¡Las tecnologías inalámbricas RFID y la privacidad humana!

"La causa de la libertad se convierte en una burla
si el precio a pagar es la destrucción de quienes deberían disfrutar la libertad."
Mahatma Gandhi

Jairo Augusto Ortegón Bolívar[*]

Resumen

Dentro de las diferentes invenciones basadas en tecnologías inalámbricas, el teléfono móvil pertenece a la categoría de las tecnologías convergentes, así mismo ha ampliado nuestro espacio personal al tamaño del planeta, luego ha logrado realmente la globalidad, así solamente lo utilicemos para llamar nuestros amigos. Hasta allí, todo parece bajo control sin embargo cuando la tecnología se encuentra expedita para controlar nuestra vida privada, los alcances de las tecnologías por refinadas y prácticas que sean, debemos de repensar su utilización.

La tecnología RFID, la cual permitirá un estrecho contacto o interconectividad con todo a nuestro alrededor y que ya está en práctica en otros países y se está extendiendo al nuestro rápidamente conlleva a que realmente pensemos, cuál sería el manejo ético de la misma. Si bien es cierto que surgió como una alternativa para sustituir etiquetas y códigos de barras en muchos productos de consumo masivo, quizá no parezca muy importante, pero está expandiendo la esfera de datos de nuestra personalidad digital y nos hará más vulnerables a la violación de nuestra privacidad y no existirá ningún lugar en donde no seamos localizables.

Palabras Clave: *RFID, Autoidentificación, Trazabilidad, Código Único, Privacidad*

1.0 Tecnología RFID

Antecedentes. Dentro de los inicios de lo que hoy conocemos como **RFID,** una tecnología similar, el transpondedor (repetidor de radiofrecuencia) de **IFF** (identificador de amigo o enemigo), fue inventado por los británicos en 1939, y fue utilizado de forma rutinaria por los aliados en la Segunda Guerra Mundial para identificar los aeroplanos como amigos o enemigos.

Otro trabajo temprano que trata el **RFID** es el artículo de 1948 de Harry Stockman, titulado "*Comunicación por medio de la energía reflejada*" (Actas del IRE, pp1196-1204, octubre de 1948). Stockman predijo que... *el trabajo considerable de investigación y de desarrollo tiene que ser realizado antes de que los problemas básicos restantes en la comunicación de la energía reflejada se solucionen, y antes de que el campo de apli-*

[*] El autor es Ingeniero Electrónico, Especialista en Administración y Magíster en Teleinformática, Doctorando en Gestión del Conocimiento y la Sociedad de la Información de la Universidad Oberta de Cataluña., y actualmente se desempeña como Profesor Adjunto del Área de Redes y Servicios de Telecomunicaciones del Programa de Ingeniería Electrónica de la Universidad Autónoma de Colombia, y Catedrático de otras Universidades. E-mail: jortegonb@yahoo.com

caciones útiles se explore. Como puede observarse se requirieron más treinta años de avances en multitud de campos diversos antes de que **RFID** se convirtiera en una realidad.

La tecnología **RFID** (Radio Frequency Identification), o lo que es lo mismo, la identificación por radiofrecuencia, es una tecnología de identificación remota e inalámbrica en la cual un dispositivo lector o reader vinculado a un equipo de computo, se comunica a través de una antena alimentada por un transceptor (también conocido como tag o etiqueta) mediante ondas de radio. Por tanto es un tipo de tecnología emergente que permite asignar a cualquier producto desde un cepillo para el cabello hasta un camión, un número de identificación.

Así, cuando un proveedor de cepillos para el cabello fabrica un cepillo, puede incorporar en dicho cepillo una etiqueta electrónica (o tag) que lleva incorporado un chip con un número de identificación. Mediante este número, el producto en este caso el cepillo para el cabello puede ser rastreado y factiblemente controlado a lo largo de toda la cadena de distribución, desde el fabricante hasta el comprador, pasando por las empresas de almacenaje y distribución o el comercio que vende dicho producto.

1.1 Características Técnicas

Una de las principales características tecnificas del **RFID** es la auto identificación segura. Miremos entonces que la identificación segura es la aplicación de las tecnologías de auto identificación de manera que aseguren la fiabilidad y la confidencialidad de la información contenida en un objeto, un producto, etc. El término *"identificación"* tiene diferentes significados y aplicaciones, pero lo que tienen en común todas estas acepciones es que un "identificador" es capaz de diferenciar una persona de otra, o un objeto de otro: es decir, cada persona u objeto tiene una identidad única. Tradicionalmente, este concepto se ha usado para identificar personas y asegurarse de que sólo las personas autorizadas pueden hacer lo que ellas y nadie más tienen capacidad para hacer (por ejemplo, sacar dinero de una determinada cuenta corriente, firmar un cheque, etc.). Pero el término tiene connotaciones negativas cuando sirve para denegar un derecho a una persona porque no posee la identificación adecuada (por ejemplo, en los controles de pasaportes).

Entonces, *Auto identificación* es la habilidad de una máquina para leer una identidad y se aplica normalmente cuando es un objeto el que tiene que ser identificado. La combinación de la *Auto identificación* de objetos con el *tracking* (es decir, el seguimiento de los movimientos de un objeto) da como resultado la *trazabilidad*, un concepto que puede tener enormes implicaciones que miraremos más adelante.

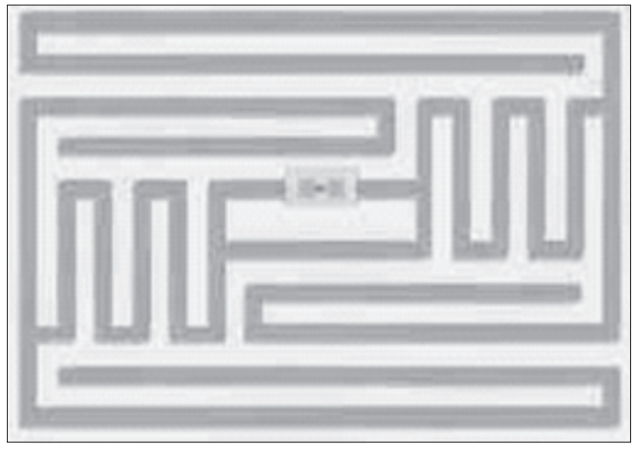
1.2 Componentes y funcionamiento de la tecnología de identificación por radiofrecuencia

Un sistema de identificación por radiofrecuencia **RFID** está formado por tres elementos básicos:

- Una etiqueta electrónica o tag que lleva incorporado un transceptor, y una microantena.
- Un lector de tags.
- Una base de datos.

- Un tag es una etiqueta que lleva un microchip (transceptor y memoria) incorporado y que puede adherirse a cualquier producto (por ejemplo, un cepillo para el cabello) o puede incorporarse a cualquier otro producto, animal o persona. El microchip almacena un número de identificación, una especie de matrícula única de dicho producto.

Hay varios tipos de esquemas propuestos para estos números, como por ejemplo el *Electronic Product Code*, diseñado por Auto-ID Center define este número como un *código único (CU).* De esta forma el sistema, se convierte en un método de almacenamiento y recuperación de datos remotos y lo hace a través de los tags o dispositivos denominados etiquetas, pegatinas o *tags RFID*. Las etiquetas pasivas (**Gráfica No 1)** no necesitan alimentación eléctrica interna, mientras que las activas (**Gráfica No 2)** sí lo requieren. Los Tags activos requieren batería adicional, la cual se construye para que dure varios años.

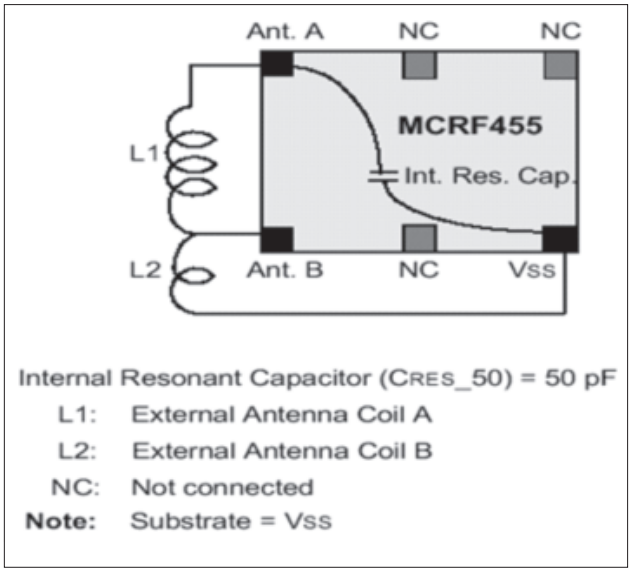


Gráfica No. 1. Etiquetas pasivas usada por Wal-Mart.

Gráfica No. 2. Una etiqueta activa para recaudación con peaje electrónico.

1.3 Teoría de Operación

El sistema funciona de la siguiente manera. El lector envía una serie de ondas de radiofrecuencia al tag, que son captadas por la microantena de éste. Dichas ondas activan el microchip, el cual, a través del transceptor, la microantena y mediante ondas de radiofrecuencia, transmite al lector acerca de cuál es el *CU* del producto. Para que exista esta comunicación, el transceptor no necesita contar con una batería debido a que en la mayoría de los casos, se induce una corriente a su circuito integrado o chip mediante el campo electromagnético que produce la antena del reader (lector de identificación). La corriente requerida por el transceptor es tan baja, que la energía inducida a través del campo en su rango de acción basta para activarlo, completar un protocolo de comunicación y enviar información de vuelta a la antena del reader (lector de identificación). Un esquema eléctrico de uno de tantos modelos se ilustra en la Gráfica No 3.



Gráfica No. 3. Esquema eléctrico de un tag RFID

Finalmente, el lector recibe cuál es el *CU* del producto y lo envía a una base de datos en la que previamente se han registrado las características del producto (fecha de fabricación, fecha de caducidad, peso, color, material, etc.). De esta manera, cualquier agente de la cadena de suministros puede consultar de forma rápida cualquiera de las características del producto que está vendiendo y/o distribuyendo.

1.4 Comportamiento frente al ambiente circundante

Frente al ambiente que lo circunda habría que compararlo ante su competencia tradicional o sea frente a tecnologías de identificación convencionalmente empleadas como es el Código de Barras (que popularmente conocemos en los supermercados), ante el cual presenta las siguientes ventajas:

- No requiere una línea de visión
- No requiere de intervención humana (ideal para automatizar)
- Distancias de lectura de 1 a 10m
- Lectura simultánea de múltiples artículos (protocolo anticolisión)
- Hasta 500 lecturas por minuto (más de 5 veces más rápido que un código de barras)
- No le afectan los ambientes sucios
- Alta Capacidad de lectura y escritura

2.0 Aplicaciones y usos de la tecnología RFID

La tecnología **RFID** aplicada a productos tiene un objetivo básico: permitir que todos los agentes que participan en la cadena de suministro puedan tener un producto localizado y controlado (un concepto que los estadounidenses han bautizado como *supply chain visibility*). Esta característica de monitoreo sobre la cadena de suministro del producto permitirá lo siguiente:

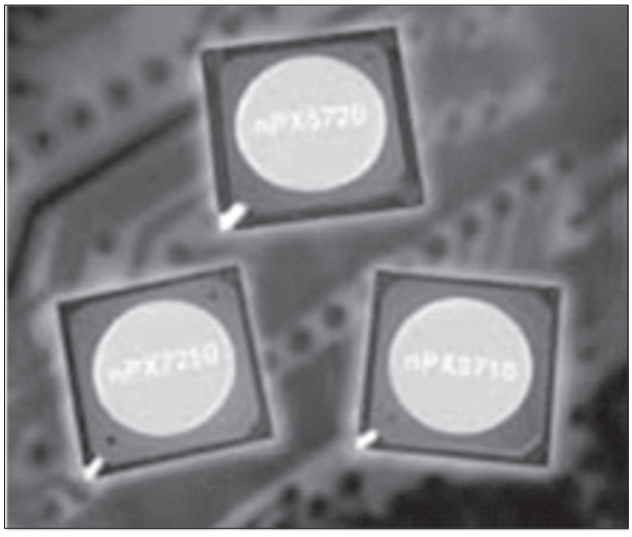
- Aumentar la eficiencia de la cadena de distribución.
- Reducir errores en la información acerca de los productos.
- Tener un mayor control sobre la calidad de los productos.
- Tener mayor control sobre el stock almacenado.
- Liberar a personal de tareas mecánicas para que puedan realizar labores más complicadas.

- Mejorar el tiempo de respuesta de todos los agentes.
- Tener información real e inmediata sobre las tendencias de venta de un producto.
- Evitar las colas en los comercios.
- Evitar los pequeños hurtos en los comercios.
- Evitar las falsificaciones.
- Mejorar el reciclaje de productos.

Actualmente, la tecnología **RFID** se utiliza en aplicaciones menos futuristas y mucho más cotidianas, como los peajes automáticos y las tarjetas contactless de pago y de acceso.

2.1 Efectos e implicaciones específicas de la implementación de dicha tecnología en el comportamiento social.

Uno de los efectos inmediatos que se deducen de la aplicación de la tecnología **RFID (Gráfica No 4)**, es la *Trazabilidad*. Recordemos que es la combinación de la *autoidentificación* de objetos con el *tracking* (es decir, el seguimiento de los movimientos de un objeto) da como resultado la *Trazabilidad*, un concepto que puede tener enormes implicaciones entre otros, los siguientes:



Gráfica No. 4. Ilustración de algunos modelos de tags RFID.

- La identificación segura depende de que cada objeto pueda tener una identidad única, que no pueda ser falsificada, perdida o tergiversada. Esto implica que debe existir una avanzada tecnología aplicada a los tags de identidad (una especie de dispositivos electrónicos que contienen la identidad del objeto) y a los lectores de tags (los aparatos capaces de descodificar y extraer la información de los tags).

- La identificación segura depende también del uso y gestión controlada y confidencial de los datos generados por la autoidentificación y el tracking. Ello implica que, además de aplicar una avanzada tecnología, deben existir también *efectos técnicos y un marco legal y ético establecido.*

2.2 Comentario sobre sus efectos e implicaciones para los sistemas mediáticos 'tradicionales'.

Esta tecnología **RFID** en mi opinión no tiene ningún efecto (o por lo menos hasta el momento, no lo puedo percibir) sobre los Media tradicionales que conocemos como la radio, la televisión. Si tiene un efecto sobre medios como la Telefonía fija, la Telefonía móvil celular, Internet, Televisión Digital, los GPS por cuanto desde el punto de vista tecnológico se puede soportar sobre estos mismos medios, es decir puedo emplear estas últimas tecnologías para tener al tanto a los interesados en tiempo real sobre los resultados del objeto rastreado por la tecnología **RFID**. Esto representa para los operadores de estos servicios, otra oportunidad de negocio, por cuanto son servicios adiciónales que pueden prestar.

2.3 Valoración de los aspectos positivos y/o negativos de las consecuencias señaladas anteriormente

Como la mayoría de las tecnologías su implementación e implantación tiene efectos positivos y negativos sobre la sociedad, veamos los dos aspectos:

2.3.1 Aspectos positivos

Los aspectos positivos son evidentes y de gran amplitud en la práctica de la aplicación de dicha tecnologías en situaciones como su uso en aplicaciones como:

- Las etiquetas **RFID** de baja frecuencia se utilizan comúnmente para la identificación de animales, seguimiento de camiones, y como llave de automóviles con sistema antirrobo. En ocasiones se insertan en pequeños chips en mascotas, para que puedan ser devueltas a su dueño en caso de pérdida.

- Las etiquetas **RFID** de alta frecuencia se utilizan en bibliotecas y seguimiento de libros, seguimiento de contenedores, control de acceso en edificios, seguimiento de equipaje en aerolíneas, seguimiento de artículos de ropa y ahora último en pacientes de centros hospitalarios para hacer un seguimiento de su historia clínica. Un uso extendido de las

etiquetas de alta frecuencia como identificación de acreditaciones, substituyendo a las anteriores tarjetas de banda magnética. Sólo es necesario acercar estas insignias a un lector para autenticar al portador.

- Las etiquetas **RFID** de UHF se utilizan comúnmente de forma comercial en seguimiento de camiones y remolques en envíos.

- Una etiqueta **RFID** puede ser empleada para la recaudación con peaje electrónico.

- Las etiquetas **RFID** de microondas se utilizan en el control de acceso en vehículos de gama alta. En algunas autopistas, como por ejemplo la Fast Track de California, el sistema I-Pass de Illinois, el telepeaje TAG en las autopistas urbanas en Santiago de Chile y la *Philippines South Luzon Expressway E-Pass* utilizan etiquetas **RFID** para recaudación con peaje electrónico. Las tarjetas son leídas mientras los vehículos pasan; la información se utiliza para cobrar el peaje en una cuenta periódica o descontarla de una cuenta prepago. El sistema ayuda a disminuir el tráfico causado por las cabinas de peaje.

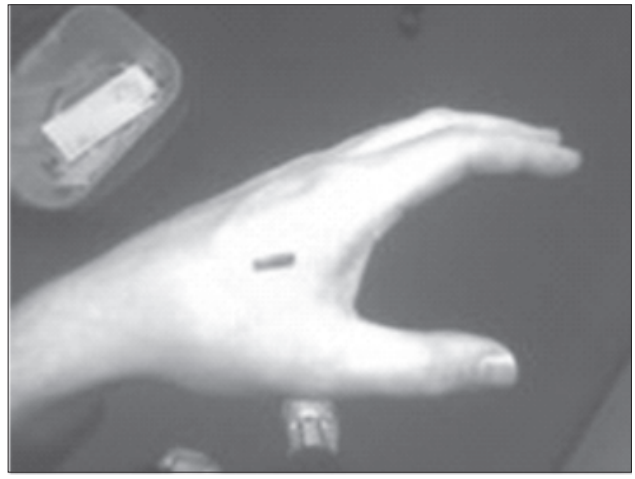
- Sensores como los sísmicos pueden ser leídos empleando transmisores-receptores **RFID**, simplificando enormemente la recolección de datos remotos.

- Michelín el fabricante de llantas anunció que había comenzado a probar transmisores-receptores **RFID** insertados en neumáticos. Después de un período de prueba estimado de 18 meses, el fabricante ofrecerá neumáticos con **RFID** a los fabricantes de automóviles. Su principal objetivo es el seguimiento de neumáticos en cumplimiento con la *United States Transportation, Recall, Enhancement, Accountability and Documentation Act.*

- Las tarjetas con chips **RFID** integrados se usan ampliamente como dinero electrónico, como por ejemplo la tarjeta *Octopus* en Hong-Kong y en los Países Bajos como forma de pago en transporte público y ventas menores, en Bogotá, D.C., se implementa para el pago del servicio de transporte Transmilenio.

- En la industria de automóvil está disponible una "llave inteligente" como opción en el Toyota Prius y algunos modelos de Lexus. La llave emplea un circuito de **RFID** activo que permite que el automóvil reconozca la presencia de la llave a un metro del sensor. El conductor puede abrir las puertas y arrancar el automóvil mientras la llave sigue estando en la cartera o en el bolsillo.

- Veamos esta última para iniciar con los aspectos negativos. El Departamento de Rehabilitación y Corrección de Ohio (ODRH) aprobó un contrato de 415.000 dólares para ensayar la tecnología de seguimiento con Alanco Technologies. Los internos tienen unos transmisores del tamaño de un reloj de muñeca que pueden detectar si los presos han estado intentando quitárselas y enviar una alarma a los ordenadores de la prisión. Este proyecto no es el primero que trabaja en el desarrollo de chips de seguimiento en prisiones estadounidenses **(Gráfica No. 5 y Gráfica No. 6)**. Instalaciones en Michigan, California e Illinois emplean ya esta tecnología. En Colombia de conformidad con el articulo 27 de la ley 1142 de 2007, ya se esta implementando en la sustitución de la detención preventiva.



Gráfica No. 5. Mano previo al implante del tag RFID

Gráfica No 6 - Mano posterior al implante del tag RFID

2.3.2 Aspectos Negativos

El uso de la tecnología **RFID** ha causado una considerable polémica e incluso boicots de productos. Las cuatro razones principales por las que **RFID** resulta preocupante en lo que a *privacidad* se refiere son:

- El comprador de un artículo no tiene por qué saber de la presencia de la etiqueta o ser capaz de eliminarla.
- La etiqueta puede ser leída a cierta distancia sin conocimiento por parte del individuo.
- Si un artículo etiquetado es pagado mediante tarjeta de crédito o conjuntamente con el uso de una tarjeta de fidelidad, entonces sería posible enlazar la **ID** única de ese artículo con la identidad del comprador.
- El sistema de etiquetas EPCGlobal crea, o pretende crear, números de serie globales únicos para todos los productos, aunque esto cree problemas de privacidad y sea totalmente innecesario en la mayoría de las aplicaciones.

3.0 Implicaciones

- La mayoría de estas preocupaciones giran alrededor del hecho de que las etiquetas **RFID** puestas en los productos siguen siendo funcionales incluso después de que se hayan comprado los productos y se hayan llevado a casa, y esto puede utilizarse para vigilancia, y otros propósitos infames sin relación alguna con sus funciones de inventario en la cadena de suministro.
- Aunque la intención es emplear etiquetas **RFID** de corta distancia, éstas pueden ser interrogadas a mayores distancias por cualquier persona con un transceptor provisto de una antena de alta ganancia, permitiendo de forma potencial que el contenido de una casa pueda ser explorado desde una cierta distancia. Incluso un escaneado de rango corto es preocupante si todos los artículos detectados aparecen en una base de datos cada vez que una persona pasa un lector, o si se hace de forma malintencionada (por ejemplo, un robo empleando un escáner de mano portátil para obtener una evaluación instantánea de la cantidad de víctimas potenciales). Con números de serie **RFID** permanentes, un artículo proporciona información inesperada sobre una persona incluso después de su eliminación; por ejemplo, los artículos que se revenden, o se regalan, pueden permitir trazar la red social de una persona.

- Otro problema referente a **la privacidad** es debido al soporte para un protocolo de singulation (anticolisión). Ésta es la razón por la cual un lector puede enumerar todas las etiquetas que responden a él sin que ellas interfieran entre sí. La estructura de la versión más común de este protocolo es tal que todos los bits del número de serie de la etiqueta salvo el último se pueden deducir por eavesdropping (detección a distancia) pasivo tan sólo en la parte del protocolo que afecta al lector. Por esta razón, si las etiquetas **RFID** están cerca de algún lector, la distancia en la cual la señal de una etiqueta puede ser escuchada es irrelevante. Lo que importa es la distancia a la que un lector de mucho más alcance, pueda recibir la señal, independientemente de que esto dependa de la distancia a la que se encuentre el lector y de qué tipo sea. En un caso extremo algunos lectores tienen una salida de energía máxima (4 W) que se podría recibir a diez kilómetros de distancia.

- Varios países han propuesto la implantación de dispositivos **RFID** en los nuevos pasaportes, para aumentar la eficiencia en las máquinas de lectura de datos biométricos. El experto en seguridad Bruce Schneier dijo a raíz de estas propuestas: "Es una amenaza clara tanto para la seguridad personal como para la privacidad. Simplemente, es una mala idea." Los pasaportes con **RFID** integrado únicamente identifican a su portador, y en la propuesta que se está considerando, también incluirían otros datos personales. Esto podría hacer mucho más sencillos algunos de los abusos de la tecnología **RFID** que se acaban de comentar, y se podría expandir la cantidad de datos para incluir, por ejemplo, abusos basados en la lectura de la nacionalidad de una persona. Por ejemplo, un asalto cerca de un aeropuerto podría tener como objetivo a víctimas que han llegado de países ricos, o un terrorista podría diseñar una bomba que funcionara cuando estuviera cerca de personas de un país en particular. El Departamento de Estado de los Estados Unidos rechazó en un primer momento estas hipótesis porque pensaban que los chips sólo podrían ser leídos desde una distancia de 10 cm., sin tener en cuenta más de 2.400 comentarios críticos de profesionales de la seguridad, y una demostración clara de que con un equipo especial se pueden leer los pasaportes desde 10 metros. La autoridad de los pasaportes de Pakistán ha comenzado a expedir pasaportes con etiquetas **RFID.**

- El estado estadounidense de Virginia ha pensado en poner etiquetas **RFID** en los carnés de conducción con el objetivo de que los policías y otros oficiales realicen comprobaciones de una forma más rápida. La Asamblea General de Virginia también espera que, al incluir las etiquetas, cueste mucho más obtener documentos de identidad falsos. La propuesta se presentó por primera vez en el Driver's License Modernization Act de 2002, que no fue promulgada, pero en 2004 el concepto

todavía estaba considerándose. La idea fue promovida por el hecho de que varios de los piratas aéreos de los atentados del 11 de septiembre tenían carnés de conducir de Virginia fraudulentos. Sin embargo, la American Civil Liberties Union dijo que *además de ser un riesgo para la privacidad y la libertad*, la propuesta del **RFID** no habría entorpecido a los terroristas, dado que la documentación falsa que portaban era válida, pues eran documentos oficiales obtenidos con otra identificación falsa. La debilidad del sistema es que no falla cuando se validan documentos en el momento, sino que falla es al verificar la identidad antes de expedirlos.

- Finalmente comparémoslo en aspectos de privacidad contra su competencia, es decir, el código de barras:

1. Con la tecnología de Código de Barras de hoy, por ejemplo cada lata de Coca Cola tiene el mismo UPC o número de código de barra como cada otra lata (una lata de Coca Cola en Toronto tiene el mismo número que una lata de Coca Cola en Tokio). Con **RFID**, cada lata del individuo de Coca Cola tendría un único ID, número que podría unirse a la persona que lo compra cuando ellos examinan una tarjeta del crédito o una tarjeta del comprador frecuente (es decir, un "sistema de registro de artículo").

2. Diferente de un Código de la Barra, estas pegatinas basadas en **RFID** pueden leerse a una distancia a través de su ropa, cartera, morral sin su conocimiento o con consentimiento por alguien con el dispositivo del lector correcto. En cierto modo, permite que los extraños tengan una visión radiográfica sobre usted, lo están espiando e identificando y saben las cosas que día a día, usted esta trayendo o llevando a su domicilio.

3. Diferente del Código de la Barra, **RFID** podría ser dañino para su salud. Los partidarios de **RFID** prevén un mundo donde los **RFID** lector dispositivos estén por todas partes en tiendas, en los suelos, en puertas, en aviones incluso en los refrigeradores y botiquines de nuestras propias casas. Lo anterior implica que existe una radioactividad permanente. Los investigadores saben que la salud sufre deterioro a exposición de largo plazo por la energía emitida por éstos dispositivos portátiles basados en **RFID** y por su sistema lector.

4.0 Conclusiones

Como vemos, con la invención de sistemas basados en tecnología **RFID** las aplicaciones y los efectos son de diversa índole, lo único que nos tranquilizaría es poder fijar **un código de ética** que se observe y se cumpla para la aplicación de esta y cualquier otra tecnología de tal forma que siempre se respeten los valores del ser humano entre estos, una de los más preciados es su libertad y dentro de ella, esta el derecho a la privacidad. En el futuro nos esperan las etiquetas y los sistemas de identificación inalámbricos en todas partes. Sólo nuestras acciones y el futuro, nos dirá como terminará esto, yo espero que todo sea en beneficio de la humanidad.

Incluyo algunas referencias de entidades que luchan por el respeto a la privacidad del ser humano:

- Privacy International
- Parar al RFID (http://www.spychips.com/index.html), un sitio web activista especializado en privacidad y RFID.
- Información y opiniones en contra de RFID (http://www.rfidkills.com)
- Informe de los consumidores de RFID (http://www.zombiewire.com/)
- Posición de la EFF en lo que se refiere a RFID (http://www.eff.org/Privacy/Surveillance/RFID/)
- Trabajo de EPIC sobre RFID (http://www.epic.org/privacy/rfid)
- Kriptópolis publica noticias sobre RFID principalmente cuando tienen que ver con vulnerabilidades de éstas o con la privacidad (en español)
- Academic Papers on RFID & inventory problems.
- Sistema de Control de Accesos Liberté: http://www.alfi.it/es/liberte.html

Referencias

Industrias ID Track, Sure Identificatiòn and Traceability, U.S. A. http://www.idtrack.org/IDtrack/

"El punto de control Reenfoca Esfuerzo de RFID, " el Periódico de RFID, Oct 23, 2006

Gestiopolis.com. http://www.gestiopolis.com/Canales4/ger/rfid.htm

http://www.spychips.com/airport1.swf-

Medidas para la Prevención y Represión de la Actividad Delictiva, Ley 1142 del 28 de junio de 2007. Congreso de la República de Colombia


Universidad
Autónoma
de Colombia