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)

INTRODUCCIÓN

El uso de los identificadores por radiofrecuencia o RFID (Radio Frequency Identification) está suscitando serias preocupaciones respecto de la protección de la vida privada de los ciudadanos por los nuevos riesgos que plantean para el ejercicio de sus derechos y libertades.

Los RFID surgen para perfeccionar la utilidad de los actuales códigos de barras facilitando el control de los productos y mercancías en general, pero en sus posibilidades se está ampliando a otros usos como el seguimiento e identificación de personas, En este contexto, la tradición europea en materia de protección de datos personales, cobra su importancia y así lo quiere hacer saber el Grupo de Trabajo del artículo 29 Directiva 95/46/CE, al elaborar un documento que expone los principales riesgos, y propuestas para evitarlos, en la utilización de esta nueva tecnología. El peligro que puede suponer una implantación generalizada de los RFID, 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 personalidad, significa la aparición de otros peligros mayores en cuanto posibilita, entre otras cosas, "rastrear" (*tracking)* a los individuos y no ya solamente "realizar su perfilar". Por todo ello se hace necesario delimitar de forma precisa su uso, de acuerdo con los principios de protección de datos implementados tanto por la Directiva 95/46/CE como por la Directiva 2002/58/CE.

A la luz del documento de trabajo elaborado y presentado por el Grupo 29, la Comisión de Libertades e Informática, ha identificado como más preocupantes los siguientes riesgos:

> La elaboración indiscriminada de perfiles. Este riesgo es inherente a cualquier tecnología que permite recabar datos de carácter personal de forma masiva y ha sido desde los albores de la protección de datos, el objeto de todas las preocupaciones. Hoy en día, es importante recordar una vez más los peligros que suponen este tipo de tratamiento y la necesidad de

enmarcarlos dentro de los principios recogidos en las Directivas de protección de datos

La utilización de los RFIDs con fines de identificación y los problemas que pueda suponer la intercepción fraudulenta de datos y su posterior uso con fines distintos, en particular el problema del "robo de identidad" (*Identity theft)*. Este problema ha aparecido estos últimos años en Estados Unidos, causando daños irreversibles en ciudadanos que han tenido que hacer frente a las consecuencias nefastas de actos que no habían cometidos. Hoy en día, esta figura delictiva se expande a medida de la implantación de las redes de voz IP, pudiendo constituir un problema de entidad para la Unión Europea si no se toman las medidas adecuadas. Un uso generalizado de los RFID, vulnerables a ataques externos y a la intercepción de datos de carácter personal por terceros no autorizados podría generar unos riesgos de mayor entidad para los ciudadanos europeos.

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.

La implantación de RFID en personas, que se está dando actualmente en el ámbito de la salud, tiene una implicaciones éticas importantes que no se tratarán en el presente documento por exceder de la mera protección de la vida privada de los individuos e incidir de manera sensible sobre el respeto a la dignidad humana. La Comisión de Libertades e Informática se felicita de que organismos como el European Group on Ethic hayan empezado un debate sobre el tema, a raíz del dictamen presentado el día 18 de marzo de 2005.

En respuesta a la consulta pública lanzada por el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, sobre el mencionado documento de trabajo (The Working Document 105) la Comisión de Libertades e Informática, siempre a favor del desarrollo tecnológico en la Sociedad de la Información, no sólo suscribe las propuestas recogidas por este documento, sino que plantea las suyas propias participando, en su afán de protección de los derechos y libertades de los individuos frente a los riesgos que suponen la aparición y uso de nuevas tecnologías cada día más potentes.

(http://europa.eu.int/comm/internal_market/privacy/workingroup/consultations/consultation_en.htm)

COMENTARIOS DE LA COMISIÓN DE LIBERTADES E INFORMÁTICA A LAS PROPUESTAS DEL WP 105:

1. PROTECCIÓN DE DATOS E IMPLICACIONES SOBRE LA PRIVACIDAD.

La utilización de los RFID en **ámbitos de diferente naturaleza** (personas, animales, productos de consumo, documentos de identificación, transportes, billetes, ... etc.), habrá de ser sistematizada estableciendo los límites específicos necesarios para las personas y para los usos que afecten a éstas, a sus datos de carácter personal, evitando siempre todo riesgo de "cosificación" de los individuos. En Francia, es de señalar que la Commission Nationale de l'Informatique et des Libertés (CNIL) ha clasificado ya las etiquetas RFID entre las tecnologías de riesgo para las libertades individuales porque considera que son datos personales a la luz de la Ley Informática y Libertades francesa de 1978.

A efectos de la exposición, la Comisión de Libertades e Informática ha creído conveniente distinguir entre los RFID implantados en productos y destinados a su seguimiento, y los RFID destinados a la localización de personas.

A. RFID destinados al seguimiento de productos

Esta modalidad de utilización únicamente se vuelve intrusiva sobre la vida privada de los individuos en cuanto la información recabada por el dispositivo se ve asociada a una persona identificada o identificable, conforme a lo dispuesto en la Directiva 95/46/CE.

Las etiquetas inteligentes se han ganado ya la confianza en el sector de la actividad comercial, que ve en ellas el medio de optimizar la trazabilidad de las mercancías en toda la cadena de distribución, desde el almacén hasta la caja: más precisión en la gestión de stocks, reducción de costes, protección antirrobo,... etc. Alguno ejemplos gráficos de tales ventajas, se encuentran también en su aplicación al sector del reciclaje, facilitando la clasificación de los residuos con robots, en el sector de la alimentación para controlar la temperatura de los alimentos, en el sector textil para controlar los fraudes sobre las marcas...etc. Hay que tener en cuenta además que también brindarán muchas ventajas al consumidor, por ejemplo, se acabarían las colas en las cajas del supermercado porque el contenido de los carros se identificará a distancia con una sencilla lectura por radio.

El peligro de esta tecnología es que cada producto puede estar etiquetado con un número identificativo único (a diferencia del código de barras que es el mismo para todos los productos iguales), permitiendo asociarlo perfectamente

a su comprador. El producto podrá identificarlo unívocamente, quedando en entredicho el anonimato y la privacidad de los compradores. Por poner un ejemplo, a largo plazo, cualquiera que tuviera un lector de chips RFID podría saber los aparatos, electrodomésticos, ropa, … que tenemos en casa sin necesidad de entrar. Un chip RFID en nuestro móvil, reloj o cartera podría permitir saber si hemos estado en un determinado establecimiento. El uso no advertido de esta nueva tecnología ya es objeto de preocupación de las organizaciones de defensa del consumidor frente a experimentos llevados a cabo por marcas como Gillette, Prada, Wal-Mart o Benetton... a veces sin advertir a los clientes. Más llamativo aún es el uso de esta tecnología en el ámbito de productos no perecederos con fines de control de los individuos, como es el caso, por ejemplo, de su inserción en las matrículas de los vehículos británicos con el fin de ser leídas para imponer multas, o su aparición en parkings, en zonas de peaje, para sancionar a conductores infractores, ...etc.

B. **RFID destinados a la localización, identificación y seguimiento de individuos**

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 alzheimer, 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. Pongamos por ejemplo que se generaliza la obligación de “soportar” un RFID para acceder al sistema sanitario, al sistema de transporte público, a determinadas ayudas sociales...etc, sin que exista un sistema de acceso alternativo, llevaría a que el prestador del servicio (en los ejemplos la Administración Pública) tuviera no sólo demasiada información (más de la necesaria para la prestación del servicio), sino el control de lo que necesitamos o creen que necesitamos.

La gravedad de las implicaciones mencionadas, sería materializada por cualquier tratamiento de datos de carácter personal que se realizase sin el consentimiento informado del afectado. (fuera de los supuestos legalmente previstos, un tratamiento de este tipo necesariamente habría de ser autorizado por la **autoridad judicial** competente). Se quiere asimismo llamar la atención del Grupo 29 sobre las iniciativas existentes que prevén la incorporación de los RFID a los documentos oficiales de identificación personal (DNI, pasaporte, carné de conducir, etc.) en cuanto pueden suponer una invasión desproporcionada de la intimidad y limitación de la libertad de movimiento en caso de uso fraudulento o ilegítimo de los datos recabados.

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, por lo que se formulan las siguientes recomendaciones:

El **consentimiento** debe ser:

- **Libre**; el afectado, nunca podrá ver su voluntad condicionada por la necesidad de utilizar esta tecnología. Esto significa que la denegación del acceso a un lugar, producto o servicio, si no consiente la implantación del RFID, salvo que medie expresa autorización judicial, debe ser prohibida, y en todo caso, se propone la exigencia, a quienes establezcan los sistemas RFID en sus actividades, de habilitar un medio alternativo de acceso a ese lugar, producto o servicio que no implique necesariamente la utilización de estos dispositivos. Este consentimiento además habrá de ser expreso y escrito en el caso de que se traten datos de carácter sensible, según el art. 8 de la Directiva 95/46/CE. La generalización del uso de estos dispositivos no debe suponer un menoscabo del derecho al anonimato de los individuos quienes deberían tener en cualquier caso una alternativa a su uso, en la medida de lo posible y razonable, para hacer efectivo la libertad de la prestación del consentimiento.

- **Informado**; La información que se proporcione a los interesados, habrá de ser completa, explícita y sencilla en su comprensión, para cada supuesto en el que se vaya a recaba datos de carácter personal. El responsable del tratamiento deberá proporcionar al interesado, como mínimo, la siguiente información:

1. la presencia de un RFID,
2. los datos que se contienen en el RFID de manera inicial,
3. los que, en su caso, se podrían ir almacenando,
4. las consecuencias del almacenamiento de datos y de su negativa por el interesado,
5. la vida útil del RFID,
6. la condición de “activado” o “desactivado” del RFID.
7. la localización de los lectores y su alcance.
8. los sistemas de activación y desactivación de esta tecnología,
9. la identidad de los responsables de los lectores, quienes implanten los dispositivos y quienes tengan acceso a la información que en ellos se almacene. La propia tecnología del dispositivo deberá permitir la localización e

identificación de los responsables, con el fin de poder determinar las responsabilidades en caso de uso ilegítimo de los datos recabados.

10. Las modalidades del ejercicio de los derechos que le asisten (derechos de acceso, rectificación, cancelación y oposición)

Toda esta información, de manera clara y completa deberá ser siempre puesta a disposición del potencial afectado, de manera que siendo conocedor de la existencia y presencia de RFIDs y lectores, se le permita saber a qué se está exponiendo exactamente. En particular, y a parte de la obligación de que dicha información conste en el producto, se sugiere que los responsables del tratamiento tengan obligación de hacer público esta información de forma genérica en sus establecimientos o en sus páginas web.

2. APLICACIÓN DE LA LEGISLACIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS EN LA RECOPILACIÓN DE INFORMACIÓN A TRAVÉS DE LA TECNOLOGÍA RFID.

La Directiva es aplicable a los tratamientos de datos de carácter personal, pues la diferencia estriba hoy en día en el tipo de soporte utilizado para ello, y el alcance de las consecuencias que la tecnología permite. La cuestión principal es que se hace necesaria la elaboración de unas instrucciones específicas por las Autoridades de Control que guíen la aplicación de sus legislaciones a este tema mientras se estudie, desde la Comisión Europea, la necesidad de elaborar una legislación específica que limite su alcance técnico, y el de otras tecnologías que en el futuro pudieran aparecer para cumplir iguales finalidades, recabar y tratar información (en el caso que nos ocupa, datos de carácter personal), previendo en lo posible el amplio abanico de posibilidades que se ofrecen, y respetando en todo caso la legislación específica existente en materia de protección de datos.

3. REQUISITOS TÉCNICOS Y ORGANIZATIVOS PARA ASEGURAR LA ADECUADA IMPLEMENTACIÓN DE LOS PRINCIPIOS DE PROTECCIÓN DE DATOS.

Conforme a lo mencionado anteriormente, sobre la inicial utilidad que se quiere dar a la tecnología RFID (sustituir los códigos de barras en la identificación de productos) la Comisión de Libertades e Informática quiere señalar las diferencias entre uno y otro sistema, viendo cuales son además las diferencias sobre las aplicaciones que posibilitan. Las etiquetas RFID difieren de los códigos de barras en tres importantes aspectos:

1. La tecnología RFID, permite dar un identificador único a cada producto, que lo hacen localizable de forma individual, y por tanto, permiten localizar a quien posea ese producto.

2. Pueden ser leídos a distancia, sin necesidad de acercarlos al lector, lo que permite elimina barreras y permite la ocultación de éstos de forma que se impida saber si está o no recabando información.
3. Las etiquetas RFID son también “activas” y no sólo “pasivas” como lo es un código de barras. Los RFID permiten recabar información, no sólo ofrecerla o “contenerla”.

Esta primera aproximación a las implicaciones de la utilización de la tecnología RFID, hace que la Comisión de Libertades e Informática proponga que en todo caso la información que almacene un RFID sea de forma codificada, tanto si la introduce el propio interesado, como si la reproduce el RFID automáticamente (recoge conductas del poseedor). Esta codificación, podrá permitir que el portador de un RFID evite accesos no autorizados o consentidos a la información, protegiéndole contra situaciones de “robo de identidad”.

En todo caso, y en la medida que ello sea siempre técnicamente posible, deberá procederse a la disociación de los datos, siendo tan sólo una clave la que se almacene en los RFID y ésta diese el acceso autorizado a la información contenida en un servidor. Se trata de permitir dicha “disociación” en un momento previo al tratamiento, todo ello al margen de que sea exigible, siempre que sea posible, para todo momento posterior o de tratamiento de los datos.

Una posibilidad más que exige la intimidad y su defensa, es que el portador de un RFID es el conocer en todo momento cuando está activado emitiendo información, y cómo poder desactivarlo desactivarlo y/o eliminarlo físicamente sin recurrir a complejos mecanismos o sistemas electrónicos. Se completaría este derecho de “control” permitiendo al individuo, detectar los dispositivos lectores de RFID. En relación con esto, la Comisión del Ibertades e Informática (CLI) propone que la generalización que del uso de estos dispositivos se pudiera hacer en determinados sectores (comercio, productos), lo sea siempre en hacia la implantación de dispositivos pasivos, es decir, que no recojan información, sino que emitan la que tiene almacenada en su memoria, para que el control de un producto, no se convierta en el control de la persona.

En cualquier caso, la propuesta es concreta, cualquier tratamiento de datos personales que se haga utilizando este sistema, habrá de verse limitado por los principios de necesidad, proporcionalidad y calidad de los datos, de manera que éstos sean eliminados automáticamente cuando la finalidad que determinó su almacenamiento haya caducado. Y sobre todo, que en el caso de ser dispositivos “activos”, es decir, que almacenen información, tan sólo lo hagan sobre aquella información que necesita en su finalidad, siendo automáticamente borrado o filtrado todo aquello que pueda recabar y no se atenga a la necesidad de su implantación.

La Comisión de Libertades e Informática alienta a la Unión Europea a potenciar y desarrollar las tecnologías protectoras de la vida privada, las "PET" (Privacy Enhancement Technologies), de tal forma que se incida sobre todo –sin perjuicio de la reprensión de la ilegalidades y la reparación de los daños- en la faceta de prevención, es decir, impidiendo -en la medida de lo posible- las recogidas y tratamiento ilegítimos o fraudulentos de datos de carácter personal.

4. CONCLUSIÓN

Dependiendo de la evolución de la tecnología RFID y sus aplicaciones, el Grupo de Trabajo 29 decidirá sobre la especificidad requerida para los diferentes ámbitos dónde pueda ser implantado, estableciendo pautas concretas para ello.

La CLI manifiesta su apoyo a la iniciativa de perfeccionar la legislación, que ordenando el uso de la tecnología RFID, en defensa de la intimidad y la protección de datos de carácter personal.

Habrá de tenerse en cuenta que afectará a todo tipo de datos personales, todo tipo de soportes, y todo tipo de finalidades y tratamientos en su uso, a la hora de establecer las pautas de su regulación, pues la tecnología hoy conocida que permite esta forma de recabar datos, no debe limitar las posibilidades que el futuro pueda abrir en igual sentido. Se propone por ello, establecer 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 incluiría los sistemas de localización con tecnología GPS).

La Comisión de Libertades e Informáticas (CLI) propone que la norma que desarrolle los principios expuestos por el Grupo de Trabajo 29, y a los que reitera su adhesión, contemplen no sólo los tratamientos de datos individualizados a través de ésta tecnología, sino también los posibles tratamientos colectivos (muestreos o estadísticas) que, aún no identificando directamente a cada individuo sino a un grupo al que pudiera pertenecer, puedan por ello verse afectados por los resultados de dicho tratamiento de datos, de forma que se vea menoscabada su dignidad, honor o intimidad al hacerlos identificables individualmente como parte de ese colectivo. En igual sentido se propone que, sobre las consecuencias de un tratamiento de datos así realizado, con el fin de evaluar la personalidad del grupo o individuo, se establezca una prohibición expresa para la toma de decisiones con efectos jurídicos perjudiciales.

La Comisión de Libertades e Informáticas (CLI) se muestra a favor de los desarrollos tecnológicos que faciliten nuestra vida de una u otra manera, pero siempre que el individuo esté capacitado para conocer su alcance y consentir sobre su utilización, pues esa es la forma de ejercer los derechos y libertades que nuestra normativa promulga y desarrolla en Europa, por ello, instamos a las autoridades europeas a promover el apoyo al desarrollo de tecnologías que impidan invasiones en la

intimidad de sus ciudadanos, y protejan su dignidad. En definitiva, que el control del servicio o del producto no se convierta en el control de la persona.