Du är bevakad

Elektronisk övervakning på arbetsplatsen

Rapport av Andrew Bibby
Omslagsdesign av Jane Shepherd

UNI/GS/06-2006/0035/SW

Marta Redding arbetade för ett stort, multinationellt försäkringsbolag. Eller hon hanterade i alla fall ersättningskrav åt det. Försäkringsbolaget hade för två år sedan lagt ut denna del av sitt administrativa arbete på ett specialiserat företag som utnyttjade personal från ett bemanningsföretag: för att vara precis, Martas formella arbetsgivare var ett bemanningsföretag.

Marta hade arbetat för detta bemanningsföretag i närmare ett år. Det var ett av flera jobb hon hade haft sen hon slutade skolan som 18-åring. Hennes arbetsplats var ett kontorshus i ett obestämbart industriområde. Varje morgon drog hon sitt personalkort genom läsaren vid ingångsspärren i receptionen och tog sig till första våningen, där hennes skrivbord stod. Formellt arbetade hon i ett arbetslag, men ansiktena vid skrivborden runt henne förändrades regelbundet. Hon behövde i alla fall inte ha några kontakter med dem. Raderna av nya ersättningshandlingar som hon skulle bearbeta kom automatiskt till hennes dator, och hennes uppgift var helt enkelt att gå igenom dem. Varje ersättningskrav skulle i genomsnitt ta henne 6 minuter och 42 sekunder att bearbeta. Datorn visste exakt hur snabbt hon arbetade, och om hon låg under prestationsmålet vid veckans slut kallades hon till ett samtal med arbetslagets ledare.

Det var ett monotont jobb, men det var i alla fall ett jobb: hennes första barn var på väg, och hon behövde lönen. De första månaderna av graviditeten hade varit svåra, men hon hade ansträngt sig för att komma till jobbet varje dag, även om hon hade måst ta fler raster. Hon gjorde, tyckte hon, sitt bästa.

Men det var inte vad företaget tyckte. Det var fredag eftermiddag när hon kallades till en av chefernas kontor. Chefen hade flera datorutskrifter på sitt bord. "Vi måste låta dig gå," sade han. "Jag har tittat på dina raster. Titta här. Fyra raster på bara en förmiddag förra veckan. Det är för mycket."

Där, på datorutskriften, fanns en detaljerad redovisning av exakt vad hon hade gjort på arbetet under de senaste veckorna, minut för minut, inklusive tiden som hon inte suttit vid sitt bord. Marta var förbluffad. "Jag visste inte att jag bevakades på det här sättet," sade hon till slut. Chefen tittade upp från papperen. "Visste du inte?" frågade han. "Vi vet var alla i byggnaden finns hela tiden. Din personalbricka innehåller en radioanordning. Förresten, det är bäst att du lämnar den här, du kommer inte att behöva den igen."[1]

Marta Redding heter inte så – men detta hände henne i verkligheten.

Förord

Ingen tycker om att man spionerar på honom eller henne. Många arbetstagare känner avsmak inför att deras arbetsgivare i hemlighet övervakar dem. Det kan knappast bidra till det förtroende som ett framgångsrikt anställningsförhållande måste bygga på.

Som det sägs i denna rapport, finns det dock många nya tekniker och anordningar som arbetsgivarna kan använda om de vill utsätta sina anställda för en hård elektronisk kontroll och övervakning.

Ta till exempel de mycket små etiketterna för radiofrekvensidentifikation (RFID), som kan användas för att spåra var enskilda personer befinner sig minut för minut under hela dagen, och som kan fästas på personalpass eller till och med sys in i arbetsuniformer.

RFID och annan spårningsteknik, som GPS-satellitsystem, kan komma att betyda att anställda aldrig kan känna sig lediga, ens under raster och ledighet.

Vidare finns videoövervakning (som nu effektiviserats med hjälp av programvara för att analysera digitala bilder), tangenttrycksövervakning, telefonsamtalsövervakning, e-postkontroll, samt en uppsjö av andra sätt att ständigt bevaka enskilda arbetstagare.

Vi är långt ifrån idén om att informationstekniken skall hjälpa till att frigöra människans potential och skapa ett kunskapssamhälle. Istället verkar det ibland som att tekniken används för att minska möjligheterna till oberoende tänkande och handlande på arbetsplatserna. Samtidigt ser vi att den grundläggande mänskliga rättigheten till respekt och värdighet på arbetet hotas.

Ny teknik är naturligtvis inte i sig något negativt, som måste motarbetas. Syftet med denna rapport är att belysa några av överdrifterna som förekommer på arbetsplatserna, ibland kanske för att arbetsgivarna helt enkelt har velat utnyttja de möjligheter som nya programvaror erbjuder, utan att grundligt tänka igenom saken.

UNI är fast beslutet att stoppa dessa överdrifter, samtidigt som organisationen vill stödja arbetet med att utveckla de bästa arbetsmetoderna.

Philip J. Jennings
UNIs generalsekreterare

Inledning

På senare år har den elektroniska övervakningen på arbetsplatserna ökat betydligt. Nya och mycket sofistikerade digitala tekniker för detta har införts.

Dessa tekniker kan användas för att göra livet enklare och bättre för både arbetsgivare och anställda. Det händer dock oftare att de införs för ett mindre positivt syfte. Ibland kan arbetsgivarna använda dessa tekniker på ett ogenomtänkt sätt ("programvaran gör detta möjligt"), ibland kan den pådrivande faktorn vara en (allmänt grundlös) övertygelse att en hårt kontrollerad arbetskraft är mer produktiv. En del arbetsgivare kan vilja utnyttja möjligheten att få en passiv och oföretagsam arbetskraft som har mindre möjligheter att utöva sin rätt till en kollektiv organisation och representation.

Nästan alla UNI-sektorer berörs på ett eller annat sätt direkt.

Denna rapport går in i detalj på sju metoder som idag används för att elektroniskt övervaka människor på arbetet:

- Radiofrekvensidentifikation (RFID)
- Påsättsdatorer och datorröster
- Satellit- och mobiltelefonspårning
- Videoövervakning
- E-post- och webbövervakning; tangenttrycksövervakning
- Telefonsamtalsövervakning och arbete på teletjänstcentraler
- Övervakning med hjälp av biometri och implantat.

Vi utreder vidare några av den elektroniska övervakningens konsekvenser för fackföreningarna, särskilt vad gäller organisering och rekrytering, arbetsmiljö, skyddet av den privata sfären och utvecklingen av ett verksamhetsprogram som bygger på Internationella arbetsorganisationens koncept om anständigt arbete. Vi avslutar med ett antal konkreta förslag till framtida åtgärder av UNI och dess medlemsförbund.

1. Radiofrekvensidentifikation (RFID)

Radiofrekvensidentifikation ser ut att kunna bli en av de mest allstädes närvarande nya teknikerna. Radioetiketter används redan i många olika sammanhang, som i elektroniska betalkort, som i många länder används för att betala vägtullar, buss- och tunnelbanebiljetter, i stöldskyddsetiketter som klädbutiker använder för att avskräcka från snatteri, i "intelligenta" bagageetiketter som nu används på vissa flygplatser, och även i tidtagningsutrustningen som används under maratonlopp. Inom handeln används radioetiketter för logistiken för att följa lagervaror. Stora handelsföretag, som Wal-Mart, kräver av sina leverantörer att de använder dem.

Radioetiketter är små mikrochip, i vissa fall så små som ett sandkorn, som innehåller unika uppgifter som identifierar det märkta föremålet. Dessa etiketter, som är utrustade med en liten antenn, kan avläsas på avstånd av en RFID-läsare. Beroende på vilken radiofrekvens som används och vilken slags etikett det är kan de i vissa fall avläsas på flera kilometers avstånd. Det är dock vanligare att tekniken används på kortare avstånd. Etiketterna kan vara passiva (de "väcks" när de läses av) eller aktiva, utrustade med ett eget mikrobatteri och en egen radiosändare.

Priset för de billigaste radioetiketterna har fallit till mindre än en halv USA-dollar, så det blir alltmer möjligt att använda tekniken i stor skala. Handelsföretag förutser att radioetiketter inom kort kommer att ersätta streckkoder på stormarknadernas varuhyllor. Den viktiga skillnaden är att streckkoderna är desamma för enskilda varuslag, medan man med radioetiketter kan *ge varje enskild förpackning* en unik radiokodidentifikation. Det har genomförts pilottester i flera länder.

Denna användning av radioetiketter är kontroversiell. En aktiv amerikansk konsumentförening som kallar sig Konsumenter mot supermarknadernas numrering och intrång i den privata sfären, CASPIAN, säger att radioetiketter gör det möjligt att kartlägga enskilda personers inköpsmönster. CASPIAN menar att "spionetiketterna" kan vara effektiva mekanismer för att inkräkta i enskilda personers privatliv[2].

Radioetiketter kan användas för att identifiera och spåra människor, lika väl som varor. De används redan i länder som USA och Japan för att spåra gamla människor i ålderdomshem, patienter och personal i sjukhus, spädbarn på förlossningsavdelningar och skolbarn när de är i skolan. Även denna senare användning har varit kontroversiell. En grundskola nära Sacramento i Kalifornien tvingades nyligen på grund av påtryckningar från föräldrar att upphöra med att spåra eleverna med hjälp av radiochip.[3]

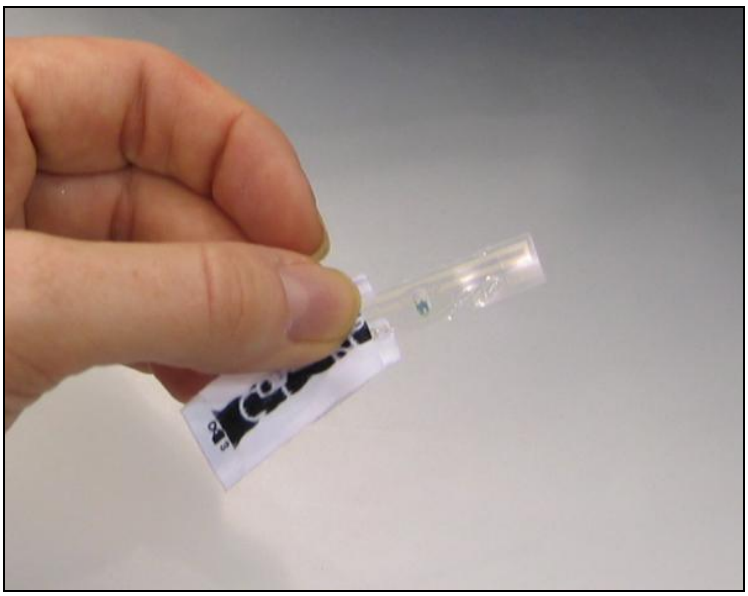
Vad gäller arbetsplatser kommer betänkligheterna om RFID-tekniken förmodligen att gälla två frågeområden.[4] För det första kan radioetikettering av varor och föremål bidra till en kompetensavveckling av en del jobb och till nya arbetsmetoder, där arbetet alltmer styrs av teknikens krav. Vi återkommer till detta när vi beskriver förändringar i arbetet på varulager.

Mer betydelsefulla är de möjligheter som RFID-tekniken erbjuder för att spåra anställda under hela arbetsdagen (och även därefter). Det finns tillfällen då detta är önskvärt; enligt en rapport har till exempel gruvarbetare i Sydafrika och Chile idag radioetiketter i sin andningsutrustning för att kunna spåras i fall av olyckor.[5] Önskvärda användningsområden som dessa hör dock förmodligen till undantagen.

Ta till exempel denna rapport om användning av RFID-tekniken tillsammans med andra former av elektronisk övervakning som det japanska elektronik-företaget Omron infört på sin anläggning i Kyoto:

"Omrons nya produktionsledningssystem använder radioetiketter, video-kameror, tillträdes- och säkerhetskontrollsystem, m.m. för att övervaka hur mycket anställda bidrar till produktionen. Anställda måste bära radioetiketter för att det skall kunna kontrolleras var de befinner sig, men också för att kontrollera deras arbetsprestationer. På grundval av dessa åtgärder kan fördelningen av de anställda optimeras, och produktkvaliteten höjas."[6]

Ett sätt att spåra anställda med RFID-tekniken är att sy in radioetiketter i uniformer. Etiketterna kan till exempel fästas i märkesetiketter (bilden nedan[7] visar baksidan på en liten märkesetikett från Calvin Klein, med den genomskinliga radioetiketten). RFID-industrin arbetar också med att använda klädernas fibrer som antenner. Sådana kläder kan tvättas på vanligt sätt utan att radioetiketterna skadas.



Ett exempel är att servitriser på ett kasino i Las Vegas nu har uniformer med radioetiketter. En högre chef på företaget sade enligt rapporter att man nästan redan på försökets första dag ertappade en anställd som "slog dank".[8]

Kasinoarbetare i det stora Star City-komplexet i Sydney, Australien, har också fått radioetiketter insydda i sina uniformer,[9] vilket dock mest verkar ha gjorts för att hantera uniformskläderna. Även om anställda inledningsvis hade vissa betänkligheter, har användningen i allmänhet accepterats. Anställda i Star City är fackligt organiserade i UNI-förbundet LHMU (Liquor, Hospitality and Miscellaneous Union). LHMU påpekar att de anställda inte bär uniformerna hemma, så de spåras inte under ledig tid.

Det är dock inte nödvändigt att ha en radioetikett i uniformen för att kunna spåras under arbetsdagen. Den absolut vanligaste platsen för en radioetikett på arbetet är namn- och identitetsbrickor som bärs för att kontrollera tillgången till byggnader och rum.

De tas idag för givet som normala säkerhetsåtgärder på många arbetsplatser, men inte bara ingångskontrollsystemen utnyttjar idag informationen som samlas in med hjälp av identitetsbrickor med radioetiketter. Uppgifterna samkörs vanligtvis med andra databaser i företaget, inklusive personal- och lönedatabaser. Ett IT-företag erbjuder till exempel programvara som utnyttjar information från ingångskontroller för att ta fram olika rapporter, "inklusive närvarorapporter, tidkortrapporter, lönerapporter, övertidsrapporter, lönesammanfattningar, frånvarorapporter, närvarolistor, personallistor, för tidig hemgång…".[10]

RAND Corporation undersökte nyligen användningen av uppgifter som inhämtats med hjälp av radioetiketter i sex företag i USA. Man fann att de anställda nästan genomgående hölls ovetande om tekniken, och sammanfattade sina resultat så här:

"Företagen använder RFID-kort för tillträde till arbetsplatsen för mer än bara att öppna dörrar (t.ex. för att genomdriva regler om beteendet på arbetsplatsen). En uttrycklig och skriven politik för hur korten används existerar i allmänhet inte, och de anställda får inte veta vilken politik som tillämpas. Användningen av sådana system har förändrat den traditionella balansen mellan personlig bekvämlighet, säkerhet på arbetsplatsen och skydd för den privata sfären, och minskat de praktiska möjligheterna att vara obemärkt. Sådana system innebär också att det uppkommer frågor om innebörden och genomförandet av en rimlig informationshanteringspraxis."[11]

RANDs forskare var tydligt överraskade och upprörda över att anställda inte fick del av en skriven informationspolitik eller information om användningen av dessa tekniker, och kom till slutsatsen att "Varje läsare som använder RFID-kort för tillträde borde känna sig illa till mods efter att ha sett dessa resultat."

En inledande diskussion om innebörden av radiofrekvensidentifikation med avseende på skyddet av den privata sfären och dataskydd anordnades år 2003 under internationella konferensen om data- och dataskyddsinspektioner.[12] Även EUs dataskyddsarbetsgrupp har tagit upp frågan.[13] EU-gruppen menar att radioetikettövervakning bör ske i enlighet med principerna för dataskydd, inklusive förhandsinformation om etiketternas existens, och enskilda personers rätt att få tillgång till sina personuppgifter. Det står dock klart att det fortfarande är för tidigt för att utarbeta tydliga internationella regler.

Även fackföreningar har börjat ta upp frågan om RFID-övervakning.

 Det brittiska fackförbundet GMB kritiserade i juli 2005 EUs dataskyddsarbetsgrupp för att man inte tog upp dataskyddsaspekterna av RFID-teknikens användning på arbetsplatserna, och krävde att RFID-etikettering av arbetstagare skulle olagligförklaras inom EU. Förbundet menade att arbetstagarnas rätt till en privat sfär undergrävdes.[14]

 Tyska Ver.di föreslår att följande checklista används när RFID-tekniken används på en arbetsplats:[15]

- Har anställda i god tid fått nödvändig information om planer på att införa RFID-tekniken?
- Finns det några hälsofrågor eller –risker i samband med användning av radiovågor, skanningsutrustning eller fotoelektriska lås på arbetsplatsen?
- Hur påverkar tekniken arbetsrutinerna och hur förändras i praktiken arbetsvillkoren och arbetsmiljön?
- Vilka följder kommer införandet av RFID-tekniken att få för rationaliseringsarbetet?
- Kommer anställda att få tillräcklig utbildning om användningen av RFID-tekniken?
- Vilka uppgifter, och i synnerhet vilka personliga uppgifter, kommer att lagras, var kommer de att lagras, och hur länge?
- Kommer uppgifterna, när de ackumuleras, att användas för att kontrollera de anställdas beteende och prestationer?
- Vem är ansvarig för att sådana uppgifter inte är missvisande?
- Hur kan de anställda skydda sig mot missbruk?

UNI Handel har antagit ett uttalande om införandet av RFID. Man kräver en seriös arbetsmarknadsdialog med företagen innan det vidtas åtgärder för att införa tekniken.[16]

2. Påsättsdatorer och datorröster

Produktidentifiering med RFID och vanliga streckkoder kombineras med ny teknik för syntetiska röster och påsättsdatorer för att skapa en arbetsmiljö där arbetstagarna alltmer förvandlas till automater. Det sker särskilt i varuupplag.

Det brittiska fackförbundet GMB genererade en betydande nationell och internationell uppmärksamhet under mitten av år 2005, när man pekade på arbetsförhållanden i vissa brittiska lagerlokaler, som man sade liknade hönsfarmer: "Arbetstagarnas enda uppgift är att följa datorkommandon. Dessa anordningar räknar ut hur lång tid det tar att gå från en del av lagret till en annan, vilka raster arbetstagarna behöver och hur länge de behöver för att gå på toaletten. Avvikelser från dessa tider tolereras inte. Anordningarna har i själva verket gjort arbetstagarna till ett stöd för datorerna snarare än tvärtom."[17]

Ett typexempel som GMB nämner är ett lager på 12 000 kvadratmeter i Wales som betjänar 240 affärer. Arbetstagarna som plockar varor är utrustade med påsättsdatorer som fästs på vristen och underarmen. Datorn har också en skanner som spänns fast på pekfingret. Utrustningen tillverkas av det specialiserade IT-företaget Symbol och väger 320-350 gram (se bild)[18].

Enligt Symbol erhåller vristterminalen plockningsinstruktioner via det trådlösa lokala nätverket från företagets styrdatorsystem. "När tomma lastvagnar anländer i plockningsområdet skannas dess streckkod av en plockare.

Vristterminalen instruerar sedan honom eller henne att gå till rätt gång och plats, och säger vilka varor som skall plockas. När en plockare kommer fram till en gång skannas streckkoden där, för att verifiera att det är rätt gång. Sedan skannas ytterligare en streckkod vid plockplatsen för att verifiera att det är rätt plats. Slutligen skannas varje vara som läggs i vagnen."[19] Med GMBs ord, "Människans enda funktioner är bitarna som ännu inte har automatiserats."

Påsättsdatorer finns idag av två slag, sådana som bärs på vristen och fingret (som på bilden), och sådana som bärs på huvudet eller i bältet. De kombineras ofta med datorröster, varvid lagerarbetare får hörlurar genom vilka de får datorgenererade instruktioner om vad de skall plocka. Datorröstsystemen är vanligtvis kopplade till orderhanterings- eller lagerprogramvara, vars utdata omvandlas till röstkommandon.[20]

Både GMB och Professor Michael Blakemore, den brittiska akademiker som arbetar med denna fråga åt GMB, har pekat på arbetsmiljöaspekter av denna teknik. Blakemore menar att det endast finns en mycket liten insikt om att den nya utrustningen kan få negativa hälsoeffekter, trots att man vet att tidigare tekniker lett till problem med belastningsskador på grund av ensidigt upprepat arbete.[21]

Lagerplockningssystem som dessa automatiserar inte bara arbetsprocessen, de är också ett fenomenalt medel för att kontrollera arbetstagarna. Blakemore citerar ett yttrande från ett företag: "Det är också mycket lätt att använda som ledningsverktyg. Möjligheten att spåra och följa vad varje person gör är fantastisk."

3. Satellit- och mobiltelefonspårning

Förutom radiofrekvensidentifikation finns det även andra sätt än att spåra föremål eller personer med stor precision.

Satellitnavigering bygger idag på det amerikanska GPS-systemet (GPS = Global Positioning System). Systemet arbetar med ett nätverk av satelliter, som ursprungligen hade militär användning. Systemet sköts fortfarande från USAs försvarshögkvarter Pentagon. Varje satellit sänder kontinuerligt ut data som fastställer dess position. GPS-mottagare analyserar dessa signaler, och genom att jämföra signaler från fyra satelliter eller fler kan den egna positionen och höjden över havet fastställas med stor precision. (Minst fyra satelliter bör vara "synliga" över horisonten för varje mottagare vid varje enskild tidpunkt.)

Europeiska unionen håller på att utveckla ett rivaliserande satellitnavigerings-system med namn Galileo. Den första satelliten i Galileonätverket sköts upp i december 2005.

Mobiltelefontekniken gör det också möjligt att spåra enskilda mobiltelefoner. Tekniskt sker det genom att man jämför mobiltelefonens avstånd till de närmaste mobilmasterna, som tillsammans utgör mobiltelenäten som mobiltelefonin bygger på. Särskilt i storstadsområden, där det finns många basstationer, kan mobiltelefoner spåras med stor precision. I typfallet är felmarginalen 10-25 meter. Telefonerna kan spåras även när det inte pågår något telefonsamtal.

Dessa två tekniker håller på att växa samman, då mobiltelefoner och elektroniska planeringskalendrar allt oftare är GPS-kapabla. I till exempel Japan fungerar 20 % av mobiltelefonerna nu också som GPS-mottagare.[22]

Både GPS och mobiltelefonspårning erbjuds redan idag kommersiellt, ofta i kombination med digitala karttjänster. GPS används till exempel alltmer i navigationssystem i bilar. Mobilteleoperatörerna håller på att utforska lokaliseringstjänsternas potential (till exempel kan telefonanvändare få reda på var närmaste snabbmatsrestaurang, bankomat, eller till och med vänner och bekanta, befinner sig).

På arbetsplatserna finns det, liksom med andra tekniker, positiva sätt att använda GPS och mobiltelefonspårning, som kan underlätta för arbetstagarna. Några exempel:

- Att spåra bilar kan göra arbetet säkrare för förare av värdetransportbilar, som riskerar att rånas.
- Geografisk spårning kan bidra till att skydda mobila arbetstagare, särskilt sådana som arbetar ensamt på isolerade eller kanske farliga platser, eller nattetid.
- Geografisk spårning kan också hjälpa till att spåra mobila arbetstagare eller förare i fall av dåligt väder.

Tyvärr finns det också många exempel på hur arbetsgivare använder spårningstekniken på mycket mindre positiva sätt. Ett exempel som tagits upp av den amerikanska ideella organisationen *National Workrights Institute*:

Howard Boyle, chef för ett företag som installerar brandsprinkleranläggningar, i Woodside i den amerikanska delstaten New York, gav sina anställda mobiltelefoner, utan att informera dem om att de var utrustade med GPS. Boyle kan vid varje tidpunkt ta reda på var de befinner sig, inklusive under raster och när de är lediga. "De behöver inte veta det," sade Boyle. "Jag kan ringa upp dem och fråga, 'Var är du nu?* samtidigt som jag tittar på skärmen och vet exakt var de är."[23]

Kontinuerlig spårning innebär en ständig press på arbetstagarna, som känner att de bevakas varje ögonblick under arbetsdagen. En chaufför i USA, vars lastbil var utrustad med GPS, har sagt följande:

"Det är lite grann som 'Storebror ser dig'… Jag blir retlig på fiket när jag står i kö och väntar på kaffet. Jag har lust att säga 'skynda på, de kollar. Jag måste gå'".[24]

I Kanada har postarbetareförbundet CUPW uppmanat sina medlemmar att noggrant informera sig om postföretagets åtgärd att utrusta flera hundra varubilar med GPS-kapabla datorer. Datorerna övervakar var varje bil befinner sig, om motorn är på, om bilen rör sig, och i så fall hur fort, samt om dörrarna är stängda. Canada Post sade till fackförbundet att syftet var att göra det möjligt för arbetsledare att ta reda på – med hjälp av så kallade "särfallsrapporter" som utarbetas av datorn – om förarna kör på ett säkert sätt och följer säkerhetsföreskrifterna.[25]

CUPW har hänvisat till det gällande kollektivavtalet med Canada Post för att försäkra sig om att denna övervakning inte utnyttjas i disciplinärt syfte.

 Bestämmelsen som handlar om övervakning i CUPWs kollektivavtal med Canada Post lyder som följer: "Sådana [övervaknings- och observationssystem] får inte användas för att utvärdera anställdas prestationer eller för att samla uppgifter för att stödja disciplinära åtgärder, med undantag för när sådana disciplinära åtgärder är följden av kriminella handlingar."[26]

Även i andra länder har fackföreningar ingripit för att kontrollera användningen av GPS-system. I USA har fackförbundet *Teamsters* förhandlat med UPS för att GPS-spårningsuppgifter inte skall användas för utvärdering av anställda, eller för disciplinära syften.[27] Teamsters har också ifrågasatt användningen av GPS-system i andra transport- och kurirföretags, och av offentliga myndigheter.

När det finns spårningssystem är det särskilt viktigt att arbetstagarna kan se till att de inte är i funktion under raster och efter arbetsdagens slut.

 Amicus (Storbritannien/Irland) har rapporterat att man med framgång lyckats ifrågasätta ett bilspårningssystem som ett intrång i den privata sfären, och sett till att anställda skall ha möjlighet att stänga av det.[28]

Geografiska spårningstjänster, i synnerhet GPS, har spritt sig snabbt på senare år, även om vi förmodligen bara befinner oss i de första stadierna av teknikens utbredning. 2005 års undersökning om elektronisk övervakning och kontroll som *American Management Association* genomfört i 526 företag i USA visar att 8 % av dem använde sig av GPS eller GPS och mobiltelefonspårning av fordon, medan 5 % spårade anställdas mobiltelefoner.[29]

Det är fortfarande relativt tidig i arbetet med att fastställa lämpliga skyddsmekanismer och goda arbetsmetoder för att skydda det som kallas för det "geografiska privatlivet".[30] I en handledning som den kanadensiska juridiska rådgivaren David Canton erbjuder arbetsgivarna föreslås det en checklista på fyra punkter för GPS-spårning:[31]

- fastställ behovet
- fastställ en politik om skydd av den privata sfären
- bevaka stämningen på arbetsplatsen
- be om samtycke.

Canton varnar att GPS visserligen kan leda till högre effektivitet och produktivitet, men "det kan också leda till låg arbetsmoral, motreaktioner från anställda och möjligen juridiska processer".

Mer allmänna betänkligheter om att enskilda individer skall kunna skydda sitt "geografiska privatliv," i synnerhet under sin fritid, har tagits upp av *National Workrights Institute*. Som de säger, "Om en anställd vet att chefen följer hans vardag, tänker han sig kanske för innan han deltar i vissa aktiviteter. Om chefen till exempel är en aktiv anhängare av det republikanska partiet, väljer en anställd kanske att inte gå på det demokratiska partiets nationella konvent."[32]

4. Videoövervakning

Öppen och dold övervakning av arbetsplatser med hjälp av videokameror har varit en angelägenhet för fackföreningar under flera år. Redan 1993 gjorde till exempel *Communications Workers of America* en amerikansk senatskommitté uppmärksam på ett fall där kvinnliga anställda hade funnit att företagsledningen hade dolt en kamera i deras omklädningsrum. Kameraövervakningen sköttes av manliga väktare, som tittade på när de anställda bytte till sina uniformer.[33] Rapporter om liknande fall, där kameror installerats i tvättrum eller omklädningsrum har inkommit även från andra länder.[34]

Videoövervakning är en fråga som regelbundet ger upphov till dispyter på arbetsplatser, i synnerhet när det sätts upp kameror utan föregående samråd, eller när de används i hemlighet för att kontrollera anställdas prestationer eller i disciplinärt syfte. Ett exempel på detta på senare tid är att Deutsche Post installerat kameror i huvudsorteringsanläggningen i Berlin, där det finns 650 anställda. Enligt planen skulle kamerorna vara igång uppemot femtio timmar varje vecka. Denna användning bedömdes vara överdriven av en federal arbetsdomstol i Tyskland.[35]

Användningen av övervakningskameror skapar idag fler problem än tidigare, då kamerabilder övervakades i realtid eller spelades in på magnetband. Idag är kamerabilderna ofta digitala och kan sparas på obestämd tid tillsammans med andra datafiler. Det blir då möjligt att koppla samman uppgifter från övervakningskameror som riktats mot enskilda anställda med andra uppgifter om denna person, till exempel personaluppgifter, uppgifter som härrör från e-postkontroller eller inspelade telefonsamtal. Därmed skulle arbetsgivaren kunna samla mycket allsidig information om enskilda anställd.

EUs dataskyddsarbetsgrupp har uppmärksammat olika risker i samband med utvecklingen av programvaror som kan analysera videobilder, till exempel program för ansiktsigenkänning, som kan identifiera enskilda individer. I sin rapport från år 2004 om videoövervakning skriver arbetsgruppen: "Trenden i utvecklingen av programvara som bygger på både ansiktsigenkänning och på att man studerar och förutser ett tänkt mänskligt beteende bör utvärderas för att förhindra att vi oövertänkt går mot en dynamisk-preventiv övervakning – i motsats till en konventionell övervakning, som främst syftar till att dokumentera

specifika händelser och personer som utför vissa handlingar. Denna nya form av övervakning bygger på en automatisk registrering av individers ansiktsdrag, samt av 'avvikande' beteende, i förbindelse med att det finns automatiska alarm och signaler, vilket kan innebära risker för diskriminering."[36]

Det blir med andra ord allt viktigare att se videoövervakning inte bara som en fristående säkerhetsåtgärd, utan som en källa till uppgifter i vilka man kan göra sökningar och som kan analyseras med den aktuella datorteknikens alla möjligheter. Ett tecken på denna trend är Cisco Systems utveckling av AVVID-systemet (Architecture for Voice, Video and Data) som samlar röst-, video- och datauppgifter. Man säger att det kan användas inte bara för att höja säkerheten i bankbranschen, utan också för marknadsföringen och i kundrelationerna, för att maximera bankkontorens värde.[37]

Mot bakgrund av en sådan utveckling blir det än viktigare att sörja för att videoövervakningen kontrolleras på ett lämpligt sätt. EUs dataskyddsgrupp pekar på centrala dataskyddsprinciper, inklusive att användningen måste stå i proportion till syftet och att de som utsätts för övervakningen måste informeras om detta i förväg. Speciellt för arbetsplatser säger arbetsgruppen att man måste skydda de anställdas "rättigheter, friheter och värdighet," och man gör följande kommentarer:

"Videoövervakningssystem som direkt syftar till att på avstånd kontrollera arbetsverksamheters kvalitet och kvantitet… bör som regel inte tillåtas…"

"Erfarenheterna har dessutom visat att övervakningen inte bör omfatta platser som antingen har reserverats för de anställdas privata användning, eller som inte är avsedda för att där utföra arbetsuppgifter – som toaletter, duschrum, omklädningsrum eller vilorum, att bilderna som registrerats uteslutande för att skydda egendom eller för att upptäcka, förhindra och kontrollera allvarliga brott inte bör användas för att anklaga anställda för mindre disciplinbrott, samt att anställda alltid bör kunna framföra egna synpunkter genom att använda innehållet i de insamlade bilderna. Anställda och andra personer som arbetar på platsen måste informeras."

Hemlig övervakning leder till särskilda problem, som ett exempel från Sverige visar. För närvarande förhandlar Svenska Transportarbetareförbundet med Securitas för att kontrollera företagets användning av hemliga övervakningsbilar utrustade med kameror för att filma egna fordon och anställda.

Securitas har redan idag kameror i sina fordon, men dessa börjar filma endast om bilar attackeras, eller om dörrar öppnas på ett obehörigt sätt, en praxis som accepteras av fackförbundet. Det väpnade rånet av en Securitasbil på en motorväg söder om Stockholm i december 2005 visade hur viktigt det är med tillräckliga säkerhetsåtgärder. Hemlig kameraövervakning från omärkta bilar har dock kritiserats hårt av Securitasanställda.

Transportarbetareförbundet förutser ett tillfredsställande resultat av förhandlingarna och hoppas på ett avtal med företaget, som skall kunna tillämpas i alla de nordiska länderna.[38] UNIs danska medlemsförbund DFF har redan gjort en överenskommelse med Securitas som begränsar videoövervakningen och förhindrar att inspelade videofilmer används för disciplinära ändamål. Anställda måste informeras om övervakningen under rekryteringsprocessen.

Mer allmänt finns det redan flera exempel på bra sätt att kontrollera videoövervakning. I flera länder har det antagits lagar; i Nya Sydwales, Australien, har skyddet av arbetstagarna i lagen om videövervakning på arbetsplatser, från 1998 (som infördes efter en rad arbetskonflikter i delstaten) nyligen utsträckts till andra former av elektronisk övervakning. I Österrike krävs det ett godkännande av företagsnämnden innan permanent videoövervakning kan införas.[39]

I Belgien regleras användningen av kameror på arbetsplatser i ett kollektivavtal med laglig kraft från 1998 som täcker in hela den privata sektorn.

Det belgiska avtalet bygger på principen om proportionalitet och slutligt syfte. Permanent övervakning kontrolleras strikt, och tillåts endast när syftet är att skydda arbetstagares säkerhet eller företagets egendom. Hemlig videoövervakning är förbjudet, utom när det finns tydliga tecken på kriminell verksamhet. Kameror kan installeras endast efter samråd med fackföreningarna, och berörda arbetstagare måste informeras på förhand. Syftet med kameraövervakningen måste tydligt anges.[40]

5. E-post- och webbaccesskontroll; tangentnedslagskontroll

Olika frågor i samband med att arbetsgivare övervakar anställdas e-post och Internetanvändning har fått stor uppmärksamhet på senare år, delvis för att övervakningen har lett till praktiska problem på många arbetsplatser, och lagt grunden för ett växande antal enskilda disciplinära fall.

UNI (och UNIs föregångare FIET) har redan tidigt, genom kampanjen om näträttigheter för direktkopplade arbetstagare, som lanserades 1998, intresserat sig för området. UNIs kod för näträttigheter fastlägger riktlinjer för bra arbetsmetoder, som anammats av både fackföreningar och andra organisationer.

UNIs kod tar upp fyra frågeområden som griper i varandra, och som rör e-post och Internetanvändning på arbetsplatsen: arbetstagarnas representanters rätt att kunna kommunicera elektroniskt, i vilken utsträckning enskilda anställda skall kunna använda e-post och Internet för personliga syften, villkoren för att tillåta en sådan personlig användning, och slutligen bevakning och kontroll av e-post och Internetanvändning. I denna rapport skall vi endast beröra det sista frågeområdet.

 UNIs kod innehåller följande avsnitt om övervakning och kontroll av kommunikation:

Arbetsgivaren förbinder sig att inte i hemlighet övervaka och kontrollera anställdas användning av företagets elektroniska kommunikationsanordningar.

Kommunikation kommer att övervakas endast om det tillåts i kollektivavtal, om arbetsgivaren är förpliktad till det enligt lag, eller om arbetsgivaren har rimliga skäl att tro att en anställd har brutit mot lagen eller begått ett allvarligt disciplinbrott. Tillgång till inspelningar som hänför sig till enskilda anställda skall endast ske i närvaro av en fackföreningsrepresentant eller en representant som utsetts av de anställda.

UNIs kod bygger på principer som redan är allmänt etablerade i procedurer för dataskydd i samband med hantering av uppgifter om enskilda personer, liksom i ILO-regler och skyddsåtgärder för mänskliga rättigheter.[41]

I anslutning till UNIs initiativ har flera medlemsförbund tagit upp frågan, och i många fall också utarbetat egna riktlinjer och koder. Några är GPA (Österrike), MSF (idag Amicus, Storbritannien och Irland), CFDT BETOR-PUB (Frankrike) och FNV Bondgenoten (Nederländerna, se nedan).

 FNV Bondgenotens modellavtal för skydd av den privata sfären vid användning av Internet och e-post innehåller följande bestämmelse:

Arbetsgivaren skall inte läsa innehållet i personliga e-brev eller -affärsbrev. Personliga uppgifter om antal e-brev, e-postadresser eller andra relevanta uppgifter skall heller inte registreras eller kontrolleras. Detta påverkar dock inte arbetsgivarens rätt att göra sporadiska kontroller på grundval av tvingande skäl som ligger i företagets intresse. Sådana kontroller skall rapporteras till medbestämmanderådet.[42]

I Tyskland har Ver.di tillsammans med IG Metall och huvudorganisationen DGB startat en kampanj om näträttigheter och webbplatsen www.onlinerechte-fuer-beschaeftigte.de. Kampanjen startades i mars 2002 från ett Internetkafé i Berlin, och den har fått stort utrymme i medierna. Den interaktiva webbplatsen innehåller information om gällande lagar och ett diskussionsforum.[43] Initiativet har följts av ett uttalande i sex punkter om användningen av Internet, intranät och e-post som godkänts av DGB-styrelsen i februari 2004[44].

Detta flygblad togs fram för de tyska fackföreningarnas kampanj om näträttigheter. Texten lyder: "Jag skriver brev, för min chef läser min e-post."

I flera länder, som Österrike och Danmark (i avtalet mellan HK-Service och de danska handelsarbetsgivarna),[45] har man ingått kollektivavtal på detta område. Det viktigaste nationella kollektivavtalet är det som de belgiska arbetsmarknadsparterna enades om i april 2002.

Det belgiska kollektivavtalet[46] (som har laglig kraft) fastlägger att övervakningen av anställdas nätanvändning endast får ske inom vissa gränser. Vad gäller Internet kan arbetsgivare samla uppgifter om hur länge uppkopplingar varat, men inte om vilka webbplatser enskilda individer besökt. Beträffande e-post kan volymen och antalet e-brev registreras, under förutsättning att dessa inte kopplas till individer.

Frågan om anställdas användning av e-post och Internet har också uppmärksammats av Europeiska unionen. EUs dataskyddsgrupp har fastställt allmänna principer för e-post- och internetövervakning. De sammanfattas under följande rubriker: nödvändighet, syfte, genomsynlighet, legitimitet, proportionalitet, precision och bevarande av data, samt säkerhet.[47] I EU-kommissionens dokument för andra fasen i ett samråd med arbetsmarknadens parter om personuppgifter om arbetstagare föreslås också en europeisk ram som täcker in elektronisk övervakning.[48] Denna omfattar följande:

- Hemlig övervakning bör tillåtas endast i enlighet med de garantier som föreskrivs i nationell lag, eller om det finns skälig misstanke om brottslig verksamhet eller andra allvarliga missgärningar.
- Personliga uppgifter som insamlats genom elektronisk övervakning bör inte vara de enda faktorerna i en utvärdering av arbetstagares prestationer och för att fatta beslut som berör dem.
- Det är i princip förbjudet för arbetsgivare att läsa privat e-post eller andra privata filer…

Det skulle dock vara fel att tro att all denna verksamhet på ett tillfredsställande sätt har löst problemen med e-post- och Internetanvändning. I Kanada fann man till exempel under en färsk akademisk undersökning att spännvidden mellan olika praxisar var mycket stor, även i fall där man hade uppnått kollektivavtal. I de svagaste avtalen erkände enligt forskaren fackföreningarna arbetsgivarnas rätt att använda sig av alla möjliga former av elektronisk övervakning när och var de önskade det.[49]

Även i USA är den elektroniska övervakningen mycket utbredd. Enligt utbildningsinstitutionen *American Management Association* övervakar 76 % av alla arbetsgivare de anställdas Internettillgång; 55 % sparar och går igenom anställdas e-post. 2005 års AMA-undersökning visade att mer än vart fjärde företag hade avskedat anställda för påstått missbruk av Internet, och att ytterligare 25 % hade avskedat anställda för e-postmissbruk. Trots detta fann AMA också att vart tionde företag inte talade om för sina anställda att man övervakade Internetanvändningen; 14 % talade inte om att e-posten kontrollerades.[50]

Det är svårt att inte hålla med Hubert Bouchet från den franska IT-kommissionen CNIL, som har pekat på att anställda till stor del är ovetande om den övervakning som sker på arbetsplatserna: "Den nödvändiga balansen mellan en legitim kontroll från företagets sida och respekten för arbetstagarnas rättigheter verkar inte fungera i många fall.[51]

Det är intressant att notera att det i AMA-undersökningen också står att en av tre arbetsgivare (36 %) övervakar antalet nedslag på tangentbord, vilken tid arbetstagare befinner sig vid tangentbord eller innehållet i materialet som matas in. Facket har kritiserat en rutinmässig övervakning av arbetstagares tangent-nedslag, särskilt för lågavlönad personal som arbetar med grundläggande datainmatning, i många år. Krav på en orealistiskt hög produktivitet vid

tangentbord kan vara en bidragande orsak till förslitningsskador, som har nått en närapå epidemisk spridning i vissa länder.

En detaljerad inventering av maskin- och programvara som kan användas för att registrera tangentnedslag har gjorts för tyska fackföreningar av Gerrit Wiegand, som har skrivit om sina resultat i boken *Im Netz@work*.[52]

I detaljhandeln har det funnits liknande betänkligheter med avseende på automatisk övervakning av kassörers skanningstakt sedan streckkoder och elektronisk kassautrustning först infördes. Tekniken kan användas för att i detalj övervaka exakt vad anställda gör under sin arbetstid, inklusive sådana saker som precisa tidpunkter för när de går på toaletten. Men bara för att tekniken möjliggör elektroniskt spionerande av detta slag behöver den inte användas så. Det kan vara värt att notera att de anställda i Metros nya "framtidsbutik" i Rheinberg har möjlighet att logga in anonymt för att sköta sådana saker som affärens elektroniska vågar, så att inga personliga uppgifter registreras.

6. Övervakning av telefonsamtal, arbete på teletjänstcentraler

Telefonsamtal kan övervakas på olika sätt. Det går att registrera antalet samtal och hur länge de varar, telefonnummer som rings upp kan registreras, själva telefonsamtalen kan avlyssnas av arbetsledare, öppet eller i hemlighet, och samtalen kan spelas in. Även röstmeddelanden kan sparas och avlyssnas.

I USA övervakar nästan exakt hälften av företagen telefonsamtal genom att registrera uppringda telefonnummer och samtalstiden; två tredjedelar av dessa företag gör denna övervakning regelbundet, eller löpande. Enligt *American Management Association* informerar 22 % av företagen dock inte sina anställda om övervakningen. Nästan vart fjärde företag spelar in telefonsamtal.[53]

I vissa industrier (som bank och försäkring) kan det finnas juridiska skäl eller regleringskrav som gör att telefonsamtal måste spelas in. Det betyder dock inte att inspelade samtal rutinmässigt skall kunna utnyttjas för andra ändamål, som för att bevaka enskilda arbetstagares produktivitet, eller för disciplinära syften. Telefonsamtal sparas alltmer i digital form, och liksom med digital videofilm från övervakningskameror öppnar detta för att sparat material integreras med andra personuppgifter och analyseras med datorprogramvara.

Anställda bör informeras om att samtal spelas in.

En del företag säger att de lyssnar på eller spelar in samtal "i utbildningssyfte". Det kan under vissa förhållanden vara legitimt att företagen gör detta, om syftet är att upprätthålla kvaliteten i arbetet med att hantera telefonsamtal. Anställda som behöver stöd på detta område bör absolut få en lämplig utbildning. Denna sorts övervakning bör dock inte missbrukas för andra syften av arbetsgivaren.

Arbetstagare i teletjänstcentraler ställs mer än de flesta andra inför dessa frågor. I en UNI-rapport om teletjänstcentraler påpekades det redan tidigt att "tekniken på teletjänstcentraler i allmänhet ger arbetsgivarna möjlighet att utsätta de anställda för en häpnadsväckande elektronisk övervakning."[54]

Teletjänstarbetare har mycket liten kontroll över sitt arbete. De tar samtal som dirigeras till dem av automatisk vidarekopplingsutrustning, de är i många fall tvungna att följa färdiga manuskript när de talar med uppringare, och de har

rigida försäljnings- eller prestationsmål. Den automatiska vidarekopplingsutrustningen registrerar vanligtvis alla aspekter av samtalshanteringen, inklusive tiden för raster eller toalettbesök. I UNIs globala nyhetsbrev om teletjänstcentraler rapporterades det nyligen om en kvinna som tvingades att berätta för sin chef, innan hon ens hade talat om det för sin egen familj, att hon var gravid, för att förklara varför hon hade gjort "för många" toalettbesök.[55] (Det var bland annat detta fall som inspirerade oss till den fiktiva berättelsen om Marta, som inleder den här rapporten.)

UNIs stadga för teletjänstcentraler och handlingsplanen som utarbetades i samband med UNIs första teletjänstkonferens i oktober 2005 tar båda upp frågan om den övervakning som sker.

 UNIs stadga för teletjänstcentraler innehåller sex punkter under rubriken övervakning, elektronisk registrering och skydd för den privata sfären:

- Övervakning får endast ske om syftet är känt och acceptabelt.
- Insamlade uppgifter får endast användas i detta syfte.
- Anställda måste veta att de övervakas eller kan övervakas.
- Avlyssning får endast ske tillfälligtvis och inte kontinuerligt.
- Anställda måste ges tillgång till inspelningar och insamlade uppgifter och kunna rätta felaktigheter.
- Inspelningar måste förstöras efter en viss tidsperiod.

En annan konkret åtgärd har nyligen vidtagits av UNI Telekom inom ramen för den europeiska sociala dialogen med arbetsgivarföreningen ETNO; man har verkat för en bestämmelse om övervakning i de överenskomna riktlinjerna för kundtjänstcentraler. En av de centrala principerna är att teletjänstarbetare måste informeras om det pågår prestationsövervakning.

UNI-förbundens erfarenheter visar att det är möjligt att förhandla om bättre arbetsförhållanden för teletjänstarbetare. Flera fackföreningar i telekomsektorn har till exempel förhandlat om kollektivavtal med bestämmelser om övervakning.

 I USA har fackförbundet Communications Workers of America (CWA) förhandlat om avtal med flera telekomföretag, inklusive AT&T, Qwest, Bell South och SBC.[56]

Avtalet med AT&T innehåller bestämmelser om avlyssning av samtal:

- Anställda skall informeras på förhand dagen det tas stickprov, och var och en skall ha möjlighet att välja mellan övervakning på avstånd eller sida vid sida.
- Arbetet med att ta stickprov av enskilda samtal skall ske från den övervakade arbetstagarens arbetsområde.
- Ingen anställd skall bli föremål för disciplinstraff på grundval av stickprover av enskilda samtal, med undantag för fall av grovt ohyfsat beteende mot kunder, bedrägeri, yppande av förtroliga uppgifter, eller när andra ansträngningar för att uppnå förbättringar inte har gett resultat.

Avtalet med Pacific Bell (SBC) begränsar övervakningen av de anställda till tio samtal per månad.

I Australien har CEPU (Communication Electrical and Plumbing Union) också tacklat frågan om överdriven övervakning i teletjänstcentraler. Fackförbunden försöker att förmå de australiska delstaterna att fastställa miniminormer för arbetet på teletjänstcentraler.

Ett skäl till att övervakningen är en så viktig fråga på teletjänstcentraler är att det i ett flertal undersökningar har visats att den är en viktig orsak till stress för arbetstagarna. I en brittisk akademisk rapport skriver man "Det råder inget tvivel om att många arbetstagare verkligen tycker att övervakningsmekanismerna bidrar till pressen på arbetet. Över en tredjedel ansåg att inspelningen av deras samtal bidrog 'mycket' eller 'till en viss grad' till pressen på arbetet."[57] Vi skall återkomma till detta längre ned.

7. Övervakning med hjälp av biometri och implantat

I den avslutande delen av denna rapport skall vi kort behandla möjligheterna till elektronisk övervakning av arbetstagare på ett ännu mer direkt och påträngande sätt – genom att kartlägga och spåra individens kropp.

Biometri (att känna igen individer från unika fysiska drag) används redan i olika dagliga sammanhang. Skanning av fingeravtryck har införts i USA för att kontrollera utlänningar som besöker landet. Teknik för att känna igen ögats regnbågshinna anses vara ett särskilt lovande område när det gäller identifikation i framtiden.

Till skillnad mot hur till exempel polis förr tog fingeravtryck av misstänkta, med bläckdynor och papper, är biometrisk information digitaliserad – den sparas i digital form och kan därför bli föremål för en detaljerad, datoriserad analys. Biometrin har djupgående konsekvenser för den privata sfären. Fackföreningar kommer att behöva följa försök att införa tekniken på arbetsplatserna mycket noga.

Det finns redan exempel på att biometri har införts. Det rapporteras att McDonalds har infört skanning av tumavtryck och händer för anställda i några restauranger i Kanada.[58] Postarbetareförbundet CUPW, också i Kanada, har ifrågasatt det kanadensiska postföretagets försök att kräva att vissa brevbärare skall lämna fingeravtryck, som en del av en säkerhetskontroll.[59]

Tillverkare av radioetiketter har gått ett steg längre, med idén att implantera små radiochip under huden på enskilda personer. Det skulle vara lugnande att kunna säga att detta är science fiction, men det är det tyvärr inte. Det amerikanska företaget *Applied Digital* tillverkar redan en sådan produkt, med namnet *VeriChip*.

VeriChip marknadsförs främst som ett sätt för människor att alltid ha tillgång till sina medicinska uppgifter. Det har också använts av en nattklubb, som uppmanat stamkunder att implantera ett VeriChip för att få tillträde till klubben och betala i baren. VeriChip-implantat har också redan använts i arbetssammanhang. 18 anställda på den mexikanska justitieministerns kontor har frivilligt gått med på att ha implantat. Radiochipen (se bilden nedan[60]) används för att ge anställda tillträde till skyddade områden.

Möjliga hälsoproblem med radiochipimplantat diskuteras nedan. Även utan eventuella hälsoproblem är det dock tydligt att nya produkter som VeriChip kan få stor betydelse för skyddet av den privata sfären, både på arbetsplatsen och utanför den.

Några problem som elektronisk övervakning ger upphov till

Varför sker detta? Varför verkar en elektroniskt stödd ledningsstil för beslut och kontroll breda ut sig samtidigt som informationssamhället, enligt retoriken om "mänskliga resurser" kräver intelligent arbete och mer samarbete från anställda?

Ett cyniskt svar vore: för att tekniken för denna övervakning nu existerar. Professor Michael Blakemore, som har varit rådgivare åt det brittiska fackförbundet GMB, talar om det "lugnande" budskap som denna teknik verkar kunna erbjuda: "Djupt inbäddad i denna retorik finns löftet om säkerhet, trygghet och vinster," skriver han.[61] Men han påpekar också att det kan få långtgående följder på arbetsplatserna att man förlitar sig på teknik: "Resultatet är att relationen mellan chefer och personal ändras, så att de förra inte längre talar med de senare, utan endast övervakar dem."

Han och andra akademiker använder sig alltmer av konceptet "pervasive computing" (ung. "genomträngande datoranvändning"), som definieras som en process där datorer är inbäddade i vardagen på sådana sätt att de blir osynliga och tagna för givna.[62] En genomträngande övervakning är i analogi med detta en situation (med Blakemores ord) "där allting, eller nästan allting, som en anställd gör kan övervakas, analyseras och kontrolleras."

ILO har i sin viktiga rapport om arbetsförhållanden från år 1993 skrivit om övervakning på arbetsplatserna, att en del arbetstagare berörs mer än andra av det: arbete som utförs av kvinnor, av minoritetsgrupper och mer allmänt av lågavlönade kommer förmodligen i högre grad än annat arbete att bli föremål för en intensiv övervakning.[63] I detta sammanhang är det signifikativt att brittiska GMB i sin kampanj mot "hönsfarmförhållanden" i lagerlokaler (se ovan), rapporterade att många av arbetstagarna i de undersökta lagren var invandrare.

Poängen är därför att några arbetstagare, som i informationsåldern sysslar med kunskapsarbete med högt mervärde, kanske kommer att kunna frigöra sig från de restriktioner som en hierarkisk övervakning innebär, men att många fler kan komma att bli hårt bundna av tekniken. De kan i själva verket komma att få i samma relation till tekniken som tidigare oftast förknippats med arbete vid ett löpande band.

Tillsyn med elektroniska metoder kanske känns "tryggt" för företagen, men fungerar det? Mycket ofta verkar svaret vara: förmodligen inte. Gary Marx från MIT gjorde följande bedömning år 1999: "För närvarande är det vetenskapliga stödet för den övervakningspositiva retoriken inte starkt. Som vi kommer att notera finns det goda skäl att förvänta sig att otyglad övervakning motverkar sitt syfte. En möjlig negativ inverkan på arbetstagarnas fysiska och mentala välbefinnande kan komma att uppväga vinster genom en förment ökad effektivitet som beror på övervakningen."[64]

Men frågan är inte huruvida övervakningen fungerar för företagen. Även om det tydligt kunde visas att en genomträngande övervakning av arbetstagare ger affärsmässiga fördelar finns det flera starka skäl till att fackföreningarna bör bekämpa en sådan praxis. Vi skall ta upp tre av dem nedan.

Rätten till kollektiv representation

För det första, och mest pragmatiskt, har fackföreningarna anledning att oroa sig för att fientligt inställda arbetsgivare skall utnyttja övervakningen av arbetstagare som ett verktyg för att avskräcka från en fungerande kollektiv representation.

Det har förekommit ett antal fall där övervakning har införts just när fackföreningar har försökt att organisera arbetstagare. Ett exempel kommer från det notoriskt mest antifackliga företaget av dem alla, Wal-Mart, som riktade övervakningskameror mot "suspekta" anställda i en butik i Kentucky när UFCW försökte att organisera dem. Företaget verkar ha betett sig på ett liknande sätt i en butik i Indiana och förmodligen även på annat håll i USA.[65]

Även på platser där fackföreningarna är etablerade bidrar ett arbete under hård bevakning knappast till ett fungerande fackligt arbete. Eric Lee har påpekat att arbetstagare förr hade det lättare att viska om sina problem till fackliga representanter när de till exempel stod vid en dricksfontän.[66] Ju hårdare arbetsdagen kontrolleras, ju mindre är möjligheterna för denna slags informella kontakter mellan arbetstagare och fackombud.

Arbetsmiljöfrågor

Ny teknik för med sig nya arbetsmiljörisker. När datorarbete vid tangentbord infördes för uppgifter som datainmatning ökade antalet fall av förslitningsskador betydligt, och akustisk chock har blivit en arbetsmiljörisk för teletjänstarbetare.

Det är inte nödvändigtvis lätt att idag se exakt vad en "genomträngande datoranvändning" kommer att få för konsekvenser för arbetstagarnas hälsa. Företagen som tillverkar utrustning som har beskrivits i denna rapport lägger i allmänhet inte stor vikt vid ergonomin eller arbetsmiljön i den tekniska information de tillhandahåller.

Några potentiella frågeområden kan dock lätt urskiljas. För det första kan påsättsdatorer (som de som beskrivits tidigare i denna rapport) orsaka fysiska problem vid en långvarig användning. Som redan nämnt väger en vanlig vristdator 320 gram, och det ökar till 350 gram om den är utrustad med en radiosändare. Pekfingermonterade skannrar väger vanligtvis omkring 50 gram, varvid skanningen genomförs med regelbundna tumtryckningar.[67]

Den globala ökningen av antalet mobiltelefoner har lett till frågan om huruvida den elektromagnetiska strålningen kan medföra risker, ett forskningsområde där resultaten hittills inte är entydiga. Det verkar ha utförts endast liten forskning om andra spårningstekniker. Beträffande implanterade radiochip har USAs kontrollmyndighet *Federal Drugs Agency* godkänt användningen av VeriChip, men man har också uppmärksammat potentiella hälsorisker: "bortstötnings-reaktioner i vävnaden, migration av den implanterade transpondern, dataintrång, funktionsstörningar på inplanterad transponder, misslyckad insertion, funktionsstörningar på elektronisk skanner, elektromagnetisk interferens, elektriska risker, oförenlighet med skanning med magnetisk resonans, och nålstick."[68]

Mer allmänt finns det ett betydande forskningsmaterial som antyder en koppling mellan prestationsövervakning och ökade hälsoproblem bland arbetstagare. Den mest uppenbara hälsorisken med elektronisk övervakning är den därmed förknippade ökade stressen på arbetet. Redan 1993 anmärkte ILO följande i sin rapport om övervakning på arbetsplatser:

En studie om elektronisk övervakning och stress på arbetet som genomförts av forskare på universitetet i Wisconsin och Communications Workers of America har bekräftat tidigare studier

som har pekat på elektronisk övervakning som en viktig stressfaktor på arbetsplatsen, och som delvis är kopplad till den maktlöshet som övervakade anställda känner.[69]

Stress har fastställts vara ett viktigt problem i teletjänstcentraler, något som diskuterades under UNIs teletjänstkonferens år 2005. Konferensdeltagarna efterlyste en satsning på bättre hälsa och välbefinnande för de anställda i världens teletjänstcentraler, inklusive åtgärder för att minska stress, oro, utbrändhet och depression.

 Prestationsmätningar på Verizon-South i New Jersey bygger på gruppens snarare än individens prestationer, en praxis som rekommenderades av CWA-Verizons stresskommitté.[70]

På senare år har stress på arbetet börjat tas mer på allvar som arbetsmiljöfråga. År 2004 enades till exempel arbetsmarknadsparterna inom EU formellt om ett ramavtal om arbetsrelaterad stress. Ickedestomindre verkar det fortfarande saknas tillräcklig kunskap om kopplingen mellan elektronisk övervakning och stress. EU-ramavtalet pekar till exempel inte specifikt på relationen mellan övervakning och stress.

Skydd för den privata sfären och anständigt arbete

Den kanske viktigaste sakfrågan som övervakningen ger upphov till rör arbetstagarnas grundläggande rätt till skydd av den privata sfären. Som EU skriver i ett arbetsdokument; "Arbetsgivarna avstår inte från sin rätt till skydd för den privata sfären och dataskydd varje morgon vid dörren till arbetsplatsen."[71] I själva verket blir skyddet allt viktigare när gränserna mellan arbete, den privata tiden och det privata rummet blir alltmer suddiga genom utvecklingar som distansarbete och avtal om flexibla arbetstider.

Det har nu gått nästan tio år sedan ILO försökte att tackla privaträttsfrågorna i samband med lagring av personuppgifter om arbetstagare. ILOs (frivilliga) kod innehåller en kort bestämmelse om övervakning.[72]

 ILOs kod, avsnitt 6.14, lyder sålunda:
Om arbetstagare övervakas bör de i förväg informeras om skälen till övervakningen, tidsplanen för den, metoden och tekniken som används och vilka uppgifter som skall insamlas. Arbetsgivaren måste dessutom minimera intrånget i arbetstagarnas privata sfär.

Hemlig övervakning bör tillåtas endast:
- om det tillåts i nationell lag
- om det finns skälig misstanke om brottslig verksamhet eller andra allvarliga missgärningar.

Kontinuerlig övervakning bör tillåtas endast om det krävs av hälso- eller säkerhetsskäl, eller för att skydda egendom.

Sedan dess har frågor som rört skydd av arbetstagarnas privata sfär tenderat att hanteras indirekt, med mer allmänna dataskyddslagar. Inom EU skall till exempel medlemsländerna införa kraven i 1995 års dataskyddsdirektiv i de nationella lagapparaterna. EU-kommissionen har föreslagit att den särskilda frågan om dataskydd på arbetet tas upp i den sociala dialogen mellan arbetsmarknadens parter. År 2002 utarbetade EU-kommissionen ett detaljerat förslag till ett ramavtal (se nedan), som skulle användas i dessa diskussioner. En förväntad uppföljningsrapport från kommissionen kom dock inte under år 2004, och frågan verkar för närvarande i tysthet ha "parkerats".

 Det föreslagna europeiska ramavtalet fastlägger ett antal principer, däribland arbetstagarrepresentanternas rätt till information och samråd innan en övervakning inleds eller förändras, restriktioner för kontinuerlig övervakning, strikta riktlinjer om hemlig övervakning och förbud av rutinmässig övervakning av e-post och Internettillgång. Dessutom sägs att "personliga uppgifter som insamlats genom elektronisk övervakning skall inte vara den enda faktorn i en utvärdering av arbetstagarnas prestationer."[73]

Ett framträdande exempel på ett lagstiftningsinitiativ kommer från Nya Sydwales (Australien), där den Labor-kontrollerade delstatsregeringen år 2005 antog Lagen om övervakning på arbetet. I denna lag utsträcks de kontroller som först infördes år 1998 i Lagen om videoövervakning på arbetet till andra och nyare elektroniska övervakningsmetoder. I USA har fackförbundet CWA verkat för att Representanthuset skall anta en liknande lag för att inskränka användningen av video- och audio-övervakning på arbetet.[74]

Flera fackliga huvudorganisationer och enskilda fackförbund har tagit fram koder om skyddet av arbetstagarnas privata sfär. Ett exempel är FNV (Nederländerna), som har utarbetat modellregler för dataskyddet.[75] Brittiska IT-arbetarföreningen *IT Professionals Association* (som ingår i det brittisk-irländska fackförbundet Amicus) har tagit fram en liknande uppsättning uppföranderegler.[76]

Vad initiativ som dessa hjälper till att visa är att arbetsgivarnas insamling av elektronisk information om arbetstagare med hjälp av olika övervakningstekniker inte bara är en teknisk fråga, som handlar om att uppfylla dataskyddsnormer. Det rör sig här om grundläggande människorättsfrågor. I grunden handlar det om mänsklig värdighet.

Slutsats: UNIs fortsatta arbete

Den elektroniska övervakningen ökar i många olika sektorer, men vi behöver ändå inte falla in i någon teknisk-deterministisk förstämning. Det finns redan nu gott om exempel på bra fackliga och andra rutiner för att svara på dessa utvecklingar. UNI har självt erfarenheter både av den framgångsrika kampanjen för näträttigheter för direktkopplade arbetstagare och av kampanjarbete kring arbete i teletjänstcentraler, inklusive den globala teletjänstkonferensen nyligen. UNI-förbund och andra fackliga organisationer har också positiva erfarenheter (några av dem har nämnts i denna rapport) som kan spridas.

Ickedestomindre är det lämpligt att UNI betänker hur man kan maximera den roll man spelar i arbetet med att tackla frågan om elektronisk övervakning. Det finns i synnerhet ett antal ytterligare åtgärder som bör övervägas.

1 Den snabba utvecklingen av RFID-tekniken har ägnats mycket liten uppmärksamhet. RFID-spårning blir allt vanligare, i synnerhet genom radioetiketter i namnbrickor. En UNI-kod (som liknar den lyckade koden om näträttigheter) kommer att ges ut för att bistå medlemsförbunden i deras arbete.

2 Frågan om RFID-övervakning knyter också an till mer allmänna frågor om spårning av arbetstagare med hjälp av GPS och mobiltelefoner. UNI kommer att inleda ett bredare globalt kampanjarbete (*Vem är dig på spåren – Who's on Your Tracks?*) för att hjälpa både medlemsförbunden och deras medlemmar att förstå och tackla dessa frågor. Rapporten kommer att läggas fram för diskussion i var och en av UNIs globala fack.

3 ILO kommer att uppmanas att ta upp frågan om elektronisk övervakning. Det är nu mer än tio år sedan ILO genomförde något större forskningsarbete på detta område. Frågan om elektronisk övervakning kan kopplas direkt till ILOs verksamhet för att främja anständigt arbete.

4 UNI kommer att kontakta EU och andra regionala organisationer om dessa frågor, och delta i EU-kommissionens aktuella samråd om RFID-tekniken.

5 UNI kommer att publicera information om hälsoeffekter av en överdriven övervakning, i synnerhet med avseende på stress på arbetet, på sin webbplats.

6 UNI kommer att fortsätta att kraftfullt verka för stadgan för teletjänstcentraler och koden om näträttigheter.

7 Elektronisk övervakning är inte ett problem enbart på arbetet. UNI-förbund uppmanas att samarbeta med medborgarrätts- och dataskyddsorganisationer, liksom med bredare kampanjer (som konsumentkampanjen i USA mot användning av RFID-tekniken för att samla information om kunder) som oroar sig för hur nya teknologier införs.

[1] Denna historia bygger på verkliga händelser
[2] http://www.nocards.org, http://www.spychips.com
[3] Alorie Gilbert, Elementary school nixes electronic ID, 17 februari 2005 http://news.com.com/2102-1029_3-5581275.html
[4] Andrew Bibby, Invasion of the privacy snatchers, Financial Times, 9 januari 2006
[5] Paul Tyrrell, Tuned in to the right frequency, Financial Times, 15 december 2004
[6] Se Smart Mobs, http://www.smartmobs.com/archive/2005/05/04/rfid_employee_m.html. Se även http://ubiks.net/local/blog/jmt/archives3/003741.html
[7] Från http://www.spychips.com
[8] Will Sturgeon, Las Vega casino goes for RFID, 15 april 2005, http://software.silicon.com/security/0,39024888,39129583,00.htm
[9] Accenture, Silent Commerce Chips Away at Star City Casino Wardrobe Worries, fallstudie, http://www.accenture.com/Global/Services/By_Subject/Radio_Frequency_Identification/Client_Successes/StarCityCasino.htm
[10] WaspTime, se http://www.waspbarcode.com/wasptime/wasptime_premium.asp
[11] RAND, Research brief, Privacy in the Workplace, 2005. Se även RAND, Technical Report, 9-5: Do you know if your boss knows where you are? 2005 http://www.rand.org
[12] Resolution om radiofrekvensidentifikation, 20 november 2003
[13] Artikel 29, dataskyddsarbetsgruppen, arbetsdokument om dataskyddsfrågor i samband med RFID-tekniken, 19 januari 2005, WP105
[14] Pressmeddelande från GMB, "GMB seeks changes to European law to outlaw worker tagging," 18 juli 2005 http://www.gmb.org.uk/Templates/Internal.asp?NodeID=92057
[15] Cornelia Brandt, Klüger als die intelligenten Dinge sein… Risikoabshätzung bei RFID-Anwndung fordert Handeln auf verschiedenen Ebenen, 2005
[16] UNI Handel, Technology and RFID must be negotiated, 26 januari 2005, http://www.union-network.org/UNIsite/Sectors/Commerce/Social%20dialogue%20articles/EU_dialogue_increasingly_important.htm
[17] Pressmeddelande från GMB, "GMB Congress demands to electronic tagging of workers 'battery farm; workplaces, 6 juni 2005, http://www.gmb.org.uk/Templates/Internal.asp?NodeID=91861
[18] http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
[19] Fallstudie, "Hands-free Plus real-time, equals business advantage," http://www.symbol.com/category.php?fileName=CS-27_Peacocks.xml
[20] Se t.ex. Katrina Arabe, Wearable Computers: the new warehouse wear, 13 februari 2003, http://news.thomasnet.com/IMT/archives/2003/02/wearable_comput.html
[21] Michael Blakemore, I-DRA Ltd/GMB, Surveillance in the Workplace – an overview of issues of privacy, monitoring and ethics, september 2005
[22] Eurotechnology Japan, Location Based Mobile Services in Japan, http://www.gii.co.jp/english/ek32275-mobile-services.html
[23] National Workrights Institute, Privacy Under Siege: Electronic Monitoring in the Workplace, inget datum
[24] Adam Geller, Bosses keep sharp eye on mobile workers via GPS, Associated Press, 3 januari 2005, http://www.workrights.org/in_the_news/in_the_news_associatedpress.html
[25] On Board Computer – Big Brother Comes to CPC
[26] Överenskommelse mellan Canada Post Corporation och Canadian Union of Postal Workers (löper ut den 31 januari 2007)
[27] National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace (inget datum); Gundars Kaupins och Robert Minch, Legal and Ethical Implications of Employee Location Monitoring, Proceedings of the 38th Hawaii International Conference on System Sciences
[28] David Hencke, AA to log cal centre staff's trips to loo in pay deal, The Guardian, 31 oktober 2005
[29] American Management Association, 2005 års undersökning om elektronisk övervakning
[30] Se t.ex. Jonathan Raper, Technology Trends- brave new world?, http://www.geoplace.com/ge/2001/0101/0101tt.asp
[31] David Canton, Employee Tracking and Monitoring, http://www.canton.elegal.ca/archives/2005/06/. En annan checklista för anställda föreslås av Gundars Kaupins och Robert Minch, Legal and Ethical Implications of Employee Location Monitoring.

[32] National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace, inget datum
[33] Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[34] Till exempel på Guy's Hospital, London. Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[35] Gregor Wittich, Rechtsprechungsübersicht zur Verwendung neue Medien im Betrieb, in DGB, Internet und E-Mail: Neue Medien im Betrieb, 2004
[36] Artikel 29, dataskyddsarbetsgruppen, Opinion, 4/2004, Om behandling av personuppgifter från videoövervakning, antagen 11 februari 2004. Se även Artikel 29, dataskyddsarbetsgruppen, arbetsdokument om behandling av personuppgifter från videoövervakning, antagen den 25 november 2002.
[37] Anthony Hildebrand, Branching Out, http://www.smtdirect.co.uk/story.asp ?sectioncode=0&storyCode=3060661
[38] Information från fackförbundet, januari 2006
[39] Prof Frank Hendrickx, Protection of workers' personal data in the European Union, Study 2: surveillance and monitoring at work
[40] FGTB, Surveillance par caméras: la CCT no 68, http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0404.htm
[41] http://www.union-network.org/UNIsite/Sectors/IBITS/ICT/online.htm
[42] FNV Bondgenoten, Model Protocol: privacy in the use of the internet and e-mail, inget datum.
[43] Cornelia Brandt, Onlinerechte für Beschäftigte, DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004
[44] Eckpunkte der Nutzung von Internet, Intranet und E-mail im Arbeitsverhältnis, DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004
[45] European Industrial Relations Observatory, New technology and respect for privacy at the workplace, 2003 http://www.eiro.eurofound.eu.int
[46] http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0405.htm
[47] Artikel 29, dataskyddsarbetsgruppen, arbetsdokument om övervakning av elektroniska kommunikationer på arbetet, antaget 29 maj 2002, WP55
[48] EU-kommissionen, andra stegets samråd med arbetsmarknadens parter om skyddet av arbetstagarnas personuppgifter, 2002 http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf
[49] Professor Vincent Mosco, What are Workers Doing about electronic surveillance in the workplace? En utredning om fackliga överenskommelser i Kanada, förslag för presentation under 2005 års konferens i IFIP-arbetsgrupp 9-2
[50] American Management Association, 2005 års undersökning om elektronisk övervakning
[51] Hubert Bouchet, La cybersurveillance sur les lieux de travail, CNIL, mars 2004
[52] Michael Sommer, Cornelia Brandt och Lothan Schröder (red.), Im Netz@work, VSA-Verlag, 2003
[53] American Management Association, 2005 års undersökning om elektronisk övervakning
[54] Andrew Bibby, Organising in Financial Call Centres, UNI, 2000
[55] UNI Global Call Centre News, april 2004
[56] Communications Workers of America, http://www.cwa-union.org/workers/customer/protections.asp
[57] Philip Taylor och Peter Bain, Trade Unions and Call Centre Survey, undersökning för finansmannaförbund, 2000
[58] Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[59] http://www.cupw.ca/pages/document_eng.php?Doc_ID=595
[60] Foto från http://www.spychips.com
[61] Michael Blakemore, Every breath you take, every move you make, http://www.unionweb.co.uk/view/PageView.aspx?Page=273
[62] 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
[63] ILO, Conditions of work digest volume 12: Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993
[64] Gary Marx, Measuring Everything that Moves: the new surveillance at work, ur I and R Simpson, The Workplace and Deviance, 1999, http://web.mit.edu/gtmarx/www/ida6.html
[65] How Wal-Mart keeps Unions At Bay, Business Week, 28 oktober 2002 http://72.14.207.104/search?q=cache:YRWfcqtIO2IJ:www.2110uaw.org/gseu/archive/How%252

0WalMart%2520Keeps%2520Unions%2520at%2520Bay.htm+surveillance+cameras+workplace+union+organizing+drive&hl=en&gl=uk&ct=clnk&cd=2
[66] Eric Lee, Trade Unions in the electronic workplace, 13 april 2004 http://www.ericless.me.uk/archive/000079.html
[67] http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
[68] http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt
[69] ILO, Conditions of work digest volume 12: Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993
[70] Communications Workers of America, http://www.cwa-union.org/workers/customer/protections.asp
[71] Artikel 29, dataskyddsarbetsgruppen, arbetsdokument om övervakning av elektronisk kommunikation på arbetet, antaget 29 maj 2002, WP55
[72] ILO, Protection of Workers' Personal Data, 1997 http://www.ilo.org/public/english/support/publ/pdf/protect.pdf
[73] EU-kommissionen, andra stegets samråd med arbetsmarknadens parter om skyddet av arbetstagarnas personuppgifter, http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf
[74] CWA-Backed bill would protect workers' privacy in changing areas, pressmeddelande från CWA, 1 mars 2005. http://www.cwa-union.org/news/cwa-news/page.jsp?itemID=27374804
[75]http://home.fnv.nl/02werkgeld/arbo/wetgeving/privacy/Model%20Privacyreglement/model_privacyreglement1.htm
[76] http://www.amicus-itpa.org/juneconf2.shtml