Sie werden beobachtet

Elektronische Überwachung und Kontrolle am Arbeitsplatz

Verfasser : Andrew Bibby
Titelblattgestaltung : Jane Shepherd

UNI/GS/06-2006/0035/DE

Marta arbeitete für eine große multinationale Versicherungsgesellschaft. Zumindest bestand ihre Aufgabe darin, für sie Versicherungsforderungen zu bearbeiten. Die Versicherungsgesellschaft selbst hatte diese administrative Funktion vor zwei Jahren an ein Fachunternehmen ausgelagert, welches Leiharbeitnehmer beschäftigte: genauer gesagt, so war Martas neuer Arbeitgeber eine Leiharbeitagentur.

Marta hatte für die Agentur seit beinahe einem Jahr gearbeitet. Diese war eine von vielen Stellen, die sie seit ihrem Schulabschluss im Alter von 18 Jahren hatte. Ihr Arbeitsplatz befand sich in einem Bürogebäude in einem gewöhnlichen Industriepark. Täglich zog sie ihren Personalpass am Hautpeingang bei der Rezeption und ging zu ihrem Schreibtisch nach oben. Offiziell arbeitete sie in einem Team, aber die Gesichter an den benachbarten Schreibtischen wechselten ständig. Sie brauchte ohnehin keinen Kontakt mit ihnen zu haben. Die von ihr zu bearbeitenden Schadensfallsdokumente kamen automatisch an ihren Computer und sie hatte diese lediglich durch zu arbeiten. Jeder Fall sollte im Durchschnitt in 6 Minuten und 42 Sekunden fertig bearbeitet sein. Der Computer wussten genau, wie gut sie arbeitete und wenn sie ich Ziel am Ende der Woche nicht erreicht hatte, bekam sie es von ihrem Vorgesetzten zu hören.

Es war ein monotoner Job, aber zumindest ein Job: sie erwartete ihr erstes Kind und brauchte das Einkommen. Die ersten Monate der Schwangerschaft waren schwierig gewesen und sie zwang sich jeden Tag zur Arbeit, obwohl sie mehr Pausen gebraucht hätte. Sie meinte, ihr Bestes zu geben.

Das Unternehmen aber sah das anders. An einem Freitagnachmittag wurde sie von ihrem Schreibtisch ins Büro eines der Vorgesetzten gerufen. Dieser hatte eine Menge von Computerausdrucken vor sich liegen. „Wir müssen Sie entlassen“, sagte er. “Wir haben geprüft, wie oft sie an einem Vormittag Pause gemacht haben. Sehen sie her, vier Pausen an einem einzigen Vormittag letzte Woche. Das ist zu viel.“

Hier auf dem Ausdruck stand nach einzelnen Minuten aufgeschlüsselt genau im Detail beschrieben, was sie in den letzten Wochen am Arbeitsplatz gemacht hatte, auch jedes Mal, wenn sie ihren Schreibtisch verlassen hatte. Marta war verblüfft. „ Ich wusste nicht, dass ich so überwacht werde. Der Vorgesetzte blickte von seinen Papieren auf. „Wirklich nicht? sagte er. “ Wir wissen genau, wo jeder in unserem Gebäude sich zu jedem Zeitpunkt befindet. Ihr Personalnamensschild ist mit einem Funkgerät ausgerüstet. Das können übrigens sie gleich hier abgeben, denn das brauchen sie jetzt nicht mehr.“

Marta Redding ist nicht ihr wirklicher Name, aber das Ereignis authentisch.

Vorwort

Niemand lässt sich gerne heimlich beobachten. Bei vielen Arbeitnehmern hinterlässt das Gefühl, heimlich beobachtet zu werden, ein schlechtes Gefühl. Es fördert wohl kaum das Vertrauen, auf dem erfolgreiche Arbeitsbeziehungen aufgebaut sind.

Leider zeigt dieser Bericht, dass es eine Reihe von technologischen Gadgets und Dingern gibt, die Arbeitgeber einsetzen können, um ihre Mitarbeiter einem hohen Maß an elektronischer Überwachung und Kontrolle zu unterziehen.

Beispielsweise die winzigen Funkfrequenzidentifizierungs-Etiketten, (Radio Frequency Identification (RFID) tags), mit deren Hilfe man feststellen kann, wo eine Person sich jeweils während des Tages aufhält; diese können auch in Personalkarten integriert oder in Arbeitsuniformen eingenäht werden.

RFID und andere Suchtechnologien, wie z.B. GPS-Satellitensysteme, können im Grunde genommen bedeuten, dass jemand nie wirklich das Gefühl haben kann, frei zu machen, auch nicht in Pausen und in Freistellungsphasen.

Ebenso gibt es die Video-Überwachung (heute weitgehend verbessert durch Software zur Analyse von digitalen Bildern), Tastaturkontrollen und die Überwachung von Telefongesprächen, E-Post und eine Reihe von anderen Formen der Kontrolle, die einzelnen Arbeitnehmern das Gefühl der ständigen Überwachung geben können.

Diese Technologie ist weit davon entfernt, menschliches Potential freizusetzen und eine “Wissensgesellschaft” aufzubauen, sondern sie scheint eher die Fähigkeit zu beeinträchtigen, am Arbeitsplatz unabhängig zu denken und zu arbeiten. Gleichzeitig erleben wir, dass das grundlegende Menschenrecht auf Anerkennung und Würde bei der Arbeit gefährdet wird.

Natürlich ist die neue Technologie nicht an sich schlecht und ablehnenswert. Dieser Bericht will vielmehr auf einige Formen des Missbrauchs hinweisen, die in einzelnen Fällen vielleicht durchaus darauf zurückzuführen sind, dass

Arbeitgeber sich für Lösungen entschieden haben, die ihnen durch Software-Programme geboten werden, ohne dass sie wirklich näher darüber nachdachten.

UNI ist entschlossen, zu einem Abbau dieser Praktiken beizutragen und unterstützt gleichzeitig die Förderung der besten Praxis.

Philip J. Jennings
UNI General Sekretär

Einführung

In den letzten Jahren war ein starker Anstieg an elektronischer Überwachung und Kontrolle am Arbeitsplatz zu beobachten, wobei auch neue und hoch entwickelte digitale technologische Instrumente zum Einsatz gelangten.

Diese Technologien können positiv in einer Form eingesetzt werden, die das Leben sowohl für Arbeitgeber als auch für Arbeitnehmer erleichtert. Allerdings werden sie häufig in einer nicht unbedingt harmlosen Form eingesetzt. In einigen Fällen erfolgte die Verwendung durch Arbeitgeber ohne gründliches Nachdenken (‘Die Software bringt uns dazu’), und in anderen Fällen kommt der Anstoß von der (im Allgemeinen nicht fundierten) Vorstellung, dass streng überwachte Arbeitnehmer produktiver arbeiten. Es gibt Arbeitgeber, die einfach die Gelegenheit nutzen wollen, passive, stillschweigende Arbeitnehmer zu schaffen, die weniger in der Lage sind, ihre Rechte auf gewerkschaftliche Organisation und Vertretung auszuüben.

Beinahe alle UNI Sektoren sind in irgendeiner Form direkt davon betroffen.

Dieser Bericht befasst sich detailliert mit sieben Formen der derzeit an Arbeitsplätzen durchgeführten elektronischen Überwachung und Kontrolle:

- Funkfrequenz-Identifikation (RFID)
- Tragbare Datengeräte und Voice-Technologie
- Überwachung über Satelliten und Mobiltelefone
- Video-Überwachung
- Email und Web-Überwachung, Tastaturkontrollen
- Überwachung der Telefonanrufe und Arbeit in Callcenters
- Überwachung durch Biometrie und Implantate

Der Bericht versucht ferner, einige der Auswirkungen der elektronischen Überwachung und Kontrolle auf Gewerkschaften zu untersuchen und beschäftigt sich besonders mit den Auswirkungen auf die Rekrutierungs- und Organisationsarbeit, sowie Arbeitsschutz, den Schutz des Privatlebens der Arbeitnehmer und die Ausarbeitung eines Programms auf der Grundlage der Vorstellung von anständiger Arbeit der Internationalen Arbeitsorganisation. Er

enthält eine Reihe von konkreten Vorschlägen für zukünftige Aktionen für UNI und ihre Mitgliedsverbände.

1. Funkfrequenz-Identifikation (RFID)

Die Funkfrequenz-Identifikation ist dabei, eine der überzeugendsten neuen Technologien zu werden. RFID-Etiketten werden bereits vielfach eingesetzt; unter anderem für elektronische Zahlkarten, die in vielen Ländern für die Bezahlung von Mautgebühren, Bus- und Metrokarten verwendet werden, sowie elektronische Sicherheitsetiketten für Kleider im Einzelhandel, um Ladendiebstählen vorzubeugen, intelligente Gepäckschilder, die bereits in einigen Flughäfen eingesetzt werden, und auch elektronische Zeitchips für Marathonläufer. Im Handel werden RFID-Etiketten vielfach in der Logistik eingesetzt, um die Lagerbestände zu organisieren; die größten Einzelhändler wie beispielsweise Wal-Mart fordern sie bei ihren Zulieferern.

RFID- ‘Etiketten’ sind winzige Mikrochips, die manchmal nur sandkorngroß sind und spezifische Daten zur Identifizierung des etikettierten Objekts enthalten. Diese Etiketten sind mit einer kleinen Antenne bestückt und durch einen entfernt liegenden RFID-Leser ablesbar. Je nach verwendeter Funkfrequenz und Art des Etiketts, können RFID-Etiketten in einigen Fällen in Entfernungen von bis zu mehreren Kilometern abgelesen werden, obwohl sie eher in Situationen mit kürzeren Übertragungsentfernungen zur Anwendung kommen. Etiketten können passiv sein (sie werden beim Ablesen aktiviert) oder aktiv und mit einer eigenen Mikro-Batterie und einem Sender ausgerüstet sein.

Der Preis für die billigsten RFID-Etiketten liegt mittlerweile bei gut unter 50 US Cents, was den massiven Einsatz dieser Technologie immer mehr möglich macht. Der Einzelhandel rechnet damit, dass RFID-Etiketten die Strichkode in den Supermarktregalen schon bald ersetzen werden. Der Unterschied besteht darin, dass die Strichkodes für jede Verkaufsstelle generisch gelten, aber jedes *einzelne* Stück im Verkauf einen eigenen einzigartigen RFID-Identifikator erhalten kann. In mehreren Ländern werden bereits entsprechende Pilotversuche durchgeführt

Diese Verwendung von RFID's ist umstritten. Eine aktive Verbraucherkampagne in den USA unter der Bezeichnung CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) behauptet, dass man mit RFID-Etiketten das Verbraucherverhalten von einzelnen Einkäufern überwachen kann. Laut CASPIAN bieten diese "Spion-Chips" sehr gut die Möglichkeit, in das Privatleben des einzelnen Menschen einzudringen.[1]

RFID Chips können sowohl Menschen als auch Gegenstände orten und identifizieren. Sie sind auch bereits in Ländern wie den USA und Japan im Einsatz, um die Bewegungen älterer Menschen in Altersheimen, von Patienten und Personal in Krankenhäusern, Säuglingen in Entbindungsstationen und Kindern in Schulen zu überwachen. Letzteres erwies sich ebenfalls als umstritten. In einer Grundschule in der Nähe von Sacramento in Kalifornien forderten die Eltern eine Schule auf, den Einsatz von RFID-Etiketten zur Ortung von Schulkindern einzustellen[2].

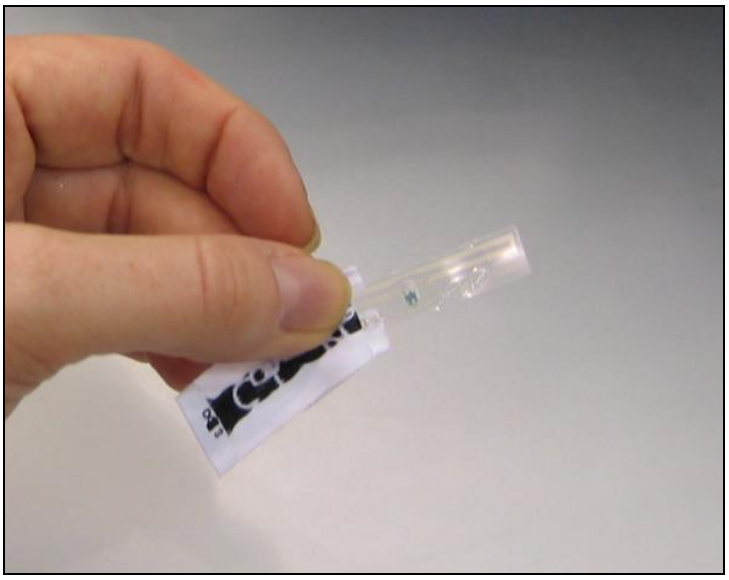
Am Arbeitsplatz[3] konzentrieren sich die Einwände gegen RFID vermutlich gegen zwei Bereiche: Erstens führt die Kennzeichnung von Waren und Gegenständen mit RFID zu einem Verlust beruflicher Fähigkeiten an gewissen Arbeitsplätzen und zu Arbeitsmethoden, wo die Arbeit von Beschäftigten immer mehr durch technologische Vorgaben kontrolliert wird. Wir gehen im Zusammenhang mit Veränderungen bei der Lagerarbeit später noch näher darauf ein.

Sehr viel wichtiger ist die Möglichkeit, durch RFID Arbeitnehmer während des gesamten Arbeitstages (und sogar darüber hinaus) zu orten. In einzelnen Situationen mag dies durchaus positiv sein; so geht beispielsweise aus einem Bericht hervor, dass Bergarbeiter in Südafrika und Chile ihre Atemgeräte mit RFID-Tags ausgerüstet haben, damit sie in Notsituationen gefunden werden können[4]. Allerdings bilden diese Arten von positivem Einsatz wohl eher die Ausnahme.

Nachstehend ein Bericht über den Einsatz von RFID in Kombination mit anderen Formen der elektronischen Überwachung, den das japanische Elektronikunternehmen Omron in seinem Werk in Kioto eingeführt hat:

“Omron’s neues Produktionsmanagementsystem verwendet RFID -Tags, Video-Kameras, Zugangs-/Sicherheitskontrollsysteme, usw., um zu kontrollieren, wie viel die Arbeitnehmer zur Produktion beitragen. Die Beschäftigten sind gezwungen, RFID-Etiketten zu tragen, damit das System ihren Standort und auch ihren Arbeitsleistung kontrollieren kann. Durch diese Schritte verbessern sich die Einteilung der Arbeiter und die Produktqualität.[5]”

Eine Art, Arbeiter zu orten besteht darin, RFID-Etiketten in Uniformen einzuheften. So können beispielsweise RFID-Tags an Etiketten angeheftet werden. (Dieses Bild zeigt die Rückseite einer kleinen Calvin Klein Etikette mit einem durchsichtigen RFID-Tags); die RFID Industrie arbeitet derzeit daran, den eigentlichen Textilfasern eine Funktion als RFID Antennen zuzuordnen. Diese Art von Kleidung kann ganz normal gewaschen werden ohne die RFID-Etiketten zu zerstören.



So arbeiten beispielsweise Kellnerinnen in einem Kasino von Las Vegas jetzt in Uniformen mit RFID Etiketten, um bei der Arbeit kontrolliert werden zu können. Einer der Chefs im Unternehmen berichtete, dass bereits an einem der ersten Tage ein Mitarbeiter wegen „Nichtstun“ bestraft wurde[6].

Die im Kasino des riesigen Star City Komplex in Sydney, Australien, beschäftigten Mitarbeiter benutzen ebenfalls in ihre Uniformen eingenähte RFID-Chips[7]. Dies scheint allerdings vorwiegend wegen der Kleiderordnung der Fall zu

sein und hat sich (obwohl anfangs vom Personal als bedenklich betrachtet) allgemein als akzeptierbar erwiesen. Die Mitarbeiter von Star City sind über das UNI-Mitglied LHMU
(Liquor, Hospitality and Miscellaneous Union) gewerkschaftlich organisiert.. LHMU weist darauf hin, dass die Uniformen zu Hause nicht getragen werden, und somit kann das Personal in der Freizeit nicht beobachtet werden kann.

Man braucht allerdings nicht ein RFID-Chip in der Uniform zu haben, um während des gesamten Arbeitstages auffindbar zu sein. Die am meisten verwendeten RFID Chips befinden sich in Namensschildern und ID-Ausweisen, die zur Kontrolle beim Betreten von Gebäuden und Räumen zu tragen sind.

Obwohl man sie heute an vielen Arbeitsplätzen als normale Sicherheitseinrichtungen betrachtet, bieten mit RFID bestückte ID-Schilder in Wirklichkeit Angaben über viel mehr als nur Eingangssysteme. Es ist üblich, diese erhobenen Daten mit anderen Datenbanken im Unternehmen zu verknüpfen, auch mit denen der Personalabteilung und Lohnabrechnung. Eine IT-Gesellschaft bietet beispielsweise Software an, mit deren Hilfe die Eingangssystemdaten für eine Reihe von Berichten verwendet werden können, „einschließlich Berichte zur Anwesenheit, Stempelkarten, Lohn, Überstunden, Lohnsstufenzusammenfassung, Abwesenheit, Namensaufruf, Mitarbeiterliste, Bericht über zu frühes Verlassen des Arbeitsplatzes….“[8].

Die RAND Corporation untersuchte vor kurzem die Verwendung von Daten aus RFID -Namensschildern im Rahmen einer Erhebung in sechs Unternehmen in den USA. Es wurde festgestellt, dass praktisch keiner der Beschäftigten über die Art des Einsatzes dieser Technologie informiert war. Die Erkenntnisse lassen sich wie folgt zusammenfassen:

“Unternehmen verwenden RFID-Zutrittskarten zum Arbeitsplatz für mehr als nur zum Türen öffnen (z.B. zur Durchsetzung von Vorschriften über das Verhalten am Arbeitsplatz). Eine ausdrückliche und schriftlich festgelegte Politik über die Art der Anwendung solcher Karten gibt es im allgemeinen nicht, und den Mitarbeitern wird nicht mitgeteilt, welche Politik für diesen Bereich gilt. Der Einsatz dieser Art von Systemen hat das bisherige Gleichgewicht zwischen persönlicher Zweckmäßigkeit, Sicherheit am Arbeitsplatz und dem Privatleben des Einzelnen verändert und zum Verlust der

„praktisch bedingten Undurchsichtigkeit“ geführt. Solche Systeme schaffen auch Probleme im Zusammenhang mit einer sinnvollen Durchführung fairer Informationspraktiken.”[9]

Die Forscher von RAND waren deutlich überrascht und verstört über den Mangel an einer schriftlich festgelegten Politik oder Informationen an die Mitarbeiter zu diesen Praktiken, und sie kommen in ihrer Untersuchung zu folgender Schlussfolgerung: „Jeder Leser, der eine RFID-Zutrittskarte verwendet, sollte sich verunsichert fühlen, nachdem er diese Ergebnisse gesehen hat.“

Ein erstes Gespräch über die Auswirkungen von RFID auf das Privatleben und den Datenschutz fand 2003 im Rahmen der Internationalen Konferenz der Beauftragten für Datenschutz und Privatleben[10] statt, und die Arbeitsgruppe für Datenschutz der EU beschäftigte sich ebenfalls mit dieser Frage [11]. Letztere fordert dazu auf, RFID Kontrollen nach den Grundsätzen des Datenschutzes durchzuführen, einschließlich einer vorherigen Bekanntgabe, dass RFID-Etiketten im Einsatz sind und das Recht der betroffenen Person auf Einsicht in die aufgezeichneten persönlichen Angaben. Allerdings ist deutlich festzustellen, dass in beiden Fällen die Ausarbeitung einer klaren internationalen Politik noch nicht sehr weit gediehen ist.

Auch die Gewerkschaften haben begonnen, sich mit der Frage der RFID-Ortung zu beschäftigen.

 Die britische Gewerkschaft GMB kritisierte im Juli 2005 die EU Arbeitsgruppe für Datenschutz, sie habe das Problem des Schutzes der Privatsphäre und die Auswirkungen der Ortung von Personen Arbeitsplatz durch RFID nicht in Angriff genommen und forderte auf, die Verwendung von RFID bei Arbeitnehmern in der EU zu verbieten. Die Gewerkschaft erklärte, dass dadurch die Rechte von Arbeitnehmern auf Schutz des Privatlebens unterlaufen werden. [12]

 ver.di (Deutschland) schlägt folgende Checkliste vor, wenn RFID-Technologie am Arbeitsplatz eingesetzt wird[13]:

- Erhalten die Mitarbeiter rechtzeitig die notwendige Information über Pläne des Unternehmens, RFID-Technologie einzuführen?

- Besteht eine Gefährdung der Gesundheit oder gibt es andere Gefahren beim Einsatz von Funkfrequenzen, Scannern oder photoelektrischen Sperren am Arbeitsplatz?
- Wie wirkt sich die Technologie auf den Arbeitsablauf aus, und wie verändert sie konkret die Arbeitsbedingungen und die Arbeitsumwelt?
- Wie wirkt sich die Einführung der RFID-Technologie auf die Rationalisierung aus?
- Werden die Mitarbeiter entsprechend geschult im Umgang mit RFID?
- Welche Daten, vor allem persönliche Daten, werden wo und wie lange gespeichert?
- Werden Daten im Verlauf der Aufzeichnung zur Verhaltenskontrolle und Leistungskontrolle der Mitarbeiter verwendet?
- Wer garantiert, dass solche Daten nicht falsch verwendet werden?
- Wie können sich Arbeitnehmer selbst gegen einen Missbrauch wehren?

UNI Handel hat auch eine Erklärung über die Einführung von RFID verabschiedet, in der ein eingehender sozialer Dialog mit den Unternehmen vor Einführung dieser Technologie gefordert wird[14].

2. Tragbare Datengeräte und Voice-Technologie

RFID und die herkömmlichen Strichkodes werden zur Identifikation von Produkten vor allem in Lagerhäusern im Einzelhandel mit neuen Formen von Voice-Technologie und tragbaren Datengeräten eingesetzt, und schaffen so ein Arbeitsumfeld, in dem die Arbeiter immer mehr zu Robotern werden.

Die Gewerkschaft GMB erlebte Mitte 2005 sehr starkes Interesse bei den Medien, als sie auf die Arbeitsbedingungen in einigen britischen Lagerhäusern verwies, die ihrer Meinung nach wie Batteriehühnerfarmen betrieben wurden: "Die Rolle des Arbeiters besteht nur noch darin, die Befehle eines Computers auszuführen. Diese Geräte berechnen, wie lange es dauert, sich von einem Teil des Lagers in einen anderen Teil zu bewegen, welche Pausen dem Arbeiter zustehen und wie lange ein Toilettenbesuch dauert. Von diesen vorgegebenen Zeiten darf er nicht abweichen. Diese bei Lieferungen von Lebensmitteln an Supermärkte verwendeten Geräte haben aus Arbeitern Helfer von Computern gemacht anstatt umgekehrt.[15]"

Als typisches Beispiel erwähnte GMB ein Lager in Wales von 12.000 m2, welches 240 Einzelhandelsgeschäfte beliefert. Die Arbeiter, welche die Produkte holen, sind mit tragbaren Computern am Handgelenk oder Unterarm ausgerüstet, die an einen Scanner angeschlossen sind, der am Zeigerfinger festgemacht wird. Dieses Gerät wird vom IT-Hersteller Symbol produziert und wiegt 320 – 350 Gramm (siehe Bild unten)[16].

Laut Symbol erhält „das am Handgelenk befestigte Endgerät die Suchanweisungen über das drahtlose LAN Host System [des Unternehmens]. Wenn der leere Wagen in den Abholbereich kommt, gibt der Lagerarbeiter den entsprechenden Strichkode ein und das LCD-Endgerät gibt an, in welches Regal er sich bewegen soll und von welchem Standort er welche Produkte abholen soll. Wenn der Arbeiter dann am Abholstandort angekommen ist, scannt er zuerst den Strichcode am Ende des Ganges ein. So wird festgestellt, ob er sich im richtigen Gang des Lagers befindet. Dann scannt er einen anderen Strichkode am Produktstandort ein, um festzustellen, dass er sich an der richtigen Stelle befindet. Zuletzt scannt er dann beim Verladen in den Wagen jedes einzelne Produkt ein.[17] ”Somit“, stellt GMB fest, “ führt der Mensch nur noch jene Aufgaben aus, die noch nicht automatisiert sind”.

Es gibt derzeit zwei Arten von tragbaren Datengeräten. Geräte, die (wie das Bild zeigt) am Handgelenk oder am Finger getragen werden und/oder Geräte, die am Kopf oder am Gürtel befestigt sind. Sie werden oft mit Voice-Technologie verbunden, wodurch die Lagerarbeiter mit Kopfhörern ausgerüstet werden, über die sie mündliche von Computern produzierte Anweisungen erhalten, die ihnen

sagen, welche Produkte sie zu suchen haben. Voice-Technologiesysteme arbeiten meistens mit Auftragsverwaltungs- und Lagerhaltungs-Software-Programmen, wobei Daten aus diesen Programmen in Sprache umgewandelt werden[18].

Auf mögliche Auswirkungen auf Gesundheit und Sicherheit, die sich bei der Anwendung dieser Technologie ergeben, verwiesen sowohl GMB als auch Professor Michael Blakemore, ein britischer Wissenschaftler, der die Gewerkschaften in dieser Frage beraten hat. Blakemore behauptet, dass trotz gewisser Probleme mit der früheren Technologie, die zu Schäden durch repetitive Belastungen (RSI) führte, bisher die möglichen Auswirkungen auf die Gesundheit durch diese neuen Geräte nur in begrenztem Ausmaß erfasst werden. [19].

Diese Art von Lagerabrufsystemen haben nicht nur eine Automatisierung des Arbeitsvorganges zur Folge, sondern sie eignen sich auch für die Überwachung von Arbeitnehmern. Blakemore kommentiert die Aussage eines Unternehmens: “Es kann auch aus der Sicht der Unternehmer sehr leicht eingesetzt werden, da es sich hervorragend eignet, um festzustellen, wo sich jemand befindet und was er gerade tut ”.

3. Standortbestimmung über Satelliten und Mobiltelefon

Neben RFID, gibt es auch verschiedene andere technologische Lösungen, um den jeweiligen Standort von Objekten oder Menschen einigermaßen genau bestimmen zu können.

Die Satelliten-Navigation basiert derzeit auf dem amerikanischen GPS-System (Global Positioning System). GPS benutzt ein Netzwerk von Satelliten, die ursprünglich für militärische Zwecke eingesetzt wurden und die auch heute noch vom Pentagon in den USA betrieben werden. Jeder Satellit überträgt laufend Angaben zur Feststellung der Position. GPS-Empfänger analysieren diese Signale und durch einen Vergleich der Übertragungen von vier oder mehr

Satelliten können die präzise Position und die Meereshöhe festgestellt werden. (Mindestens vier Satelliten sollten für jeden Empfänger jederzeit ‘sichtbar’ sein.)

Die Europäische Union entwickelt derzeit ihr eigenes konkurrierendes Satellitennavigationssystem, bekannt unter dem Namen Galileo; der erste Satellit für das Galileo Netzwerk wurde im Dezember 2005 in Umlauf gebracht.

Die Mobiltelefontechnologie bietet ebenfalls die Möglichkeit der Standortbestimmung an Orten, wo aktivierte Mobiltelefone getragen werden. Es funktioniert durch eine Feststellung der Entfernungen zwischen Handy und dem nächst gelegenen Basisübertragungsmasten, die gemeinsam das zellulare Netzwerk bilden, auf dem die Mobiltelefontechnologie aufgebaut ist. Besonders in Stadtgebieten, wo die Basisstationen eng beisammen liegen, ist es möglich, eine genaue Standortbestimmung von normalerweise 10 bis 25 m vorzunehmen. Die Telefone müssen nicht aktiv im Einsatz sein, um einen Standort bestimmen zu können.

Diese beiden Technologien sind miteinander verbunden, da Mobiltelefone und persönliche Zeitplaner immer häufiger über GPS laufen. In Japan funktionieren derzeit beispielsweise 20% aller Mobiltelefone als GPS-Empfänger[20].

Sowohl GPS als auch zellulare Standortbestimmungsdienste werden bereits kommerziell genutzt, häufig im Zusammenhang mit digitalen Kartendiensten. GPS wird immer häufiger für Navigationssysteme in beispielsweise Kraftfahrzeugen eingesetzt. Handybenutzer interessieren sich für die Möglichkeit von “standort-basierten Diensten” (beispielsweise die Übertragung an Telefonbenutzer einer Standortangabe eines Fast Food Restaurants, von Mini-Banken, Geldautomaten oder gar Freunden und Bekannten).

Am Arbeitsplatz können Standortermittlungen über GPS und Mobiltelefone ebenso wie die anderen technologischen Mittel in einer Form angewendet werden, die den Arbeitnehmern das Leben erleichtern. Zum Beispiel:

- Die Ortung von Fahrzeugen kann für die Fahrer von Sicherheitstransporten, die das Ziel von Raubüberfällen sein können, mehr Sicherheit bedeuten.

- Geografische Ortsbestimmungen können für mobile Arbeitnehmer erhöhte Sicherheit bedeuten; dies kann besonders bei Personen der Fall sein, die allein an einsam gelegenen oder potentiell gefährlichen Orten oder nachts im Einsatz sind.
- Ortung kann auch dazu beitragen, mobile Arbeitskräfte bei schlechtem Wetter zu finden.

Leider liegen ausreichend Nachweise vor, dass die Ortung durch Arbeitgeber wesentlich weniger positiv ausgeübt wird. Hier ein Fall, den das Nationale Institut für Arbeitsrecht der USA zitiert:

Howard Boyle, Leiter einer Herstellerfirma von Sprinkleranlagen in Woodside, N.Y. gab seinen Mitarbeitern Mobiltelefone, ohne ihnen mitzuteilen, dass sie mit GPS ausgerüstet waren. Herr Boyle kann zu jedem Zeitpunkt feststellen, wo sich seine Mitarbeiter befinden, auch während der Pausen und nach Feierabend. „ Sie brauchen das nicht zu wissen" erklärte Herr Boyle. „Ich kann sie anrufen und fragen: Wo sind sie denn? Gleichzeitig sehe ich auf den Schirm und weiß genau, wo sie sich befinden"[21].

Ständig anhaltende Ortung kann Arbeiter auf heimtückische Weise unter Druck setzen, wenn sie das Gefühl haben, jeden Augenblick während der Arbeitszeit beobachtet zu werden. Ein amerikanischer Fahrer, dessen LKW mit GPS ausgerüstet ist, wurde wie folgt zitiert:

"Es ist wie eine Art Big Brother, der ein bisschen beobachtet…. Ich werde gereizt, wenn ich im Laden für eine Tasse Kaffee in der Warteschlange stehe, denn ich habe das Gefühl, he, die schauen zu, ich muss weiter….[22]."

In Kanada hatte die kanadische Postarbeitergewerkschaft (CUPW) ihre Mitglieder aufgefordert, die Bestrebungen der kanadischen Post, GPS-gebundene Bordcomputer in mehreren hundert Postautos einzubauen, genau zu verfolgen. Diese überwachen (über GPS) den Standort jedes Fahrzeugs, auch ob der Motor läuft, ob sich das Fahrzeug bewegt, und wenn ja, in welcher Geschwindigkeit und ob die Wagentüren verschlossen sind. Canada Post erklärte der Gewerkschaft, es sei ihr Ziel, Vorgesetzten die Möglichkeit zu geben, festzustellen (über so genannte vom Computer erarbeitete ‚Ausnahmeberichte') ob die Fahrer sicher fahren und die Sicherheitsvorschriften beachten[23].

Die CUPW verwies auf den derzeit geltenden Tarifvertrag mit Canada Post um sicher zu stellen, dass diese Überwachung nicht für disziplinäre Zwecke eingesetzt wird.

 Die Klausel im CUPW Tarifvertrag mit der kanadischen Post zum Thema Überwachung lautet wie folgt: "Zu keinem Zeitpunkt dürfen solche Systeme [zur Kontrollen und Überwachung] als Mittel zur Leistungsmessung von Beschäftigten und zur Erhebung von Beweismaterial zur Unterstützung von Disziplinarverfahren eingesetzt werden, außer wenn solche Disziplinarverfahren auf die Ausübung einer verbrecherischen Tätigkeit zurück zu führen ist..[24]"

Auch in anderen Ländern haben die Gewerkschaften reagiert, um die GPS Überwachung zu kontrollieren. In den USA hat die Gewerkschaft der Lastwagenfahrer mit UPS verhandelt, dass eine GPS-Ortung nicht verwendet werden darf, um Mitarbeiter im Zusammenhang mit Disziplinarverfahren zu beurteilen[25]. Die Lastwagenfahrer haben sich auch gegen den Einsatz von GPS durch andere Transport- und Kurierdienstunternehmen und durch öffentliche Behörden ausgesprochen.

Wo Ortungsgeräte im Einsatz sind, muss besonders darauf geachtet werden, dass die Ortung bei Pausen und nach Abschluss des Arbeitstages eingestellt wird.

 Amicus (UK/Irland) berichtete, dass es erfolgreich ein Fahrzeugortungsgerät bei einem Unternehmen als Eindringen in die Privatsphäre verteidigen konnte, wodurch der Mitarbeiter die Möglichkeit hatte, es zu umgehen.[26].

Geo-Ortungsdienste, besonders GPS, haben in den letzten Jahren besonders schnell zugenommen, obwohl wir vermutlich erst die erste Phase der Einführung dieser Technologie erleben. Die 2005 von der American Management Association durchgeführte Erhebung bei 526 US-amerikanischen Unternehmen ergab, dass 8% der Unternehmen GPS oder GPS/zellulare Ortung von Fahrzeugen anwenden, und dass 5% ihre Mitarbeiter über zellulare Ortung kontrollieren. [27]

Es ist noch etwas früh, um angemessene Vorkehrungen und gute Praxis zum Schutz der so genannten „Privatsphäre am Standort“ [28] einzuführen. Ein Leitfaden für Arbeitgeber des kanadischen Rechtsberaters David Canton schlägt im Falle der geplanten Einführung von GPS-Ortung eine Checkliste von vier Punkten vor[29]:

- Feststellung des Bedarfs
- Einführung eines Programms zum Schutz der Privatsphäre
- Berücksichtigung der Stimmung (beim Personal)
- Einverständnis hinsichtlich der Vorteile

Er warnt davor, dass GPS zwar die Effizienz und Produktivität verbessern kann, dass aber “ auch bei den Mitarbeitern eine Verschlechterung der Arbeitsmoral, eine Gegenreaktion auf Seiten der Arbeitnehmer und eventuelle Gerichtsverfahren ausgelöst werden können.“

Allgemeiner Besorgnis hinsichtlich der Notwendigkeit, bei Privatpersonen die ‚Privatsphäre des Standorts’ zu schützen, vor allem im Zusammenhang mit ihrem Privatleben, wurde vom US National Workrights Institute zum Ausdruck gebracht. Sie sagen: “Wenn ein Arbeitnehmer weiß, dass ihn sein Vorgesetzter bei seinen täglichen Vorhaben beobachtet, so überlegt er sicherlich lange, bevor er sich an eventuellen Aktivitäten beteiligt. Ist beispielsweise ein Vorgesetzter begeisterter Republikaner, wird sich ein Arbeitnehmer vielleicht dazu entschließen, nicht am Parteikongress der Demokraten teilzunehmen.”[30]

4. Video-Überwachung

Offene und verdeckte Kontrolle am Arbeitsplatz durch Video-Überwachung ist schon seit vielen Jahren ein Thema für die Gewerkschaften. Im Jahr 1993 hat beispielsweise die Gewerkschaft der Arbeitnehmer von Amerika einen Senatsausschuss in den USA auf einen Fall aufmerksam gemacht, wo weibliche Mitarbeiterinnen festgestellt hatten, dass die Werksleitung in ihrem Garderobeschrank eine Kamera versteckt hatte. Die Kamera wurde von männlichen Sicherheitskräften überwacht, die die Frauen beim Umkleiden in ihre

Uniformen beobachteten. [31] Ganz ähnliche Fälle, in denen Kameras verdeckt in Waschräumen oder Umkleideräumen angebracht wurden, sind auch aus anderen Ländern bekannt. [32].

Video-Überwachung ist nach wie vor ein Problem, welches am Arbeitsplatz zu Streit führt, vor allem, wenn Kameras ohne vorherige Absprache eingebaut werden oder heimlich zum Zwecke der Leistungskontrolle oder für disziplinäre Zwecke verwendet werden. Ein jüngstes Beispiel war der Einbau von Sicherheitskameras durch die Deutsche Post in der Hauptsortieranlage in Berlin, wo 650 Mitarbeiter beschäftigt sind. Es war geplant, dass diese Kameras bis zu 50 Stunden pro Woche eingeschaltet sein sollten. Dies wurde vom bundesdeutschen Arbeitsgerichtshof als übertriebener Einsatz verurteilt.[33]

In vielfacher Hinsicht ist die Verwendung von Überwachungskameras heute problematischer als in der Vergangenheit. Damals wurden die Bilder in Echtzeit überwacht und auf Magnetbänder aufgenommen. Heute sind die Aufzeichnungen von Kameras viel eher in digitaler Form und können unbegrenzt lange gemeinsam mit anderen digitalisierten Daten gespeichert werden. Solche digitale Aufzeichnungen aus Überwachungskameras, die auf einzelne Mitarbeiter ausgerichtet sind, könnten im Grunde genommen auch mit anderen digitalen Aufzeichnungen verknüpft werden, z.B. Daten aus der Personalabteilung oder Angaben aus einer E-Mail Überwachung oder aufgezeichnete Telefongespräche, die alle ein sehr starkes integriertes Informationsinstrument für einen Arbeitgeber sein könnten.

Die Arbeitsgruppe für Datenschutz der Europäischen Union verwies auf die Gefahren, die sich aus der Entwicklung von Software-Anwendungen ergeben könnten, welche Video-Bilder ‚interpretieren' können, indem beispielsweise in Bildern festgehaltene Personen durch den Gesichtsausdruck identifizierbar sind. können. In ihrem Bericht über Video-Überwachung von 2004 erklärt die Arbeitsgruppe für Video-Überwachung: "Diese Trends bei der Entwicklung von Video-Überwachungstechniken sind vernünftig zu überprüfen, um die Entwicklung von Software-Anwendungen zu verhindern, die sowohl die Gesichtszüge erkennen als auch das Verhalten der abgebildeten Person studieren und vorhersagen können, was bis zu einem gewissen Masse zu einer dynamisch- präventiven Überwachung führen würde, im Gegensatz zur

herkömmlichen statischen Überwachung, die vorwiegend auf spezielle von bestimmten Personen ausgelöste Ereignisse und deren Urheber ausgerichtet ist Diese neue Form der Überwachung ist möglich durch die automatisierte Darstellung der Gesichtszüge von Einzelpersonen und deren „abnormales Verhalten“ kombiniert mit vorhandenen automatischen Warn- und Mahnsignalen, was auch mit der Gefahr der Diskriminierung verbunden ist [34].

Mit anderen Worten, die Video-Überwachung ist nicht als alleinstehende Sicherheitsmassnahme zu betrachten, sondern sie ist eine Quelle an vorhandenen Daten, mit denen alle Möglichkeiten der modernen Computertechnologie zur Suche und Analyse wahrgenommen werden können. Ein Hinweis auf diesen Trend ist die von Cisco System entwickelte Technologie des AVVID (Architecture for Voice, Video and Data), welche angeblich im Bankwesen nicht nur für Sicherheitsfragen sondern auch für Marketing und Kundenbeziehungen zur maximalen Wertnutzung von Bankfilialen genutzt werden kann[35].

Angesichts dieser Art von Entwicklung ist es umso wichtiger, dafür zu sorgen, dass der Einsatz von Video-Überwachung angemessen kontrolliert wird. Die Arbeitsgruppe für Datenschutz der EU betont die Wichtigkeit der Einhaltung der wichtigsten Grundsätze des Datenschutzes, einschließlich der Proportionalität des Einsatzes und eine vorherige Information der von der Überwachung betroffenen Personen. Bezogen speziell auf den Arbeitsplatz fordert die Arbeitsgruppe den Schutz der „Rechte, Freiheiten und Würde“ der Arbeitnehmer. Sie kommentiert wie folgt:

“Video –Überwachungssysteme, die direkt von einem entfernt gelegenen Standort die Qualität und die Menge der geleisteten Arbeit prüfen sollen…… sollten nicht grundsätzlich zugelassen werden....

“Die Erfahrung mit der Umsetzung hat ferner auch gezeigt, dass eine Überwachung an Orten, die den Mitarbeitern für den privaten Gebrauch zur Verfügung stehen, oder nichts mit der Erbringung einer Arbeitsleistung zu tun haben – wie z.B. Toiletten, Duschräume, Schließfächer und Freizeitbereiche – nicht zulässig sein sollte; dass Bilder, die ausschließlich zum Zwecke der Sicherung des betriebseigenen Geländes und/oder zur Aufdeckung, Verhinderung und Kontrolle schwerer gesetzlicher Vergehen gedacht sind, nicht gegen einen Mitarbeiter wegen geringfügiger

Disziplinarverstöße verwendet werden können; und dass den Beschäftigten immer die Möglichkeit zu bieten ist, den Inhalt der festgehaltenen Bilder für eine Widerklage in Anspruch zu nehmen. Die Mitarbeiter und alle anderen Personen, die auf dem Betriebsgelände arbeiten, sind zu informieren".

Verdeckte Überwachung ist ein besonderes Anliegen, wie ein Beispiel aus Schweden zeigt. Das UNI Mitglied, die schwedische Transportarbeitergewerkschaft, verhandelt derzeit mit Securitas über den jüngsten Einsatz von geheimen mit Kameras ausgestatteten Überwachungsfahrzeugen, mit denen die eigenen Fahrzeuge und das Personal gefilmt werden.

Securitas rüstet bereits ihre Fahrzeuge mit Kameras aus; allerdings beginnen diese nur im Falle eines Angriffs auf die Fahrzeuge oder wenn verbotene Türen geöffnet werden, zu filmen; diese Praxis wird von der Gewerkschaft akzeptiert. Der bewaffnete Überfall auf ein Securitas Fahrzeug auf der Hauptstrecke der Autobahn südlich von Stockholm im Dezember 2005 hat gezeigt, wie wichtig gute Sicherheitsvorkehrungen sind. Allerdings wurde die Einführung geheimer Filmaufzeichnungen aus nicht gekennzeichneten Fahrzeugen von den Mitarbeitern von Securitas scharf kritisiert.

Die Gewerkschaft der schwedischen Transportarbeiter rechnet mit einem positiven Abschluss der Verhandlungen und einem Abkommen mit dem Unternehmen, welches in allen Nordischen Ländern zur Anwendung kommen wird[36]. In der Zwischenzeit hat DFF, das dänische Mitglied von UNI, bereits ein Abkommen mit Securitas unterzeichnet, welches den Anwendungsbereich für Video-Aufzeichnungen einschränkt und vor einer Verwendung von Videofilmen zu disziplinären Zwecken beschützt. Die Mitarbeiter müssen während des Einstellungsverfahrens über die Überwachung informiert werden.

Im Allgemeinen gibt es bereits einige Beispiele für gute Praxis bei der Kontrolle der Überwachung durch Video-Kameras. In einer Reihe von Ländern gibt bereits entsprechende Gesetze; im australischen Bundesstaat New South Wales wurde der im Gesetz über Video-Überwachung am Arbeitsplatz aus dem Jahre 1988 (das nach einer Reihe von Arbeitskonflikten im Bundesstaat zustande kam) festgeschriebene Schutz der Arbeitnehmer vor kurzem auch auf andere Formen

der elektronischen Überwachung ausgeweitet. In Österreich muss der Betriebsrat seine Zustimmung zu einer ständigen Video-Überwachung geben. [37]

In Belgien wurde der Einsatz von Kameras am Arbeitsplatz von den Sozialpartnern 1998 im Rahmen eines Tarifvertrags geregelt und hat gesetzliche Wirkung. Er gilt für den gesamten privatwirtschaftlichen Bereich.

Das belgische Abkommen basiert auf dem Grundsatz der Proportionalität und des letztlichen Zieles. Ständige Überwachung ist streng kontrolliert und nur dann erlaubt, wenn sie der Sicherheit des Arbeitnehmers oder dem Schutz des betrieblichen Eigentums dient. Verdeckte Video-Überwachung ist verboten, außer wenn ausreichend Nachweise für kriminelle Handlungen vorliegen. Kameras dürfen nur nach vorheriger Absprache mit Gewerkschaften eingeführt werden, und die davon betroffenen Arbeitnehmer müssen im Vorfeld informiert werden. Der Gegenstand der Überwachung muss klar definiert sein.[38]

5. Email und Web-Kontrolle; Tastaturkontrolle

Fragen im Zusammenhang mit der Überwachung von E-Mail und Internet von Mitarbeitern durch Arbeitgeber erregten in den letzten Jahren sehr viel Aufmerksamkeit, teilweise weil dadurch an vielen Arbeitsplätzen praktische Probleme entstanden und zu einer Reihe von einzelnen Disziplinarverfahren führten.

UNI (und ihr Vorgänger FIET) ist es zu verdanken, dass in diesem Bereich bereits sehr früh mit Arbeiten begonnen wurde als diese die Kampagne „Online Rechte für Online Arbeiter“ 1998 einleitete. UNI’s Praxiskodex für Online Rechte am Arbeitsplatz hat gute praktische Leitlinien eingeführt, die sowohl von den Gewerkschaften als auch von anderen Organisationen übernommen wurden.

UNI’s Kodex stellt vier miteinander verbundene Probleme fest, die mit der Verwendung von E-Mail und Internet am Arbeitsplatz verbunden sind - das Recht der Arbeitnehmervertreter auf Zugang zu elektronischen Einrichtungen; das Ausmaß, in dem einzelne Mitarbeiter E-Mail und Internet für persönliche Zwecke benutzen können; die Bedingungen, unter denen diese persönliche Nutzung

zulässig ist, und schließlich die Frage der Kontrolle und Überwachung von E-Mail und Internet. Dieser Bericht behandelt nur den letzten dieser vier Punkte.

 Der UNI Praxiskodex enthält folgenden Abschnitt zu Kontrolle und Überwachung der Kommunikation:

Der Arbeitgeber sorgt dafür, dass die Nutzung der elektronischen Vorrichtungen des Unternehmens durch den Arbeitnehmer nicht Heimlich kontrolliert und überwacht wird.

Die Kommunikation wird nur dann überwacht und kontrolliert, wenn es im Rahmen des Tarifvertrages zulässig ist, wenn der Arbeitgeber gesetzlich dazu verpflichtet ist oder wenn der Arbeitgeber ausreichende Gründe hat, anzunehmen, dass ein Mitarbeiter eine Straftat begangen hat, oder wenn eine ernsthafte Verletzung im disziplinarischen Bereich vorliegt. Ein Zugriff auf Aufzeichnungen von Kontrollen und Überwachungsvorgängen von einzelnen Mitarbeitern hat s zu erfolgen.

UNI's Praxiskodex beruft sich weitgehend auf bereits anerkannte Grundsätze im Bereich der Datenschutzverfahren, die eine angemessene Handhabung von einzelnen persönlichen Daten regeln, sowie auf die ILO und den Schutz der Menschenrechte[39].

Ähnlich wie UNI haben auch eine Reihe von Mitgliedsverbänden ähnliche Initiativen eingeleitet; viele haben ihre eigenen Leitlinien und Kodexe für gute Praxis erstellt. So beispielsweise GPA (Österreich), MSF (heute Amicus) (UK/Irland), CFDT BETOR-PUB (Frankreich), FNV Bondgenoten (Niederlande)(siehe unten).

 Protokoll von FNV Bondgenoten: Zur Privatsphäre im Zusammenhang mit E-Mail und Internet gibt es folgende Klausel:

Der Arbeitgeber darf weder den Inhalt von persönlichen noch kommerziellen E-Mail Sendungen lesen. Auch persönliche Angaben über die Anzahl der E-Mails, E-Mail Adressen oder andere Daten dürfen nicht registriert und/oder geprüft werden. Dies berührt nicht sein Recht, gelegentliche

Prüfungen vorzunehmen, wenn es zwingende Gründe gibt, welche Interessen des Unternehmens berühren. Diese Art von Prüfungen sind dem Betriebsrat mitzuteilen. [40]

In Deutschland hat ver.di gemeinsam mit IG Metall und dem DGB (Deutscher Gewerkschaftsbund) die Web-Seite www.onlinerechte-fuer-beschaeftigte.de und eine damit zusammenhängende Kampagne für Online-Rechte ins Leben gerufen. Die Aktion wurde im März 2002 von einem Internetcafé in Berlin aus organisiert und wurde in den Medien umfassend behandelt. Diese interaktive Web-Seite enthält juristische Informationen und ein Diskussions-Forum[41]. Diese Initiative wurde begleitet von einer 6-Punkte-Erklärung über Internet, Intranet und E-Mail, die vom DGB Vorstand im Februar 2004 angenommen wurde[42].

In dieser Broschüre der Deutschen Gewerkschaftskampagne für Online Rechte steht: " Ich schreibe Briefe, weil mein Chef meine E-Mails liest"

In mehreren Ländern wurden Tarifabkommen zu diesem Bereich abgeschlossen. Dies gilt für Österreich und Dänemark (im Abkommen zwischen HK-Service und den dänischen Arbeitgebern für Handel)[43]. Das wichtigste nationale Tarifabkommen wurde in Belgien im April 2002 von den Tarifpartnern unterzeichnet.

 Das belgische Tarifabkommen[44] (welches als nationales Gesetz gilt) schreibt fest, dass für die Kontrolle der online Nutzung durch Beschäftigte Einschränkungen gelten. In Bezug auf Internet können die Arbeitgeber Daten über die Dauer des Web-Anschlusses erheben, aber nicht die Web-Besuche von Einzelpersonen identifizieren. Für E-Mail gilt, dass die Menge und die Zahl der E-Mails aufgezeichnet werden können sofern sie nicht an einzelne Personen gekoppelt sind.

Die Frage der Nutzung von E-Mail und Web durch Arbeitnehmer wurde auch in der Europäischen Union behandelt. Die Arbeitsgruppe für Datenschutz der EU hat allgemeine Grundsätze zur Überwachung von E-Mail und Internet festgelegt, die unter folgenden Begriffen zusammengefasst werden können: Notwendigkeit, Endzweck, Transparenz, Legitimität, Proportionalität, Genauigkeit und Datenaufzeichnung , sowie Sicherheit[45]. Das Dokument der Europäischen Kommission für die zweite Konsultationsstufe der Sozialpartner über persönliche Arbeitnehmerdaten schlägt auch einen Europäischen Rahmen für den Bereich Elektronische Überwachung vor. Es geht dabei um folgendes:

- Geheime Überwachung ist nur zulässig in Übereinstimmung mit den Vorschriften nationaler Gesetze oder, wenn ausreichender Verdacht einer verbrecherischen Tätigkeit oder andere schwerwiegende Regelverletzungen vorliegen.
- Persönliche Daten, die auf dem Wege der elektronischen Überwachung erhoben werden, sollten nicht ausschließlich als Faktoren für die Bewertung der Leistung von Arbeitnehmern und auf sie bezogene Entscheidungen herangezogen werden..
- Ein grundsätzliche Verbot für den Arbeitgeber, private E-Mails und/oder private Dateien zu öffnen…

Dennoch wäre es falsch, zu denken, dass all diese Arbeiten die Probleme mit E-Mail und Internet zufrieden stellend gelöst haben. In Kanada stellte beispielsweise eine neuere wissenschaftliche Erhebung fest, dass es eine ganze Reihe unterschiedlicher Politiken gibt, auch in Fällen in denen ein Tarifabkommen vorliegt. Der Forscher bestätigt, dass in den schwächsten Abkommen steht, dass die Gewerkschaften ausdrücklich die Rechte der Arbeitgeber anerkannten, Formen der elektronischen Überwachung anzuwenden, wann und wo auch immer sie wünschen[46].

In den USA ist elektronische Überwachung ebenfalls weitgehend verbreitet. Laut der American Management Association überwachen 76% der Arbeitgeber die

Internetanschlüsse ihrer Mitarbeiter, 55% speichern und prüfen die E-Mails der Arbeitnehmer. Die Erhebung von AMA von 2005 stellte fest, dass mehr als eines von vier Unternehmen Mitarbeiter wegen angeblichen Missbrauchs des Internet und weitere 25% Mitarbeiter wegen E-Mail Missbrauch entlassen haben. Trotzdem konnte AMA auch gleichzeitig feststellen, dass eines von 10 Unternehmen ihre Mitarbeiter nicht darüber informierte, dass deren Gebrauch des Internet überwacht wurde; 14% haben ihre Mitarbeiter nicht darüber informiert, dass ihr E-Mail überwacht wurde[47].

Man kann Hubert Bouchet von der französischen Informationskommission CNIL nur zustimmen, denn er hat darauf hingewiesen, dass das Personal in den meisten Fällen nicht darüber informiert wird, dass diese Form der Überwachung am Arbeitsplatz stattfindet. “Das notwendige Gleichgewicht zwischen einer berechtigten Kontrolle durch das Unternehmen und der Rücksichtnahme auf die Arbeitnehmerrechte scheint nicht in vielen Fällen zu bestehen“, schreibt er[48].

Es ist interessant, festzustellen, dass die Erhebung zum Thema Kontrolle und Überwachung der American Management Association ebenfalls feststellt, dass einer von drei Arbeitgebern (36%) die Anzahl der Tastaturanschläge, die an der Tastatur verbrachte Zeit und/oder den Inhalt des eingegebenen Materials prüft. Die Gewerkschaft kümmert sich seit bereits vielen Jahren um die routinemäßig durchgeführte Überwachung, die bei Arbeitnehmern zu schreibbedingten Depressionen führten, besonders bei schlecht bezahlten Mitarbeitern, die grundlegende Daten eintippen. Forderungen nach einer unrealistisch hohen Produktivität bei Tastaturarbeiten können zum Entstehen von Erkrankungen durch repetitive Aufgaben führen, die in einigen Ländern beinahe epidemische Ausmaße erreicht haben.

Eine detaillierte Untersuchung von Software- und Hardware Produkten, welche Tastaturanschläge anzeigen, wurde für die deutschen Gewerkschaften von Gerrit Wiegand durchgeführt, dessen Erkenntnisse in seinem Buch „Im Netz@work“ veröffentlicht sind[49].

Auch im Einzelhandel begann man sich mit der automatischen Überwachung zu beschäftigen, als mit der Einführung von Strichkoden und elektronischer Ladenkassentechnologie die Scanning-Raten von Mitarbeitern kontrolliert

wurden. Die Technik kann so verwendet werden, dass man im Detail genau überwachen kann, wie das Personal den Arbeitstag verbringt, einschließlich der genauen Zeitdauer einer Toilettenpause. Aber allein die Möglichkeit, anhand dieser Technologie diese Art von elektronischer Beschnüffelung durchzuführen, bedeutet nicht, dass sie auch so eingesetzt werden muss. Es ist zu erwähnen, dass bei Metros neuem „Geschäft der Zukunft“ in Rheinberg das Personal die Möglichkeit hat, sich anonym in Dinge wie die ladeneigenen elektronischen Waagen einzuloggen, so dass persönliche Daten nicht erhoben werden.

6. Überwachung von Telefongesprächen und Arbeit in Callcenters

Telefongespräche können in unterschiedlicher Form überwacht werden. Anzahl und Dauer der getätigten Anrufe und die angerufenen Nummern können aufgezeichnet werden; die eigentlichen Telefongespräche können von Vorgesetzten entweder offen oder verdeckt abgehört werden; Gespräche können aufgenommen werden, auch Voice-Mail Mitteilungen können gelagert und überwacht werden.

In den USA überwachen ziemlich genau die Hälfte aller amerikanischen Unternehmen Telefongespräche, indem sie die angerufenen Nummern und die Dauer von Telefongesprächen aufzeichnen; zwei Drittel dieser Unternehmen führen diese Form der Kontrolle regelmäßig oder laufend durch. Dennoch informieren nach Aussagen der American Management Association 22% ihre Mitarbeiter nicht entsprechend. Annähernd eines von vier Unternehmen nimmt getätigte Telefongespräche auf. [50]

In einigen Industriezweigen (z.B. im Bank- und Versicherungswesen) mag es vielleicht juristische oder regulatorische Gründe für eine Tonaufnahme von Telefongesprächen geben. Das bedeutet allerdings nicht, dass aufgenommene Anrufe notwendigerweise routinemäßig für andere Zwecke verwendbar sind, wie z.B. zur Kontrolle der Produktivität einzelner Mitarbeiter oder für disziplinäre Zwecke. Telefongespräche werden immer häufiger in digitaler Form gespeichert; wie bei Aufnahmen mit Überwachungskameras besteht auch hier die Möglichkeit,

Daten mit anderen persönlichen Angaben zu integrieren werden und einer peinlich genauen Analyse durch Computer Software zu unterziehen.

Das Personal sollte informiert werden, wenn Anrufe aufgezeichnet werden.

Einige Unternehmen behaupten, Anrufe zum „Zwecke der Schulung“ abzuhören und mitzuschneiden. Obwohl dieses Vorgehen von Unternehmen in einzelnen Situationen berechtigt sein man, um den Standard der Telefonbetreuung zu erhalten, sollte Mitarbeitern, die in diesem Bereich eine Unterstützung brauchen, auch wirklich die Möglichkeit einer entsprechenden Schulung geboten werden.

Mitarbeiter von Callcenters erfahren dies in stärkerem Masse als die meisten anderen. Aus einem früheren UNI Bericht über die Beschäftigung in Callcenters geht hervor, dass „im Allgemeinen die Technologie im Callcenter den Arbeitgebern die Macht gibt, einen durchaus beeindruckenden Grad an elektronischer Kontrolle und Überwachung ihres Personals zu vollziehen“[51].

Beschäftigte in Callcenters haben darüber hinaus nur sehr wenig Kontrolle über ihren Arbeitstag, da sie Anrufe entgegennehmen, die automatisch über eine automatische Anrufverteilanlage (ACD) an sie weitergeleitet werden, und in vielen Fällen sind sie gezwungen, im Gespräch mit den Anrufenden einem vorgegebenen Text zu folgen, und sie haben strenge Verkaufs- und Leistungskriterien zu erfüllen. Bezeichnenderweise hält die ACD Technologie alle Aspekte der behandelten Anrufe fest, auch die Dauer von Pausen oder Toilettenbesuchen. UNI’s Globales Rundschreiben über Callcenter berichtete vom Fall einer Frau, die ihrem Vorgesetzten erzählen musste, sie sei schwanger, bevor es die eigene Familie erfuhr, denn sie musste erklären, weshalb sie ‚zu häufig die Toilette aufsuchte[52]. (Dieser Fall war teilweise die Anregung für unsere Erzählung über ‘Marta’ zu Beginn dieses Berichts).

UNI’s Callcenter Charta und der im Rahmen der 1. UNI Callcenter-Konferenz im Oktober 2005 aufgestellte Aktionsplan beschäftigen sich jeweils Kontrolle und Überwachung.

 Die UNI Callcenter Charta enthält sechs Punkte unter dem Titel Kontrolle, elektronische Überwachung und Schutz des Privatlebens.

- Überwachung ist nur dann zulässig, wenn der Zweck bekannt und akzeptierbar ist
- Die erfassten Daten dürfen nur für diesen Zweck verwendet werden
- Der Arbeitnehmer muss wissen, dass er/sie überwacht wird oder werden kann
- Mithören darf nur gelegentlich und nicht ununterbrochen stattfinden
- Der Arbeitnehmer muss Zugang zu den registrierten Daten haben und Ungenauigkeiten korrigieren können
- Aufzeichnungen müssen nach einem bestimmten Zeitraum gelöscht werden

Eine weitere konkrete vor kurzem durchgeführte Maßnahme von UNI Telecom im Rahmen des Europäischen Sozialen Dialogs mit der Arbeitgeberorganisation ETNO bestand darin, eine Klausel zur Überwachung in die angenommenen Leitlinien für den Betrieb von Kundenkontaktzentren aufzunehmen. Einer der wichtigsten Grundsätze besteht darin, dass die Arbeitnehmer in Callcenters über alle geltenden Leistungsüberwachungsvorkehrungen aufmerksam zu machen sind.

Die Erfahrungen von UNI Mitgliedern zeigen, dass es möglich ist, für Beschäftigte in Callcenters bessere Arbeitsbedingungen zu verhandeln. Mehrere Gewerkschaften des Telekomsektors haben beispielsweise Tarifverträge mit Klauseln zur Kontrolle und Überwachung unterzeichnet.

 In den USA hat die Gewerkschaft Communications Workers of America (CWA) mit einer Reihe von Telecomfirmen Abkommen verhandelt, darunter auch AT&T, Qwest, Bell South und SBC[53].

Das Abkommen mit AT&T regelt die Praxis des Mithörens von Telefongesprächen:

- Die Mitarbeiter werden an dem Tage, an dem das Mithören erfolgt, vorab informiert und jeder hat die Möglichkeit, zwischen einer Überwachung von einem entfernten Ort oder direkt nebenan zu wählen.
- Einzelne Anrufstichproben werden innerhalb des Arbeitsbereichs durchgeführt, in dem der Mitarbeiter kontrolliert wird.

- Kein Beschäftigter soll nach einer individuellen Service-Stichprobe einer Disziplinarstrafe ausgesetzt werden, außer bei grober Kundenbeschimpfung, Betrug, der Verletzung des privaten Schutzes bei Kommunikation, oder wenn sich Entwicklungsversuche als erfolglos erwiesen haben

Das Abkommen mit Pacific Bell (SBC) beschränkt die Überwachung von Personal auf 10 Anrufe pro Monat.

In Australien, hat die Gewerkschaft CEPU (Communication Electrical and Plumbing Union) ebenfalls mit der Frage einer übertriebenen Überwachung in Callcenters befasst. Die Gewerkschaften fordern die australischen Bundesstaaten auf, Mindestarbeitsnormen für Callcenter zu unterzeichnen.

Die Kontrolle und Überwachung in Callcenters ist deshalb ein so wichtiges Thema, weil in einer Reihe von Erhebungen nachgewiesen wurde, dass dies eine der wichtigsten Ursachen von Stressbelastung der Beschäftigten darstellt. Ein wissenschaftlicher Bericht aus dem Vereinigten Königreich besagt, dass „kein Zweifel daran besteht, dass viele Mitarbeiter das System der Kontrolle und der Überwachung als zusätzliche Arbeitsbelastung erleben. Über ein Drittel geben an, dass die Aufzeichnung der Gespräche “erheblich” oder” bis zu einem gewissen Maβe” den Arbeitsdruck erhöhen[54]”. Diese Frage wird nachstehend näher behandelt.

7. Überwachung durch Biometrie und Implantate

Der letzte Abschnitt dieses Berichtsteils befasst sich kurz mit der Form der elektronischen Überwachung von Mitarbeitern in einer noch direkteren und verletzenden Weise, nämlich mit einer eigentlichen Kontrolle des Körpers von Personen.

Die Technologie der Biometrie (Erkennung von Personen auf Grund ihrer einzigartigen körperlichen Merkmale) wird bereits in einer Reihe von Situationen angewendet. Das Einscannen von Fingerabdrücken wurde in den USA für Kontrollen einreisender ausländischer Besucher des Landes eingeführt. Die Iris-

Erkennung gilt als besonders viel versprechend für die Erkennung und Identifizierung von Personen.

Anders als bisher, wo die Polizei Fingerabdrücke von Verdächtigen anhand von Tintenkissen und Papier erfassten sind biometrische Daten digitalisiert – d.h. die aufgezeichneten Angaben liegen in digitaler Form vor und können somit einer detaillierten Computeranalyse unterzogen werden. Die Biometrie kann tiefgehende Probleme im Zusammenhang mit dem Schutz des Privatlebens aufwerfen. Die Gewerkschaften haben eine mögliche Einführung am Arbeitsplatz sehr eingehend zu prüfen.

Es gibt bereits Beispiele für die Einführung von biometrischen Techniken. McDonalds soll angeblich Daumen- und Handscanning des Personals an einigen Stellen in Kanada eingeführt haben[55]. Ebenfalls in Kanada hat die Postarbeitergewerkschaft CUPW versucht, Bemühungen der Canada Post Corporation zu verhindern, die von einigen ihrer Briefboten Fingerabdrücke forderte, sozusagen als Teil einer “Zuverlässigkeitskontrolle“ [56].

Hersteller von RFID-Etiketten sind mit dem Konzept von Implantaten winziger RFID-Chips in die Haut von Personen noch einen Schritt weiter gegangen. Es wäre schön, behaupten zu können, dass diese Idee heute noch Science Fiction ist; leider stimmt es nicht. Das amerikanische Unternehmen Applied Digital erzeugt bereits ein solches Produkt, den so genannten VeriChip.

Der VeriChip wird vorwiegend als eine Lösung vermarktet, die es Menschen ermöglicht, ihre medizinischen Einzelangeben jederzeit zur Verfügung zu haben. Er wurde auch von einem Nachtklub angewendet, der feste Kunden zu einem VeriChip-Implantat anregte, um an der Bar Getränke bestellen und bezahlen zu können. VeriChips sind auch bereits im Arbeitsleben im Einsatz, denn 18 Beamte des Mexikanischen Staatsanwaltschaftsbüros haben sich freiwillig einer solchen Implantierung unterzogen. Die Chips (siehe unten[57]) dienen dem Zugang des Personals zu Bereichen, in denen der Zutritt begrenzt ist.

Die Gesundheitsrisiken, die mit dem Tragen eines implantierten RFID Chips verbunden sein könnten, werden nachstehend erörtert. Abgesehen von gesundheitlichen Aspekten im Zusammenhang mit RFID-Chips steht fest, dass neue Produkte wie der VeriChip wichtige Folgen für den Schutz des Privatlebens, sowohl bei der Arbeit als auch privat, beinhalten.

Einige Fragen im Zusammenhang mit elektronischer Überwachung und Kontrolle

Wie kommt es zu all dem? Weshalb scheint ein elektronisch gestützter Kommando- und Kontroll-Managementstil sich gerade in einer Zeit durchzusetzen, wo laut Rhetorik der Personalpolitiker das Informationszeitalter "intelligente Arbeitsformen" und mehr auf Zusammenarbeit ausgerichtete Formen der Beteiligung der Arbeitnehmer fordert?

Eine zynische Antwort wäre, dass es jetzt eben die Technologie gibt, die diese Kontrolle möglich macht. Prof. Michael Blakemore, der Berater der britischen Gewerkschaft GMB, spricht von dem „beruhigenden" Signal, die diese Art von Technologie zu bieten scheint: "Tief eingebettet in diese Art von Sprachgebrauch ist die Aussicht auf Sicherheit und Gewinn", schreibt er [58]. Er weist auch darauf hin, dass ein Rückgriff auf Technologie am Arbeitsplatz weitgreifende Ergebnisse zur Folge haben kann: "Das Ergebnis verändert die Beziehungen zwischen Vorgesetzten und Personal, wodurch erstere den Mitarbeitern nicht mehr im Gespräch begegnen, sondern sie einfach nur überwachen."

Er und andere Wissenschaftler sprechen immer häufiger vom Konzept des „schleichenden Computing", definiert als ein Prozess, bei dem Computer in den Alltag so integriert werden, dass sie unsichtbar und als selbstverständlich hingenommen werden[59]. Allgegenwärtige Überwachung ist somit eine Situation (so Blackwell) "wo alles, oder beinahe alles, was ein Mitarbeiter tut, überwacht, analysiert und geprüft wird."

Wie die ILO in ihrem bahnbrechenden Bericht über Arbeitsbedingen zur Überwachung am Arbeitsplatz im Jahr 1993 hervorhob, sind einige Arbeitnehmer stärker davon betroffen als andere: die Arbeitsaufgaben, die am wahrscheinlichsten einer hochintensiven Überwachung untezogen werden, sind häufig von Frauen oder Minderheitsgruppen geleistete Arbeitsfunktionen, wobei es sich im allgemeinen um schlecht bezahlte Arbeit handelt[60]. In diesem Zusammenhang ist es wichtig, dass der GMB in seiner britischen Kampagne gegen die "Batteriehühnerfarmen" über die Bedingungen in britischen Lagerhäusern (siehe oben) berichtete und dabei erwähnte, dass viele der in Lagerhäusern überwachten Personen Wanderarbeitnehmer waren.

Deshalb ist es zwar durchaus möglich, dass einige Arbeitnehmer, die im Informationsalter hochwertige wissensbasierte Arbeit leisten, sich von den Zwängen einer Kontrolle durch die Hierarchie befreit fühlen, während wiederum viele andere sich stark von der Technologie kontrolliert fühlen, eigentlich in einer Form von Beziehung zur Technologie, die man früher oft mit Fliessbandarbeit verband.

Überwachung durch elektronische Kontrolle ist vielleicht „beruhigend“ für die Unternehmen, aber ist sie auch wirklich effizient? Die Antwort scheint häufig zu sein, dass sie es wahrscheinlich nicht ist. Gary Marx vom MIT schrieb 1999 folgendes: „Derzeit gibt es keine starken Beweise, die für eine Überwachung sprechen. Wie wir feststellen können, kann mit gutem Grund damit gerechnet werden, dass uneingeschränkte Überwachung kontraproduktive wirkt. Eine mögliche negative Wirkung auf das körperliche und geistige Wohlbefinden der Beschäftigten kann die Gewinne aus einer angeblich erhöhten Effizienz durch Überwachung wieder aufheben. [61]“

Es geht allerdings nicht darum, ob eine Überwachung für das Unternehmen „effektiv“ ist oder nicht. Selbst wenn eindeutig erwiesen wäre, dass eine eindringliche Überwachung von Arbeitnehmern geschäftliche Vorteile mit sich bringt, gibt es mehrere gute Gründe für die Gewerkschaften, sich gegen diese Praxis zu wehren. Wir untersuchen der Reihe nach drei dieser Gründe.

Recht auf gewerkschaftliche Vertretung

Erstens und ganz pragmatisch gesehen, können die Gewerkschaften mit gutem Grund befürchten, dass eine Überwachung von negativ eingestellten Arbeitgebern als Instrument eingesetzt werden kann, um eine gute gewerkschaftliche Vertretung zu unterbinden.

Es gab eine Reihe von Fällen, in denen die Überwachung gerade zu jenem Zeitpunkt eingeführt wurde, als die Gewerkschaften versuchten, nicht gewerkschaftlich organisierte Arbeitnehmer für die Gewerkschaft zu gewinnen. Ein Beispiel kommt von Wal-Mart, dem gewerkschaftsfeindlichsten Unternehmen

überhaupt, welches den Einsatz von Überwachungskameras bei „verdächtigen“ Arbeitnehmern in einem Laden in Kentucky versuchte, als die dortigen Vertreter der UFCW versuchten, das Ladenpersonal gewerkschaftlich zu organisieren. Das Unternehmen scheint einen ähnlichen Ansatz bei einer Filiale in Indiana und vermutlich auch an anderen Orten in den USA versucht zu haben[62].

Selbst dort wo Gewerkschaften anerkannt sind, ist ein Arbeitstag mit strenger Überwachung nicht unbedingt geeignet, gute gewerkschaftliche Arbeit zu fördern. Eric Lee wies darauf hin, dass es früher leichter war, einem Betriebsrat ein Anliegen ins Ohr zu flüstern, wenn er beispielsweise an einem Wasserkühler stand.[63] Je kontrollierter der Arbeitstag, desto weniger Möglichkeiten gibt es, diese Form der informellen Kontaktaufnahme zwischen Arbeiter und Betriebsrat durchzuführen.

Arbeitsschutzfragen

Neue Technologie bringt neue Gefahren für Gesundheit und Sicherheit. Die Einführung von Tastaturarbeit am Computer für Programmieraufgaben führte zu einem weitgehenden Anstieg der Fälle von Schäden durch repetitive Belastungen, während Hörsturz als Gefahr für Personal in Callcenters festgestellt wurde.

Es ist nicht unbedingt einfach, heute genau festzustellen, welche Auswirkungen die zunehmende „eindringliche Computeranwendung“ auf die Gesundheit von Arbeitnehmern hat. Es hilft sicherlich nicht, dass die Hersteller der in diesem Bericht beschriebenen Technologie im Allgemeinen den technischen Informationen zu Fragen der Ergonomie und des Arbeitsschutzes nicht viel Aufmerksamkeit schenken.

Einige mögliche Probleme lassen sich jedoch trotzdem feststellen. Erstens, gibt der Einsatz von tragbaren Datengeräten (wie sie hier in diesem Bereicht beschrieben wurden) zur Sorge über mögliche körperliche Folgen bei einem andauernden Gebrauch Anlass. Wie bereits erwähnt, wiegt ein häufig verwendeter am Handgelenk zu befestigender Computer 320g, und das Gewicht erhöht sich auf 350g, wenn ein Radiosender/Empfänger angeschlossen ist. Am

Zeigefinger befestigte Scanner wiegen normalerweise ca. 50gms, wobei das Scannen durch regelmäßiges Drücken mit dem Daumen erfolgt[64].

Der weltweit zunehmende Gebrauch von Mobiltelefonen weckte Besorgnis angesichts eventueller Gefahren durch elektro-magnetische Strahlung, ein Forschungsbereich, in dem bis heute noch keine eindeutigen Erkenntnisse vorliegen. Wenig Arbeit scheint bisher den Auswirkungen anderer Ortungstechnologien gewidmet zu sein. Bezüglich der implantierten RFID Chips hat die Arzneimittelbehörde der USA die Verwendung des VeriChip genehmigt, allerdings mit folgender Auflistung zu eventuellen Gesundheitsrisiken: “negative Gewebereaktion, Wandern des implantierten Transponders, gestörte Datensicherheit, Fehler beim Einsetzen, Versagen des elektronischen Scanners, elektromagnetische Interferenz, elektrische Risiken, Unverträglichkeit bei MR-Bilddarstellungen, und Nadeleinstich”[65].

Ganz allgemein gibt es eine Menge von Forschungsarbeiten, die andeuten, dass eine Beziehung zwischen der Einführung von Leistungskontrolle und den Gesundheits- und Sicherheitsrisiken von Arbeitnehmern besteht. Die deutlichsten Gesundheits- und Sicherheitsfragen im Zusammenhang mit elektronischer Überwachung und Kontrolle hängen mit erhöhtem Arbeitsstress zusammen. Bereits 1993 stellte der ILO Bericht über Kontrolle und Überwachung am Arbeitsplatz folgendes fest:

> Eine Studie, die gemeinsam von Forschern der Universität Wisconsin und der Gewerkschaft der Kommunikationsarbeiter der USA zum Thema elektronische Überwachung und Kontrolle durchgeführt wurde, bestätigt frühere Untersuchungen, aus denen hervorgeht, dass elektronische Überwachung ein starker Stressfaktor am Arbeitsplatz ist, was teilweise damit zusammenhängt, dass die überwachten Arbeitnehmer eine Gefühl der Machtlosigkeit erleben. [66]

Stress wurde in Callcenters als wichtiges Problem erkannt und im Rahmen der UNI Callcenter Konferenz 2005 behandelt. Die Konferenz forderte einen Einsatz zur Verbesserung von Gesundheit und Wohlbefinden der Mitarbeiter in den Callcenters in aller Welt und forderte Maßnahmen zum Abbau von Stress, Angst, Burn-Out und Depressionen.

 Leistungsmessung beruht eher auf der Leistung von Teams als der auf der von Einzelpersonen in Verizon-South in New Jersey, eine Praxis, die vom Ausschuss für Stressfragen von CWA-Verizon empfohlen wird.[67].

In den letzten Jahren begann man, die Stressbelastung am Arbeitsplatz als Problem des Betriebssicherheits- und Gesundheitsschutzes etwas ernster zu nehmen. So haben beispielsweise 2004 die Europäischen Sozialpartner sich formell auf ein Rahmenabkommen über berufsbezogenen Stress geeinigt. Dennoch scheinen die Beziehungen zwischen elektronischer Überwachung und Stress bisher noch nicht ausreichend verstanden zu sein. Das EU-Rahmenabkommen bezieht sich zum Beispiel nicht spezifisch auf die Beziehung zwischen Überwachung und Stress.

Schutz des Privatlebens und anständige Arbeit

Die vielleicht wichtigste Frage im Zusammenhang mit Kontrolle und Überwachung am Arbeitsplatz bezieht sich auf das grundlegende Recht der Arbeitnehmer auf den Schutz ihres Privatlebens. Ein EU Bericht besagt, dass "die Arbeitnehmer ihr Recht auf Privatleben und Datenschutz nicht morgens am Werkstor abgeben"[68]. Der Schutz des Privatlebens wird insofern immer wichtiger als die herkömmlichen Grenzen zwischen Zeit und Raum für "Arbeit" und "Persönliches" immer mehr durch Entwicklungen wie Telearbeit und flexible Stundenverträge verwischt werden.

Bereits vor annähernd 10 Jahren hat die ILO versucht, Fragen im Zusammenhang mit dem Schutz des Privatlebens, die sich durch die Lagerung von persönlichen Daten von Arbeitnehmern ergeben, in Angriff zu nehmen. Ihr (freiwilliger) Praxiskodex enthält eine kurze Klausel zur Überwachung.[69]

 Abschnitt 6.14 des ILO Codex lautet wie folgt :

Falls Arbeitnehmer überwacht werden, sollten sie vorher über die Gründe für diese Überwachung, den Zeitplan, die Methode und die verwendete Technik und die zu erhebenden Daten informiert werden, und der Arbeitgeber muss eine Einmischung in die Privatsphäre auf ein Minimum reduzieren.

Heimliche Überwachung sollte nur dann zugelassen werden, wenn:

- sie in Übereinstimmung mit der Gesetzgebung des Landes ist, oder
- wenn ausreichender Verdacht vorliegt, dass verbrecherische Tätigkeiten oder anderes Fehlverhalten vorliegt

Ständige Überwachung sollte nur dann zugelassen werden, wenn sie aus Gründen der Gesundheit und Sicherheit oder zum Schutz des Eigentums erforderlich ist.

Seither wurden Fragen im Zusammenhang mit dem Schutz des Privatlebens von Arbeitnehmern eher nur am Rande und im Rahmen einer hallgemeineren Datenschutzgesetzgebung behandelt. In der Europäischen Union wurden zum Beispiel die Mitgliedsstaaten verpflichtet, die Vorschriften der Datenschutzrichtlinie aus dem Jahr 1995 in ihre Gesetzgebung aufzunehmen. Die Europäische Kommission schlug vor, dass die besonderen Fragen zum Datenschutz am Arbeitsplatz im Rahmen des sozialen Dialogs mit den Sozialpartnern behandelt werden. Die Kommission legte 2002 einen detaillierten Vorschlag für ein Rahmenabkommen vor (siehe unten), welcher in diesen Gesprächen verwendet werden sollte. Dennoch erschien der für 2004 angekündigte Nachfolgbericht der Kommission nicht, und diese Frage scheint derzeit “zu ruhen”.

 Das vorgeschlagene Europäische Rahmenabkommen legt eine Reihe von Grundsätzen fest, darunter auch das Recht der Arbeitnehmervertreter auf Information und Konsultation vor der Einführung oder Änderung von Überwachungs-Kontrollmaßnahmen, Einschränkungen bei der ständigen Überwachung, strenge Vorschriften gegenüber heimlicher Überwachung und das Verbot von routinemäßigen Kontrollen der Nutzung von E-Mail und Internet. Darüber hinaus sollten persönliche Daten, die auf dem Wege der elektronischen Überwachung erhoben werden, nicht als ausschließlicher Faktor für die Leistungsbeurteilung von Arbeitnehmern herangezogen werden[70].

Ein bekanntes Beispiel für eine gute Gesetzesinitiative kommt aus New South Wales (Australien), wo die von der Labourpartei kontrollierte Regierung im letzten Jahr (2005) das Gesetz zur Überwachung am Arbeitsplatz verabschiedet hat. Dieses Gesetz erweitert die bereits 1998 im Gesetz zur Video-Überwachung festgeschriebenen Kontrollen auf andere, neuere Formen der elektronischen Überwachung. In den US hat sich die Gewerkschaft CWA (Communication Workers of America) darum bemüht, beim Kongress ein ähnliches Gesetz zur Verabschiedung zu bringen, welches die Verwendung von Video- und Audio-Kontrollen am Arbeitsplatz einschränken würde[71].

Eine Reihe von Gewerkschaftsverbänden und Einzelgewerkschaften haben Kodices für gute Praxis zum Schutz des Privatlebens von Arbeitnehmern eingeführt. Ein Beispiel ist FNV (Niederlande), welche eine Modellvorschrift für den Schutz der Privatsphäre erarbeitet haben. [72] Der Verband der IT-Fachleute (Teil der britisch/irischen Gewerkschaft Amicus) hat ebenfalls einen ähnlichen Praxiskodex erarbeitet [73].

Diese Art von Initiativen versucht zu verdeutlichen, dass die Erhebung von elektronischen Daten durch Arbeitgeber über unterschiedliche Formen der Überwachung und Kontrolle nicht nur eine technische Frage der Einhaltung von Datenschutznormen ist. Hier werden grundlegende Menschenrechtsprobleme angesprochen. Letztlich geht es hier um eine Frage der menschlichen Würde.

Schlussfolgerung: die weiteren Schritte für UNI

Obwohl elektronische Überwachung und Kontrolle in vielen verschiedenen Sektoren immer häufiger angewendet wird, besteht kein Grund, in eine technologisch bedingte Hoffnungslosigkeit zu verfallen. Es gibt bereits eine Menge von Beispielen für gute Praxis bei Gewerkschaften und anderen, die auf diese Entwicklung reagieren. UNI selbst hatte Erfolg mit ihrer Initiative Online Rechte für Online Arbeiter und der Kampagne zur Arbeit in Callcenters, sowie mit der jüngsten Globalen Callcenter Konferenz. UNI Mitgliedsverbände und andere Gewerkschaftsorganisationen haben ebenfalls positive Erfahrungen gewonnen (von denen einige in diesem Bericht erwähnt wurden), die sie mit anderen teilen können.

Dennoch sollte UNI überlegen, wie sie ihre Rolle in Fragen der elektronischen Überwachung und Kontrolle stärken kann. Eine Reihe weiterer Schritte wären zu überlegen.

1 Man hat sich bisher nur wenig mit der sich sehr rasch verbreitenden RFID-Technologie befasst. Die Ortung über RFID findet immer häufiger Anwendung, besonders im Zusammenhang mit RFID bestückten Namensschildern. Ein Kodex für gute Praxis von UNI (ähnlich wie der erfolgreiche Praxiskodex von Uni für Online Rechte) soll veröffentlicht werden, um die Mitgliedsverbände bei ihrer Arbeit zu unterstützen.

2 Die Überwachung durch RFID hängt mit der Frage der Ortung von Arbeitnehmern über GPS und Mobiltelefone zusammen. UNI wird eine breitere globale Kampagne einleiten (*Wer ist ihnen auf der Spur?),* die sowohl die Mitgliedsverbände als auch deren Mitglieder bei der Behandlung der hierzu anstehenden Probleme unterstützen soll. Der Bericht wird in jeder einzelnen globalen UNI Gewerkschaft zur Diskussion stehen.

3 ILO wird angeregt, die Frage der elektronischen Überwachung und Kontrolle zu behandeln. Die letzte wichtige Forschungsarbeit der ILO in diesem Bereich liegt mehr als 10 Jahre zurück. Die Frage der elektronischen Überwachung und

Kontrolle kann direkt an den letzten Aufruf der ILO nach anständiger Arbeit angebunden werden.

4 UNI wird sich gemeinsam mit der Europäischen Union und anderen regionalen Organisationen mit dieser Frage beschäftigen und an der derzeitigen Konsultation der Europäischen Kommission über RFID Technologie teilnehmen.

5 Informationen über Gesundheits- und Sicherheitsrisiken bei zu starker Überwachung vor allem im Zusammenhang mit arbeitsbedingtem Stress werden von UNI auf deren Website veröffentlicht.

6 UNI wird sich weiterhin stark für die Callcenter Charta und den Praxiskodex über Online Rechte einsetzen.

7 Elektronische Überwachung und Kontrolle sind Themen, die nicht nur den Arbeitsplatz berühren. Die UNI Mitgliedsverbände werden ermutigt, mit Bürgerrechts- und Datenschutzorganisationen zusammenzuarbeiten, und sich breiteren Kampagnen anzuschließen (wie die Verbraucherkampagne gegen den Einsatz von RFID bei der Kundenüberwachung in den USA), die Bedenken äußern gegenüber der Art, in der diese neuen Technologien Eingang finden.

[1] http://www.nocards.org, http://www.spychips.com
[2] Alorie Gilbert, Elementary school nixes electronic ID, February 17 2005 http://news.com.com/2102-1029_3-5581275.html
[3] Andrew Bibby, Invasion of the privacy snatchers, Financial Times, January 9 2006
[4] Paul Tyrrell, Tuned in to the right frequency, Financial Times, December 15 2004
[5] Posting on Smart Mobs, http://www.smartmobs.com/archive/2005/05/04/rfid_employee_m.html. See also http://ubiks.net/local/blog/jmt/archives3/003741.html
[6] Will Sturgeon, Las Vega casino goes for RFID, April 15 2005 http://software.silicon.com/security/0,39024888,39129583,00.htm
[7] Accenture, Silent Commerce Chips Away at Star City Casino Wardrobe Worries, case study, http://www.accenture.com/Global/Services/By_Subject/Radio_Frequency_Identification/Client_Successes/StarCityCasino.htm
[8] WaspTime see http://www.waspbarcode.com/wasptime/wasptime_premium.asp
[9] RAND, Research brief, Privacy in the Workplace, 2005. See also RAND, Technical Report, 9 to 5: Do you know if your boss knows where you are? 2005 http://www.rand.org
[10] Resolution on Radio Frequency Identification, 20 November 2003
[11] Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, January 19 2005, WP105
[12] GMB Pres release, GMB seeks changes to European law to outlaw worker tagging, July 18 2005 http://www.gmb.org.uk/Templates/Internal.asp?NodeID=92057
[13] Cornelia Brandt, Klüger als die intelligenten Dinge sein… Risikoabshätzung bei RFID-Anwndung fordert Handeln auf verschiedenen Ebenen, 2005
[14] UNI Commerce, Technology and RFID must be negotiated January 26 2005 http://www.union-network.org/UNIsite/Sectors/Commerce/Social%20dialogue%20articles/EU_dialogue_increasingly_important.htm
[15] GMB Press release, GMB Congress demands to electronic tagging of workers 'battery farm; workplaces, June 6 2005 http://www.gmb.org.uk/Templates/Internal.asp?NodeID=91861
[16] http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
[17] Case study, Hands-free Plus real-time, equals business advantage, http://www.symbol.com/category.php?fileName=CS-27_Peacocks.xml
[18] See for example Katrina Arabe, Wearable Computers: the new warehouse wear, February 13 2003, http://news.thomasnet.com/IMT/archives/2003/02/wearable_comput.html
[19] Michael Blakemore, I-DRA Ltd/GMB, Surveillance in the Workplace – an overview of issues of privacy, monitoring and ethics, September 2005
[20] Eurotechnology Japan, Location Based Mobile Services in Japan, http://www.gii.co.jp/english/ek32275-mobile-services.html
[21] National Workrights Institute, Privacy Under Siege: Electronic Monitoring in the Workplace, n.d.
[22] Adam Geller, Bosses keep sharp eye on mobile workers via GPS, Associated Press, January 3 2005 http://www.workrights.org/in_the_news/in_the_news_associatedpress.html
[23] On Board Computer – Big Brother Comes to CPC
[24] Agreement between Canada Post Corporation and Canadian Union of Postal Workers (expires January 31 2007)
[25] National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace n.d.; Gundars Kaupins and Robert Minch, Legal and Ethical Implications of Employee Location Monitoring, Proceedings of the 38th Hawaii International Conference on System Sciences
[26] David Hencke, AA to log cal centre staff's trips to loo in pay deal, The Guardian, October 31 2005
[27] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[28] See for example Jonathan Raper, Technology Trends- brave new world?, http://www.geoplace.com/ge/2001/0101/0101tt.asp
[29] David Canton, Employee Tracking and Monitoring, http://www.canton.elegal.ca/archives/2005/06/. Another checklist for employers is offered by Gundars Kaupins and Robert Minch, Legal and Ethical Implications of Employee Location Monitoring.

[30] National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace n.d
[31] Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[32] For example at Guy's Hospital, London. Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[33] Gregor Wittich, Rechtsprechungsübersicht zur Verwendung neue Medien im Betrieb, in DGB, Internet und E-Mail: Neue Medien im Betrieb, 2004
[34] Article 29 Data protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, adopted February 11 2004. See also Article 29 Data Protection Working Party, Working Document on the Processing of Personal Data by means of Video Surveillance, adopted November 25 2002.
[35] Anthony Hildebrand, Branching Out, http://www.smtdirect.co.uk/story.asp ?sectioncode=0&storyCode=3060661
[36] Information from the union, Jan 2006
[37] Prof Frank Hendrickx, Protection of workers' personal data in the European Union, Study 2: surveillance and monitoring at work
[38] FGTB, Surveillance par caméras: la CCT no 68, http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0404.htm
[39] http://www.union-network.org/UNIsite/Sectors/IBITS/ICT/online.htm
[40] FNV Bondgenoten, Model Protocol: privacy in the use of the internet and e-mail, n.d.
[41] Cornelia Brandt, Onlinerechte für Beschäftigte, in DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004
[42] Eckpunkte der Nutzung von Internet, Intranet und E-mail im Arbeitsverhältnis, in DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004
[43] European Industrial Relations Observatory, New technology and respect for privacy at the workplace, 2003 http://www.eiro.eurofound.eu.int
[44] http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0405.htm
[45] Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, adopted May 29 2002, WP55
[46] Professor Vincent Mosco, What are Workers Doing about electronic surveillance in the workplace? An examination of trade union agreements in Canada, proposal for presentation at the 2005 Conference of IFIP Working Group 9-2 Conference
[47] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[48] Hubert Bouchet, La cybersurveillance sur les lieux de travail, CNIL March 2004
[49] Michael Sommer, Cornelia Brandt and Lothan Schröder (eds), Im Netz@work, VSA-Verlag, 2003
[50] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[51] Andrew Bibby, Organising in Financial Call Centres, UNI, 2000
[52] UNI Global Call Centre News, April 2004
[53] Communications Workers of America, http://www.cwa-union.org/workers/customer/protections.asp
[54] Philip Taylor and Peter Bain, Trade Unions and Call Centre Survey, for Finance Sector Unions, 2000
[55] Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[56] http://www.cupw.ca/pages/document_eng.php?Doc_ID=595
[57] Photo from http://www.spychips.com
[58] Michael Blakemore, Every breath you take, every move you make, http://www.unionweb.co.uk/view/PageView.aspx?Page=273
[59] Martin Dodge, Rob Kitchin, The ethics of forgetting in an age of pervasive computing, UCL, http://www.casa.icl.ac.uk. A Galloway, Intimations of everyday life: ubiquitous computing and the city, Cultural studies, 18 (2/3), 2004
[60] ILO, Conditions of work digest volume 12: Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993
[61] Gary Marx, Measuring Everything that Moves: the new surveillance at work, in I and R Simpson, The Workplace and Deviance, 1999, http://web.mit.edu/gtmarx/www/ida6.html

[62] How Wal-Mart keeps Unions At Bay, Business Week, October 28 2002 http://72.14.207.104/search?q=cache:YRWfcqtIO2IJ:www.2110uaw.org/gseu/archive/How%2520WalMart%2520Keeps%2520Unions%2520at%2520Bay.htm+surveillance+cameras+workplace+union+organizing+drive&hl=en&gl=uk&ct=clnk&cd=2
[63] Eric Lee, Trade Unions in the electronic workplace, April 13 2004 http://www.ericless.me.uk/archive/000079.html
[64] http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
[65] http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt
[66] ILO, Conditions of work digest volume 12: Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993
[67] Communications Workers of America, http://www.cwa-union.org/workers/customer/protections.asp
[68] Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, adopted May 29 2002, WP55
[69] ILO, Protection of Workers' Personal Data, 1997 http://www.ilo.org/public/english/support/publ/pdf/protect.pdf
[70] European Commission, Second stage consultation of social partners on the protection of workers' personal data, http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf
[71] CWA-Backed bill would protect workers' privacy in changing areas, CWA press release, March 1 2005. http://www.cwa-union.org/news/cwa-news/page.jsp?itemID=27374804
[72]http://home.fnv.nl/02werkgeld/arbo/wetgeving/privacy/Model%20Privacyreglement/model_privacyreglement1.htm
73 http://www.amicus-itpa.org/juneconf2.shtml