Te están siguiendo

Control y vigilancia electrónicos en el lugar de trabajo

Autor : Andrew Bibby
Ilustración de la portada : Jane Shepherd

UNI/GS/06-2006/0035/ES

Marta trabajaba en una gran multinacional de seguros. O, por lo menos, su trabajo comprendía procesar indemnizaciones de seguros para ella. La propia empresa había externalizado este aspecto de su servicio de gestión hacía dos años a una empresa especializada que recurría a personal de agencia: para ser precisos, el verdadero empleador de Marta era una agencia de empleo.

Marta llevaba casi un año trabajando para la agencia, uno de los varios empleos que había tenido desde dejar el colegio a los 18 años. Su lugar de trabajo era un edificio de oficinas en un parque industrial anodino. Cada día mostraba su pase en la recepción y subía a su escritorio. Oficialmente formaba parte de un equipo, pero las personas de los escritorios circundantes cambiaban regularmente. De todas maneras no necesitaba tratar con ellas. Los documentos de solicitud de indemnización nuevos le llegaban automáticamente en el ordenador, su trabajo consistía en procesarlos. Se suponía que en promedio tenía que consagrar 6 minutos y 42 segundos a cada uno de ellos para terminarlos. El ordenador sabía exactamente si cumplía con el objetivo y si no era así al final de la semana su director de equipo hablaba con ella.

Era un trabajo monótono, pero por lo menos era un empleo: con el primer hijo en camino necesitaba el sueldo. Los primeros meses del embarazo habían sido difíciles, pero se las había arreglado para trabajar todos los días, aunque tenía que hacer más pausas. Estaba haciendo todo lo posible, pensaba.

Pero la empresa no estaba de acuerdo. Era viernes por la tarde cuando la llamaron a la oficina de uno de los directores. El director tenía ante sí un montón de hojas impresas. "Tenemos que prescindir de sus servicios", dijo. "He estado controlando los recesos que ha estado tomando. Mire, cuatro en una mañana la semana pasada. Es demasiado"

En una de las hojas figuraba un desglose detallado de lo que había hecho en las últimas semanas, incluso cada vez que se había ausentado del escritorio. Marta estaba atónita. "No sabía que se me controlaba así", dijo por último. El director la miró "¿Ah no?", dijo. Sabemos dónde está cada uno en el edificio en todo momento. Su identificación tiene un dispositivo radio. Por cierto, mejor déjela aquí. Ya no va a necesitarla.[1]"

Marta Redding es un nombre ficticio – pero el incidente es real.

Prefacio

A nadie le gusta sentirse espiado. Para muchos trabajadores la sensación de que su empleador podría estarlos controlando subrepticiamente les deja mal sabor en la boca. Resulta difícil creer que esto puede llevar al sentimiento de confianza, base de toda relación de empleo.

Lamentablemente, como se destaca en este informe, hay cantidad de nuevos artilugios y artefactos disponibles para los empleadores que deciden que quieren someter a su personal a altos niveles de control y vigilancia electrónicos.

Por ejemplo, las diminutas tarjetas de identificación por radiofrecuencia (RFID, por la sigla inglesa del sistema), que pueden utilizarse para ver donde se encuentra una persona cada minuto del día y que pueden integrarse en los pases del personal o incluso coserse en los uniformes de trabajo.

El RFID junto con otras tecnologías de seguimiento como los sistemas por satélite GPS pueden significar potencialmente que las personas nunca puedan sentirse verdaderamente libres, incluso durante sus recesos y precisamente su tiempo libre.

Luego está la videovigilancia (ahora muy acentuada por la capacidad de los programas de analizar imágenes digitales), el monitoreo del teclado, el control de llamadas telefónicas, el control del correo electrónico y una multitud de otras formas por las que los trabajadores individuales pueden sentirse permanentemente vigilados.

Lejos de una tecnología de información que ayuda a liberar el potencial humano y a construir una “sociedad del conocimiento”, a veces parecería que más bien se está usando para reducir el potencial de pensamiento y acción independientes en el lugar de trabajo. Simultáneamente estamos viendo amenazado el derecho humano fundamental al respeto y a la dignidad en el trabajo.

Evidentemente, la nueva tecnología de por sí no es algo malo a lo que hay que oponerse. El objetivo de este informe es más bien poner de relieve algunos de los abusos que están teniendo lugar en el lugar de trabajo, a veces muy posiblemente porque los empleadores sencillamente han caído en adoptar opciones que les ofrecen los programas sin verdaderamente detenerse para pensarlo bien.

UNI está determinada a contribuir a erradicar estos abusos, buscando simultáneamente apoyar el desarrollo de la mejor práctica.

Philip J. Jennings
Secretario General de UNI

Introducción

Estos últimos años se ha visto un aumento considerable del control y de la vigilancia electrónicos en el lugar de trabajo, incluyendo la introducción de dispositivos de tecnología digital nuevos y sumamente sofisticados.

Estas tecnologías pueden utilizarse positivamente, de manera a facilitar y mejorar la vida tanto a los empleadores como a los empleados. Ahora bien, la mayoría de las veces se introducen de maneras menos benignas. Algunas veces el uso de estos útiles por parte de los empleadores puede ser irreflexivo (“es por el programa”), a veces puede deberse a una creencia (generalmente no corroborada) de que una fuerza de trabajo muy controlada en cierto modo es una fuerza de trabajo más productiva. Algunos empleadores sencillamente quieren aprovechar la oportunidad de crear una fuerza de trabajo inactiva, pasiva, menos capaz de ejercer sus derechos de organización colectiva y de representación.

De una manera u otra casi todos los sectores de UNI están directamente afectados.

El presente informe analiza detalladamente siete formas de control y vigilancia electrónicos utilizadas actualmente en el trabajo:

- Identificación por radiofrecuencia (RFID)
- Ordenadores que se llevan puestos (ponibles) y programas de reconocimiento vocal
- Sistemas de localización por satélite y telefonía celular
- Videocontrol
- Control del correo electrónico y de la web; monitoreo del teclado
- Control de llamadas telefónicas y trabajo en telecentros
- Control mediante sistemas biométricos e implantes

El informe también explora algunas de las consecuencias para los sindicatos del control y vigilancia electrónicos, analizando especialmente la incidencia en la organización y la afiliación, la salud y la seguridad, la privacidad de los trabajadores y el desarrollo de un orden del día basado en el concepto de trabajo decente de la Organización Internacional del Trabajo. Concluye con un número

de sugerencias concretas en lo concerniente a acción futura de UNI y de sus afiliadas.

1. Identificación por radiofrecuencia (RFID)

La identificación por radiofrecuencia tiene toda la apariencia de llegar a ser una de las tecnologías nuevas dominantes. Ya se utilizan dispositivos RFID en una gran variedad de contextos, que incluyen tarjetas de pago electrónicas utilizadas en muchos países para pagar peajes, billetes de bus y de metro, tarjetas de seguridad electrónicas que los minoristas ponen en la ropa para desalentar del robo, tarjetas para equipaje “inteligentes” que se usan ahora en algunos aeropuertos y incluso chips de cronometraje electrónicos utilizados por los corredores de maratón. En el sector de comercio, las tarjetas RFID se usan mucha en la logística para seguir la pista a existencias de almacenes y se ahora son obligatorias para los proveedores de importantes minoristas como Wal-Mart.

Las “tarjetas” RFID son microchips diminutos, en algunos casos del tamaño de un grano de arena, que continente datos propios del objeto etiquetado. Estas tarjetas, que llevan una pequeña antena, se leen a distancia por un lector RFID. Dependiendo de la radiofrecuencia utilizada y el tipo de tarjetas, las tarjetas RFID puede leerse en algunos casos a una distancia de hasta varios kilómetros, aunque es más corriente que la RFID se utilice en circunstancias en las que son adecuadas distancias de transmisión más cortas. Las tarjetas pueden ser pasivas (“se despiertan” cuando se las lee) o activas, equipadas con su propia microbatería y un transmisor.

El precio de las tarjetas RFID más baratas ha disminuido muy por debajo de 50 centavos de US$, por lo que la utilización en gran escala de la tecnología cada vez es más factible. Los minoristas pronostican que las tarjetas RFID pronto reemplazarán a los códigos barras en las estanterías de los supermercados. La diferencia principal es que, mientras que el código barras es genérico por cada línea de ventas, cada objeto *individual* en venta puede recibir su propio

identificador RFID exclusivo. Se han llevado a cabo experiencias piloto en varios países.

Este uso de RFID es controvertido. Una activa campaña basada en los consumidores y llevada a cabo en Estados Unidos, CASPIAN (Los consumidores contra la invasión de la privacidad y la numeración en los supermercados) afirma que las tarjetas RFID proporcionarán un mecanismo para controlar los modelos de comportamiento individuales de los compradores. CASPIAN alega que estos "chips espía" ofrecen potencialmente una mecanismo poderoso para invadir la privacidad individual. [2].

Los chips RFID pueden utilizarse para seguir la pista a gente, así como a objetos. También se usan en países como Estados Unidos y Japón para seguir los movimientos de gente de edad en residencias de ancianos, a pacientes y personal en hospitales, a bebés en maternidades y a niños en las escuelas. Esta última utilización también ha dado lugar a polémica. Recientemente, se obligó a una escuela elemental cercana a Sacramento en California a dejar de seguir a los alumnos mediante dispositivos RFID tras que los padres hubiesen ejercido presiones al respecto.[3].

En el contexto del lugar de trabajo[4], las inquietudes con respecto a la RFID probablemente se concentrarán en dos aspectos, en primer lugar el tarjeteado RFID de bienes y objetos podría tener por consecuencia la descualificación de algunos empleos y la imposición de prácticas de trabajo por las que se controlará cada vez más el trabajo de los empleados por imperativos tecnológicos. Volveremos a esto más adelante, en el contexto de los cambios en el trabajo en almacenes.

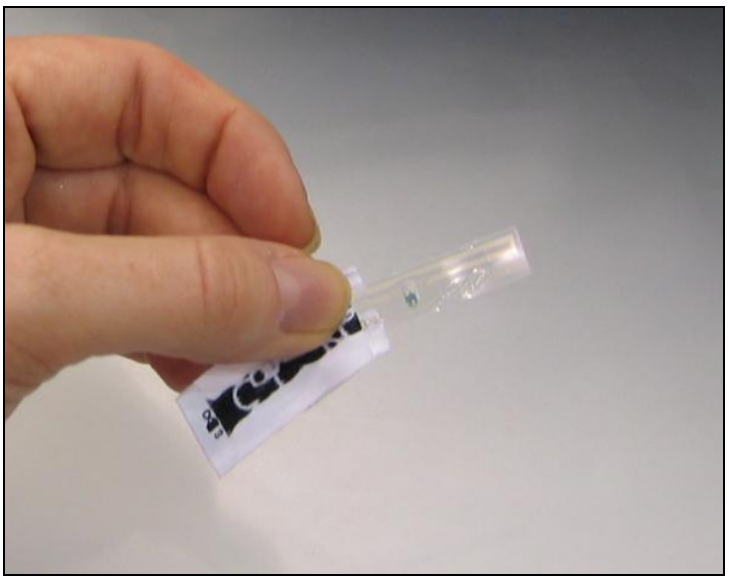
Bastante más significativa es la oportunidad que ofrece la RFID para localizar a trabajadores a lo largo de la jornada laboral (y efectivamente más allá) Hay ocasiones en las que esto puede ser conveniente, por ejemplo, según un informe en Sudáfrica y Chile los mineros llevan ahora tarjetas RFID insertadas en su respirador para poderlos encontrar en emergencias[5]. Ahora bien, usos positivos como éste muy probablemente son la excepción.

Tomemos por ejemplo este informe sobre uso de la RFID, combinado con otras formas de vigilancia electrónica, introducidas por la empresa de electrónica Morón en su fábrica de Kyoto:

“El nuevo sistema de gestión de la producción de Omron explota dispositivos RFID, cámaras video, sistemas de control de acceso/seguridad, etc. para controlar en qué medida contribuyen los empleados a la producción. Los empleados llevan tarjetas RFID obligatorias de manera que el sistema puede controlar su paradero, pero también su rendimiento. Gracias a estas medidas, se optimiza la cuota de los empleados y se mejora la calidad de los productos.[6]”

Una manera de seguir la pista a los empleados vía RFID es colocar tarjetas RFID en los uniformes. Estos dispositivos pueden ponerse, por ejemplo, en las etiquetas (la foto que sigue[7] muestra el reverso de una etiqueta Calvin Klein mostrando la tarjeta RFID transparente); el sector de RFID también esta viendo la posibilidad de utilizar las propias fibras de la ropa como antena RFID.

Este tipo de ropa puede lavarse de la manera habitual sin estropear la tarjeta RFID.



En un ejemplo, ahora las camareras de un casino de Las Vegas llevan uniformes equipados con RFID para controlar su trabajo. Presuntamente un alto directivo

de la empresa dijo que casi el primer día de la prueba un miembro del personal fue “castigado” por “gandulear”[8].

Los trabajadores de casino en el gran complejo Star City en Sydney, Australia, también llevan tarjetas RFID cosidas en sus uniformes[9]. Ahora bien, esto parece ser ante todo a fines de gestión de la guardarropa y, en general, ha resultado ser aceptable (a pesar de la desconfianza inicial del personal). Los empleados de Star City están organizados a través de la afiliada de UNI LHMU (Liquor, Hospitality and Miscellaneous Union – sindicato de bebidas alcohólicas, hospitalidad y afines). El LMU destaca que los uniformes no se llevan en casa, por lo que el personal no es objeto de control en su tiempo libre.

Sin embargo, no es necesario tener un chip RFID en su uniforme para ser localizado durante la jornada laboral. De lejos, la manera más corriente de utilizar chips RFID en el lugar de trabajo es en el pase que se lleva para controlar la entrada en edificios y salas.

Aunque hoy en día se consideran una medida de seguridad normal en numerosos lugares de trabajo, las identificaciones equipadas de RFID en realidad proporcionan datos que no se limitan ni mucho menos a los sistemas de entrada. Normalmente, los datos recogidos se vinculan con otras bases de datos de la empresa, incluidas las relativas a los recursos humanos y a las nóminas. Por ejemplo, una empresa de TI ofrece programas que utilizan los datos del sistema de entrada para producir una variedad e informes “incluyendo informes sobre presencia, sobre tarjetas de marcar, salarios, horas extraordinarias, resumen de nóminas, ausencias, lista de empleados, informe sobre salidas anticipadas por algún motivo….”[10].

Recientemente RAND Corporation hizo una encuesta sobre el uso de datos contenidos en las identificaciones RFID en seis empresas estadounidenses. La conclusión fue que casi universalmente se mantenía a los empleados en la más total ignorancia sobre el uso que se hacía de esta tecnología. Resumió sus conclusiones como sigue:

“Las empresas utilizan tarjetas RFID de acceso al lugar de trabajo sin limitarse a sencillamente abrir puertas (v.g. para hacer aplicar las normas que rigen la conducta relacionada con el lugar de

trabajo). No hay políticas escritas y explícitas sobre la manera en que se utilizan estos dispositivos en general y no se informa a los empleados sobre qué políticas se siguen. El uso de estos sistemas has modificado el equilibrio tradicional de conveniencia personal, seguridad y salud en el lugar de trabajo y privacidad individual, conduciendo a la pérdida de la "oscuridad práctica". Estos sistemas también plantean retos en cuanto al sentido y a la aplicación de prácticas de información justas.."[11]

Los investigadores de RAND quedaron muy sorprendidos e inquietos ante la ausencia de políticas escritas y por el hecho de que no se informase a los empleados sobre estas prácticas, y concluyeron su estudio afirmando "Todo lector que utilice una tarjeta de acceso basada en la RFID debería sentirse preocupado ante estos resultados".

En 2003 tuvo lugar una discusión sobre la incidencia de la RFID en términos de privacidad y protección de datos en la conferencia internacional de comisarios de protección de datos y privacidad,[12], y el Grupo de Trabajo de la UE sobre Protección de Datos también ha abordado la cuestión. [13]. Este último organismo solicita que el control por RFID se lleve a cabo en conformidad con los principios de protección de datos, incluyendo la notificación previa de la presencia de tarjetas RFID y el derecho de la persona objeto de los datos a acceder a sus datos personales. Sin embargo, es evidente que en ambos casos se está en los inicios en términos de desarrollar políticas internacionales claras.

Los sindicatos también han comenzado a abordar la cuestión del seguimiento por RFID.


En julio de 2005 el sindicato británico GMB criticó al Grupo de Trabajo sobre Protección de Datos de la UE por fracasar en abordar la incidencia de la RFID en materia de privacidad y seguimiento del personal en el lugar de trabajo y pidió que se proscribiese la identificación del personal vía RFID en la Unión Europea. Se están socavando los derechos de privacidad de los trabajadores, dijo el sindicato.[14]


ver.di (Alemania) sugiere que se utilice la lista de control siguiente si se aplica tecnología RFID en el lugar de trabajo[15]:

- ¿Se da a los empleados con la antelación debido la información necesaria en lo concerniente a planes de introducir tecnología RFID y a su aplicación?
- ¿Hay algún problema de salud o riesgos asociados con el uso de radiofrecuencias, sistemas de escaneo o barreras fotoeléctricas en el lugar de trabajo?
- ¿Cómo afecta la tecnología a la rutina de trabajo y cómo altera en términos concretos las condiciones de trabajo y el ambiente de trabajo?
- ¿Qué efecto tendrá la introducción de la tecnología RFID en la racionalización?
- ¿Se dará a los empleados suficiente formación en materia de uso de RFID?
- ¿Qué datos, especialmente qué datos personales, se almacenarán dónde y por cuánto tiempo?
- ¿Se utilizarán los datos, a medida que se acumulan, para controlar el comportamiento y el rendimiento de los empleados?
- ¿Quién se asegurará de que estos datos no sean distorsionados?
- ¿Cómo podrán defenderse los trabajadores contra el abuso?

UNI Comercio también aprobó una declaración sobre la introducción de la tecnología RFID, invitando a un diálogo social serio con las empresas a la vanguardia en cuanto a maniobras para introducir la tecnología. [16].

2. Ordenadores que se llevan puestos y tecnología de reconocimiento vocal

La identificación de productos mediante RFID y mediante los códigos barras tradicionales se está combinando, especialmente en almacenes minoristas, con nuevas formas de tecnología de reconocimiento vocal y ordenadores que se llevan puestos para crear un ambiente de trabajo en el que los trabajadores pasan a ser autómatas en medida cada vez mayor.

A mediados de 2005 el sindicato GMB del Reino Unido recibió interés considerable de los medios de comunicación nacionales e internacionales cuando señaló a la atención las condiciones de trabajo en algunos almacenes británicos que, dijo, se asemejaban a granjas de cría intensiva: “La única función del trabajador es hacer lo que le ordena el ordenador. Estos sistemas calculan cuánto tiempo toma ir de un lugar del almacén a otro y los recesos que necesitan los trabajadores y cuánto tiempo necesitan para ir al baño. No se tolera ningún desvío de este programa. Efectivamente, estos mecanismos para despachar productos alimenticios a supermercados y tiendas han hecho de los trabajadores auxiliares del ordenador en lugar de a la inversa. [17]”

UN ejemplo típico mencionado por el GMB es un almacén de 12.000m² en Gales que abastece a 240 tiendas al por menor. Los trabajadores que seleccionan mercancía están equipados con ordenadores portátiles que se sujetan en la muñeca y el antebrazo al que está conectado un escáner atado con una correa al índice. El ordenador, fabricado por la empresa de TI especializada Symbol, pesa de 320 a 350 gramos (véase ilustración) [18].

Según Symbol, “el terminal atado a la muñeca recibe instrucciones de selección vía el LAN inalámbrico del sistema huésped (de la empresa). A medida que llegan los carros vacíos en la zona de selección, un recolector escanea su código barras y la pantalla LCD del terminar le indica a qué pasillo ir, el emplazamiento en el que tiene que recolectar y qué mercancía. Cuando el recolector llegar al lugar, en primer lugar escanea el código barras instalado al final del pasillo. Esto verifica que está en el buen lugar. Seguidamente, escanea otro código barras en el lugar de las mercancías para verificar que está en el lugar correcto. Por ultimo, escanea cada producto a medida que lo coloca en el carro[19]” Ahora bien, en los términos del GMB “Las únicas funciones que realiza el ser humano son las partes que aún no se han automatizado”.

Actualmente hay dos categorías principales de ordenadores que se ponen, los que se llegan en la muñeca a/o atados al dedo (como en la ilustración) y los que se llevan sujetos a la cabeza o el cinturón. A menudo están combinados con tecnología vocal, lo que entraña que se distribuyen auriculares a los trabajadores que reciben instrucciones generadas por el ordenador, que indican los objetos que deben seleccionar. Los sistemas de tecnología vocal habitualmente trabajan con programas que transmiten las órdenes de la dirección o de la dirección del almacén y los datos de estos sistemas se sintetizan en palabras[20].

Tanto el GMB como el Profesor Michael Blakemore, académico británico que ha advertido al sindicato de esta cuestión, han planteado las posibles implicaciones de salud y seguridad de esta tecnología. Blakemore afirma que, a pesar de

problemas con tecnologías anteriores de lesiones por esfuerzos repetitivo (RSI), los conocimientos sobre las posibles consecuencias para la salud de este nuevo equipo son muy limitados.[21].

Los sistemas de recolección en almacenes como éstos no solamente automatizan el proceso de trabajo, también ofrecen un útil valioso para supervisar a los trabajadores. M. Blakemore cita un comentario de la empresa: “También es muy fácil de utilizar de una perspectiva de la dirección ya que las posibilidades de seguir la pista de lo que hace cada persona son fantásticas”.

3. Localización por satélite y teléfono celular

Además de la tecnología RFID hay varias otras a disposición que permiten la localización de objetos o de personas que pueden identificarse con exactitud considerable.

La navegación por satélite depende actualmente del Sistema de Posicionamiento Global de Estados Unidos. GPS utiliza una red de satélites originalmente introducidas para uso militar y aún operada por el Pentágono. Cada satélite transmite continuamente datos identificando su posición. Los receptores de GPS analizan estas señales y comparando las transmisiones de cuatro o más satélites pueden identificar su propia posición precisa y su altura por encima del nivel del mar. (Por los menos cuatros satélites deben ser "visibles" para cada receptor en cualquier momento).

La Unión Europea está desarrollando su propio sistema de navegación por satélite rival conocido por el nombre de Galileo. El primer satélite de la red Galileo fue lanzado en diciembre de 2005.

La tecnología de telefonía celular (móvil) también ofrece la posibilidad de seguir la pista los emplazamientos en los que se llevan auriculares móviles activos. Esto funciona identificando las distancias del aparato a las torres de transmisión de base más cercanas, que juntas, crean las redes celulares en las que se basa la telefonía móvil. Especialmente, en zonas urbanas en las que las estaciones de base están muy cercanas, es posible el seguimiento preciso del emplazamiento, característicamente hasta de 10 a 25 metros. Los teléfonos no necesitan estar activamente en uso para ser localizados.

Estas dos tecnologías están fusionando, considerando que los teléfonos celulares y las agendas electrónicas funcionan con GPS en medida cada vez mayor. Por ejemplo, en Japón, 20% de los teléfonos celulares también funcionan con receptores GPS[22].

Tanto los servicios de GPS como los de ubicación celular ya están siendo explotados comercialmente, a menudo combinados con servicios de mapeo digital. Por ejemplo, el GPS se utiliza en medida cada vez mayor para los sistemas de navegación en automóvil. Los usuarios de teléfonos móviles están explorando el potencial de servicios basados en el emplazamiento (v.g. la transmisión a usuarios de teléfonos del emplazamiento de filiales cercanas de restaurantes de comida rápida, cajeros automáticos o incluso de amigos y conocidos).

En el lugar de trabajo, al igual que con otras tecnologías, hay maneras positivas de utilizar el seguimiento por GPS y teléfono celular que pueden facilitar la vida a los trabajadores, v.g.:

- Localización a vehículos para aumentar la seguridad de los chóferes de furgonetas de seguridad en peligro de ser atracadas
- La localización geográfica puede contribuir a la seguridad de los trabajadores móviles. Esto puede aplicarse especialmente a los que trabajan solos en lugares aislados o potencialmente peligrosos, o por la noche
- El sistema también puede ayudar a localizar a trabajadores o conductores en caso de mal tiempo

Lamentablemente, hay muchas pruebas de que los empleadores están introduciendo estos sistemas de ubicación de maneras mucho menos positivas. Por ejemplo, puede citarse el caso mencionado por el US National Workrights Institute:

Howard Boyle, Presidente de una empresa de instalación de extintores de incendios en Woodside, N.Y., distribuyó a sus empleados teléfonos móviles sin informar que estaban equipados con GPS. El Sr. Boyle puede estar al corriente de dónde están en todo momento, incluyendo los recesos y su tiempo libre. “No tienen porqué saberlo”, dijo el Sr. Boyle. “Puedo llamarlos y decirles, ¿dónde están en este preciso momento?” mientras consulto la pantalla y sé exactamente dónde están.”[23].

La localización permanente puede crear presiones insidiosas para los trabajadores, que se sienten observados en todo momento de su jornada laboral. Se cita a un chofer estadounidense cuyo camión tiene GPS:

"Es como una sensación de Gran Hermano que vigila … Me pongo nervioso en la cafetería cuando tengo que hacer cola para el café, porque es como si me estuvieran viendo y me tengo que ir [24]."

En Canadá, el Canadian Union of Postal Workers (CUPW) advirtió a sus miembros que siguiesen muy de cerca la iniciativa de Canada Post de introducir ordenadores vinculados con GPS en varios centenares de furgonetas. Controlan (vía GPS) la ubicación de cada furgoneta, y también si el motor está en marcha, si el vehiculo está en movimiento y si es el caso a qué velocidad y si las puertas están cerradas. Canada Post dijo al sindicato que su objetivo era permitir a los supervisores saber si los chóferes conducen como es debido y si siguen las directrices de seguridad (mediante los llamados "informes de excepción" generados por ordenador)[25].

El CUPW invocó el convenio colectivo actual con Canada Post para asegurar que este control no se use a fines disciplinarios.

 La cláusula del convenio colectivo del CUPW con Canada Post que cubre la vigilancia establece que en ningún momento estos sistemas (de vigilancia y de observación) deberán utilizarse como medio para evaluar el rendimiento de los empleados ni para reunir pruebas en apoyo de medidas disciplinarias, a no ser que estas medidas deriven de la perpetración de un acto criminal. .[26]"

Los sindicatos también intervinieron en otros países para controlar el uso de control por GPS. En Estados Unidos, el sindicato de los Teamsters negoció con el UPS que los datos de la localización por GPS no se utilizasen para la evaluación de los empleados ni a fines disciplinarios[27]. El Teamsters también puso en tela de juicio el uso de GPS por otras empresas de transporte y de mensajerías y por las autoridades públicas.

Cuando hay sistemas de localización, es especialmente importante para los trabajadores poder asegurarse que estos sistemas cesen de operar durante los recesos y al término de la jornada laboral.

 Amicus (Reino Unido/Irlanda) informó que pudo oponerse con éxito al sistema de ubicación de automóviles de una empresa como una interferencia en la privacidad, permitiendo al empleado tener la oportunidad de hacer caso omiso de él[28].

Los sistemas de ubicación geográfica, especialmente el GPS, aumentaron rápidamente en los últimos años, aunque probablemente aún nos encontremos en las primeras etapas de la aplicación de esta tecnología. Las encuesta realizada en 2005 sobre el control y la vigilancia electrónicos por la American Management Association en 526 empresas estadounidenses confirmó que 8% de ellas utilizaban el GPS o la ubicación por GPS/celular de vehículos, mientras que 5% ubicaban a los empleados con teléfonos celulares[29].

Sigue siendo algo prematuro en términos de establecer salvaguardias adecuadas y buena práctica para proteger la llamada "privacidad locacional"[30]. Una guía ofrecida a los empleadores por el asesor legal canadiense David Canton sugiere una lista de cuatro puntos para introducir la localización por GPS[31]:

- Determinar la necesidad
- Establecer una política en materia de privacidad
- Controlar la moral
- Obtener el consentimiento

Advierte que si bien el GPS puede llevar a mayor eficiencia y productividad, "también puede llevar a bajar el ánimo del personal, a una reacción violenta de los empleados y a la posibilidad de procesos".

El US National Workrights Institute planteó inquietudes de carácter más general sobre la necesidad de asegurar que las personas puedan proteger su "privacidad locacional", especialmente en relación con su vida privada." Como dicen "Cuando un empleado sabe que su patrón observa sus actividades cotidianas, puede pensárselo dos veces antes de participar en determinadas actividades. Por ejemplo, si el patrón es un Republicano vigilante, en empleado podría optar por no ir a la Convención Nacional Demócrata.[32]

4. Videocontrol

El control manifiesto y disimulado en el lugar de trabajo utilizando cámaras de videocontrol es un problema para los sindicatos desde hace muchos años. Por ejemplo, ya en 1993, el Communication Workers of América señaló a la atención de una comisión del Senado un caso en el que personal femenino había descubierto que la dirección había ocultado una cámara en su vestuario. Esta cámara estaba controlada por guardas de seguridad masculinos que miraban cuando las empleadas se cambiaban de ropa[33]. Otros países también han informado de casos muy similares de cámaras disimuladas en servicios y vestuarios.[34].

La videovigilancia sigue siendo un problema conducente regularmente a conflictos en el lugar de trabajo, especialmente cuando se instalan cámaras sin consulta previa o se utilizan subrepticiamente para controlar el rendimiento de los empleados y a fines disciplinarios. Un ejemplo reciente es la instalación de cámaras de seguridad por Deutsche Post en la oficina de clasificación principal en Berlín, donde trabajan 650 empleados. La idea era que las cámaras funcionasen hasta cincuenta horas por semana. Un tribunal de empleo federal juzgó que esta utilización era excesiva[35].

Actualmente, en varios aspectos clave el uso de cámaras de vigilancia plantea más inquietudes que en el pasado, cuando las imágenes se controlaban en tiempo real o se grababan en una cinta magnética. Actualmente, hay muchas más probabilidades de que los datos procedentes de estas cámaras se presenten de forma digital y, como tales, pueden almacenarse en una base indefinida junto con otros datos digitalizados. Potencialmente, por ejemplo, los datos digitalizados de cámaras de vigilancia concentrados en empleados individuales pueden vincularse con otros datos digitales sobre esta persona, v.g. datos en materia de recursos humanos o datos tomados del control del correo electrónico y conversaciones telefónicas grabadas, formando un conjunto muy poderoso de información integrada a disposición del empleador.

El Grupo de Trabajo sobre Protección de Datos de la Unión Europea ha señalado a la atención los riesgos que podrían emanar del desarrollo de "software" capaz de "interpretar" imágenes video, v.g. identificando a personas plasmadas en imágenes mediante reconocimiento facial. En su informe de 2004 sobre la videovigilancia el Grupo de Trabajo declara que estas tendencias que se aplican a la evolución de las técnicas de la videovigilancia podrían evaluarse fructuosamente para prevenir el desarrollo de aplicaciones software basadas a la vez en reconocimiento facial y el estudio y previsión del comportamiento de la persona retratada llevando inconsideradamente a una vigilancia dinámica-preventiva – a diferencia de la vigilancia estática convencional, cuyo propósito es esencialmente documentar eventos específicos y sus autores. La nueva forma de vigilancia se basa en la recuperación automatizada de los rasgos faciales de las personas, así como su conducta "anormal" en asociación con la disponibilidad de alarmas y avisos automatizados, que eventualmente entrañan peligro de discriminación[36].

En otras palabras, cada vez es más necesario considerar la videovigilancia no sencillamente una medida de seguridad independiente, sino una fuente de datos disponible para investigar y analizar utilizando el pleno poder de la computación actual. Un indicio de esta tendencia es el desarrollo por parte de Cisco Systems de AVVID (Arquitectura de voz, video y datos integrados) de la que afirma que puede utilizarla el sector bancario no solamente a fines de seguridad, sino también de comercialización y relaciones con los clientes maximizando el valor de las filiales bancarias[37].

En vista de este tipo de evolución, todavía es más importante asegurar el control adecuado de la videovigilancia. El Grupo de Trabajo sobre Protección de Datos de la UE destaca la importancia de los principios de protección de datos calve, incluyendo la proporcionalidad de uso y la notificación previa de las personas concernidas. En el contexto particular del lugar de trabajo, el Grupo de Trabajo insta a la salvaguardia de los "derechos, libertades y dignidad" de los empleados. Hace los comentarios siguientes:

"Los sistemas de videovigilancia destinados directamente a controlar desde un emplazamiento alejado la calidad y la cantidad de las actividades de trabajo … no deben permitirse por norma …

"La experiencia adquirida en la aplicación ha demostrado además que la vigilancia no debe incluir locales reservados para el uso privado de los empleados o que no están previstos para el cumplimiento de tareas relacionadas con el empleo – tales como servicios, duchas, vestuarios o áreas de recreo: que las imágenes recogidas exclusivamente para salvaguardar la propiedad y/o detectar, prevenir y controlar infracciones graves no deben utilizarse para acusar a un empleado de infracciones leves a la disciplina; y que siempre se permita a los empleados presentar sus reconvenciones utilizando el contenido de las imágenes recogidas. Debe informarse a los empleados y a cualquier otra persona que trabaje en los locales." (traducción libre)…

El control oculto plantea especial inquietud como muestra un ejemplo de Suecia. Actualmente, el sindicato de transporte de Suecia, afiliado a UNI, está en negociaciones con Securitas para controlar el uso reciente por parte de la empresa de furgonetas de vigilancia clandestina equipadas con cámaras y que su utilizan para filmar sus propios vehículos y personal.

Securitas ya equipa sus furgonetas con cámaras. Sin embargo, solamente se firma en caso de atraco o de apertura no autorizada de puertas, práctica que el sindicato acepta. El atraco a mano armada de una furgoneta de Securitas en la autopista al Sur de Estocolmo en diciembre de 2005 demostró la importancia de medidas de seguridad apropiadas. Sin embargo, el personal de Securitas criticó enérgicamente la introducción de filmación clandestina a partir de vehículos anónimos.

El sindicato del transporte sueco prevé un resultado fructuoso de las negociaciones y un acuerdo con la empresa que se aplicará en los países nórdicos[38]. Entretanto, DFF, afiliada de UNI danesa, ya concluyó un acuerdo con Securitas que restringe la utilización de video y que incluye protección contra el uso de material video a fines disciplinarios. Debe informase a los empleados del control en el momento de la contratación.

En términos más generales, ya hay varios ejemplos de buena práctica en el control de la videovigilancia. Varios países tienen legislación al respecto. En New South Wales, Australia, la protección ofrecida a los trabajadores por la Workplace Video Surveillance Act (ley en materia de videovigilancia en el lugar de trabajo) de 1998, introducida tras una serie de conflictos laborales) recientemente se amplió a otras formas de control electrónico. En Austria, es

necesaria la aprobación del comité de empresa antes de instaurarse el videocontrol permanente[39].

En Bélgica, el uso de cámaras en el lugar de trabajo está sujeto a un convenio colectivo negociado entre los interlocutores sociales en 1998 y que tiene fuerza de ley. Cubre al sector privado en su conjunto.

El convenio belga se basa en los principios de proporcionalidad y objeto final. La vigilancia permanente está estrictamente controlada y solamente se autoriza en casos en que está destinada a proteger la seguridad de los trabajadores o la propiedad de la empresa. La vigilancia clandestina está prohibida, salvo cuando ha pruebas considerables de actividad delictiva. Solamente se pueden introducir cámaras en consulta con los sindicatos y debe informarse a los trabajadores con antelación. Debe exponerse claramente el objeto de la videovigilancia[40].

5. Vigilancia del uso de Internet y el correo electrónico: monitoreo de teclado

En los últimos años, se ha prestado considerable atención a cuestiones relacionadas con la vigilancia de los empleadores del uso que los trabajadores hacen de Internet y el correo electrónico. En parte, ello obedece a que esas cuestiones crearon problemas prácticos en muchos lugares de trabajo y fueron causa de un creciente número de casos disciplinarios.

Hay que reconocerle a la UNI (y la FIET su predecesora) el mérito de la presteza con que abordó la cuestión mediante la campaña Derechos en línea para los trabajadores en línea, iniciada en 1998. El *Código de Práctica de la UNI – Derechos en línea en el trabajo* contiene directrices idóneas que fueron seguidas por sindicatos y otras organizaciones.

Dicho código versa sobre cuatro cuestiones estrechamente relacionadas con el uso de la web y el correo electrónico en el lugar de trabajo, a saber: el acceso de los representantes de los trabajadores a las instalaciones electrónicas; la medida en que los trabajadores pueden usarlas con fines personales; las condiciones que rigen esa utilización y, por último, el control y la supervisión del uso de la web y el correo electrónico.

La sección sobre control y supervisión de las comunicaciones del Código de Práctica de la UNI dice:

El empleador se compromete a que el uso de los medios electrónicos de la empresa por parte del empleado no será objeto de supervisión y control.

La comunicación solamente será objeto de supervisión y control si el convenio colectivo lo permite, si el empleador está jurídicamente obligado a hacerlo, o si el empleador tiene motivos justificados de pensar que un empleado ha cometido un delito penal o una grave infracción disciplinaria. Solamente se permitirá acceso a actas de supervisión y control de empleados individuales en presencia de un representante sindical y de un representante elegido por el empleado.

Gran parte de este código se basa en principios ampliamente establecidos en los procedimientos de protección de datos para manejar los datos personales y en las salvaguardas de los derechos humanos adoptados por la OIT.

Tras la iniciativa de la UNI, una serie de afiliadas iniciaron actividades similares y, en muchos casos, establecieron sus propias directrices y códigos de buena práctica. Citemos como ejemplo, GPA de Austria; Amicus (ex MSF) del Reino Unido/Irlanda; CFDT BETOR-PUB de Francia y FNV Bondgenoten de los Países Bajos.

El protocolo modelo de FNV Bondgenoten sobre privacidad en el uso de Internet y correo electrónico contiene la cláusula que sigue:

El empleador no leerá el contenido de los mensajes personales o comerciales. Tampoco registrará ni verificará datos personales en lo que respecta al número de direcciones y mensajes electrónicos ni ningún otro dato pertinente. Esto ultimo no afecta sus derechos de proceder a controles ocasionales por razones de fuerza mayor donde entre en juego el interés de la empresa. Dichos controles habrán de ser notificadas al comité de empresa[41].

En Alemania, ver.di se unió a IG Metall y DGB (federación sindical alemana) para crear el sitio web www.onlinerechte-fuer-beschaeftigte.de y se asoció a la campaña Derechos en línea. La prensa dio gran difusión a esta campaña lanzada en marzo de 2002 en un cibercafé de Berlín. El sitio web es interactivo y ofrece información sobre la legislación y un foro de debate[42]. Tras esta iniciativa, se redactó una declaración de seis puntos sobre el uso de la Internet, la intranet y el correo electrónico que fue aprobada por el Ejecutivo de la DGB en febrero de 2004[43].

En esta tarjeta, creada en el marco de la campaña de los sindicatos alemanes sobre Derechos en línea, dice: "Escribo cartas, porque mi jefe lee mis mensajes electrónicos"

En varios países hay convenios colectivos que incluyen este asunto, entre ellos, Austria y Dinamarca (convenio entre HK-Service y los empleadores de comercio)[44]. A escala nacional, el convenio colectivo más importante es el que adoptaron los interlocutores sociales de Bélgica en abril de 2002.

El convenio colectivo de Bélgica[45] (que tiene rango de ley nacional) estipula los límites de la supervisión de las comunicaciones en línea de los empleados. En lo que respecta a Internet, el empleador puede recabar datos sobre la duración de las conexiones, pero sin identificar los sitios consultados. En cuanto al correo electrónico, puede llevar un registro del volumen y el número de mensajes, a condición de que éstos no se vinculen con nadie.

La Unión Europea también se ocupó de la cuestión del uso de la web y el correo electrónico por parte de los empleados. El Grupo de Trabajo sobre Protección de Datos estableció los principios generales que se aplican a la vigilancia de las comunicaciones electrónicas y los dividió por temas, a saber: necesidad;

finalidad; transparencia; legitimidad; proporcionalidad; exactitud y conservación de los datos, y seguridad[46]. En el documento de la Comisión Europea para la segunda etapa de la consulta de los interlocutores sociales sobre datos personales de los trabajadores también se propone un marco europeo que comprenda la vigilancia electrónica[47]. Dicho documento prevé lo que sigue:

- La vigilancia sólo debería permitirse de conformidad con las salvaguardas estipuladas en la legislación nacional o cuando haya fundada sospecha de actividad delictiva u otras infracciones graves.
- Los datos personales recabados mediante vigilancia electrónica no deberían ser los únicos factores que intervengan en la evaluación del rendimiento de los trabajadores y las decisiones que se tomen respecto a ellos.
- En principio, el empleador tiene prohibido abrir el correo electrónico y cualquier otro fichero privado... (traducción libre)

Ahora bien, sería erróneo pensar que toda esa actividad haya resuelto satisfactoriamente las cuestiones relativas al uso de Internet y el correo electrónico. En Canadá, por ejemplo, una reciente encuesta académica reveló la aplicación de una amplia gama de políticas, incluso allí donde existen convenios colectivos. Según el investigador, en los convenios más flojos, los sindicatos reconocen los derechos de los empleadores a utilizar cualquier forma de vigilancia cuándo y dónde quieran[48].

En Estados Unidos, la vigilancia electrónica también está muy extendida. Según la American Management Association (AMA), 76% de empleadores vigila las comunicaciones electrónicas de los empleados y 55% almacena y examina los mensajes electrónicos de su personal. En la encuesta de AMA de 2005 se constata que en más de una empresa de cada cuatro hubo despedidos por uso indebido de Internet y en otro 25% por uso indebido del correo electrónico. Además, AMA descubrió que una de cada 10 compañías no había informado a sus empleados que rastreaba el uso de Internet y que 14% había omitido notificarles que se vigilaba el correo electrónico[49].

Es difícil contradecir a Hubert Bouchet de la comisión francesa de información que advirtió que la mayoría del personal ignoraba la vigilancia que se lleva a cabo en el lugar de trabajo. Según él, en muchísimos casos no hay equilibrio

entre el legítimo control que practica la compañía y el respeto de los derechos de los trabajadores[50].

Cabe señalar que la encuesta de la American Management Association sobre control y vigilancia también reveló que uno de cada tres empleadores (36%) controla el número de pulsaciones del teclado, el tiempo que se usa el teclado y/o el contenido del material incorporado. Desde hace muchos años, preocupan a los sindicatos las depresiones que sufren los trabajadores, a raíz del constante monitoreo de teclado, en particular, aquellos poco remunerados que se ocupan de la introducción de datos básicos. Las descabelladas exigencias de niveles de productividad en el uso del teclado pueden contribuir a causar lesiones por esfuerzos repetitivos que en algunos países han cobrado proporciones rayanas a la epidemia.

Gerrit Wiegand hizo una minuciosa investigación para sindicatos alemanes sobre los programas y equipos informáticos que pueden utilizarse para registrar las pulsaciones del teclado. Los resultados se publicaron en el libro Im Netz@work[51].

También son de larga fecha las inquietudes en el sector minorista respecto al control automático de la rapidez con que los empleados pasan los artículos por el escáner, pues remontan a la época en que se empezó a usar la tecnología del código de barras y las cajas registradoras automatizadas. La tecnología se puede utilizar para controlar con minucia y exactitud lo que hace el personal en horas de trabajo, incluido el tiempo que tarda en el servicio. Ahora bien, el hecho de que la tecnología permita esta clase de curiosidad electrónica, no implica que tenga que utilizarse de esa forma. Cabe señalar que en la nueva “tienda del futuro” de la Metro en Rheinberg se instalarán balanzas automáticas que los empleados podrán utilizar sin contraseña a fin de que no se recaben datos personales.

6. Control de llamadas telefónicas y trabajo en telecentros

Las llamadas telefónicas se pueden controlar de varias maneras. La cantidad y la duración de las llamadas, así como los números a los que se llama pueden registrarse; las llamadas telefónicas pueden ser escuchadas por el personal de supervisión, ya sea encubierta o abiertamente; las llamadas se pueden grabar y los mensajes de correo vocal también se pueden grabar y controlar.

En Estados Unidos, casi la mitad de las empresas controla las llamadas mediante el registro de los números a los que se llamó y la duración de las comunicaciones; dos tercios de esas empresas hace ese control a intervalos regulares o constantemente. Sin embargo, según la American Management Association, el 22% no informa al personal al respecto. Casi una de cada cuatro empresas "graba" las llamadas[52].

En algunos sectores, como banca y seguros, puede haber motivos de orden jurídico o reglamentario de grabar las llamadas telefónicas, pero eso no significa forzosamente, que las grabaciones se utilicen rutinariamente con fines tales como controlar la productividad de cada empleado o a efectos disciplinarios. De más en más, las llamadas telefónicas se almacenan en formato digital, lo que sumado a la filmación de las cámaras de vigilancia ofrece la posibilidad de integrar datos con otros datos personales y estar sometido a un análisis minucioso mediante un programa de informática.

Se debería informar a los empleados que las llamadas se graban.

Algunas compañías argumentan que escuchan o graban las llamadas con fines de formación. Si bien en algunas circunstancias puede ser legítimo que lo hagan para mantener el nivel de la atención telefónica, el personal que necesita asistencia al respecto, en realidad, debería tener la oportunidad de acceder a una formación adecuada. Tampoco en este caso, los empleadores deberían abusar y utilizar esta clase de control con otros fines.

Los trabajadores de telecentros se ven mucho más afectados por estos asuntos que la mayoría de los demás. Tal como se señalaba en el temprano informe de la UNI sobre el trabajo en telecentros: En general, la tecnología confiere a los

empleadores el poder de mantener niveles bastante sorprendentes de control y vigilancia electrónicos de su personal[53].

Además, los trabajadores de telecentros tienen poquísimo control sobre su jornada laboral, pues no sólo atienden las llamadas que reciben mediante la tecnología de distribución automática sino que también, en muchos casos, están obligados a seguir un guión cuando hablan con los clientes y se les imponen rígidos objetivos de venta y rendimiento. Habitualmente, esta tecnología permite almacenar todos los aspectos del manejo de llamadas, incluidas las pausas y las idas al servicio. Recientemente, en el boletín global de telecentros de la UNI se informó del caso de una mujer que se vio obligada a decirle a su jefe, antes que a su familia, que estaba embarazada para explicar por qué iba tan seguido al servicio[54]. (El relato ficticio de Marta con que empieza el presente informe se inspira en parte de su caso).

En la Carta de la UNI para Telecentros y en el Plan de acción establecido en el marco de la 1.ª Conferencia de la UNI sobre Telecentros, que tuvo lugar en octubre de 2005, se aborda la cuestión del control y la supervisión.

La Carta de la UNI para Telecentros contiene estos seis puntos bajo el epígrafe Supervisión, control electrónico y privacidad.

- Solamente se permitirá el control si se conocen los motivos y si son aceptables.
- Los datos recabados solamente se utilizarán a estos fines.
- El/la empleado(a) estará informado(a) de que es o va a ser objeto de control.
- La escucha solamente tendrá lugar casualmente y nunca de manera permanente.
- Se permitirá al empleado acceder a los datos registrados y podrá corregir inexactitudes.
- Se destruirán las grabaciones después de un determinado período de tiempo.

Otra medida concreta, tomada recientemente por UNI Telecom en el contexto del Diálogo Social Europeo con la Asociación de Operadores Europeos de Redes de Telecomunicaciones (ETNO), consistió en garantizar que se incluyera una cláusula sobre supervisión en las Directrices europeas para los centros de servicio a la clientela. Uno de los principios fundamentales es que se debe

informar a los trabajadores de telecentros de todo dispositivo de control del rendimiento que se prevea instalar.

Las experiencias de las afiliadas de la UNI demuestran que se pueden negociar mejores condiciones de trabajo para el personal de los telecentros. Varios sindicatos del sector de telecom, por ejemplo, concluyeron convenios colectivos que contienen cláusulas sobre control y supervisión.

 En Estados Unidos, el sindicato Communications Workers of America (CWA) negoció acuerdos con una serie de compañías de telecom, incluidas AT&T, Qwest, Bell South y SBC[55].

El convenio con AT&T contiene las siguiente disposiciones sobre el uso de escucha de llamadas.

- Se notificará a los empleados el día en que se tomarán muestras y cada uno tendrá la posibilidad de que la supervisión se haga a distancia o a su lado.
- La muestra de llamada individual se tomará en la zona de trabajo del empleado a quien se supervisa.
- Ningún empleado será objeto de sanciones disciplinarias a raíz de una muestra individual de servicios, salvo en caso de abuso del cliente, fraude y violación de la privacidad de las comunicaciones o cuando los esfuerzos de superación no hayan dado resultado.

El convenio con Pacific Bell (SBC) limita la supervisión del personal a 10 llamadas por mes.

En Australia, el sindicato Communication Electrical and Plumbing Union (CEPU) también abordó la cuestión del control excesivo en los telecentros. Los sindicatos ejercen presión para que los Estados australianos establezcan mínimas condiciones de trabajo en los telecentros.

Un motivo de que la cuestión del control y la supervisión sea tan importante en los telecentros reside en que numerosas encuestas muestran que es una de las causas principales del estrés de los trabajadores. El informe de un académico del Reino Unido dice que no cabe duda que muchos trabajadores consideran que los mecanismos de control y vigilancia contribuyen a las presiones del puesto de trabajo. Más de un tercio estima que la grabación de sus llamadas contribuía “en gran medida” o “en alguna medida” a dichas presiones[56]. Volveremos sobre esta cuestión, más adelante.

7. Control mediante biometría e implantes

En la última sección de esta parte del informe daremos una mirada al alcance de una vigilancia de los trabajadores en forma más directa e invasiva, pues tiene que ver con el cuerpo.

La tecnología de la biometría (reconocimiento de las características físicas propias a una persona) ya se utiliza en varios contextos diarios. El escáner de huellas digitales se practica en EE.UU. para controlar a los extranjeros que visitan el país. El reconocimiento del iris se considera un elemento muy prometedor de la futura identificación individual.

A diferencia de la forma tradicional en que la policía tomaba las huellas digitales de los sospechosos utilizando almohadillas de tinta y papel, los datos biométricos son digitalizados, es decir, registrados y conservados en forma digital por lo que pueden someterse a un detallado análisis informático. La biometría puede tener repercusiones de fondo en la privacidad. Los sindicatos tendrán que seguir muy de cerca los intentos de incorporar esta tecnología en los lugares de trabajo.

Ya tenemos ejemplos de esa incorporación como en el caso de McDonalds que, en algunos de sus puestos de venta de Canadá, utiliza el escáner del pulgar y la mano de los trabajadores[57]. También en Canadá, el CUPW, sindicato de trabajadores de correos, impugnó el intento de la Canada Post Corporation de exigir que se tomaran las huellas digitales de algunos de sus carteros como parte del “control de fiabilidad”[58].

Los fabricantes de etiquetas RFID fueron todavía más allá con el concepto de implantar minúsculos dispositivos RFID en la piel. Sería reconfortante poder decir que esa idea sigue perteneciendo a la ciencia ficción, pero, por desgracia, no es así. La compañía estadounidense Applied Digital ya fabrica ese dispositivo denominado VeriChip.

El VeriChip se comercializa sobre todo como un medio de que la gente disponga en todo momento de su historial médico. También fue utilizado en una discoteca

que alentó a sus clientes a implantárselo para facilitar la entrada y pagar los tragos en el bar. Además, los VeriChips ya se utilizan en el contexto laboral: 18 funcionarios que trabajan en la oficina del Fiscal General mexicano se los hicieron implantar voluntariamente. Estos dispositivos (véase la imagen[59]) se utilizan para autorizar el acceso del personal a zonas restringidas.

Más adelante, se indican los posibles riesgos para la salud del implante de dispositivos RFID, pero incluso si se dejan de lado esos riesgos, está claro que nuevos productos como el VeriChip tienen consecuencias de talla para el derecho a la privacidad, dentro y fuera del lugar de trabajo.

Algunas cuestiones planteadas por el control y la supervisión electrónicos

¿Qué está pasando? ¿Por qué el estilo de gestión con asistencia electrónica de comando y control, al parecer, se va imponiendo justo en un momento en que según la retórica de recursos humanos, la era de la información requiere un "trabajo inteligente" y formas de mayor colaboración en la participación de los empleados?

Una respuesta falaz podría ser: simplemente porque ahora se dispone de tecnología para hacer esa vigilancia. El Profesor Michael Blakemore, que asesoró al sindicato GMB del Reino Unido, habla del mensaje "tranquilizador" que, al parecer, puede ofrecer esa tecnología. A su entender, en esa retórica está profundamente incrustada la promesa de seguridad y beneficios[60], pero también señala que la confianza en la tecnología puede tener consecuencias de largo alcance en el lugar de trabajo, ya que modifica la relación entre gerentes y trabajadores, pues los primeros dejan de entablar conversaciones con los segundos y se limitan a vigilarlos.

Él y otros académicos usan cada vez más el concepto de "informática invasora", entendida como un proceso en el cual, los ordenadores se incrustan en la vida diaria de manera que se vuelven, prácticamente, invisibles y se dan por descontados[61]. Por analogía, la vigilancia invasora, según Blakemore, es aquella situación en que casi todo lo que hace un empleado se puede vigilar, analizar y controlar.

Tal como se señala en el memorable informe de la OIT sobre las condiciones de trabajo, algunos trabajadores se ven más afectados que otros por la vigilancia en el lugar de trabajo: los tipos de trabajo donde existen mayores probabilidades de estar sujeto a una vigilancia muy intensiva suelen ser los que hacen mujeres, trabajadores de grupos minoritarios y, en general, aquellos trabajadores poco remunerados[62]. Al respecto, es significativo que el GMB, en su campaña contra las condiciones de trabajo, tipo "granja de cría intensiva", que existen en los

almacenes (véase arriba) informara que muchos trabajadores de los almacenes incluidos en la encuesta fueran inmigrantes.

Por lo tanto, la cuestión reside en que en esta era de la información, algunos trabajadores con puestos que exigen conocimientos de alto valor pueden, de hecho, verse librados de la apremiante supervisión jerárquica, mientras muchos otros se ven seriamente constreñidos por la tecnología. En efecto, este tipo de relación con la tecnología, a menudo, se ha equiparado con el trabajo en cadena de montaje.

La supervisión mediante control electrónico puede resultar “tranquilizadora” para las empresas, pero, ¿es realmente eficaz? Al parecer, la respuesta más común es no. En 1999, Gary Marx del MIT, escribía que no había pruebas contundentes que respaldaran la retórica a favor del control, pero sí, buenos motivos de prever que un control desenfrenado fuera contraproducente, pues el impacto negativo en el bienestar físico y mental de los trabajadores podía dar por tierra con los beneficios que se descontaba obtener gracias a la mayor eficiencia resultante de ese control[63].

Ahora bien, no se trata de saber si la vigilancia es o no “efectiva” para las empresas. Incluso si *hubiera* pruebas que demostraran cabalmente las ventajas para éstas, hay razones de peso por las cuales, los sindicatos deberían oponerse a esa práctica. Veamos tres de ellos uno por uno.

Derecho a la representación colectiva

En primer lugar, y desde un punto de vista más pragmático, tienen motivo de preocuparse porque empleadores hostiles pueden servirse del control y la vigilancia de los trabajadores para desalentar una verdadera representación colectiva.

Hubo una serie de casos en que la vigilancia se puso en marcha justo cuando los sindicatos se proponían organizar a trabajadores que no estaban sindicados. Citemos el ejemplo de la Wal-Mart, sumamente conocida por su antisindicalismo, que instaló cámaras para vigilar a los trabajadores “sospechosos” de una tienda donde el UFCW intentaba organizar al personal. Al parecer, esta empresa hizo lo

mismo en una de sus tiendas de Indiana y, con toda probabilidad, en muchas otras partes de Estados Unidos[64].

Incluso allí donde se reconoció a los sindicatos, una jornada laboral sujeta a un control estricto no crea, forzosamente, un clima propicio para una efectiva labor sindical. Tal como señalara Eric Lee, en otros tiempos, los trabajadores tenían más facilidad de comunicar sus preocupaciones en voz baja a los representantes sindicales, por ejemplo, cerca de un refrigerador de agua[65]. Cuanto más se controla la jornada laboral, menos posibilidades hay de que se establezca este tipo de contacto informal entre el trabajador y el representante sindical.

Cuestiones de salud y seguridad

La nueva tecnología conlleva nuevos riesgos para la salud y la seguridad. El uso del teclado del ordenador para tareas como la introducción de datos multiplicó las lesiones por esfuerzos repetitivos y los trabajadores de telecentros se exponen al riesgo del choque acústico.

En este momento no resulta nada fácil detectar las consecuencias que pueda tener la creciente "informática invasora" para la salud de los trabajadores. Indudablemente, tampoco ayudará que los fabricantes de los dispositivos tecnológicos descritos en este informe, por lo general, no prestan mucha atención a la información técnica que ponen a disposición sobre cuestiones de ergonomía o de salud y seguridad en el trabajo.

Ahora bien, algunas cuestiones potenciales saltan a la vista. En primer lugar, preocupan los efectos físicos que pueda tener el constante uso de ordenadores que se llevan puestos descritos anteriormente. Tal como indicado, un popular reloj pulsera con ordenador incorporado pesa 320 gramos y 350 cuando incluye un transmisor-receptor de radio. El escáner, tipo dedal, que se coloca en el índice pesa 50 gramos y funciona con una simple presión del pulgar[66].

La proliferación mundial de los teléfonos celulares conlleva preocupaciones sobre los posibles peligros de la radiación electromagnética, campo de investigación donde, por el momento, los resultados no son concluyentes. Según

parece, se ha trabajado muy poco acerca de las consecuencias de otras tecnologías de rastreo. En cuanto a los dispositivos RFID implantados, la Agencia Federal de Medicamentos de Estados Unidos concedió la licencia, pero enumeró los probables riesgos para la salud: reacción cutánea adversa; migración del transpondedor implantado; información de seguridad comprometida; averías del transpondedor, el insertador y el escáner electrónico; interferencia electromagnética; riesgo eléctrico; incompatibilidad de imagen de resonancia magnética y pinchazo de aguja[67].

En términos generales, una cantidad considerable de investigaciones sugiere que existe un vínculo entre la incorporación del control de rendimiento y el aumento de problemas de salud y seguridad de los trabajadores. El problema de salud y seguridad más frecuente respecto al control y la vigilancia electrónicos es el consiguiente aumento del estrés en el lugar de trabajo. Ya en 1993, el informe de la OIT sobre el tema señalaba lo que sigue.

Un estudio conjunto de investigadores de la Universidad de Wisconsin y la Communications Workers of America sobre control electrónico y estrés en el trabajo confirmó estudios anteriores que sostienen que dicho control es uno de los principales factores de estrés en el lugar de trabajo, lo que, en parte, está vinculado con el sentimiento de impotencia que sienten los empleados controlados[68] (traducción libre).

El estrés en los telecentros preocupa en grado sumo y fue una de las cuestiones tratadas en la Conferencia Mundial de la UNI sobre Telecentros, celebrada en 2005. Esta última llamó a hacer una campaña para mejorar la salud y el bienestar del personal de todos los telecentros del mundo que incluyera medidas para reducir el estrés, la ansiedad, el agotamiento profesional y la depresión.

 En Verizon-South, New Jersey, la medición del rendimiento se basa más bien en el equipo que en cada trabajador, práctica recomendada por el comité de CWA-Verizon que se ocupa del estrés[69].

En los últimos años, el estrés en el lugar de trabajo comenzó a considerarse más seriamente en términos de salud y seguridad en el trabajo. En 2004, por ejemplo, los interlocutores sociales de Europa adoptaron oficialmente un

acuerdo marco sobre el estrés relacionado con el trabajo. No obstante, los vínculos entre el control electrónico y el estrés, al parecer, aún no se entienden muy bien. En el acuerdo marco de la UE, por ejemplo, no se alude concretamente a la relación entre vigilancia y estrés.

Privacidad y trabajo decente

Tal vez, la cuestión de mayor peso que plantean el control y la vigilancia guarde relación con el derecho fundamental de los trabajadores a la privacidad. En un informe de la UE se dice que los trabajadores no dejan cada mañana su derecho a la privacidad y la protección de datos a las puertas del lugar de trabajo[70]. De hecho, la privacidad cobra aún mayor importancia cuando las fronteras entre el tiempo y el espacio "laborales" y el tiempo y el espacio "personales" son cada vez más borrosas debido, por ejemplo, al teletrabajo y los contratos con horario flexibles.

Hace casi 10 años que la OIT trató de abordar las cuestiones de privacidad que conlleva el almacenamiento de datos personales de los trabajadores. Su repertorio de recomendaciones prácticas contiene una corta cláusula sobre vigilancia[71].

 El párrafo 6.14 del Repertorio de la OIT dice:

Cuando los trabajadores sean objeto de medidas de vigilancia, éstos deberían ser informados de antemano de las razones que las motivan, de las horas en que se aplican, de los métodos y técnicas utilizados y de los datos que serán acopiados, y el empleador deberá reducir al mínimo su injerencia en la vida privada de aquellos.

El secreto en materia de vigilancia sólo debería permitirse cuando
- se realice de conformidad con la legislación nacional, o
- existan sospechas suficientes de actividad delictiva u otras infracciones graves.

La vigilancia continua debería permitirse solamente si lo requieren la salud, la seguridad y la protección de los bienes.

Desde entonces, se ha tendido a abordar las cuestiones relativas a la privacidad de los trabajadores en forma tangencial en la legislación general sobre protección de datos. En la Unión Europea, por ejemplo, se pidió a los Estados miembros que legislaran conforme a las disposiciones de la Directiva sobre protección de datos, de 1995. La Comisión Europea propuso que las cuestiones propias a la protección de datos en el lugar de trabajo se abordaran en el diálogo entre interlocutores sociales. En 2002, la Comisión presentó una propuesta detallada de acuerdo marco (véase más adelante) para que se usara en los debates. Ahora bien, el informe de seguimiento de la Comisión, previsto para 2004, no se publicó y, según parece, esta cuestión sigue tranquilamente "estacionada".

La citada propuesta contiene una serie de principios, entre ellos, el derecho de los representantes de los trabajadores a ser informados y consultados antes que se introduzcan sistemas de control y vigilancia; restricciones de control continuo; estrictas directrices sobre el control secreto y la prohibición de control rutinario del uso de Internet y el correo electrónico. Además, prevé que los datos personales recabados mediante control electrónico no deberían ser los únicos factores que intervengan en la evaluación del rendimiento de los trabajadores[72] (traducción libre).

Un ejemplo digno de mención sobre una valiosa iniciativa legislativa nos llega de Nueva Gales del Sur, Australia, donde el año pasado (2005) el gobierno estatal del partido laborista sancionó la ley sobre vigilancia en el lugar de trabajo. Esta última amplía a otras y nuevas formas de control electrónico, las disposiciones sobre controles de la ley en materia de videdovigilancia de 1998. En Estados Unidos, el sindicato Communications Workers of America (CWA) viene trabajando para que el Congreso apruebe una ley similar que restrinja el uso de la vigilancia de audio y video[73].

Varios sindicatos y federaciones sindicales han adoptado códigos de práctica idónea que protegen la privacidad de los trabajadores. Citemos los ejemplos del FNV de los Países Bajos que estableció un reglamento modelo en la materia[74] y

la IT Professionals Association (que forma parte del sindicato Amicus de RU/Irlanda) que también redactó un proyecto similar de código de práctica[75].

Iniciativas como éstas contribuirán a demostrar que el hecho de que los empleadores almacenen datos electrónicos sobre los trabajadores mediante distintas formas de control y vigilancia no es sólo una cuestión técnica de cumplir con las normas relativas a la protección de datos. Aquí se plantean cuestiones de derechos humanos fundamentales. La raíz de esta cuestión es la dignidad humana.

Conclusión: El camino adelante para UNI

Aunque el control y la vigilancia electrónicos están en aumento en muchos sectores, no se trata, forzosamente, de un lóbrego determinismo tecnológico. Ya abundan ejemplos de buena práctica de sindicatos y otros colectivos respecto a estos hechos. La propia UNI tiene experiencia tanto en la exitosa iniciativa Derechos en línea para los trabajadores en línea como en la lucha relativa al trabajo en los telecentros, incluida la reciente Conferencia Mundial sobre Telecentros. Las afiliadas de la UNI y otras organizaciones sindicales también tienen experiencias positivas (algunas mencionadas en el presente informe) que pueden compartir.

Aun así, conviene que la UNI considere la manera de optimizar la función que cumple en lo que se refiere a abordar la cuestión del control y la vigilancia electrónicos.

1 Se ha atendido muy poco a la rapidísima evolución de la tecnología de identificación por radiofrecuencia (RFID por la sigla en inglés). El rastreo RFID se utiliza cada vez más, en particular, las insignias RFID con el nombre. La UNI publicará un Código de Práctica, similar al de Derechos en línea en el trabajo, para ayudar a las afiliadas en su labor.

2 La vigilancia RFID también guarda relación con cuestiones más amplias en lo que respecta al rastreo de trabajadores mediante sistemas de localización por satélite (GPS por su sigla en inglés) y teléfonos celulares. La UNI ampliará su labor mundial mediante la campaña *Who's on Your Tracks? (¿Quién no le pierde pisada?*) para ayudar a las afiliadas y sus miembros a comprender y abordar las cuestiones planteadas aquí. El informe será tratado en cada uno de los Sindicatos Globales de la UNI.

3 Se alentará a la OIT a abordar cuestiones relativas al control y la vigilancia electrónicos, pues su última investigación sustantiva al respecto tiene más de 10

años. Además, la cuestión del control y la vigilancia electrónicos puede vincularse directamente al llamado de la OIT por el trabajo decente.

4 La UNI trabajará con la Unión Europea y otras organizaciones regionales en estas cuestiones y participará en la actual consulta de la Comisión Europea sobre tecnología RFID.

5 En el sitio web de la UNI se publicarán las consecuencias que tiene la vigilancia excesiva para la salud y la seguridad, sobre todo, en relación con el estrés en el lugar de trabajo.

6 La UNI seguirá promocionado vigorosamente la Carta para Telecentros y el Código de práctica sobre derechos en línea.

7 Las cuestiones relativas al control y la vigilancia no se limitan al lugar de trabajo. Se alienta a las afiliadas de la UNI a hacer causa común no sólo con las organizaciones de defensa de las libertades civiles y la privacidad, sino también con campañas más amplias (como la de los consumidores estadounidenses contra el uso de la RFID para vigilar a la clientela), preocupadas por la manera en que se están introduciendo nuevas tecnologías.

[1] This story is based on real events and real issues
[2] http://www.nocards.org, http://www.spychips.com
[3] Alorie Gilbert, Elementary school nixes electronic ID, February 17 2005 http://news.com.com/2102-1029_3-5581275.html
[4] Andrew Bibby, Invasion of the privacy snatchers, Financial Times, January 9 2006
[5] Paul Tyrrell, Tuned in to the right frequency, Financial Times, December 15 2004
[6] 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
[7] from http://www.spychips.com
[8] Will Sturgeon, Las Vega casino goes for RFID, April 15 2005 http://software.silicon.com/security/0,39024888,39129583,00.htm
[9] 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
[10] WaspTime see http://www.waspbarcode.com/wasptime/wasptime_premium.asp
[11] 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
[12] Resolution on Radio Frequency Identification, 20 November 2003
[13] Article 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, January 19 2005, WP105
[14] 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
[15] Cornelia Brandt, Klüger als die intelligenten Dinge sein… Risikoabshätzung bei RFID-Anwndung fordert Handeln auf verschiedenen Ebenen, 2005
[16] 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
[17] 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
[18] http://www.peaktech.com/html/products/barcode_scanner/wearable.htm
[19] Case study, Hands-free Plus real-time, equals business advantage, http://www.symbol.com/category.php?fileName=CS-27_Peacocks.xml
[20] 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
[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, n.d.
[24] 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
[25] On Board Computer – Big Brother Comes to CPC
[26] Agreement between Canada Post Corporation and Canadian Union of Postal Workers (expires January 31 2007)
[27] 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
[28] David Hencke, AA to log cal centre staff's trips to loo in pay deal, The Guardian, October 31 2005
[29] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[30] See for example 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/. Another checklist for employers is offered by Gundars Kaupins and Robert Minch, Legal and Ethical Implications of Employee Location Monitoring.
[32] National Workrights Institute, On Your Tracks: GPS Tracking in the Workplace n.d
[33] Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[34] For example at 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] 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.
[37] Anthony Hildebrand, Branching Out, http://www.smtdirect.co.uk/story.asp ?sectioncode=0&storyCode=3060661
[38] Information from the union, Jan 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] FNV Bondgenoten, Model Protocol: privacy in the use of the internet and e-mail, n.d.
[42] Cornelia Brandt, Onlinerechte für Beschäftigte, in DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004
[43] Eckpunkte der Nutzung von Internet, Intranet und E-mail im Arbeitsverhältnis, in DGB, Internet und E-mail: Neue Medien im Betrieb, September 2004
[44] European Industrial Relations Observatory, New technology and respect for privacy at the workplace, 2003 http://www.eiro.eurofound.eu.int
[45] http://www.fgtb.be/code/fr/Documents/2003/ViePrivee/c15_03e0405.htm
[46] Grupo de Trabajo sobre Protección de datos – Artículo 29, Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, adoptado el 29 de mayo de 2002, WP55 https://www.agpd.es/upload/Canal_Documentacion/legislacion/Union%20Europea/Articulo%2029/B.2.52)%20wp55%20%20vigilancia%20comunicaciones%20electr%F3nicas%20trabajadores.pdf
[47] European Commission, Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data 2002 http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultationdataprot_en.pdf
[48] 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
[49] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[50] Hubert Bouchet, La cybersurveillance sur les lieux de travail, CNIL March 2004
[51] Michael Sommer, Cornelia Brandt and Lothan Schröder (eds), Im Netz@work, VSA-Verlag, 2003
[52] American Management Association, 2005 Electronic Monitoring and Surveillance Survey
[53] Andrew Bibby, Organising in Financial Call Centres, UNI, 2000
[54] UNI Global Call Centre News, April 2004
[55] Communications Workers of America http://www.cwa-union.org/workers/customer/protections.asp
[56] Philip Taylor and Peter Bain, Trade Unions and Call Centre Survey, for Finance Sector Unions, 2000
[57] Hazards magazine, Stop Snooping, http://www.hazards.org/privacy/
[58] http://www.cupw.ca/pages/document_eng.php?Doc_ID=595
[59] Photo from http://www.spychips.com
[60] Michael Blakemore, Every breath you take, every move you make, http://www.unionweb.co.uk/view/PageView.aspx?Page=273

[61] 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

[62] ILO, Conditions of work digest volume 12
Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993

[63] 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

[64] 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

[65] Eric Lee, Trade Unions in the electronic workplace, April 13 2004
http://www.ericless.me.uk/archive/000079.html

[66] http://www.peaktech.com/html/products/barcode_scanner/wearable.htm

[67] http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt

[68] ILO, Conditions of work digest volume 12
Workers' privacy: Part II, monitoring and surveillance in the workplace, 1993

[69] Communications Workers of America
http://www.cwa-union.org/workers/customer/protections.asp

[70] Grupo de Trabajo sobre Protección de datos – Artículo 29, Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, adoptado el 29 de mayo de 2002, WP55

[71] Protección de los datos personales de los trabajadores, OIT, 1997
http://www-ilo-mirror.cornell.edu/public/english/protection/safework/cops/spanish/index.htm

[72] 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

[73] 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

[74]http://home.fnv.nl/02werkgeld/arbo/wetgeving/privacy/Model%20Privacyreglement/model_privacyreglement1.htm

[75] http://www.amicus-itpa.org/juneconf2.shtml