

Nota informativa

En un informe elaborado por ambas instituciones sobre seguridad y privacidad de la tecnología RFID (etiquetas de identificación por radio frecuencia)

La AEPD e INTECO advierten sobre el impacto para la privacidad de la creciente implantación de las etiquetas “RFID” en objetos de uso cotidiano

- Alertan sobre la posibilidad de rastrear a un individuo o incluso del uso indebido de datos personales para analizar su comportamiento, si éstas no son desactivadas correctamente o se producen fallos de seguridad.
- Se trata de dispositivos o etiquetas que, mediante una onda que transmite datos por radiofrecuencia, permiten vincular objetos, localizarlos e identificarlos de manera unívoca.
- En la actualidad es frecuente el uso de etiquetas RFID en prendas de ropa; calzado; o pasaportes, y ámbitos tan cotidianos como el transporte; grandes superficies; bibliotecas; o el comercio, para prevenir hurtos y controlar stock, como sistema de identificación y pago, o control de acceso.
- En España, la implantación de la tecnología RFID suele darse en mayor medida en las grandes empresas, pero las aplicaciones actuales, y las previsiones apuntan a un crecimiento exponencial en los próximos años.
- Advierten además de los riesgos de su utilización en ámbitos sensibles, como el sanitario, para el seguimiento de pacientes o el control de muestras.
- La guía incluye recomendaciones dirigidas a usuarios y empresas para prevenir riesgos y fomentar una correcta utilización de estas tecnologías.
- El Parlamento Europeo ha aprobado recientemente un informe defendiendo la necesidad de garantizar la privacidad de los usuarios en el empleo de esta tecnología.

(Martes, 27 de julio de 2010). La Agencia Española de Protección de Datos (AEPD), y el Instituto Nacional de Tecnologías de la Comunicación (INTECO), han elaborado una Guía sobre “seguridad y privacidad de la tecnología RFID”, ante la proliferación de estos sistemas en elementos de la vida cotidiana de los ciudadanos.

En dicha guía, disponible desde hoy en las páginas Web de ambos organismos (www.inteco.es, www.agpd.es, respectivamente), se analiza el funcionamiento de esta tecnología, los tipos de dispositivos existentes en la actualidad y sus usos y aplicaciones principales. Asimismo, se recogen de forma destacada los riesgos existentes en materia de seguridad, privacidad y protección de los datos en el empleo, e implantación de los dispositivos de identificación por radio frecuencia, en diversos ámbitos, y las garantías exigibles para prevenirlos.

Presencia en implantación de las RFID en España

En la actualidad los dispositivos o etiquetas de identificación por radio frecuencia (RFID- *Radio Frequency Identification Devices*), tecnología que permite identificar de forma automática un objeto, gracias a una onda que transmite los datos identificativos del objeto por radiofrecuencia, son cada vez más utilizados en elementos y objetos de uso cotidiano de la ciudadanía, mediante la implantación en dichos objetos de una micro-emisora de radio (denominada ‘tag’ o etiqueta), que actualmente son lo suficientemente pequeñas como para tener la forma de etiquetas adhesivas.

Tanto porque se trata de una tecnología cada vez más barata, como porque los dispositivos, o etiquetas cada vez son más pequeños, comienza a ser habitual su uso en: **el etiquetado de prendas de ropa y calzado** – para prevenir hurtos y controlar stock –; **en tarjetas de transporte**; en **pasaportes**; sistemas para la **identificación de mascotas**; **como sistema de control de mercancías**; **pago automático en supermercados o en peajes**, **controles de acceso a eventos** deportivos o a zonas residenciales; así como en ámbitos como el sanitario, para el **seguimiento de pacientes o el control de medicamentos y muestras**.

Actualmente, la implantación de la tecnología RFID en España se produce en mayor medida en las grandes empresas. Así, mientras el nivel de adopción de esta tecnología por parte de las microempresas es del 0,8%, y entre **las pymes** el porcentaje se eleva a 3,1%, en el caso de las entidades de 10 a 49 empleados, y al 8,9% si el rango va de 50 a 249 trabajadores, en **grandes empresas** (más de 249 trabajadores) **el porcentaje es del 20,1%**.

Según se señala en el estudio elaborado por INTECO y la AEPD, por sectores, las empresas con actividades de **transporte y almacenamiento** son las que más utilizan la tecnología RFID. Le siguen el sector financiero, la informática, telecomunicaciones y audiovisuales y el comercio mayorista y minorista. En cuanto a las **aplicaciones mayoritarias** de la tecnología RFID, se centran -en el caso de las pymes y grandes empresas españolas- **en el seguimiento y control de la cadena de suministro y de inventarios, y la identificación de personas y control de accesos**. En el caso de las microempresas, con los sistemas de pago – Ej.: peaje de carreteras o transporte de pasajeros – y la identificación de productos.

Si bien, los datos descritos e incluidos en el estudio, ponen de manifiesto, que **entre las empresas españolas el uso de la tecnología RFID es aún incipiente**, para la AEPD e INTECO las aplicaciones actuales de la tecnología RFID son muchas, y las **previsiones apuntan a un crecimiento exponencial en los próximos años**.

Riesgos para la privacidad y seguridad

En la guía sobre seguridad y privacidad de la tecnología RFID se hace hincapié en que, si bien esta tecnología ofrece grandes oportunidades y facilidades- ya que se puede aplicar a multitud de campos y resulta muy útil para las empresas y los propios ciudadanos-, **a su vez puede plantear serios riesgos**, dado que pueden llegar a **informar de la localización, identidad e historial de un individuo**.

En este sentido, en el apartado dedicado a riesgos y amenazas, ambas instituciones **advierten de la existencia de importantes riesgos para la privacidad y riesgos de seguridad**.

En cuanto a los primeros, éstos consisten en el **acceso no autorizado** a información personal de los usuarios, usando la tecnología RFID. En este ámbito, el principal ataque que puede sufrir la privacidad del usuario **es el intento de lectura de la información personal y privada almacenada en un dispositivo RFID bajo su posesión**. La Guía ilustra la problemática que puede plantearse en el **caso de una persona que** porte una prenda de un comercio – Ej.: prenda de ropa - que no haya inutilizado las etiquetas o pegatinas RFID, ya que éstas podrían ofrecer información capaz de elaborar un perfil con los gustos o aficiones de esa persona a partir de sus compras.

En este sentido, el estudio distingue entre las principales amenazas más relevantes para la privacidad:

1. **Accesos no permitidos a etiquetas:** Pueden contener datos personales de todo tipo.
2. **Rastreo de las personas y sus gustos, etc.:** Portando una etiqueta RFID una persona puede ser observada y clasificada.
3. **Uso de datos para el análisis de comportamientos individuales:** Usando la “*minería de datos*” se definen los perfiles de consumo basado en las preferencias de los clientes.

En cuanto a los **riesgos para la seguridad** estos son los riesgos que tienen que ver con ataques, o averías que afectan al servicio- interrumpiéndolo, alterándolo, o realizando algún tipo de fraude-, o con la utilización de la tecnología para acceder a información personal de los usuarios del sistema.

Se trata de **riesgos derivados de acciones encaminadas a deteriorar o aprovecharse del servicio de forma maliciosa**. Se persigue el beneficio económico o un deterioro del servicio prestado. La forma más simple de ataque es **evitar la comunicación entre la etiqueta y el lector**, pero existen otras, como:

1. **Aislamiento de etiquetas:** Impidiendo la comunicación lector-etiqueta, introduciendo la misma en una “*jaula de Faraday*”, o creando un campo electromagnético que interfiera con el creado por el lector.
2. **Suplantación:** Consiste en el envío de información falsa que parece ser válida.
3. **Inserción:** Busca la inhabilitación de lectores y otros elementos del sistema mediante la inserción de comandos ejecutables en la memoria de datos de una etiqueta.
4. **Desactivación o destrucción de etiquetas:** Consiste en deshabilitar las etiquetas RFID sometiéndolas a un fuerte campo electromagnético, inutilizando el sistema.
5. **Clonación de la tarjeta RFID:** A partir de la comunicación entre una etiqueta y el lector, se copian los datos y se replican en otra etiqueta RFID.

Recomendaciones y buenas prácticas

Frente a los riesgos descritos, la Guía incluye varios apartados específicos con **recomendaciones y buenas prácticas** dirigidas tanto a usuarios- que usan la tecnología RFID en tiendas de ropa como sistema antirrobo, en bibliotecas, o en sistemas de identificación personal, etc. – como a proveedores, **para que se asegure su correcta utilización y que se eviten situaciones de riesgo**.

Entre estas recomendaciones recogidas en el informe cabe destacar:

1. **Inutilización**, desactivación o destrucción de las etiquetas una vez se haya cumplido su misión.
2. **Notificar el uso de RFID.**
3. **No almacenar en los tags RFID información personal.**
4. **Dar a conocer** a los usuarios cuándo, dónde y por qué se va a leer una etiqueta.
5. **Utilización de etiquetas Watchdog: (en inglés “perro guardián”). Estas etiquetas informan de intentos de lectura y escritura que se hagan en su área de actuación.**
6. Ofrecer al usuario **facilidades para la retirada, destrucción o desactivación** de los dispositivos asociados a productos cuando va a abandonar las instalaciones.
7. **Cifrado:** Impidiendo que las partes no autorizadas puedan entender la información enviada utilizando técnicas de cifrado de la información.
8. **Autenticación:** Evitando así la falsificación de lectores o etiquetas, debiendo introducirse una clave secreta para validar la comunicación lector-etiqueta.

Llamamiento del Parlamento Europeo

El informe publicado hoy se suma al reciente llamamiento realizado el pasado mes de junio por el Parlamento Europeo (PE) para garantizar la privacidad y la protección de los datos ante el uso de estas tecnologías. El PE hacía este llamamiento mediante la aprobación de un informe en el que se sostiene, entre otras cuestiones, **la necesidad de establecer un marco jurídico europeo que garantice la privacidad de los ciudadanos en este ámbito**, y que los consumidores tengan derecho al silencio de los chips, es decir, "a interrumpir en cualquier momento **la conexión de los chips**".

http://www.europarl.europa.eu/news/expert/infopress_page/058-76045-165-06-25-909-20100614IPR76044-14-06-2010-2010-false/default_es.htm

https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/julio/Guia_RFID.pdf