

LOS IDENTIFICADORES POR RADIOFRECUENCIA (RFID) Y SU USO COMO UN “NOVEDOSO” MECANISMO DE CONTROL EMPRESARIAL

JORGE ARREDONDO PACHECO*

Abogado

DANIELA HIRSCH VERGARA**

Abogada

RESUMEN: La velocidad con que avanza la tecnología no es un tema nuevo, sin embargo, sí lo es, la manera en que su inserción se realiza en contextos que no fueron los originarios para su uso. En efecto, y en lo que respecta a los identificadores por radiofrecuencia (RFID), estos dispositivos vienen a ser el sustituto perfecto de los hoy en día conocidos como códigos de barra. Ideados con fines de control de gestión o de individualización de ciertos productos o artículos que se intenta monitorizar, actualmente su uso ha escapado a estas iniciales tareas. En efecto, aunque de forma aún no muy masificada, pueden en estos tiempos encontrarse experiencias en las cuales se han implementado estos chips en la empresa a objeto de concretizar el poder de control patronal. El desafío que esto trae aparejado es de qué forma la legislación laboral hace frente a esta nueva realidad y cómo lograr que derechos como la intimidad o la protección de datos de los trabajadores no se vean vulnerados. Este artículo intenta ser una primera aproximación al estudio de este adelanto tecnológico con incidencias laborales y con ello llamar la atención ante realidades que pudiesen propagarse el día de mañana.

Palabras clave: *identificadores por radiofrecuencia, facultad de control empresarial, derecho a la intimidad, derecho a la protección de datos*

ABSTRACT: The speed with which technology advances is not a new subject, nevertheless, it is in the way in which the integration of such is carried out in contexts that were not as originally intended. In this light, radio frequency identification (RFID), are devices designed to be the perfect replacement for today known “bar codes”. Designed for the purpose of management control or identification of goods or articles that are being monitored, its use has escaped these initial tasks. In effect, albeit not very popular yet, there can be experiences in which these chips have been implemented by the company to give tangible expression of management control of personnel. The challenge that this brings is how does labor law face this new reality and how does labor law protect workers from the violation of rights such as privacy or data protection. This article is intended as a first approach to the study of this breakthrough technology with labor rights implications, thereby drawing the attention to situations that could spread tomorrow.

Key words: *radio frequency identification, employer’s control attribution, intimacy right, data protection*

* Abogado, Magíster en Derecho del Trabajo y de la Seguridad Social, Universidad Rey Juan Carlos, Madrid, España. Correo electrónico: jorge.arredondo.pacheco@gmail.com

** Abogada, Diplomada en Derecho del Trabajo, Universidad Diego Portales. Correo electrónico: hirschvergara@gmail.com

1. LOS RFID: IDEAS A TENER EN CONSIDERACIÓN

Uno de los adelantos tecnológicos más revolucionarios en los últimos tiempos, y que marcará el destino hacia futuro, lo constituyen los denominados identificadores por radiofrecuencia (en adelante, RFID).

Como todo avance, es celebrado por las utilidades que presenta a la sociedad en su conjunto. Sin embargo, no debe perderse de vista la necesidad de reflexionar, analizar y solucionar los posibles problemas derivados de su implementación; cuáles serían, por ejemplo, los sujetos pasivos de esta ventaja tecnológica, y en lo que aquí interesa, su incidencia en los derechos de los trabajadores. Pero para partir este artículo, resulta pertinente, en primer lugar, describir en qué consiste este adelanto científico.

Al respecto, se ha dicho que “la identificación por radiofrecuencia (RFID) es una tecnología que permite la identificación y la captura de datos automáticos mediante la utilización de radiofrecuencias. La característica más destacada de esta tecnología es la posibilidad de asociar un identificador único junto con otra información (en un microchip) a cualquier objeto, animal o persona, y leer esta información a través de un dispositivo inalámbrico. Se considera que los dispositivos RFID constituyen la puerta de acceso a una nueva fase de la sociedad de la información, denominada «Internet de los objetos» en la que la Red conecta no sólo ordenadores y terminales de comunicaciones, sino cualquier objeto cotidiano: ropa, bienes de consumo, etc.”¹.

Agregándose a su turno, que “la principal característica de la tecnología RFID es la capacidad de identificar, localizar, seguir o monitorizar personas u objetos sin necesidad de que exista una línea de visión directa entre la etiqueta y el lector (al menos en algunas de las frecuencias de trabajo)”².

Yendo a los orígenes de esta técnica, se puede apreciar que esta nació ideada en sus inicios, –al igual de como ocurrió con el *Global Positioning System* (GPS)–, para fines militares. Sin embargo, hoy en día es frecuentemente utilizado con fines comerciales, sin desconocer, –y es ahí donde resultaría oportuno marcar el énfasis–, su posible destino en contextos laborales como un medio de control de la persona del trabajador.

Efectivamente, el:

“RFID no es una tecnología nueva, sino que lleva existiendo desde 1940. Durante la Segunda Guerra Mundial, los militares estadounidenses utilizaban un sistema de identificación por radiofrecuencia para el reconocimiento e identificación a distancia de los aviones: «Friend or Foe» (amigo o enemigo). Acabada la guerra, los científicos e ingenieros continuaron sus investigaciones sobre estos temas. En octubre de 1948, Harry Stockman publicó un artículo en los *Proceedings of the IRE* titulado «Communications by Means of Reflected Power», que se puede considerar como la investigación más cercana al nacimiento de la RFID.

¹ FERNÁNDEZ ALLE, C. “La tecnología RFID y sus implicaciones jurídicas”, en: *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 38, 2009, Madrid, España, pp. 1-8 (versión *on line*). Disponible en: [² *Ibid.*, p. 3.](http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142540502890&esArticulo=true&cidRevistaElegida=1142527411030&language=es&pag=2&pagename=RevistaDatosPersonales%2FPag%2Fhome_RDP&siteName=RevistaDatosPersonales[fecha de visita 25 de Abril de 2012]. p.2.</p></div><div data-bbox=)

A partir de ese momento, el desarrollo de la tecnología RFID ha sido lento pero constante. Durante la década de los 50 se realizaron multitud de estudios relacionados con la tecnología, principalmente orientados a crear sistemas seguros para su aplicación en minas de carbón, explotaciones petrolíferas, instalaciones nucleares, controles de acceso o sistemas antirobo”³.

1.1 CARACTERÍSTICAS BÁSICAS DEL SISTEMA

Operativamente, el sistema se compone de cuatro elementos: una etiqueta RFID, un lector, un ordenador y un *middleware*, los cuales cumplen las siguientes funciones:

- a) “La etiqueta se inserta o adhiere en un objeto, animal o persona portando información sobre el mismo. En este contexto, la palabra «objeto» se utiliza en su más amplio sentido: puede ser un vehículo, una tarjeta, una llave, un paquete, un producto, una planta, etc. Consta de un microchip que almacena los datos y una pequeña antena que habilita la comunicación por radiofrecuencia con el lector.
- b) Un lector o interrogador, encargado de transmitir la energía suficiente a la etiqueta y de leer los datos que ésta le envíe. Consta de un módulo de radiofrecuencia (transmisor y receptor), una unidad de control y una antena para interrogar los tags vía radiofrecuencia”⁴; destacándose que “algunos lectores llevan integrado un programador que añade a su capacidad de lectura, la habilidad para escribir información en las etiquetas”⁵.
- c) “Un ordenador, host o controlador, que desarrolla la aplicación RFID. Recibe la información de uno o varios lectores y se la comunica al sistema de información”⁶.
- d) “Adicionalmente, un middleware y en backend un sistema ERP de gestión de sistemas IT son necesarios para recoger, filtrar y manejar los datos”⁷.

Todas las etiquetas RFID presentan los mismos componentes, sin embargo, existen algunas que solo permiten leer la información contenida en el chip. Otras, por el contrario, aparte de esta aplicación presentan la particularidad de grabar información en la etiqueta o modificar las características con que se le ha singularizado.

Atendido a razones económicas su generalización se encuentra en cierto modo restringida, pero es de esperar que con el paso del tiempo, y la reducción de estos costes, su uso se extienda dentro de los distintos sectores y áreas del mercado⁸.

³ PORTILLO GARCÍA, J. I.; BERMEJO NIETO, A. B.; BERNADOS BARBOLLA, A. M. *Informe de Vigilancia Tecnológica Madrid. Tecnología de identificación por radiofrecuencia (RFID): aplicaciones en el ámbito de la salud*. Madrid, España: Fundación Madrid para el conocimiento, 2008, pp. 1-176. Disponible en: <http://www.madrimasd.org/informacionidi/biblioteca/publicacion/Vigilancia-tecnologica/default.asp>[fecha de visita 25 de Abril de 2012]. p. 21.

⁴ FERNÁNDEZ ALLE, C., *op. cit.* (n. 1), p. 2.

⁵ *Ibid.*

⁶ *Ibid.*

⁷ *Ibid.*

⁸ En cuanto a su costo, se ha dicho que “el precio de las tarjetas RFID más baratas ha disminuido muy por debajo de 50 centavos

En este sentido, se ha llegado a afirmar que:

“En la actualidad están disponibles etiquetas RFID de diversos tipos, prestaciones y precios, pero su coste se va reduciendo, lo que facilitará, sin duda, un uso más frecuente en el futuro. Cabe afirmar incluso que, en opinión de la Comisión Europea, la tecnología RFID puede convertirse en un nuevo motor del crecimiento y el empleo que efectúe una aportación considerable a la estrategia de Lisboa”⁹.

Añadiéndose,

“Es mucho lo que promete en términos económicos, generando nuevas oportunidades comerciales, reducciones de costes y aumentos de eficiencia, en particular en la lucha contra la falsificación y en la gestión de los residuos electrónicos, los materiales peligrosos y el reciclado de los productos al final de su vida útil (...). A lo que cabe añadir que la propia Comisión asume que estas etiquetas (...) irán formando progresivamente parte integrante de nuestra vida cotidiana”¹⁰.

1.2 USOS ACTUALES DE LA TECNOLOGÍA RFID

Por ahora, su masificación se ha dado en contextos comerciales, en donde los RFID han venido a ser el sustituto perfecto de los códigos de barra¹¹. La razón de ello estriba en que a diferencia de estos, los identificadores por radiofrecuencia permiten una singularidad individualizada del producto al cual se encuentra adherido el chip, permitiendo a su turno que la captura de esta información sea realizada a distancia¹².

El resultado, ahorro en tiempo, personal y claramente una mayor certeza y eficiencia al momento de realizar un control de gestión.

de US\$, por lo que la utilización en gran escala de la tecnología cada vez es más factible”. BIBBY, A. *Te están siguiendo: Control y vigilancia electrónicos en el lugar de trabajo*, Documento de trabajado elaborado para UNI Sindicato Global (UNI/GS/06-2006/0035/ES), 2006, pp. 1-44. Disponible en: <http://www.andrewbibby.com/pdf/Surveillance-es.pdf> [fecha de visita el 25 de Abril de 2012]. p. 6

⁹ GALA DURÁN, C.; ROIG BATALLA, A. “El uso de etiquetas de identificación por radiofrecuencia en las empresas: ¿un nuevo riesgo para los derechos de los trabajadores?”, en: *Actualidad Laboral*, n° 8, abril, 2010, Madrid, España, p. 1.

¹⁰ *Ibid.*, p. 2.

¹¹ Según los datos que se manejan, “la tecnología RFID entre las empresas españolas es incipiente. De hecho, solo 0,8 por ciento de las microempresas ha adoptado esta tecnología, mientras que ese porcentaje sube al 3,1 por ciento en el caso de las pymes, de las entidades de 10 a 49 empleados, y a 8,9 por ciento si el rango va de 50 a 249 trabajadores; por lo que respecta a las grandes empresas (más de 249) el porcentaje es del 20 por ciento.

A la cabeza de las empresas que más usan estos dispositivos, se sitúan las dedicadas al transporte y almacenamiento (12,2 por ciento). Por detrás se encuentran el sector financiero (con un 8,2 por ciento), la informática, telecomunicaciones y audiovisuales (7,5 por ciento) y el comercio mayorista (6,2 por ciento) y minorista (5 por ciento).

Las microempresas españolas, de menos de 10 empleados, la utilizan mayoritariamente en relación con sistemas de pago (peaje de carreteras o transporte de pasajeros, con un 48,5 por ciento), seguido de la identificación de productos (38,7 por ciento). Por su parte, las pymes y grandes empresas españolas las emplean para el seguimiento y control de la cadena de suministro y de inventarios (44,4 por ciento) y la identificación de personas y control de accesos (40,5 por ciento)”.

REDACCIÓN LA LEY. “Un nuevo riesgo para la privacidad: las etiquetas RFID”, en: *Diario La Ley*, n° 7473, Sección Tribuna, septiembre 2010, p. 2.

¹² Se resaltan como ventajas de esta innovación el que “permiten almacenar gran cantidad de datos, son fáciles de colocar y ocultar para evitar su visibilidad para prevenir robos, identifican de forma unívoca los productos, reducen los costes y facilitan la retirada de un producto del mercado en caso de partida defectuosa”. *Ibid.*

A ello cabe agregar, como posible –aunque también cuestionable– atributo que incentiva su uso, el hecho de que la lectura de los datos que contiene el chip al cual se encuentra adosado el producto puede ser realizado de manera que el portador de estos no se percate de esta situación¹³. Ello fue el detonante para que asociaciones de consumidores manifestaran sus reparos al uso indiscriminado de esta tecnología por parte de los proveedores.

Así, puede citarse lo ocurrido en el año 2003 en donde:

“Dos grandes firmas comerciales (Wal-Mart en EE.UU y Benetton) han tenido que suspender sus pruebas a gran escala de sistemas de control de inventario mediante la utilización de la RFID en sus establecimientos a causa de reacciones del público, receloso de ser objeto de un espionaje exhaustivo con las etiquetas insertadas en los productos adquiridos”¹⁴.

Dejando de lado aquello, y tal como ya se expresara, su implementación y desarrollo se encuentra en el ámbito comercial, destacándose en temas de “seguridad y control de accesos (gestión de pasaportes y visados, seguimiento de niños, seguimiento de animales, seguimiento de equipajes, prevención de falsificaciones, acceso a ordenadores, identificación de empleados, acceso a aparcamientos, acceso a laboratorios, recintos, peajes, pagos automáticos, reconocimiento de clientes)”¹⁵.

Teniendo esto en cuenta, cabría resaltar un sector en el cual los RFID se han masificado de manera vertiginosa. Se apunta al área de la salud, donde actualmente es utilizado en los:

“Medicamentos farmacéuticos y la gestión de sus dosis; pero también el equipamiento crítico (electrocardiógrafos, desfibriladores, sillas de ruedas) en los hospitales o centros sanitarios; sin olvidar a las personas, tanto personal sanitario como pacientes y visitas, que han de ser controladas en un entorno con zonas de acceso restringidas”¹⁶.

Se menciona este sector, no solo por el impulso que le ha dado a esta tecnología y su volumen exponencial de crecimiento en los últimos años, sino porque pudiese sacarse como una primera conclusión el hecho de que en la medida que se va socializando esta técnica y conociendo de sus bondades y aplicaciones, las empresas se muestran llanas a internalizarlas en sus procesos productivos. Y a su turno, a utilizarlo como un novedoso e incipiente sistema de control patronal.

Este desarrollo y progresión es corroborado por el informe del IDTECHEX titulado “*RFID in Healthcare 2006-2016*”, según el cual atendidos los:

“Datos sobre el volumen del mercado global de etiquetas y sistemas RFID aplicados a la salud, que se incrementará rápidamente desde los 90 millones de dólares en 2006 hasta los 2.100 millones en 2016. El citado informe afirma que las principales aplicaciones que liderarán este crecimiento serán el etiquetado de medicamentos y los Sistemas de Localización

¹³ Por ello, la doctrina ya ha expresado que “en internet, el carácter internacional e ilimitado de las conductas hacen más difícil su descubrimiento, prevención y castigo (se plantean a menudo conflictos de jurisdicción). En el caso del RFID no es el carácter internacional, pero sí la forma subrepticia de utilización y el desconocimiento por parte del ciudadano, lo que hacen que el posible seguimiento de las conductas contrarias a los derechos se lleve a cabo de forma efectiva”. FERNÁNDEZ ALLE, C., *op. cit.* (n. 1), p. 2.

¹⁴ WANT, R. “Sistemas de identificación por radiofrecuencia”, en: *Investigación y Ciencia*, n° 330, marzo 2004, p. 42.

¹⁵ FERNÁNDEZ ALLE, C., *op. cit.* (n. 1), p. 3.

¹⁶ PORTILLO GARCÍA, J. I.; BERMEJO NIETO, A. B.; BERNADOS BARBOLLA, A. M. *op. cit.* (n. 3), p. 24..

en Tiempo Real (RTLS) para el personal, los pacientes y los objetos o equipamiento crítico en general, en aras de mejorar la eficiencia, seguridad y disponibilidad, y de reducir las pérdidas que una mala gestión de los mismos conlleva”¹⁷.

Como ya puede vislumbrarse, esta tecnología no solo se está utilizando para el trazado de productos o el seguimiento de estos, sino que su novedad radicaría en la posibilidad de permitir una localización de las personas, y en lo que aquí interesa, de los trabajadores.

En ese contexto, pueden encontrarse experiencias comparadas en donde el RFID incide directamente en las personas y trabajadores, como ocurre en el caso de las residencias y ayudas para discapacitados.

Una de esas experiencias es el GEMA A.B.S., (Grupo GEMA), el cual:

“Dispone de la solución GEMA LOC+ Residencias. Basada en tecnología RFID, la solución permite la localización, identificación y monitorización en tiempo real de residentes y empleados. Así, GEMA LOC+ Residencias posibilita el control automático de errantes de tal forma que, si un residente se aproxima a un acceso no permitido para él, el sistema genera las alarmas programadas (sonoras, luminosas, envío a telefonía inalámbrica, SMS, etc.) y, si es necesario, bloquea la puerta de manera automática. Al mismo tiempo, permite localizar en todo momento a las personas, lo que permite conocer la ubicación de cualquier residente en tiempo real y visualizarla sobre el plano de la residencia, gracias a lo cual se evitan las pérdidas de las personas mayores en el centro”¹⁸.

2. LAS PRIMERAS CONTROVERSIAS EN EL USO PERSONALIZADO DE LOS RFID: EL CASO DE LAS ASOCIACIONES DE CONSUMIDORES

Precisado el aspecto operativo del sistema, y previo al análisis de la repercusión de los RFID en el ámbito laboral, parece acertado referirse, sucintamente, a cómo este mecanismo ha sido recepcionado en otras áreas de la disciplina legal que encuentran puntos de encuentro con el Derecho del Trabajo¹⁹.

¹⁷ *Ibid.*, p. 129.

En relación a su incremento e inserción en el mercado, tal como lo ha dado a conocer la prensa escrita, “Bruselas calcula que durante este año saldrán al mercado más 1.000 millones de esos microchips en Europa. Y a nivel mundial, se calcula que en 2020 podría haber 50.000 millones de productos o aparatos conectados electrónicamente.” http://www.cincodias.com/articulo/empresas/bruselas-confia-industria-proteccion-datos-etiquetas-inteligentes/20110406cdscdsemp_5/ [fecha de visita 25 de Abril de 2012].

¹⁸ PORTILLO GARCÍA, J. I.; BERMEJO NIETO, A. B.; BERNADOS BARBOLLA, A. M. *op. cit.* (n. 3), p. 115. Agregan los autores como descripción final de este sistema, “por último, el registro automático de todos los eventos producidos, permite la generación de informes a medida para facilitar la toma de decisiones por parte de la dirección.

¹⁹ Como primer acercamiento entre ambas áreas del derecho, conviene señalar que tanto las relaciones entre consumidores y proveedores, como las que caracterizan a trabajadores con empresas, presentan dos puntos en común.

Inicialmente se destaca la asimetría, tanto de poder como de información, con que cuentan los consumidores y trabajadores vs. proveedores y empleadores (respectivamente), lo que los sitúan en un plano desigualdad para poder negociar y ejercer sus derechos. Como respuesta a esta situación, y en lo que viene a hacer el segundo punto de encuentro entre ambas áreas, se halla el hecho de que el ordenamiento jurídico, consciente de esta relación dispar, crea una normativa específica tendiente a equiparar a las partes y lograr de esa forma una igualdad material entre ambas.

Este tipo de normativas no infringe de modo alguno el principio de igualdad, puesto que esta regulación constituye una manifestación del llamado principio de igualdad por diferenciación en la ley, el cual no tiene por objeto tratar a todas las personas de un modo simétrico, sino, otorgar un tratamiento que permita mayor equidad entre las personas, estableciendo diferencias entre cada una de ellas, diferencias que en ningún caso pueden ser arbitrarias.

Se alude, en específico, al ámbito de los derechos del consumidor. Más concretamente, resulta interesante detenerse en los cuestionamientos y reflexiones que se han hecho por parte de las organizaciones de consumidores.

Estas han sido las primeras que han alzado la voz al verse afectadas, en su concepto, por la implementación de esta tecnología y cuyos cuestionamientos, en algunos casos, deben tenerse presente cuando analizamos esta aplicación en el seno laboral.

En materia de consumidores, el punto central se sitúa en el año 2003. En esa época:

“Walmart, Procter & Gamble, Gillette y la cadena de supermercados Tesco realizaron pruebas piloto sobre un sistema de «estanterías inteligentes», donde se dotaba a los productos de las estanterías del supermercado con una etiqueta RFID, lo que permitía a los empleados del supermercado realizar un seguimiento inteligente del consumo y el stock. Inmediatamente surgió la pregunta de si esa información se podía utilizar para llevar cuenta de las compras realizadas por los clientes del supermercado. Finalmente, WalMart decidió retrasar las pruebas del sistema”²⁰.

Por eso no es de extrañar afirmaciones que desde organizaciones de consumidores se han expresado aludiendo:

“En defensa de la privacidad del consumidor, nos oponemos rotundamente al uso de la RFID en DNI o artículos de consumo individual. Ya desde 2003, nuestra organización CASPIAN (Consumidores Contra la Numeración y la Invasión de la Privacidad en Supermercados, en inglés), junto con la Cámara de Compensación de Derechos de la Privacidad, el Centro de Información sobre Privacidad Electrónica, la Fundación Frontera Electrónica, la Unión de Libertades Civiles Americanas y otras 40 organizaciones en pro de la privacidad y las libertades civiles, reconoció esta amenaza y publicó un documento en el que atacaba de improcedente el seguimiento de personas mediante la identificación por radiofrecuencia”²¹.

²⁰ FERNÁNDEZ ALLE, C., *op. cit.* (n. 1), p. 3.

²¹ ALBRECHT, K. “Etiquetas personales RFID”, en: *Investigación y Ciencia*, n° 386, noviembre 2008, p. 52.

En ese sentido, también se han escuchado voces críticas desde la doctrina referida al seguimiento de personas. Se ha dicho a este respecto que “si bien la utilización de un RFID para realizar el seguimiento de una persona podría tener visibles ventajas, como lo sería en el caso de la vigilancia de personas condenadas en un proceso judicial, enfermos de alzhéimer, incapaces y niños en circunstancias especiales, las consecuencias de su utilización, fuera de casos determinados podría conllevar a una restricción grave de las libertades básicas reconocidas a los ciudadanos como la libertad de movimiento o el libre desarrollo de la libertad humana”. COMISIÓN DE LIBERTADES E INFORMÁTICA. “Comentarios al Documento de Trabajo sobre protección de datos de carácter personal en relación con la tecnología RFID de 19 de Enero de 2005 (WP 105)”, 2005, p. 4. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/rfid/cflcs_es.pdf [fecha de visita 25 de Abril de 2012].

En sentido similar, llamativo son los casos que se han comenzado a dar respecto a la utilización de los RFID, por ejemplo, en “la utilización de estos chips en una escuela primaria, ubicada en Nueva York, donde el director los utiliza para llevar un registro a la hora de ingresar alumnos cada mañana. Este mismo sistema se ha utilizado en las etiquetas de las pulseras que tienen puestas los internos de una cárcel en Texas, los soldados estadounidenses prisioneros de guerra heridos en Irak. Estos microchips pueden ser utilizados para rastrear subrepticamente a la gente. Pese a ello, los expertos en privacidad han manifestado su disconformidad con el uso de etiquetas de RFID en los niños: «Pienso que el experimento está preparando a los niños para el «mundo feliz» en el que las personas serán vigiladas las 24 horas de los siete días de la semana en nombre de la seguridad», señaló Richard Smith, asesor de seguridad y privacidad en Internet. Añadiendo, “mi mayor preocupación es que una vez que comencemos a llevar objetos con etiquetas de RFID tales como tarjetas de acceso, tarjetas de cliente, prendas de vestir, etc., podamos ser rastreados sin nuestro conocimiento por una red de lectoras de RFID conectadas a Internet”. PATÓN PÉREZ, M. I. “La tecnología rfid y su problemática en protección de datos”, en: *Red Seguridad*, marzo, n° 15, 2002. Disponible en: http://www.borrmart.es/articulo_redseguridad.php?id=200&numero=15 [fecha de visita 25 de Abril de 2012].

La cuestión no termina ahí, porque no solo el eventual riesgo de crear perfiles de comportamiento era la situación que inquietaba²²; a esto, había que agregar la posibilidad de ser rastreado de forma subrepticia, dada la posibilidad de incorporar los RFID en las prendas de vestir de manera oculta.

Así aconteció:

“En la primavera de 2003, Benetton Clothing Co. anunció su intención de evaluar chips RFID introducidos en la ropa, para realizar el seguimiento de los productos en la cadena de suministro. Esto levantó una gran polémica, sobre aspectos tales como si al acercarse un consumidor con una prenda con RFID a un lector, se podrían saber aspectos privados del mismo. Al final, Benetton decidió también quitar los chips de las prendas a solicitud del consumidor”²³.

Ello demuestra la posibilidad de que la tecnología pueda ser implementada en ropas de vestir, existiendo además la alternativa de que esto pueda pasar inadvertido.

Un caso emblemático de la inserción de estos dispositivos en ropas de trabajo, eso si –hasta ahora–, sin fines de localización de los trabajadores, se presenta en Francia, más precisamente en el Hospital de Cannes (BIH), que incorporó:

“Un nuevo sistema para proporcionar trazabilidad completa de la ropa que se gestiona en la lavandería. Hasta la fecha, esta lavandería se encarga de la limpieza y gestión de los uniformes de la plantilla de tres hospitales locales, los de Cannes, Antibes y Grasse. En el proyecto, alrededor de 36.000 uniformes han sido equipados con el tag RFID de Tagsys, ARIOTM 70-TL, un tag pequeño y rígido que es capaz de resistir exposiciones repetidas al agua, al calor y a los productos químicos. Antes, esto suponía contar cada uniforme manualmente a medida que éstos entraban en las instalaciones. Con esta nueva solución, los uniformes están disponibles para poder ser trazados de manera rutinaria y registrados para el inventario, a medida que van entrando en las instalaciones. A través del escaneo de cada pieza de ropa, el personal de la lavandería cuenta con la posibilidad de determinar los stocks, identificar la ropa instantáneamente, su respectivo dueño y la unidad del hospital al que corresponde, así como determinar el tratamiento de la misma”²⁴.

²² Como ha tenido ocasión de señalarse “utilizando técnicas de «minería de datos», este análisis permitiría definir perfiles de consumo basados en las preferencias de los clientes, utilizando esta información para diseñar y orientar la estrategia de marketing y publicidad de las empresas. INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN Y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía sobre seguridad y privacidad de la tecnología RFID*. Mayo 2010, p. 36. Disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/julio/Guia_RFID.pdf (fecha de visita el 25 de Abril de 2012).

En el mismo sentido ROIG BATALLA, A. “Derechos Fundamentales y Tecnologías de la Información y de las Comunicaciones”, en: *Cuadernos de Derechos Constitucional*, 2010, Barcelona, España, p. 41, quien señala lo siguiente: “Uno de los posibles riesgos para el derecho a la intimidad de las personas proviene de la capacidad para fijar perfiles de usuario gracias a las preferencias de consumo detectadas en los centros comerciales. El riesgo existiría debido a la posibilidad técnica de haber vinculado de alguna manera un código de producto a un comprador. Por ejemplo, todos los productos tienen únicamente un número de tienda único, que se combina con el nombre del comprador, obtenido quizá con tarjeta de crédito, y que luego se incorpora a una base de datos personales de compradores. Por otro lado, al no existir incentivo económico, ni obligación legal de desconectar la etiqueta una vez se ha comprado el producto, muchas etiquetas quedan activas. Por consiguiente, los datos incorporados en la ropa, o en los complementos de los clientes, así como la información relativa a los medicamentos que pudieran llevar encima podrían en ocasiones ser detectables por lectores compatibles. En general, la etiqueta inteligente potencia las posibilidades de venta directa, pues los hábitos de compra pueden ser reconocidos por un lector cuando la persona entra en un establecimiento comercial”.

²³ PORTILLO GARCÍA, J. I.; BERMEJO NIETO, A. B.; BERNADOS BARBOLLA, A. M. *op. cit.* (n. 3), p. 80.

²⁴ PORTILLO GARCÍA, J. I.; BERMEJO NIETO, A. B.; BERNADOS BARBOLLA, A. M. *op. cit.* (n. 3), p. 113.

3. PRINCIPALES TEMORES ANTE UNA MASIFICACIÓN DESREGULADA DE LOS RFID

Evidentemente no puede dejarse al arbitrio de los particulares la forma en que se regulará el uso y destino de los RFID, y menos aún en el campo laboral, ámbito caracterizado por una asimetría de poder entre las partes.

Por ello, ya se ha expresado que se vislumbra la “necesidad de perfeccionar la legislación para que oriente el uso de la tecnología RFID de tal forma que se respeten tanto la intimidad como la protección de datos de carácter personal”²⁵, agregándose que “se debería establecer por ello, un régimen común que permita proteger la intimidad del individuo y sus datos personales ante la utilización de SISTEMAS DE LOCALIZACIÓN A DISTANCIA (que ya incluirían el aprovechamiento de la tecnología GPS y GALILEO)”²⁶.

En el caso español, estos temores también han sido compartidos por la autoridad encargada de la protección de datos. Así, se ha expresado que “el Director de la Agencia Española de Protección de Datos también ha manifestado sus reticencias en la utilización de estos dispositivos”²⁷.

Esta reticencia también ha tenido repercusión en el seno del grupo más experto, en la Comunidad Europea, en el ámbito de la protección de datos e intimidad de las personas. Se alude al Grupo de Trabajo del Artículo 29²⁸.

Este ya en el año 2005 dio a conocer un documento que se refería a los posibles riesgos que la RFID podía traer aparejado a la vida de las personas en sus distintas manifestaciones (consumidores, trabajadores, etc.)²⁹.

Dicho trabajo reconocía las ventajas que ofrece la tecnología RFID pero hacía hincapié en una serie de fundados temores y riesgos que pueden experimentar los datos privados de los ciu-

²⁵ FARRIOLS I SOLA, A. “Introducción”, en: FARRIOLS I SOLA, A. (Dir. y Coord.). *La protección de datos de carácter personal en los centros de trabajo*. Madrid, España, Cinca, 2006, p. 34.

²⁶ *Ibid.*

Cuando el autor hace mención al proyecto Galileo, se refiere a la apuesta europea por disponer de un sistema propio y bajo control civil. Al respecto se ha dicho que “sin duda cuando Galileo esté disponible la mejora en precisión, disponibilidad y continuidad que un receptor dual Galileo-GPS ofrecerá respecto a lo que conocemos hoy en día hará todavía más interesante la utilización de GNSS en numerosas aplicaciones que son realidades al día de hoy. Este es el caso de los sistemas de navegación, sistemas de gestión de flotas, localización de activos, antirrobo, etc. Otras que a día de hoy no son posibles resultarán viables y muchas otras que todavía no imaginamos surgirán”. COSMEN-SCHORTMANN, J.; MARTÍNEZ-OLAGUE, M. A. “Galileo, el sistema europeo de navegación por satélite”, *Revista técnica de la Asociación Española de la Carretera*, n^o 140, 2005, p. 118.

En el mes de Noviembre del año 2011 fueron enviados los dos primeros satélites del sistema Galileo. Así fue reportado por la prensa escrita española: http://www.elpais.com/articulo/sociedad/primeros/satelites/Galileo/GPS/europeo/lanzaran/manana/elpepusoc/20111018elpepusoc_16/Tes[fecha de visita 20 de Enero de 2012].

²⁷ PATÓN PÉREZ, M. I., *op. cit.* (n. 21).

²⁸ “El Grupo de Trabajo del Artículo 29 (GT 29) creado por la Directiva 95/46/CE tiene carácter de órgano consultivo independiente y está integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea –que realiza funciones de secretariado–. Asimismo, los Estados candidatos a ser miembros de la Unión y los países miembros del EEE acuden a las reuniones del GT 29 en condición de observadores. La Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997”. https://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php (Última consulta realizada el 25 de Abril de 2012).

²⁹ GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. Documento de trabajo en materia de protección de datos relacionada con la tecnología RFID (WP 105), 2005, pp. 1-21. Disponible en idioma inglés en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf [fecha de visita 25 de Abril de 2012].

dadanos, debido a “la posibilidad de que las empresas y los gobiernos utilicen la tecnología RFID para hurgar en la esfera íntima de las personas”³⁰.

Se menciona el hecho de que:

“La capacidad de reunir subrepticamente toda una serie de datos relacionados con una misma persona, rastrear el comportamiento de la gente que circula por lugares públicos (aeropuertos, estaciones de tren, comercios), potenciar perfiles vigilando el comportamiento de los consumidores en los comercios, analizar detalles de indumentaria y accesorios y las medicinas que llevan los clientes son otros tantos ejemplos de utilización de tecnología RFID que suscitan inquietud para la protección de la intimidad”³¹.

Este Trabajo fue sometido al escrutinio de una consulta pública. Los resultados de dicha consulta fueron plasmados en otro expediente correspondiente a Septiembre de 2005³².

En este último se señalaba, haciendo alusión a este periodo de opinión, que “la mayoría de universidades, laboratorios de ideas, particulares y empresas que proporcionan soluciones de seguridad apuntaron la necesidad de algún tipo de orientación adicional del Grupo de Trabajo del artículo 29”³³; a su vez se propuso por parte de quienes participaron de esta ronda de asesoramiento “complementar la Directiva sobre protección de datos con normas específicas para RFID”³⁴.

Corresponde expresar que las empresas dedicadas a la elaboración y desarrollo de esta tecnología eran partidarias de un «enfoque de autorregulación».

3.1 APORTE DE LA DOCTRINA ESPAÑOLA EN ESTE PROCESO

Sentados ya en esta fase de opiniones al que fue sometido el Documento de Trabajo, parece adecuado detenerse en los comentarios que sostuvieron las partes interesadas, en España, respecto al desarrollo de esta innovación³⁵.

Se apunta a las reflexiones expresadas por la Comisión de Libertades e Informáticas (CLI)³⁶ y a las emitidas por un particular con especial interés en esta temática.

Respecto de la CLI, esta manifiesta su temor y resistencia a ciertos riesgos que trae aparejado la masificación de los RFID. En particular, vislumbra como más preocupantes los siguientes:

³⁰ *Ibid.*, p. 4.

La cita en idioma español, se consigna en el GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. “Dictamen 5/2010 relativo a la Propuesta de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia (RFID)”, adoptado el 13 de julio de 2010, p. 4. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_es.pdf [fecha de visita el 25 de Abril de 2012].

³¹ *Ibid.*

³² “Results of the Public Consultation on Article 29 Working Document 105 on Data Protection Issues Related to RFID Technology”, Adoptada el 28 de Septiembre de 2005. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp111_en.pdf [fecha de visita 25 de Abril de 2012]

³³ GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *op. cit.* (n. 30), p. 4.

³⁴ *Ibid.*

³⁵ Los textos con los diversos comentarios recibidos se encuentra disponible en: http://ec.europa.eu/justice/policies/privacy/workinggroup/consultations/rfid_en.htm [fecha de visita 25 de Abril de 2012]

³⁶ “La Comisión de Libertades e Informática (CLI) es una Asociación que trabaja activamente para la defensa del derecho fundamental a la Protección de Datos Personales con el firme objetivo de concienciar a ciudadanos, empresas y Administraciones de la importancia que tiene cumplir la normativa vigente en esta materia”. <http://www.asociacioncli.es/?q=node/2> [fecha de visita 25 de Abril de 2012]

- a) “La elaboración indiscriminada de perfiles”.
- b) “La utilización de los RFIDs con fines de identificación y los problemas que pueda suponer la interceptación fraudulenta de datos y su posterior uso con fines distintos”.
- c) “El desarrollo de técnicas de «rastreo» de los movimientos y/o actos realizados por la persona ("Tracking"). Esta tecnología permite localizar en cada momento los individuos que lo llevan en su ropa, su coche, etc., permitiendo una vigilancia constante. Esta nueva característica de los tratamientos masivos de datos, que, más allá de la elaboración de los perfiles de personalidad de los individuos, permite el seguimiento detallado de todos y cada uno de los pasos que da el individuo, supone un paso más en la vulneración de su vida privada, coaccionándole en el ejercicio de sus libertades más básica”³⁷.

Ya entrando en lo sustantivo del informe, la CLI, ponderó su razonamiento distinguiendo los usos que se daba a los RFID, mostrando sus resistencias a que por la utilización de este mecanismo se logrará un control total de la persona, y a los efectos que aquí interesan, del trabajador³⁸. Así expresó que:

“Frente al peligro de que el seguimiento de objetos se transforme en el seguimiento de las personas, la Comisión de Libertades e Informática se opone expresamente a que se puedan recabar datos de carácter personal (o realizar tratamientos de datos así recabados), sin el consentimiento y conocimiento efectivo (informado, consciente y previo) del portador de un elemento con tecnología RFID. En todos estos casos, también la aplicación del principio de calidad de los datos se hace particularmente aguda en el sentido de que únicamente los datos estrictamente necesarios a la finalidad legítima del tratamiento deben ser recabados y tratados con el fin de evitar abusos cuyas consecuencias serían devastadoras para los derechos y libertades de los interesados”³⁹.

³⁷ COMISIÓN DE LIBERTADES E INFORMÁTICA, *op. cit.* (n. 21), pp. 1-2.

³⁸ Como se ha tenido ocasión de expresar, no solo a propósito de este tipo de tecnología, sino que todos los avances que se han incorporado al contexto de la empresa, “ la incidencia de este tipo de métodos sobre el ámbito privado de los trabajadores resulta clara desde el momento en que la implementación de los sensores biométricos, GPS y RFID, generan un control sobre la localización y el comportamiento de las personas, eliminan la capacidad de estar solo, con lo que, como se ha dicho, los trabajadores se vuelven completamente transparentes, pudiendo conocer el empresario en todo momento, dónde se hallan, dónde han estado y por cuánto tiempo, así como el nivel de productividad en el puesto de trabajo que desempeñan”. DESDENTADO BONETE, A.; BELÉN MUÑOZ, A.B. *Control informático, video vigilancia y protección de datos del trabajador*. España, Valladolid: LexNova, 2012, pp. 73.

En el mismo sentido, y en una de las primeras Tesis de post grado en que se estudia con más profundidad esta tecnología, la autora ha expresado “Ciertamente, queda en absoluta evidencia el hecho de que la incorporación de las etiquetas RFID al mundo de la empresa amplia, de forma bastante considerable, el control ejercido por parte del empresario con métodos más intrusivos incluso de la propia video vigilancia, ya que a través de este mecanismo de actuación resulta extremadamente fácil conocer absolutamente todos y cada uno de los movimientos de los trabajadores, sin dejar ningún espacio fuera del conocimiento del empresario. Extremo este que suscita no pocas dudas en torno al hecho de cuál es la relación que puede darse entre el uso de las etiquetas RFID y los derechos fundamentales que asisten a todos los trabajadores, en la medida en que el tipo de control que ejercen las mencionadas etiquetas resulta, como ya se ha mencionado en las líneas precedentes, ciertamente invasivo y, por tanto, pueden verse vulnerados los derechos fundamentales”. LLAMAMOSAS TRAPAGA, A. *Las Nuevas Tecnologías de la Información y Comunicación y las Relaciones Laborales*. Tesis Doctoral. Bilbao, España: Universidad de Deusto, 2012.

³⁹ COMISIÓN DE LIBERTADES E INFORMÁTICA, *op. cit.* (n. 21), p 4.

Como se aprecia, lo que hace la CLI es extraer los principios que rigen en el ámbito de protección de datos y extender su virtuosismo protector a cualquier relación, incluida la laboral, rigiendo estos, no obstante, la especificidad que pueda caracterizar este tipo de relaciones normativas⁴⁰.

La CLI postula, en consecuencia, que los principios de protección de datos operan en cualquier tipo de negocio o relación en la que una de las partes pueda acceder a información de contenido personal o sensible, independiente de que aquel vínculo se encuentre regulado por una normativa que no consagre dichos principios.

Analizadas ya las reflexiones expresadas por la CLI, resta señalar la argumentación expresada por un profesional independiente que quiso hacerse parte en este proceso deliberativo, Jorge Miguel Criscio Navarro, quien también participó de esta ronda de consulta.

Este ratifica las apprehensiones de la CLI, al ver una amenaza en cuanto a que el sistema se convierta en un medio de seguimiento a personas. Al respecto, este técnico señaló que:

“Del análisis hecho en el documento WP105, surgen dos casos de uso notorios. Cuando la aplicación de la identificación se hace directamente sobre un usuario o persona, y cuando se hace directamente sobre un artículo, un objeto de consumo o producto.

El caso de la aplicación de la identificación por radiofrecuencia a una persona, adulto, anciano o joven, exige un análisis muy detenido. Especialmente, porque con toda seguridad, se trata de una aplicación que involucra en forma más notoria el uso de datos de índole personal. Aquí pueden estar muy implicados los aspectos de seguridad personal, discriminación y bioética. Ya se trate de sistemas de identificación portátiles o no removibles como los implantes⁴¹.

3.2 OPINIÓN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Resulta interesante recalcar como el mismo año (2005) en que el Grupo de Trabajo del Artículo 29 desarrolló su primer Documento relativo a este asunto, el Supervisor Europeo de Protección de Datos (SEPD)⁴² vislumbraba de qué manera se requiere un estudio más detallado para analizar la incidencia de los RFID en la vida de los ciudadanos.

⁴⁰ Pese a ello, y como lo ha expresado la doctrina, “la generalidad de los países europeos ha configurado una normativa general, pero, a su vez, ha generado normas de carácter específico, ya sea legales o reglamentarias, referidas concretamente al tratamiento de los datos personales en el contexto de una relación laboral, en el entendido de que las normas generales resultan insuficientes y demandan una adecuación cuando tal tratamiento tiene lugar en el marco de la relación entre empleador y trabajadores”. CERDA SILVA, A. “Intimidad de los trabajadores y tratamiento de datos personales por los empleadores”, en: *Revista Chilena de Derecho Informático*, n° 2, 2003, p. 12. Disponible en: <http://www.revistas.uchile.cl/index.php/RCHDI/article/viewArticle/10645/11373>[fecha de visita 02 de Julio de 2012].

⁴¹ CRISCIO NAVARRO, J. M. “Comentarios al documento de trabajo WP105 del grupo 29 en la consulta online sobre protección de datos relacionado con la tecnología RFID del 19 de enero de 2005”, marzo, 2005, p. 5. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/rfid/jmcriscio-spain_es.pdf[fecha de visita 25 de Abril de 2012].

⁴² Esta autoridad, se define a sí misma como la responsable de “garantizar que las instituciones y organismos de la UE respeten el derecho de las personas a la intimidad en el tratamiento de sus datos personales”. “Cuando las instituciones u organismos de la UE procesan datos personales sobre una persona que pueda ser identificada, deben respetar el derecho de esa persona a la intimidad. El SEPD se asegura de que así se haga y les aconseja sobre todos los aspectos del tratamiento de los datos personales.

El “tratamiento” cubre actividades tales como la recogida, el registro y el almacenamiento de la información, la recuperación para su consulta, el envío o la puesta a disposición de otras personas, así como el bloqueo, el borrado o la destrucción de datos.

Existen normas estrictas de protección de la intimidad que regulan estas actividades. Por ejemplo, no se permite que las instituciones y organismos de la UE procesen datos personales que revelen el origen racial o étnico, las tendencias políticas, las creencias religiosas

En efecto, en el Informe Anual de dicha autoridad correspondiente al ya mencionado año 2005, se expresa bajo el epígrafe “RFID: una tecnología prometedora y estimulante” que:

“En 2005, el SEPD contribuyó a las actividades del Grupo de Trabajo del Artículo 29 en el ámbito de la RFID y acogió con satisfacción las medidas exploratorias adoptadas por la Comisión. Sin embargo, la importancia fundamental de las etiquetas RFID para la protección de los datos personales exige un análisis más detallado. Estas tecnologías son fundamentales no solo porque facilitan una nueva manera de recopilar los datos personales, sino también porque las etiquetas RFID constituirán elementos clave del «entorno inteligente». Por este motivo, es importante que en las reuniones de consulta participen todos los interlocutores implicados”⁴³.

Esta serie de debates fueron el primer paso, en el núcleo de la Unión Europea, para comenzar a tratar el impacto y alcances de esta tecnología. Ello, ya que con posterioridad a 2005 se empiezan a discutir y dictar una serie de Dictámenes y Recomendaciones relativas a esta temática así como el denominado <internet de las cosas>.

Bajo este último concepto, se engloba la idea de que la tecnología lo que permitirá el día de mañana será el que interactúen las personas y los objetos, facilitando, en cierto modo, la vida cotidiana.

Así, este proceso ha sido caracterizado como:

“Una nueva aplicación de las tecnologías de internet, que se está desarrollando tan rápidamente como lo ha hecho la red en los últimos cuarenta años. Y se prevé que, en diez o quince años, nos lo encontremos en nuestra vida diaria. Utiliza un chip, capaz de contener amplísima información sobre el objeto o la persona donde se ha depositado, que luego transmite esos datos mediante la tecnología de identificación por radiofrecuencia (RFID)”⁴⁴.

Continúa la europarlamentaria exponiendo:

o filosóficas o la afiliación a algún sindicato. Tampoco pueden procesar datos sobre la salud o la vida sexual de las personas, a menos que estos datos sean necesarios a efectos del cuidado de la salud; incluso en tal caso los datos deberán ser procesados por un profesional de la salud u otra persona que esté obligada por el secreto profesional.

El SEPD trabaja con los responsables de la protección de datos de cada institución u organismo de la UE, para garantizar que se apliquen las normas de confidencialidad de dichos datos”.

(http://europa.eu/about-eu/institutions-bodies/edps/index_es.htm) [fecha de visita 25 de Abril de 2012].

Para mayor información consultar: <http://www.edps.europa.eu/EDPSWEB/edps/EDPS?lang=es>

⁴³ Informe Anual 2005 del Supervisor Europeo de Protección de Datos Comunidades Europeas. Luxemburgo, 2006, p. 41. Disponible en: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2005/AR_2005_ES.pdf [fecha de visita 25 de Abril de 2012].

El mismo informe, se refiere también a los datos biométricos, señalando al respecto que: “En 2005 se introdujo en numerosas propuestas de la Comisión Europea el uso de datos biométricos. Estas primeras iniciativas facilitarán la introducción de la biométrica en otros muchos aspectos de la vida diaria del ciudadano europeo. Por lo tanto, las instituciones de la UE tienen una gran responsabilidad en cuanto a la manera en que se apliquen estas tecnologías”. *Ibid.*

⁴⁴ Entrevista a europarlamentaria socialista española, MaríaBadia i Cutchet, 22 de marzo de 2010. Disponible en: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100312STO70527+0+DOC+XML+V0//ES> [fecha de visita 25 de Abril de 2012].

Véase también la Resolución del Parlamento Europeo, de 15 de Junio de 2010, sobre la Internet de los objetos (2009/2224 (INI)). Disponible en: <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2010-0207&language=ES> [fecha de visita 25 de Abril de 2012].

“Es decir, es una nueva tecnología que revolucionará las relaciones entre los objetos y las personas, o entre los objetos directamente. Y ahí reside la novedad, en la forma en que se comunican los objetos. Uno de los ejemplos que siempre se citan es el uso de la RFID en los frigoríficos para detectar alimentos en mal estado, o próximos a caducar”⁴⁵.

3.3 UN PRIMER INTENTO NORMATIVO DE REGULAR LOS RFID

El que podría considerarse como el primer hito regulatorio de los RFID, se suscita en el año 2007, momento en el cual se dicta una Comunicación de la Comisión de las Comunidades Europeas dirigida al Consejo, al Parlamento, al Comité Económico y Social Europeo, y al Comité de las Regiones que lleva por nombre “La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político”⁴⁶.

Este informe realiza la importancia que los RFID pueden tener en el impacto de la economía, ayudar en fomentar el empleo y convertirse en un <motor de crecimiento> de la región. Pero asimismo, y tomando en consideración los temores que se tienen, propone “una serie de pasos cuyo propósito es superar los obstáculos que impiden una implantación generalizada de la RFID en beneficio de la sociedad y de la economía, integrando al mismo tiempo las medidas adecuadas de protección de la privacidad, la salud y el medio ambiente”⁴⁷.

De esta comunicación resulta interesante resaltar cómo se va transparentando y visualizando la forma e impacto que la innovación puede acarrear en el campo laboral, en específico, cuando se utiliza como una medida de control del trabajador.

Al respecto, ya en ese año, se señala que “la tecnología RFID podría utilizarse para seguir o rastrear los movimientos de las personas o para trazar un perfil de su comportamiento (p. ej., en lugares públicos o en el lugar de trabajo)”⁴⁸. Agregándose, posteriormente, el hecho de que “las partes interesadas han manifestado su preocupación sobre posibles violaciones de los valores fundamentales y de la privacidad, así como por la posibilidad de que una mayor vigilancia, especialmente en el lugar de trabajo, derive en discriminación, exclusión, victimización y posible pérdida del empleo”⁴⁹.

Se plantea como una idea a tener en consideración al momento de poner en práctica los RFID el hecho de que:

“La privacidad y la seguridad deben constituir un elemento intrínseco, no añadido a posteriori, de los sistemas de información RFID antes de su implantación generalizada («seguridad y privacidad a través del diseño»). A la hora de diseñar estos sistemas es imprescindible tener en cuenta las necesidades tanto de las partes que participan activamente en el establecimiento del sistema de información RFID (por ejemplo, organizaciones empresariales, administraciones públicas u hospitales) como de los usuarios finales a los que se aplicará el sistema (ciudadanos, consumidores, pacientes o empleados). Dado que los usuarios finales

⁴⁵ Entrevista a europarlamentaria socialista española, MariaBadia i Cutchet, 22 de marzo de 2010.

⁴⁶ “Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político”. Bruselas, 15 de marzo de 2007. [COM (2007) 96 final]. Disponible en: [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:ES:PDF\[fecha de visita 25 de Abril de 2012\]](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:ES:PDF[fecha de visita 25 de Abril de 2012]).

⁴⁷ *Ibid.*

⁴⁸ *Ibid.*

⁴⁹ *Ibid.*

no suelen participar en la fase de diseño de las tecnologías, la Comisión respaldará la elaboración de un conjunto de directrices (código de conducta o buenas prácticas) específicas de las aplicaciones por un grupo de expertos representativo de todas las partes”⁵⁰.

A la luz de estos temores, cabe preguntarse cuál es el espacio que se crea para que los interesados y perjudicados (incluyendo en este concepto a los trabajadores) puedan confluír, y de esa forma exponer acerca de la manera en que posiblemente se podría limitar, restringir o permitir el uso de esta innovación.

La respuesta está en el hecho de que la Comisión propuso la creación de una instancia específica que se abocara a reflexionar respecto de este asunto. Esto se materializó con fecha 28 de Junio de 2007 cuando se crea un Grupo de Expertos en Identificación por Radiofrecuencia⁵¹ el cual tenía como propósito “contribuir al establecimiento de un diálogo entre las organizaciones de consumidores, los agentes económicos y las autoridades nacionales y europeas, incluidas las de protección de datos”⁵².

En lo que a los trabajadores interesa, estos estuvieron representados en esa instancia de diálogo por la Unión Network International (UNI)⁵³, en aquel cupo que estaba dirigido a los “miembros representantes de las comunidades de usuarios finales: ciudadanos, consumidores, pacientes y empleados”⁵⁴.

4. LA IRRUPCIÓN DE LOS RFID EN EL ÁMBITO EMPRESARIAL

4.1 CONSIDERACIONES PREVIAS

Conociendo ya las ventajas y desventajas que pueden acarrear los usos y funciones de los RFID en distintas esferas, se vuelve preciso abocarse a la incursión que esta tecnología ha hecho

⁵⁰ *Ibid.*

⁵¹ “Decisión de la Comisión Europea de 28 de Junio de 2007 por la que se establece el Grupo de Expertos en Identificación por Radiofrecuencia (RFID) (2007/467/CE)”. Publicado en el Diario Oficial de la Unión Europea con fecha 6 de Julio de 2007. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:176:0025:0030:ES:PDF>[fecha de visita 25 de Abril de 2012].

⁵² Se señala en aquella decisión, en específico en su artículo 4 titulado “Composición-Nombramiento” que “al nombrar a los miembros, se procurará que estén representadas de manera equilibrada las distintas partes interesadas y, concretamente, se incluirán representantes de los siguientes campos:

a) Sociedad civil: i) las comunidades de usuarios finales afectadas por los sistemas RFID (ciudadanos, consumidores, pacientes, empleados)”.

⁵³ “UNI Global Union es la voz de 20 millones de trabajadores del sector de servicios del mundo entero. A través de 900 sindicatos afiliados, UNI representa a los trabajadores y las trabajadoras en 150 países y en todas las regiones del mundo. UNI representa a los trabajadores de los sectores de Limpieza y Seguridad; Comercio; Finanzas; Juego; Gráficos y Embalaje; Peluqueros y Esteticistas; Medios de Comunicación, Espectáculo y Artes; Correos y Logística; Seguro Social; Deporte; Trabajadores Temporales y de Agencias y Turismo”.

Su misión es “desarrollar y reforzar a los sindicatos afiliados y a UNI Global Union con el fin de mejorar las condiciones de trabajo y de vida de los trabajadores en los sectores de servicios y afines.

UNI Global Union está trabajando con sus sindicatos miembros para cambiar las reglas del juego en el mercado laboral global. La estrategia “Rompiendo barreras” de UNI es nuestro plan para organizar al personal del sector de servicios a nivel global y garantizar el respeto y la dignidad en el entorno de trabajo global”. (<http://www.uniglobalunion.org/Apps/uni.nsf/pages/HOMEPAGEEs>) [fecha de visita 25 de Abril de 2012].

⁵⁴ La lista completa de los demás miembros puede consultarse en: http://ec.europa.eu/information_society/policy/rfid/documents/reg.pdf [fecha de visita 25 de Abril de 2012].

en el ámbito laboral y, más precisamente, a su incipiente destino como un mecanismo de control empresarial.

En este sentido, como ya se ha expresado, la irrupción de los RFID en la empresa “podría tener gran importancia en el mundo laboral, pues los lectores guardan registros que podrían consultarse y de servir de prueba a efectos legales. Se necesitarían leyes que específicas en quiénes pueden acceder a esos registros de datos y con qué finalidad”⁵⁵.

A ello se agrega el efecto que en materia de empleo puede acarrear una masificación de esta tecnología, reflexionándose qué deberá hacerse frente a:

“Que los sistemas de etiquetado por RFID pueden realizar tareas que ahora dependen del esfuerzo humano, por lo que la adopción de esta técnica va a implicar la pérdida de un número apreciable de puestos de trabajo. Habrá que contar, pues, con la oposición de los sindicatos. Ya fue un primer aviso la enconada huelga de los estibadores de la Coste Oeste de Estados Unidos en 2002, en parte debida a la amenaza de las nuevas técnicas sobre los empleos futuros”⁵⁶.

Estas reivindicaciones sindicales no solo se han producido a propósito de las consecuencias que lleva aparejada esta innovación en la mano de obra, sino que también en una eventual desprotección de los derechos de los trabajadores, en virtud como se ha reclamado, de una acentuación sin límites del poder de vigilancia del empresario.

En ese contexto se sitúa la alegación efectuada en el año 2005 por el sindicato británico GMB que “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”⁵⁷.

4.2 LOS RFID COMO UN NUEVO SISTEMA DE VIGILANCIA

En el ámbito empresarial, el uso de los RFID, aparte de las ventajas en la cadena de producción y distribución, puede destinarse a dos finalidades:

a) La primera, a mejorar los controles de acceso de los trabajadores, permitiendo con ello “nuevas posibilidades de control de las salidas que realiza un trabajador durante su jornada laboral (ya sea durante la conocida como «pausa para el bocadillo» como en las salidas destinadas a hacer gestiones vinculadas con la actividad laboral) o al final de la misma”⁵⁸.

b) La segunda, referida a un mecanismo de control de la actividad laboral de los trabajadores. En efecto, y como podremos apreciar más adelante, se han dado ya algunos ejemplos y casos en que esta innovación se ha empleado para vigilar el desempeño laboral de los dependientes.

⁵⁵ WANT, R., *op. cit.* (n. 14), p. 45.

⁵⁶ *Ibid.*

En sentido contrario se ha dicho que “en opinión de la Comisión Europea, la tecnología RFID puede convertirse en un nuevo motor del crecimiento y el empleo que efectúe una aportación considerable a la estrategia de Lisboa”. GALA DURÁN, C.; ROIG BATALLA, A., *op. cit.* (n. 9), p. 1.

⁵⁷ BIBBY, A., *op. cit.* (n. 8), p. 10.

⁵⁸ GALA DURÁN, C.; ROIG BATALLA, A., *op. cit.* (n. 9), p. 2.

En relación a este uso cabe consignar que “los dispositivos de identificación por radiofrecuencia ya empiezan a sustituir a las tarjetas de seguridad con banda magnética para la apertura de puertas y el acceso a zonas reservadas, sobre todo cuando hay requisitos de seguridad especiales, como las instalaciones militares”. WANT, R., *op. cit.* (n. 14), p. 42.

Sin embargo, esta afirmación de actividad o desempeño laboral al que se hacía mención precedentemente, debe ser matizada, en razón de que dado el carácter intenso y permanente que implica el uso de esta medida, se produce una especie de control total de los movimientos del trabajador, con los cuestionamientos y reservas que ello pudiese aparejar.

A este respecto, ya la doctrina ha manifestado su sospecha expresando que:

“resulta más preocupante el hecho de que las etiquetas RFID amplían enormemente las posibilidades de control empresarial de la actividad laboral de los trabajadores, por cuanto la tecnología incorporada en dichas etiquetas permitiría localizar en todo momento a un trabajador durante su jornada laboral (o incluso más allá de la misma...). Una manera de hacerlo consistiría, por ejemplo, en colocar una etiqueta RFID en el uniforme, o en una tarjeta o chapa identificativa”⁵⁹.

Añadiéndose a esta reflexión que:

“En definitiva, la radiofrecuencia técnicamente permitiría un control automático de los desplazamientos y de todas o algunas de las actividades (en función de los intereses empresariales y/o del coste económico que se quisiera asumir) que realizase un trabajador durante todo el tiempo que dura la jornada laboral. Y, además, aquél podría ser consciente o no del uso de este tipo de tecnología y de las consecuencias que la misma implica”⁶⁰.

Así expuestas las cosas, cabe preguntarse si estos temores y aprehensiones tienen algún sustento en la realidad u obedecen más bien, a la posible imaginación y extrapolación de las aplicaciones de los RFID, pero que no serían viables. Como un primer acercamiento y respuesta a esta inquietud, pudiese afirmarse que estas sospechas encuentran un correlato fáctico en el avance que presenta la ciencia al día de hoy y su concreción real en entornos empresariales. Ello, porque ya que es posible encontrar incipientes casos en que se ha echado mano de esta tecnología para erigirse como un nuevo mecanismo de control de que dispone el empresario. No obstante, por lo que conocemos hasta ahora, su uso para estos fines no se ha masificado. Sin embargo, no por ello debe dejar de prestarse atención a este hecho, e ir perfilando y resolviendo cómo la legislación debe hacer frente a esta nueva posibilidad.

En cuanto a casos concretos, eso sí, extra laborales, que se han ido suscitando en estos tiempos, puede rescatarse la invención, destinada a espiar a los individuos, correspondiente a una:

“Patente de IBM registrada en 2001 y concedida en 2006. En ella se exponen con todo detalle las instrucciones de uso de las tarjetas para el seguimiento y análisis de conductas, aun cuando el acceso a bases de datos oficiales no exista o esté rigurosamente limitado. Bajo el título «Identificación y seguimiento de personas que utilicen artículos provistos de etiquetas RFID en entornos de almacén», describe con frialdad la capacidad de la RFID para la vigilancia en un mundo con lectores de RFID («unidades de seguimiento personal»)

⁵⁹ GALA DURÁN, C.; ROIG BATALLA, A., *op. cit.* (n. 9), p. 2.

⁶⁰ *Ibid.*

conectada en red para observar de cerca los movimientos de las personas, en casi cualquier lugar donde se congreguen”⁶¹.

Extrapolando este análisis al contexto de una empresa, no sería ilusorio pensar y suponer esta realidad al interior de una fábrica, como ya se ha encargado de hacerlo la doctrina más conocedora de esta materia.

Como se ha afirmado, “lógicamente, ese uso también puede plantearse y darse en el marco de las empresas (especialmente grandes empresas, empresas dedicadas a la fabricación de productos sensibles o de elevado riesgo, que pertenezcan a sectores punteros...), especialmente cuando el uso de esas etiquetas sea cada vez más barato”⁶², agregándose que bastaría que los uniformes de trabajo u otros implementados estén dotados de esta técnica y situar “estratégicamente lectores de etiquetas RFID en todas las zonas de la empresa (incluidos lugares como las zonas de lavabos, vestuarios, máquinas de café o refrescos, salas de descanso o comida, acceso a los locales de los representantes de los trabajadores, aparcamiento)”⁶³ para de esa forma lograr el objetivo de control.

Entrando ya de plano al tema central de este epígrafe, uno de los principales riesgos que traía aparejado el uso de los RFID radicaría en que su propagación pudiese significar un peligro para:

“El goce y disfrute de las libertades humanas más elementales como la libertad de movimiento, de acción, la dignidad y el libre desarrollo de la personalidad⁶⁴”; produciéndose en consecuencia un mayor riesgo al que se encuentran sujeto los ciudadanos en la medida que “posibilita, entre otras cosas, «rastrear» (*tracking*) a los individuos y no ya solamente «realizar su perfil»”⁶⁵.

Tal es la razón por la que se ha afirmado que:

“La empresa que decidiera recurrir a las etiquetas RFID debería, previamente a su implantación, evaluar (a través de personal interno, profesionales externos...) los riesgos que las mismas podrían suponer para la protección de los datos personales y la intimidad de los trabajadores. Y una vez evaluados esos riesgos debería adoptar las medidas técnicas y organizativas neces-

⁶¹ ALBRECHT, K., *op. cit.* (n. 21), p. 51.

⁶² GALA DURÁN, C.; ROIG BATALLA, A., *op. cit.* (n. 9), p. 2.

⁶³ *Ibid.*, p. 3. La revolución científica ha llegado a extremos que por ejemplo “en el parque de atracciones inglés Alton Towers ofrece un ejemplo real de la capacidad de seguimiento de la identificación por radiofrecuencia. Cuando un visitante entra en el parque, se le ofrece una muñequera con RFID en la que va codificado un número de identificación exclusivo. Una red de lectores RFID ubicados en puntos estratégicos detecta cada muñequera que se pone a su alcance, activa las videocámaras cercanas. La grabación obtenida de cada visitante se almacena en un archivo etiquetado con su ID, que se le entrega en un DVD de recuerdo”. ALBRECHT, K., *op. cit.* (n. 21), p. 52.

Nada obsta, por tanto, en que el día de mañana pudiese encontrarse un sistema similar al interior de una empresa.

⁶⁴ FARRIOLS I SOLA, A., *op. cit.* (n. 25), p. 33.

⁶⁵ *Ibid.* “Respecto a los aprovechamientos, el primero que con facilidad viene a la cabeza es la posibilidad de localización dinámica de una persona u objeto que lleva esta identificación y, como consecuencia, la creación de una red de personas o de productos que estén dinámicamente interconexiónados y que ofrezcan informaciones que faciliten su utilización eficaz con unos fines determinados. Esto es, millones de personas y objetos podrán estar interconexiónados formando una red de información dinámica que localice su movimiento y su ubicación en todo instante creando una nueva Internet pero esta vez de cosas o de personas que aprovecharán la posibilidad de asociación de calidades, cualidades y, en definitiva, de informaciones que enriquecerán y alimentarán el beneficio del tratamiento, físico o lógico, al que se les someta”. DAVARA RODRÍGUEZ, M. A. “La identificación mediante radiofrecuencias (RFid)”, en: *El consultor de los Ayuntamientos y los Juzgados*, nº 6, marzo-abril 2009, p. 2.

rias para garantizar dicha protección, designando a una persona o grupo de personas para que se responsabilicen de la revisión periódica de las evaluaciones y medidas técnicas implantadas. Asimismo, la evaluación debería ponerse a disposición de la autoridad competente para la protección de datos con una antelación mínima de 6 semanas. Y en todo ese proceso y, sobre todo, en su aplicación debería garantizarse siempre la seguridad de la información⁶⁶.

Asimismo, se propicia una política de información y transparencia en cuanto a la utilización por parte del empresario de esta nueva tecnología. Sin embargo, y tal como se ha dado a conocer en otros ordenamientos, ello no siempre ocurre.

En este aspecto, hace un par de años atrás:

“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 ha 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»⁶⁷.

⁶⁶ GALA DURÁN, C.; ROIG BATALLA, A., *op. cit.* (n. 9), p. 6.

Quizás este profesional pudiese ser lo que se ha venido en denominar un *data protection officer*, en el sentido de que, “para determinadas entidades se establece la obligación de establecer un responsable de la protección de datos en la empresa. Este responsable debe supervisar la implantación de las medidas para la protección de datos en la empresa”. IGLESIAS REBOLLO, C.: “Cambios próximos en la regulación de la protección de datos de carácter personal europea”. Artículo de opinión. DiarioJuridico.com. Disponible en <http://www.diariojuridico.com/opinion/cambios-proximos-en-la-regulacion-de-la-proteccion-de-datos-de-caracter-personal-europea.html> [fecha de visita 04 de Julio de 2012].

Un artículo de interés en este sentido puede encontrarse en: http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142656222391&esArticulo=true&cidRevistaElegida=1142652066397&language=es&pagename=RevistaDatosPersonales%2FPage%2FHome_RDP&siteName=RevistaDatosPersonales&urlPage=RevistaDatosPersonales%2FPage%2FHome_RDP [fecha de visita 04 de Julio de 2012]

⁶⁷ BIBBY, A., *op. cit.* (n. 8), p. 9.

“Lo que inquietó especialmente a los investigadores de RAND fue la falta de transparencia respecto al modo en que se utilizan estos datos. El informe señala «que en general, no existen políticas escritas y explícitas relativas al modo en que se utilizan las tarjetas [tarjetas de acceso de personal], y a los empleados no se les comunica el tipo de políticas que se aplican». El informe continúa con una afirmación de mayor importancia: «La utilización de tales sistemas ha modificado el tradicional equilibrio entre comodidad personal, seguridad en el lugar de trabajo y derecho a la intimidad individual, dando lugar a la pérdida de ‘oscuridad práctica’. Estos sistemas plantean dificultades también en lo que respecta al significado y la ejecución de prácticas de información equitativas».

Los investigadores de RAND se vieron indudablemente sorprendidos por sus resultados. Su estudio sugiere que todo empleado con una tarjeta de acceso basada en la RFID debería sentirse «inquieto» al leer el informe”.

BIBBY, A. “RFID y vigilancia en el lugar de trabajo”, en: *Trabajo, la Revista de la OIT*. n^o 59, abril 2007, Ginebra, pp. 17-18. Disponible en: http://www.ilo.org/global/publications/magazines-and-journals/world-of-work-magazine/issues/WCMS_091707/lang-es/index.htm [fecha de visita 26 de Abril de 2012].

4.3 CASOS CONCRETOS DE LOS RFID COMO SISTEMA DE CONTROL EN LA EMPRESA

A continuación se esbozarán algunos casos que se han suscitado en el contexto laboral, en donde los RFID han sido utilizados como un mecanismo de vigilancia y control del empresario.

Se hacía alusión anteriormente, que esta tecnología ya se encuentra en condiciones de ser incorporada y adherida a uniformes de trabajo, los cuales no obstante sean lavados, el dispositivo sigue en funcionamiento⁶⁸.

Así las cosas, un caso en que el RFID ha sido incorporado en la indumentaria de trabajo, con posibles fines de control y verificación se suscita en Estados Unidos, y más precisamente en un Casino de Las Vegas.

En aquel recinto, el director de este:

“Al parecer, supervisaba las actividades de su personal mediante los chips RFID instalados en sus uniformes, y llegó a imponer medidas disciplinarias a un trabajador por perder el tiempo. Con todo, existen otros ejemplos del mismo sector en que la implantación de etiquetas en los uniformes se ha llevado a cabo satisfactoriamente. En el gran complejo de casinos de Star City en Sydney, inicialmente el personal recibió con inquietud la inserción de etiquetas RFID en sus uniformes, pero la preocupación se superó rápidamente. Su sindicato, el Liquor, Hospitality and Miscellaneous Union (LHMU), dice que puesto que los uniformes no se utilizan fuera de las instalaciones de la empresa, no se corre el riesgo de que el personal sea vigilado cuando se encuentra fuera de servicio. El LHMU añade que, en cualquier caso, el casino ya era un entorno intensamente vigilado, dada la utilización de varios cientos de cámaras en sus instalaciones”⁶⁹.

Otro ejemplo llamativo es la utilización de esta tecnología en un espacio en que la mayoría de la doctrina coincidiría que se trata de un lugar en donde el trabajador es absolutamente libre, y por ende, no debería tolerarse, en principio, ninguna especie de intromisión por parte de terceros. Se alude al baño que se encuentra al interior de las empresas.

⁶⁸ Fuentes empresariales señalan que una sola compañía ha vendido veinte millones de unidades de ese tipo de etiquetas, diseñadas para soportar planchados y lavados frecuentes a altas temperaturas sin que se dañe el microchip. Los proveedores creen que, con el tiempo, será posible utilizar hilos tejidos en la tela de las prendas que se utilizarán como antenas RFID”.

“En general, en los casos en que los empleadores optan por colocar etiquetas RFID en los uniformes, la razón tiene que ver habitualmente con la gestión de lavandería. Las prendas objeto de procesos de lavandería comercial se han marcado tradicionalmente con etiquetas alfanuméricas o de código de barras, y cada año se venden cientos de millones de etiquetas de identificación de este tipo. La RFID constituye, en cierto sentido, un mero desarrollo de esta modalidad de uso”. *Ibid.*

Se suma, tal como se ha consignado que “ya las compañías de uniformes tales como AmeridePride y Cintas están colocando etiquetas de rastreo por RFID en sus ropas capaces de soportar las temperaturas elevadas de las lavanderías comerciales”.

ALBRECHT, K. y MCINTYRE, L. *Chips espías. Cómo las grandes corporaciones y el gobierno planean monitorear cada uno de sus pasos con RFID*. Estados Unidos: Editorial 10 Puntos, 2006, p. 4. Texto traducido al español por Enrique Chi.

Agregándose, “Cintas (que viste a los empleados de Starbucks, Disney, Sears y Wal-Mart) y AmeridePride (con clientes como OutbackSteakhouse, 3M y Chevrolet) han empezado a colocar calladamente chips espías en los uniformes de sus empleados para rastrear el lavado y la logística de alquiler.

Las etiquetas están alojadas en discos plásticos sellados, capaces de soportar años de lavandería comercial y aun transmitir sus números de identificación cuando se encuentran dentro del alcance de un dispositivo lector. Las empresas de uniformes no tienen prisa por decirles a los empleados acerca de los chips espías en sus vestimentas rastreables, pero están ansiosos por decirles a los empleadores sobre los chips espías incrustados. La página web de Amerideride, por ejemplo, dice en voz alta «Tecnología Avanzada de Rastreo» junto a una etiqueta de lavandería con RFID animada que gira y que destaca el águila del logotipo de la empresa”. *Ibid.*, p. 180.

⁶⁹ BIBBY, A. “RFID y vigilancia... (n. 67), p. 17.

Para este caso, una empresa, apoyándose en la ciencia, ha ideado la forma de cómo poder ejercer un control en las actividades que realiza el trabajador en ese lugar. Se trata de lo realizado por la empresa Woodward Laboratories la cual:

“Ha encontrado la manera de colocar un lector de tarjetas en un producto al que llaman «iHygiene Perfect Pump». Es un surtidor de jabón líquido que también funciona como lector del carné del empleado y dispositivo de supervisión.

Para los empleados incautos, el dispositivo parece ser un surtidor de jabón perfectamente normal. Pero oculto dentro de su estilizado exterior plástico se encuentra un espía electrónico que capta el número de carné de identificación de la persona que está de pie frente al lavado, observa si el empleado se lava las manos. Un informe de las prácticas de higiene en el baño de cada empleado luego se «transmite fácilmente por medio de Internet» para permitir la «supervisión del cumplimiento con las normas de higiene de toda la empresa»⁷⁰.

Pareciera ser que la finalidad de la medida es controlar los hábitos de higiene de los trabajadores, cuando aquellos tienen una calidad especial por el tipo de servicios que se ejecuta

Pudiese comprenderse la intención buscada⁷¹, sin embargo, surgiría cuestionarse por un momento, si se cumple con el principio de proporcionalidad y con ello, si no existiera otra alternativa a una medida subrepticia, que esconde la posibilidad de saber cuántas veces concurre el trabajador a realizar un acto que compete a su esfera íntima, como lo es ir al baño⁷².

⁷⁰ *Ibid.*, p.17.

⁷¹ En este sentido, no deja de llamar la atención la reciente nota periodística que hace referencia a que un “brazalete inteligente medirá qué tan bien se lavan las manos los doctores”, agregando que “El producto es una pulsera que cuenta con tags RFID (identificación por radiofrecuencia) y un acelerómetro. El sistema requiere la instalación de lectores RFID en baños y estaciones de lavado. Así, cuando una persona empieza a lavarse las manos, el lector lo identifica y toma cuánto tiempo se demora. Además, el acelerómetro entrega una idea de los movimientos hechos.

El mismo brazalete indica al usuario si se lavó bien las manos o no, o si el lavado fue muy corto. Esto a través de vibraciones en la pulsera: una vibración es un lavado bien hecho, tres vibraciones indican que hay que hacerlo de nuevo.

IntelligentM ya aplicó el sistema en un hospital en Florida y según Technology Review, acaba de sumar dos nuevos clientes. Un atractivo interesante para los administradores de un hospital es que entrega los datos de los hábitos de higiene de sus empleados y además alerta a estos cuando hay un paciente que requiere de algún tipo de precaución especial para un tratamiento”. Disponible en: <http://www.emol.com/noticias/tecnologia/2013/03/28/590783/brazalete-inteligente-medira-que-tan-bien-se-lavan-las-manos-los-doctores.html> [fecha de visita 25 de Agosto de 2013].

⁷² Las controversias respecto a la posibilidad del empleador de poder controlar el tiempo que destina el trabajador para asistir al baño, lamentablemente no dejan de ser poco usuales.

En ese sentido, resulta interesante la lectura del artículo periodístico publicado por el diario El País, titulado “La Inspección de Trabajo investiga a dos empresas que obligaban a sus empleadas a colgarse un cartel para ir al baño. Disponible en: http://sociedad.elpais.com/sociedad/2011/10/04/actualidad/1317679210_850215.html [fecha de visita 26 de Abril de 2012].

En el caso chileno, la doctrina cita lo ocurrido también con una empresa que quería controlar estos tiempos. Así, se señala que un “Dictamen de la Dirección del Trabajo, N° 4.541/319, de 22.09.98, que se pronunció acerca de la licitud de controlar, a través de un registro material de asistencia, el tiempo de ida y de regreso a los servicios higiénicos. En esa ocasión, dicho organismo público sostuvo que «al dejar establecido el artículo 19 N° 4 de la Constitución Política de la República que asegura a todas las personas el respeto y protección de la vida privada y pública y a la honra de –la persona y de su familia, se fija un límite a las facultades de administración del empleador –las que desde luego no deben interferir o perturbar el ámbito personal y privado de sus dependientes– lo que a todas luces ocurre al pretender medir el tiempo de permanencia de los trabajadores en los servicios higiénicos»”. UGARTE CATALDO, J. L. “El derecho a la intimidad y la relación laboral”, en: *Boletín Oficial de la Dirección del Trabajo*, n°. 139, Santiago, Chile, agosto 2000, p. 19.

Un caso similar se puede encontrar en Gran Bretaña, en donde se menciona que “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

Otros casos que se han suscitado, y que asemejarían ser más benévolos, son aquellos en que los RFID se instalan en instrumentos de trabajo, pero en donde puede apreciarse, en principio, que por las características que envuelven el servicio prestado, la finalidad buscada es la protección del trabajador.

Se apunta, por ejemplo, al caso de los mineros. En estas hipótesis son indiscutibles los riesgos a los que estos se exponen en el cumplimiento de su labor. Por eso, ya se cuenta con experiencias en que se dota de RFID a ciertos aparatos de trabajo que utilizan estos con la finalidad de lograr una fácil y oportuna localización en caso de accidente u otros motivos de contingencias necesarias. Así sucede en una:

“Mina en Suecia (que) lleva utilizando la RFID desde 2003 con el fin de mejorar la seguridad de los mineros. En los puntos estratégicos de acceso de la mina se han instalado registros de lectura. Las etiquetas RFID que llevan los mineros se activan cuando se encuentran en la cobertura de un punto de acceso. Cuando se produce un accidente, el registro muestra el número y la última ubicación de los mineros, y emite alarmas para advertir a los situados en las proximidades del área del accidente. El sistema precisa la localización de los mineros atrapados y facilita las operaciones de rescate. En lugares de trabajo como las minas, la RFID puede salvar vidas”⁷³.

En idéntico sentido se ha expuesto lo ocurrido en minas de Sudáfrica y Chile, en donde los mineros se verían protegidos por los RFID en la medida que estos se encuentran incorporados en los respiradores con que cuentan para desarrollar su trabajo, cumpliéndose el mismo objetivo que la situación anterior, lograr su localización en caso de emergencias⁷⁴.

Se presenta estos últimos casos como aquel tipo de situaciones en que no se pondría en juego, al menos de forma abstracta, la intimidad de los trabajadores. Costaría apreciar qué espacios o lugares pueden ser visitados por el minero al interior de un yacimiento, que quiera mantener en reserva del empleador.

No obstante este supuesto, uno de los riesgos ciertos que esta tecnología puede implicar es que a través de ella se corrobore la productividad del trabajador, en el sentido de saber si realiza muchas pausas o no dentro de su jornada. Es el caso, por ejemplo, de lo que ocurre en un país asiático en donde la innovación ha servido para determinar la productividad de los trabajadores.

Así, se ha relatado que:

“La tecnología ha sido utilizada por algunas empresas japonesas con el fin de supervisar la eficacia de sus empleados. Los trabajadores portan etiquetas RFID obligatorias, cuyos datos se analizan para determinar en qué medida contribuye cada trabajador a la producción. El sistema ha generado inquietud en lo que respecta a la confianza entre empleador y traba-

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”.

BIBBY, A. *Te están siguiendo...* (n. 8), p. 12.

⁷³ BIBBY, A. “RFID y vigilancia...” (n. 67), p. 18.

⁷⁴ TYRRELL, P. “Tuned in to the right frequency”, en: *Financial Times*, 14 de diciembre de 2004. Disponible en: <http://www.ft.com/intl/cms/s/1/57abe7ce-4dff-11d9-9351-00000e2511c8.html#axzz1yrvvjGXV> [fecha de visita 26 de Abril de 2012].

adores; en cualquier caso, la cuestión sobre la protección de datos es si los empleadores pueden aducir o no razones legítimas para tal seguimiento, y si este uso de datos personales es proporcional o no a los intereses a los que sirve”⁷⁵.

4.3.1 Un caso paradójico: RFID cutáneos en contextos laborales

En esta parte no debe perderse la oportunidad de comentar un caso que parece sumamente extraño. Se refiere a los implantes de RFID en el cuerpo humano en contextos laborales.

Aunque en un inicio pudiese parecer llamativo, efectivamente pueden encontrarse experiencias en ese sentido, las cuales han sido rechazadas con énfasis por la doctrina. Así, la Comisión de Libertades e Informática, ya expresó su preocupación con este hecho al declarar que “la CLI ve confirmados sus temores por el uso incontrolado de los identificadores por radiofrecuencia (RFID) ante la información de que una empresa en EEUU implanta chips en sus empleados”⁷⁶.

“Fabricado por una empresa de Florida llamada Applied Digital Solutions, la «VeriChip» es una etiqueta de RFID encapsulada en vidrio que se inyecta en la carne, típicamente en la zona del tríceps, en un punto medio entre el codo y el hombro. El dispositivo ya se ha implementado en millones de perros y gatos en todo el mundo y ahora sus inventores desean ponerlo en personas”⁷⁷.

En el seno laboral, los casos de los que se ha tenido noticia son dos. El primero ocurrió en América del Norte, en donde:

“Dieciocho trabajadores gubernamentales en México experimentaron esto de primera mano en Junio de 2004, cuando el ex procurador general Rafael Macedo de la Concha pidió colocarse un spychip a sí mismo y colocárselo a muchos de los empleados como medio para lograr acceso seguro a una oficina de archivos con información confidencial. En lugar de usar una llave o una tarjeta para entrar, el empleado con spychip pasa por un portal con lector RFID que escanea su Verichip implantado. Si el chip del empleado devuelve un número autorizado, se le permite pasar por la puerta”⁷⁸.

⁷⁵ BIBBY, A. “RFID y vigilancia... (n. 67), p. 18.

⁷⁶ FARRIOLS I SOLA, A., *op. cit.* (n. 25), p. 33.

Para esa organización este hecho “tiene una implicaciones éticas importantes...La Comisión de Libertades e Informática se felicita de que organismos como el European Groupon Ethic hayan empezado un debate sobre el tema, a raíz del dictamen presentado el día 18 de marzo de 2005”, en: COMISIÓN DE LIBERTADES E INFORMÁTICA, *op. cit.* (n. 21), p 2..

Con rotundidad también lo rechaza el Código de Buenas Prácticas de UNI, al expresar que “Implantation of RFID chips (for example, under the skin) is not permitted in any circumstance.” no sé si hay que traducirlo, entiendo que depende del criterio de la editorial de la revista donde se publica?

UNI: “RFID in the workplace: UNI Code of Good Practice”, Version 1.0 (Draft), 27 abril de 2007, p. 4.

⁷⁷ ALBRECHT, K. y MCINTYRE, L., *op. cit.* (n. 68), p. 181.

Otro ejemplo del uso extraño que se le dio a esta innovación se suscitó en Barcelona, España. Se trata del Club Baja Beach Club que en marzo de 2004 organizó una fiesta en la que se inyectaba un RFID a los participantes.

“La carnada: la capacidad de pasar rápido por la entrada, acceso a zonas exclusivas del club y pagar por las bebidas sin tener que dar dinero en efectivo ni tarjetas de crédito. Cuando un escáner pasaba a unos centímetros de la piel con chips espías del cliente, el dispositivo de RFID implantado transmitía un número de identificación exclusivo que podía vincularse con cuentas financieras e información de membresía en el club.” ALBRECHT, K. y MCINTYRE, L., *op. cit.* (n. 68), p. 184.

⁷⁸ *Ibid.*, p. 181.

El segundo caso que ha sido dado a conocer por la prensa se suscita en Estados Unidos, más precisamente en la ciudad de Cincinnati, lugar donde una empresa de seguridad, llamada Citywatcher, dispuso la posibilidad de que sus empleados se insertaran un dispositivo de RFID para controlar y facilitar el acceso de estos a lugares restringidos dada la información sensible que se acumulaba en ellos⁷⁹.

El tema que pareciera extravagante ha sido condenado por la doctrina, no resultando de relevancia la dictación de una normativa especial para rechazar esta posibilidad, en atención a que este tipo de situaciones pone en jaque los derechos fundamentales de los trabajadores, careciendo de importancia dictar una normativa que se refiere a este supuesto de hecho.

Sin embargo esta idea puede ser que no sea del todo tan clara en Los Ángeles, Estados Unidos, ya que como se ha dado a conocer, se discutió por los legisladores de ese Estado si debía o no regularse el uso de los RFID cutáneos por parte de los trabajadores.

Este escenario permitió visualizar cómo los congresistas del Estado de California se referían a esta situación y los argumentos que se esgrimían para sustentar sus posiciones. Finalmente la normativa señala que es necesario prohibir este tipo de supuestos⁸⁰.

4.4 CONSECUENCIAS PRELIMINARES Y PROSPECTIVA DE LOS RFID COMO MECANISMO DE CONTROL

Cuando se ha podido apreciar, un uso no regulado, desinformado e ilimitado de los RFID como mecanismo de vigilancia con que cuenta el empresario, ya sea para tutelar la actividad laboral como para medir niveles de productividad de los trabajadores, produce la consolidación de lo que pudiese venir en denominarse como el control total de la persona del trabajador.

A este respecto, surge la interrogante de cuál es el espacio de privacidad e intimidad que le queda a aquel trabajador cuyos movimientos son monitoreados. La respuesta pareciera ser que no mucha. Se afectaría aquello que la doctrina ha venido en llamar como la privacidad locacional⁸¹, o sea, el mantener reserva de los lugares o espacios que el trabajador visita al interior de una empresa o, por otra parte, no divulgar con quienes este interactúa dentro de aquella, por ser estos asuntos correspondientes a la esfera personal del trabajador:

Como con acierto reflexiona la autora, “al momento de redactar estas líneas nos enteramos que el procurador general mexicano Macedo de la Concha había renunciado a su puesto, lo que nos llevó a hacer una pregunta interesante. ¿Qué sucede cuando uno ya no necesita o no quiere el chip de RFID?”, *Ibid.*

⁷⁹ La nota periodista fue realizada por la cadena televisiva norteamericana CNN, y puede ser vista en el siguiente enlace: http://www.youtube.com/watch?v=gMd6rde4MX8&feature=player_embedded [fecha de visita el 25 de Abril de 2012].

⁸⁰ La nota de prensa fue reportada por Los Ángeles Times bajo el título “Senate blocks mandatory ID implants”. El artículo está disponible en: <http://articles.latimes.com/2007/aug/31/local/me-scan31> [fecha de visita el 25 de Abril de 2012].

La normativa puede ser consultada en el siguiente enlace: http://info.sen.ca.gov/pub/07-08/bill/sen/sb_0351-0400/sb_362_bill_20071012_chaptered.html [fecha de visita el 25 de Abril de 2012].

⁸¹ Este concepto fue acuñado por la US National Work rights Institute (<http://workrights.us/>) organismo que habría manifestado su preocupación por “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”. BIVBY, A. “RFID y vigilancia... (n. 67), p. 18.

“En este caso, recurrir a una tarjeta RFID supondría tener conocimiento de todos los desplazamientos realizados por los trabajadores dentro de la empresa así como del tiempo que han invertido en ellos y cuánto tiempo han estado en una determinada zona de la misma (por ejemplo, en los lavabos, máquinas de café, en los locales de sus representantes...). Puede concluirse que con ello la empresa podría elaborar —sumando, en su caso, el perfil de productividad antes visto— un perfil de cada trabajador de forma mucho más fácil y completa que con los medios técnicos actuales y que los trabajadores de esa empresa se volverían completamente «transparentes» por cuanto en todo momento se podría tener constancia de dónde se hallan, de dónde han estado y por cuánto tiempo e, incluso, de su nivel de productividad en el puesto de trabajo que están desempeñando”⁸².

Así también se ha agregado por los más críticos, pero a la vez mas estudiosos en este ámbito, que una masificación desregulada y desinformada de los RFID, por ejemplo insertos en los uniformes de trabajo permitirían:

“Usarse para medir el tiempo usado en visitas al baño, supervisar las visitas a una fuente de agua, o medir el tiempo pasado en un escritorio. Hasta podrían usarse para registrar quién pasa tiempo con quién, no sólo impidiendo los romances de oficina, sino potencialmente también silenciando a los que pudieran denunciar alguna mala acción”⁸³.

En cuanto a la intromisión que esta situación pudiese comprometer al derecho laboral colectivo, la doctrina ha expresado sus reparos y miedos a que por medio de este dispositivo se afecte el derecho de asociación o de libertad sindical.

Al respecto, se han formulado interrogantes en el sentido de que:

“¿No se vería coartada la actividad de representación de los trabajadores si el representante sabe que porta una etiqueta que sitúa todos sus movimientos en la empresa?, ¿se implicarían los trabajadores en actividades vinculadas con la actividad sindical —por ejemplo, una asamblea— si saben que su etiqueta RFID sirve para identificarlos como partícipes de la misma?

A este respecto, es evidente que si, como hemos visto, es necesario establecer medidas técnicas y organizativas para evitar que las etiquetas RFID sirvan para vulnerar los derechos fundamentales a la intimidad y a la protección de datos; esas medidas también tienen que tener presente —y respetar— el derecho a la libertad sindical, especialmente en su vertiente de derecho a la actividad sindical⁸⁴”.

⁸² *Ibid.*, p. 3. El autor continúa razonando “las etiquetas RFID incorporadas, por ejemplo, al uniforme de trabajo o a una tarjeta podrían permitir también ubicar al trabajador fuera de la jornada de trabajo y conocer sus hábitos y actividades extralaborales por cuanto sería posible que esa etiqueta fuera leída por lectores externos a la empresa (por ejemplo, en centros comerciales cercanos a la empresa, farmacias, locales de ocio) y que los datos obtenidos por los distintos lectores se tratasen y explotasen conjuntamente, pudiéndose ampliar con ello el perfil del trabajador”.

⁸³ ALBRECHT, K. y MCINTYRE, L., *op. cit.* (n. 68), p. 180.

⁸⁴ GALA DURÁN, C.; ROIG BATALLA, A., *op. cit.* (n. 9), p. 10.

4.5 UNA POSIBLE SOLUCIÓN: LA NECESARIA REGLAMENTACIÓN Y ACUERDO ENTRE LOS ACTORES SOCIALES (ORGANIZACIONES SINDICALES Y EMPRESARIOS)

Por todo lo expuesto, ya se han levantado voces en el sentido de conversar, negociar y regular el ámbito de acción que tendrán los RFID cuando se utilicen al interior de una organización productiva, principalmente con fines de control.

Emblemático en este sentido, lo ha constituido la iniciativa impulsada por UNI que elaboró el año 2006 una Guía conocida como:

“RFID in the work place: UNI Code of Good Practice (RFID en el lugar de trabajo: Código de Buenas Prácticas de UNI) Su objetivo es «garantizar que la tecnología RFID se adopte en el lugar de trabajo de conformidad con las normas fundamentales del trabajo de la OIT, con los principios relativos a la protección de datos, y con el derecho humano fundamental a la intimidad de la persona.

Se trata de procurar que la RFID se utilice en los lugares de trabajo en beneficio tanto de las empresas, como de sus empleados, mediante la mejora del entorno de trabajo»⁸⁵.

En este documento se postula la aplicación de una serie de medidas tendientes a regular la forma en que los RFID se utilicen en los centros de trabajo, exigiéndose siempre que esta situación sea conversada previamente con las organizaciones representativas de los trabajadores.

La Guía señala enfáticamente que:

“Any proposals to introduce RFID technologies in the work place shall be discussed and negotiated by companies through a process of social dialogue with trade unions/works councils.

As part of this period of discussion and negotiation, companies and trade unions/works councils shall assess whether the use of RFID is likely to affect working conditions and the working environment, and in particular lead to deskilling of workers.

Appropriate measures, including where relevant additional training, shall be taken to ameliorate identified negative aspects of the introduction of RFID.

Any introduction of RFID in the workplace shall be linked to an explicit commitment to the maintenance of individual workers’ privacy and dignity”⁸⁶.

En el mismo sentido, se establece una serie de restricciones para que esta innovación tecnológica no se transforme en un medio de seguimiento (*tracking*) de los trabajadores, rebasando el ámbito de vigilancia y entrometiéndose en la vida privada de estos, afectando en consecuencia el derecho a la intimidad del que son titulares⁸⁷.

⁸⁵ BIBBY, A. “RFID y vigilancia... (n. 67), p. 19.

⁸⁶ UNI: “RFID in the workplace: UNI, 2010, p. 2..

⁸⁷ Bajo el título “Restrictions on RFID tracking” la Guía expresa que “RFID-enabled staff passes or name tags shall normally be used only for purposes of access control to premises. Where employers wish to use RFID-generated data for other purposes (for

A su turno vela también por el derecho a la protección de datos que garantiza a los trabajadores, no obstante el vínculo de subordinación y dependencia que caracteriza a la relación laboral, situación jurídica que no es impedimento para que este derecho ejerza su eficacia reguladora en este ámbito. Teniendo ello en cuenta, expresa una declaración de principios al señalar que este mecanismo no puede constituirse en la vía impuesta para aplicar sanciones disciplinarias a los trabajadores, limitando esta posibilidad para casos excepcionales. En este sentido, el document señala:

“Data collected from RFID-enabled monitoring of employees are not to be used for disciplinary purposes, except in exceptional circumstances where there are strong grounds to believe that an employee has committed a criminal offence or a serious disciplinary offence. In these situations, access to RFID-generated data will only take place in the presence of a trade union representative or employee selected representative”⁸⁸.

5. CONSIDERACIONES FINALES: RFID EN EL CONTEXTO CHILENO

Resulta de interés, como corolario final al estudio realizado, plantear algunas consideraciones en torno a la eventual utilización de RFID como modo de control de trabajadores en el contexto de la legislación chilena.

Al respecto, cabe considerar que nuestro Código del Trabajo otorga al empleador facultades de control sobre los trabajadores, estableciendo a su vez los límites dentro de los cuales las mismas pueden ejercerse.

En primer lugar, el artículo 5° del referido Código establece que el ejercicio de las facultades del empleador debe sujetarse al respeto de las garantías constitucionales de los trabajadores. En particular, reconoce el derecho a la intimidad, vida privada y honra de los trabajadores.

A su vez, luego de la implementación de la reforma laboral en nuestro país, el resguardo de los derechos fundamentales de los trabajadores se vio reforzado, mediante la implementación del procedimiento de tutela de derechos fundamentales. En éste, se agrega como criterio de resguardo de los derechos del trabajador, la necesidad de que cualquier medida que afecte un derecho fundamental de un trabajador sea justificada, fundamentada y proporcionada, y no afecte el contenido esencial de dicho derecho.

example, time-keeping), this usage shall be subject to prior negotiation with the trade unions/works council.

There shall be no automatic linkage of RFID-generated data to other company data (for example, employees' personnel or medical records). Any such links, if agreed by prior negotiation with trade unions/works councils, shall be limited to purposes directly relevant and necessary to the employment of the worker.

Continuous monitoring of employees at work via RFID tracking devices is not compatible with workers' right to human dignity in the workplace. Routine monitoring of workers' geographical location at any one time is normally not permitted.

Where this is proposed to be undertaken, this usage shall be subject to prior negotiation with the trade unions/works councils and shall be solely for the purpose of work-flow management and not for employee performance assessment or disciplinary purposes.

Where monitoring of workers' geographical location is undertaken, measures shall be implemented so that RFID monitoring does not continue during comfort breaks and lunch breaks.

Workers shall have the right to switch off RFID tags or to remove them, for example when taking breaks, without penalty.

Monitoring of employees' geographical location is not permitted after working hours or during holidays. There shall be clear procedures to ensure that RFID-enabled passes and name tags are non-operational during these periods”. UNI: “RFID in the workplace: UNI Code of Good Practice”, 2010, p. 3..

⁸⁸ *Ibid.*, p. 3.

Complementando dichas garantías, el artículo 154 del Código del ramo ha establecido parámetros mínimos que deben respetarse al implementar cualquier medida de control de los trabajadores. Esta norma exige toda medida de control cumpla con los siguientes requisitos:

- a) Se encuentre establecida en el Reglamento Interno de Orden, Higiene y Seguridad de la empresa.
- b) Se efectúe por medios idóneos y concordantes con la naturaleza de la relación laboral.
- c) Su aplicación sea general e impersonal.
- d) Se respete la dignidad del trabajador.

Por último, el artículo 154 Bis del Código del Trabajo ha establecido la obligación del empleador de “mantener reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral”.

La Dirección del Trabajo ha emitido diversos pronunciamientos referidos a las medidas de control del empleador, otorgando mayores luces sobre la aplicación práctica de éstas normas. Resulta de interés –por la aplicación analógica que puede darse al caso del uso de RFID como medio de control en la empresa– los requisitos que dicho Servicio ha establecido, para autorizar el uso de cámaras de vigilancia y medidas de control audiovisual.

En dictamen N° 2328/130 de 19 de julio de 2002⁸⁹, señaló que no resulta lícito utilizar dichas medidas con el único fin de vigilar y fiscalizar la actividad del trabajador. Ello en particular considerando que la grabación audiovisual supone una forma de control permanente y continuado sobre el trabajador, que vulnera el derecho a intimidad y la dignidad del mismo. Así las cosas, su uso solo sería admitido cuando ello fuera “objetivamente necesario por requerimientos o exigencias técnicas de los procesos productivos (materiales tóxicos o peligros, alto costo de las maquinarias o de las materias primas, etc.) o por razones de seguridad”.

En cuanto a las limitaciones de uso de este sistema de control, el mismo dictamen exige que las cámaras no se dirijan directamente al trabajador, sino que capten planos panorámicos. Asimismo, su existencia debe ser conocida por los trabajadores, encontrándose prohibido el uso de cámaras ocultas. Finalmente, las mismas no pueden ubicarse dentro de aquellas dependencias de la empresa destinadas al esparcimiento de los trabajadores, o aquellas en que no se realiza actividad laborativa alguna.

La aplicación de estos criterios puede extenderse, por analogía, al uso de RFID en la empresa, lo que llevaría a concluir al menos que:

- a) El uso de esta medida deberá encontrarse justificada ya sea por una exigencia técnica del proceso productivo o por motivos de seguridad. En consecuencia, no sería admisible su uso para controlar la eficiencia en la producción, ni otros fines que no fueren el resguardo de la seguridad del trabajador y de la empresa.
- b) Su aplicación debe encontrarse regulada en el Reglamento Interno de la empresa, y los trabajadores deben encontrarse en conocimiento de la aplicación de dicho procedimiento.

⁸⁹ Criterio reiterado en Dictamen N° 2852/158 de 30 de agosto de 2002, y N° 3276/173 de 16 de octubre de 2002.

Ello implicaría no solo saber –por ejemplo– que la credencial posee tecnología RFID, sino también saber dónde se encuentran ubicados los pórticos de control o lectores de ésta.

- c) Por último, las zonas dentro de la empresa donde dicho control sería admisible se encuentran restringidas, prohibiendo su uso en zonas no destinadas a la actividad laboral propiamente tal. En este contexto, el uso –como se ha realizado en empresas de EE.UU.– en el baño de la empresa, u otros ámbitos similares, constituiría una práctica que excede los límites establecidos por la ley chilena⁹⁰.

El mismo dictamen antes citado, ha establecido el estándar sobre el uso de los datos obtenidos con la medida de control. La Dirección del Trabajo exige al empleador garantizar la custodia y almacenamiento de las grabaciones; la posibilidad de acceso de los trabajadores –y eventualmente de dirigentes sindicales– a las grabaciones; la reserva de toda información y datos privados del trabajador obtenidos a través del mecanismo de control; la obligación de eliminar, dentro de un plazo razonable, cualquier grabación que contenga datos que no se relacionen con la finalidad de dicha grabación. Por último, no puede alterarse el contenido de la información descontextualizando las imágenes obtenidas.

Estos criterios resultan aplicables al uso de RFID, y nos llevan a concluir que para el legislador chileno, la información obtenida a través de este medio debe ser resguardada por el empleador, quien tiene la obligación de garantizar que no se utilice para otra finalidad que aquella para la cual fue obtenida. Por último, resulta de interés destacar que la Dirección del Trabajo ha considerado, en este mismo dictamen, que resulta improcedente utilizar la información obtenida a través de aquellas medidas utilizadas con una finalidad técnico productivo o de seguridad –como es el caso de una grabación audiovisual, y lo sería el uso de RFID– para aplicar sanciones al trabajador. Ello, pues supondría utilizar dicha medida para una finalidad distinta de aquella para la cual ha sido concebida y admitida, afectando la intimidad y privacidad de la persona del trabajador.

En definitiva, aun cuando no existe en Chile legislación específica referida al uso de RFID, creemos que las normas vigentes, que limitan las facultades de control del empleador, estableciendo como barrera infranqueable el respeto de los derechos fundamentales del trabajador, y establecen ciertos parámetros de uso de dichas medidas, son suficientes para regular el uso de esta tecnología en el ámbito empresarial, con el debido resguardo de la intimidad, vida privada y dignidad del trabajador.

BIBLIOGRAFÍA

ALBRECHT, K.; MCINTYRE, L. *Chips espías. Cómo las grandes corporaciones y el gobierno planean monitorear cada uno de sus pasos con RFID*. Estados Unidos: Editorial 10 Puntos, 2006, 273p. Texto traducido al español por Enrique Chi.

ALBRECHT, K. “Etiquetas personales RFID”, en: *Investigación y Ciencia*, n° 386, noviembre 2008, pp.48-51.

BIBBY, A. *Te están siguiendo: Control y vigilancia electrónicos en el lugar de trabajo*. Documento de trabajado elaborado para UNI Sindicato Global (UNI/GS/06-2006/0035/ES), 2006, 44p. Disponible en: <http://www.andrewbibby.com/pdf/Surveillance-es.pdf>

⁹⁰ Ello se complementa con el criterio establecido en el Dictamen N° 4541/319 de 22 de septiembre de 1998 de la Dirección del Trabajo, que señaló que resultaba contrario a derecho controlar el tiempo que los trabajadores destinan al uso de los servicios higiénicos, por vulnerar el derecho a la intimidad y vida privada del trabajador.

- BIBBY, A. “RFID y vigilancia en el lugar de trabajo”, en: *Trabajo, La Revista de la OIT* nº 59, abril, Ginebra, 2007, pp. 16-19. Disponible en: http://www.ilo.org/global/publications/magazines-and-journals/world-of-work-magazine/issues/WCMS_091707/lang-es/index.htm
- CERDA SILVA, A. “Intimidación de los trabajadores y tratamiento de datos personales por los empleadores”, *Revista Chilena de Derecho Informático*, núm. 2, 2003, Santiago, Chile. Disponible en: <http://www.revistas.uchile.cl/index.php/RCHDI/article/viewArticle/10645/11373>
- COMISIÓN DE LIBERTADES E INFORMÁTICA. *Comentarios al Documento de Trabajo sobre protección de datos de carácter personal en relación con la tecnología RFID de 19 de Enero de 2005 (WP 105)*, 2005, 9p. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/rfid/cflcs_es.pdf
- Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político*. Bruselas, 15 de marzo de 2007. [COM (2007) 96 final]. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:ES:PDF>
- COSMEN-SCHORTMANN, J.; MARTÍNEZ-OLAGUE, M. A. “Galileo, el sistema europeo de navegación por satélite”, en: *Revista técnica de la Asociación Española de la Carretera*, nº. 140, 2005, España, pp. 114-121.
- CRISCIO NAVARRO, J. M. *Comentarios al documento de trabajo WP105 del grupo 29 en la consulta online sobre protección de datos relacionado con la tecnología RFID del 19 de enero de 2005*. Marzo, 2005, 10p. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/rfid/jmcriscio-spain_es.pdf
- “Decisión de la Comisión Europea de 28 de Junio de 2007 por la que se establece el Grupo de Expertos en Identificación por Radiofrecuencia (RFID) (2007/467/CE)”, en: *Diario Oficial de la Unión Europea*, 6 de Julio de 2007. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:176:0025:0030:ES:PDF>
- DAVARA RODRÍGUEZ, M. A. “La identificación mediante radiofrecuencias (RFid)”, en: *El consultor de los Ayuntamientos y los Juzgados*, nº 6, marzo-abril 2009, pp.1-4.
- DESDENTADO BONETE, A.; BELÉN MUÑOZ, A.B. “Control informático, video vigilancia y protección de datos del trabajador”. Valladolid, España: LexNova, 2012, 73p.
- FARRIOLS I SOLA, A. “Introducción”, en: Farrriols i Sola, A. (Dir. y Coord.). *La protección de datos de carácter personal en los centros de trabajo*. Madrid, España: Cinca, 2006, pp. 15-35.
- FERNÁNDEZ ALLE, C. “La tecnología RFID y sus implicaciones jurídicas”, en: *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, nº 38, Madrid, España, 2009, pp.1-8 (versión on line). Disponible en: http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142540502890&esArticulo=true&cidRevistaElegida=1142527411030&language=es&pag=2&pagename=RevistaDatosPersonales%2FPage%2Fhome_RD_P&siteName=RevistaDatosPersonales
- GALA DURÁN, C.; ROIG BATALLA, A. “El uso de etiquetas de identificación por radiofrecuencia en las empresas: ¿un nuevo riesgo para los derechos de los trabajadores?”, en: *Actualidad Laboral*, nº 8, abril 2010, pp. 1-14.
- GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 “Documento de trabajo en materia de protección de datos relacionada con la tecnología RFID (WP 105)”, 2005, pp. 1-21. Disponible en idioma inglés en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp105_en.pdf
- GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29 “Dictamen 5/2010 relativo a la Propuesta de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia (RFID)”, adoptado el 13 de julio de 2010. pp. 1-12. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_es.pdf
- IGLESIAS REBOLLO, C. “Cambios próximos en la regulación de la protección de datos de carácter personal europea”. Artículo de opinión. *DiarioJuridico.com*. Disponible en <http://www.diariojuridico.com/opinion/cambios-proximos-en-la-regulacion-de-la-proteccion-de-datos-de-caracter-personal-europea.html>
- Informe Anual 2005 del Supervisor Europeo de Protección de Datos Comunidades Europeas*, Luxemburgo, 2006, pp.1-76.
- INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN Y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. “Guía sobre seguridad y privacidad de la tecnología RFID”, mayo, 2010, pp.1-49. Disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/julio/Guia_RFID.pdf

- LLAMAMOSAS TRAPAGA, A. *Las Nuevas Tecnologías de la Información y Comunicación y las Relaciones Laborales*. Bilbao, España: Tesis Doctoral, Universidad de Deusto.
- PATÓN PÉREZ, M. I. “La tecnología rfid y su problemática en protección de datos”, en: *Red Seguridad*, marzo, n° 15, 2005. Artículo de opinión. Disponible en: http://www.borrmart.es/articulo_redseguridad.php?id=200&numero=15
- PORTILLO GARCÍA, J. I.; BERMEJO NIETO, A. B.; BERNADOS BARBOLLA, A. M. *Informe de Vigilancia Tecnológica madri+d. Tecnología de identificación por radiofrecuencia (RFID): aplicaciones en el ámbito de la salud.*, Madrid, España: Fundación madri+d para el conocimiento, Madrid, 176p. Disponible en: <http://www.madrimasd.org/informacionidi/biblioteca/publicacion/Vigilanciatecnologica/default.asp>
- REDACCIÓN LA LEY. “Un nuevo riesgo para la privacidad: las etiquetas RFID”, en: *Diario La Ley*, n° 7473, Sección Tribuna, septiembre 2010, pp. 1-3.
- ROIG BATALLA, A. *Derechos Fundamentales y Tecnologías de la Información y de las Comunicaciones*. Barcelona, España: Cuadernos de Derechos Constitucional, Bosch, 2010, 99p.
- TYRRELL, P. “Tuned in to the right frequency”, en: *Financial Times*, 14 de diciembre de 2004. Disponible en: <http://www.ft.com/intl/cms/s/1/57abe7ce-4dff-11d9-9351-00000e2511c8.html#axzz1ytvvjGXV>
- UGARTE CATALDO, J. L. “El derecho a la intimidad y la relación laboral”, en: *Boletín Oficial de la Dirección del Trabajo*, n° 139, agosto 2000, pp.1-23.
- UNI: “RFID in the workplace: UNI Code of Good Practice”, Version 1.0 (Draft), 2010, 27 abril, pp. – 1.4.
- WANT, R. “Sistemas de identificación por radiofrecuencia”, en: *Investigación y Ciencia*, n° 330, marzo 2004, pp. 40-49.