milliarde Euro zu viel bezahlt haben. Das ergebe sich aus der bundesweiten Statistik der Füllmengenkontrollen an Fertigpackungen der Eichbehörden der Länder. Danach sei bei rund zehn Prozent aller Lebensmittel weit weniger in der Packung als auf dem Etikett angegeben. »Viele Unternehmen kassieren die Verbraucher ab, indem sie die Verpackungen systematisch unterfüllen«, kritisierte vzbv-Vorstand Prof. Dr. Edda Müller.[33] Eine klare Stellungnahme oder Maßnahmen, was der Handel zukünftig bei dieser fehlenden »Fertigpackungs-Milliarde« zu tun gedenkt, steht noch aus – vergleichbare Anstrengungen wie bei der »Kassen-Milliarde« sind noch nicht angekündigt worden. Zur Aufdeckung und Verhinderung von Unterschlagungen und Betrug durch Beschäftigte müssen die Unternehmen etwas tun, das bestreiten auch nicht die Betriebsräte – dies ist selbstverständlich auch im Interesse der Verbraucher. Aber auch ohne Data Mining hat der Handel eine ganze Menge von Maßnahmen zur Verfügung: So gibt beispielsweise das Selbsthilferecht[34] dem Filialleiter oder dem Sicherheitsdienst die Möglichkeit bei Straftaten durch das Personal selbst, das heißt ohne staatliche Hilfe, ohne Polizei, Maßnahmen zur Wahrung der Eigentumsinteressen einzuleiten. Die herrschende Meinung gesteht den Verantwortlichen auch das Recht zur vorläufigen Festnahme[35] zu, 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 an der Tagesordnung.[36] Die Methoden der Rasterfahndung haben im Arbeitsleben nichts zu suchen. So sinnvoll es unter betriebswirtschaftlichen Gesichtspunkten sein mag, möglichst vollständige Mitarbeiterprofile zu erstellen, um die Inventurdifferenzen zu reduzieren oder so genannte Minderleister zu finden, so schwerwiegend sind dagegen die bestehenden rechtlichen Bedenken.

Die Grundrechte, auch das Grundrecht auf informationelle Selbstbestimmung, gelten zwar unmittelbar nur im Verhältnis Bürger-Staat, dennoch ist die Informationelle Selbstbestimmung auch dort zu achten, wo private Daten Verwendung finden. Damit gilt das Verbot der Anfertigung von Persönlichkeitsprofilen auch für das Verhältnis zwischen Privaten, also zwischen Arbeitgeber und Arbeitnehmer. Wenn die Eingriffe in die Grundrechte schon dem Staat nicht erlaubt sind, dann erst recht nicht privatwirtschaftlichen Unternehmen, die nicht aus öffentlichen, sondern aus kommerziellen Interessen handeln.[37]

In diesem Sinne äußerten sich auch die Datenschutzbeauftragten des Bundes und der Länder. Sie heben hervor, dass »gläserne Beschäftigte« durch Videoüberwachung, Kontrolle der Email- und Internetnutzung und durch Erstellung von Persönlichkeitsprofilen nicht entstehen dürfen.[38] Ein unzulässiger Eingriff in die Persönlichkeitsrechte kann auch nicht durch eine Betriebsvereinbarung »geheiligt« werden.[39] Für Betriebsräte gibt es hier keinen Verhandlungsspielraum – diese Technologie verletzt die Persönlichkeitsrechte der Arbeitnehmer und Arbeitnehmerinnen, dem kann der Betriebsrat nicht zustimmen!

Fazit

Bereits 1987 setzte sich das BAG mit der Frage auseinander, welche Rolle das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG spiele und stellte dabei fest, dass die Regelungsbefugnis der Betriebsparteien beim Persönlichkeitsschutz der Arbeitnehmer ihre Grenzen findet. Weil Arbeitgeber und Betriebsrat »die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern«[40] haben, kann die Mitbestimmung auch nur der Verwirklichung dieses Zieles dienen. Beide Betriebsparteien haben dazu beizutragen, dass rechtlich unzulässige Eingriffe in die Persönlichkeitsrechte unterbleiben und dass im Prinzip zulässige Eingriffe jedenfalls auf das betrieblich erforderliche Maß beschränkt werden. Mit anderen Worten, unzulässige Überwachungs-

33 Pressemeldung 28.11.2002, www.vzbv.de.
34 § 229 bis § 231, § 859 und § 860 BGB.
35 § 127 StPO und § 229 BGB.
36 Vgl. Seefried, Die Zulässigkeit von Torkontrollen, AiB 1999, S. 428.
37 Vgl. Wittich a. a. O.
38 Vgl. Pressemitteilung der Datenschutzbeauftragten, für einen gesetzlichen Arbeitnehmerdatenschutz vom 27.2.2002, http://www.bfd.bund.de.
39 Vgl. Schierbaum, Personal-Informations-Systeme: die rechtlichen Rahmenbedingungen, CF 8–9/2000, S. 22.
40 § 75 Abs. 2 BetrVG.

maßnahmen werden auch durch eine eventuelle Zustimmung des Betriebsrats – etwa im Rahmen einer Betriebsvereinbarung – nicht zulässig.[41] Bei der Frage der Verletzung des Persönlichkeitsrechts haben Arbeitgeber und Betriebsrat nämlich Grenzen zu beachten, dies hat das BAG jüngst in einem Fall zur Überwachung durch Videokamera entschieden. In diesem Zusammenhang stellte das Gericht einige Überlegungen an, die über den damals konkreten Fall hinaus gingen und allgemeine Bedeutung haben,[42] auch für Loss Prevention, Fraud Detection, Sales-Audit von SAP, McKillroy und wie sie noch heißen. Eine technische Überwachung am Arbeitsplatz ist nach Ansicht des BAG nur bei ganz konkreten Verdachtsfällen möglich, eine vorbeugende Überwachung der überwiegend ›unschuldigen‹ Belegschaft mag zwar effizient sein, sie ist aber nicht zulässig.[43] Die grundsätzlichen Erwägungen zum Datenschutz, die vor einiger Zeit wieder von den Gerichten bei der Überprüfung der Rasterfahndung im Zusammenhang mit der Verfolgung der potentiellen Terroristen angesprochen worden sind, müssen auch als Mindestmaßstab für Arbeitnehmerinnen und Arbeitnehmer gelten. Die datenschutzrechtlichen Bedenken gegen den Einsatz von Loss Prevention und vergleichbaren Systemen werden vor dem Hintergrund des relativ kostengünstigen Einsatzes deutlich. Da bereits die technische Infrastruktur weitgehend in den meisten Einzelhandelsketten vorhanden ist, können mit vergleichsweise geringen Kosten hohe Erfolge erzielt werden. Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarung verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Programm entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar.[44] Nach den Grundsätzen des Datenschutzgesetzes hat sich die Gestaltung und Auswahl von der Datenverarbeitung an dem Ziel auszurichten, keine oder so wenig wie möglich personenbezogene Daten zu verarbeiten. Die Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Die absolute und kontinuierliche Analyse von personenbezogenen Leistungs- und Verhaltensdaten mittels Data Mining und das Erstellen von Persönlichkeitsprofilen sind als unzulässige Grundrechtseingriffe anzusehen. Diese Art des Kassenmanagements ist also weder mit dem Grundsatz der »informationellen Selbstbestimmung« noch mit dem »Grundrecht auf Datenschutz« zu vereinbaren. Die Einführung und Anwendung von Data Mining stellt einen unzulässigen Eingriff in die Persönlichkeitsrechte der Arbeitnehmerinnen und Arbeitnehmer dar.

Matthias Wilke ist Berater bei der Datenschutz- und Technologieberatung in Kassel, E-Mail: Info@dtb-kassel.de

41 BAG v. 15.5.1991 – 5 AZR 115/90 und vgl. auch Grimberg, Grenzen für den Betriebsrat! CF 9/1993, S. 30.
42 Vgl. Wilke; Videoüberwachung, AiB 2005, 225 ff.
43 Vgl. BAG v, 29.6.2004 – 1 ABR 21/03.
44 Vgl. ebenda.

Die Tücken der Zusammenarbeit

Vom Umgang zwischen Arbeitgeber und Betriebsrat

Sie ist in aller Munde – und wird vor allem auch von Arbeitgebervertretern gerne angeführt, wenn der Betriebsrat sich in ihren Augen nicht »genehm« verhält. Die Rede ist von der so genannten vertrauensvollen Zusammenarbeit. Sie soll das Verhältnis zwischen Arbeitgeber und Betriebsrat prägen. Doch was ist eigentlich unter diesem oft strapazierten Begriff zu verstehen und wie kann die vertrauensvolle Zusammenarbeit betriebliche Wirklichkeit werden?

Grundsätze der Zusammenarbeit

Arbeitgeber und Betriebsrat arbeiten unter Beachtung der geltenden Tarifverträge vertrauensvoll und im Zusammenwirken mit den im Betrieb vertretenen Gewerkschaften und Arbeitgebervereinigungen zum Wohl der Arbeitnehmer und des Betriebs zusammen.[1] Die Betriebsparteien sollen mindestes einmal im Monat zu einer Besprechung zusammenkommen. Sie haben über strittige Fragen mit dem ernsten Willen zur Einigung zu verhandeln und Vorschläge für die Beilegung von Meinungsverschiedenheiten zu machen.[2] Maßnahmen des Arbeitskampfes zwischen Arbeitgeber und Betriebsrat sind unzulässig.[3] Das hört sich ja toll an, was der Gesetzgeber sich da überlegt hat, um zwei Parteien, die unterschiedliche Interessen verfolgen, zu ver-

1 § 2 Abs. 1 BetrVG.
2 § 74 Abs. 1 BetrVG.
3 § 74 Abs. 3 BetrVG.