



CENTRO DE ALTOS
ESTUDIOS UNIVERSITARIOS
CENTRO DE ALTOS
ESTUDIOS UNIVERSITÁRIOS



Agencia Española
de Cooperación
Internacional
para el Desarrollo

Proyecto Iberoamericano de Divulgación Científica Comunidad de Educadores Iberoamericanos para la Cultura Científica

ESTA ETIQUETA INTELIGENTE SIGUE TODOS SUS PASOS



REFERENCIA: 6MMG115

La sociedad digital



sociedad

Alarma científica por la pérdida de fitoplancton

Esta etiqueta inteligente sigue todos sus pasos

- Los dispositivos de radiofrecuencia presentes en los objetos de consumo podrían servir para espiar los hábitos del cliente
- Las instituciones temen los riesgos y estudian una regulación

RAQUEL SECO / ROSARIO G. GÓMEZ

Sirven para alertar de robos en las tiendas, para controlar las mercancías de un almacén o para pagar de forma automática en un peaje. Son las etiquetas inteligentes, pequeños chips adheridos a todo tipo de objetos que funcionan mediante radiofrecuencias: desde bolsos hasta pasaportes, pasando por medicamentos o entradas para el fútbol. Su uso sin control ha sido puesto en cuarentena por las autoridades de protección de datos. Se quejan de que pueden invadir la privacidad y poner en riesgo la seguridad de los ciudadanos al poner al descubierto datos personales.

Estos artilugios funcionan mediante tecnología RFID (etiquetas de identificación por radiofrecuencia) y son cada vez más frecuentes en la vida cotidiana. Llevan incorporada una microemisor de radio que en la mayoría de los casos pasa inadvertida. Los consumidores pueden llevarla conectada sin enterarse de que van dejando un rastro sobre sus gustos y comportamientos.

Son un perfecto chivato. Aunque hay que distinguir, al menos, entre dos tipos de *tags* o etiquetas: las pasivas, que emiten señales solo cuando entran en el campo de acción de un lector, y las activas. El campo de alcance de las primeras varía, depen-

Esta nueva tecnología almacena datos en un chip minúsculo

El 20% de las grandes empresas ya utiliza estos artilugios

diendo de muchos factores, entre unos pocos milímetros y los siete metros. Las activas, por su parte, emiten señales todo el día (igual que un teléfono móvil, por ejemplo) y son mucho más caras y menos frecuentes. Se encuentran, por ejemplo, en los peajes automáticos de las autopistas. Se trata de etiquetas inteligentes que almacenan información en un chip de minúsculo

Riesgos para los consumidores

- **Accesos no permitidos a las etiquetas.** Las tarjetas RFID pueden contener datos personales (nombres, fechas de nacimiento, direcciones...) o tenerlos asociados a un sistema central. El ataque puede dirigirse contra ambos.
- **Rastreo.** Una etiqueta RFID que contenga datos personales y sea utilizada para pagar compras, transportes públicos, accesos a recintos, etcétera, podría servir también para observar y clasificar a un consumidor según sus gustos, edad y otras características.
- **Análisis de comportamientos.** Empleando técnicas de *minería de datos* (extracción de información a partir de las bases de datos), se pueden analizar comportamientos individuales y así definir perfiles de consumo para diseñar y orientar las estrategias publicitarias de las empresas.
- **Aislamiento de etiquetas.** Consiste en el bloqueo de la comunicación entre lector y etiqueta, mediante, por ejemplo, una *jaula de Faraday* o revestimiento metálico que impide que penetren las ondas de radio.
- **Saturación del servicio.** Se satura el sistema enviando de forma masiva más datos de los que este es capaz de procesar. Invalida el sistema para la detección de etiquetas, con lo que los objetos etiquetados escapan al control del sistema. Puede ser utilizado para la sustracción de mercancía a pequeña o gran escala.
- **Inutilización de las tarjetas.** El atacante puede inhabilitar las etiquetas sometiéndolas a un fuerte campo electromagnético.
- **Suplantación.** Consiste en el envío de información falsa, por ejemplo, sustituyendo una tarjeta RFID por otra para comprar productos al precio de otros más baratos.
- **Inserción.** Se insertan comandos ejecutables en la memoria de datos de una etiqueta donde habitualmente se esperan datos. Los comandos pueden inhabilitar lectores y otros elementos del sistema para desactivar el sistema permitiendo algún tipo de fraude, o una denegación de servicio.
- **Repetición.** El atacante envía al lector RFID una señal que reproduce la de una etiqueta válida, suplantando la identidad.
- **Ataque 'Man in the Middle'.** El atacante interviene en la comunicación entre dispositivo y lector, reemplazando a una de las dos partes. De esta manera puede interceptar información.
- **Clonación de la tarjeta RFID.** A partir de la comunicación entre una etiqueta y el lector, se copian dichos datos y se replican en otra etiqueta RFID para ser utilizados posteriormente.

tamaño. Un lector permite identificar, a distancia, cualquier producto.

El abaratamiento de costes ha hecho que cada vez proliferen más estos sistemas. En España se calcula que el 3% de las pequeñas y medianas empresas tienen instaladas esta modalidad de etiquetas mientras que en las grandes compañías el porcentaje se eleva al 20%. Según un estudio

elaborado por el Instituto Nacional de Tecnología de la Comunicación (Inteco), las empresas dedicadas al transporte y almacenamiento son las que más los emplean. Pero su uso está en plena expansión en otros sectores, como la informática o el comercio.

El Parlamento Europeo ha alertado sobre ellos. El pasado mes de junio instó a los Estados a poner en marcha mecanismos

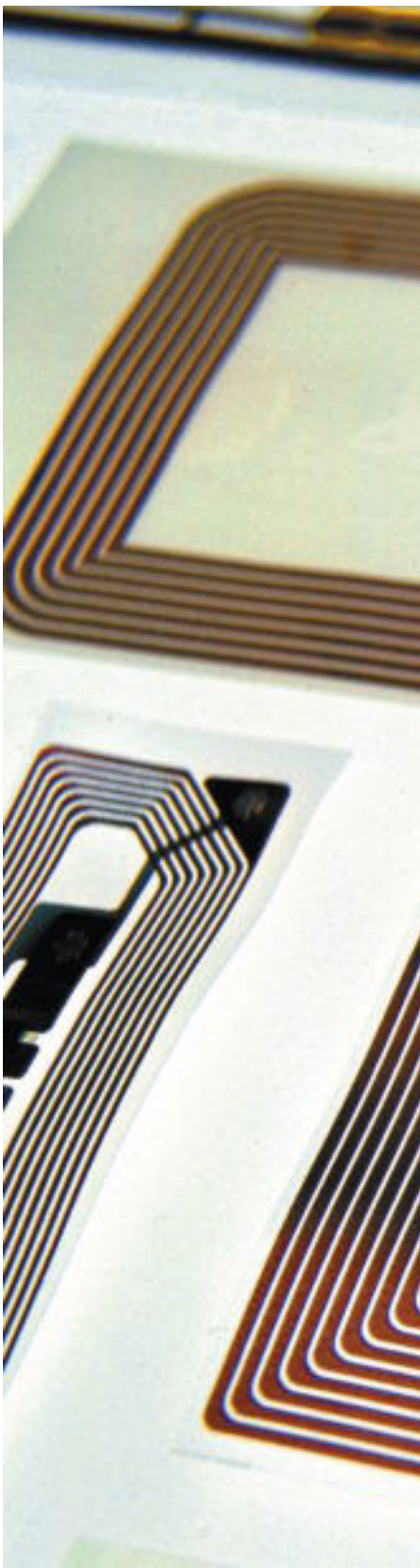
para que el uso de estos artilugios garantice la privacidad y la protección de datos de los ciudadanos. Para preservar los derechos de los usuarios, ese organismo apuesta por crear un marco jurídico europeo que garantice la privacidad de los ciudadanos, y en el que los consumidores tengan derecho a interrumpir en cualquier momento la conexión a estos chips.

La Unión Europea, de hecho, pidió a finales de 2009 a tres entidades europeas de normalización (Celenec, CEN y ETSI) un estudio sobre la posible regularización para proteger al consumidor final. Actualmente una comisión estudia la creación de un logo que identifique la tecnología RFID —de la misma forma que ahora se indica la presencia de cámaras de vigilancia— y se está debatiendo el establecimiento de niveles de intrusión en la privacidad, según Paloma Llana, abogada especializada en nuevas tecnologías.

La industria, por su parte, defiende las utilidades de esta tecnología y niega que pueda llegar a emplearse para intromisiones en la intimidad del consumidor. En opinión de Sergi Cardona, responsable de RFID en la Asociación Española de Codificación Comercial (AECOC), se suele dar protagonismo al “mal uso” de los sistemas de identificación de radiofrecuencia pese a que es “el mismo que se puede dar a cualquier tecnología”.

Aplicando las recomendaciones europeas (desactivando por defecto el *tag* en el punto de venta a no ser que el usuario indique específicamente lo contrario, por ejemplo) no debería haber inconvenientes ni se debería desatpar ningún dato personal del cliente, para Cardona. Además, de este modo se sacaría partido a los beneficios del RFID “consiguiendo una gestión empresarial más eficiente, ofreciendo al cliente más facilidades en el momento de pago...”

Pero los riesgos están ahí. La Agencia Española de Protección de Datos, especialmente alerta a cualquier posible vulneración de la privacidad, ha lanzado la voz de alarma. Advierte de que, pese a las bondades que puedan tener estos mecanismos, es necesario que se exijan garantías para prevenir los efectos perversos. Para evitar riesgos, la Agencia de Protección de Datos y el



Las etiquetas inteligentes pueden almacenar información personal de los usuarios. / GETTY IMAGES

Instituto Nacional de Tecnologías de la Comunicación han editado una guía para que el usuario pueda defenderse de estos supuestos “perros guardianes”. Aconsejan que se inutilicen, desactiven o destruyan cuando el usuario haya efectuado una compra en una tienda y, en todo caso, creen necesario que el ciudadano sea informado del uso de estos artilugios. Se evitaría así que algunos objetos, un bolso, por ejemplo, pitaran al pasar por un establecimiento para alarma y sorpresa de su propietaria, como ha ocurrido en determinadas tiendas de Madrid. No obstante, desde AECOC insisten en que las utilidades de esas etiquetas antihurto son “muy diferen-



sociedad

El cannabis, en una píldora para la esclerosis



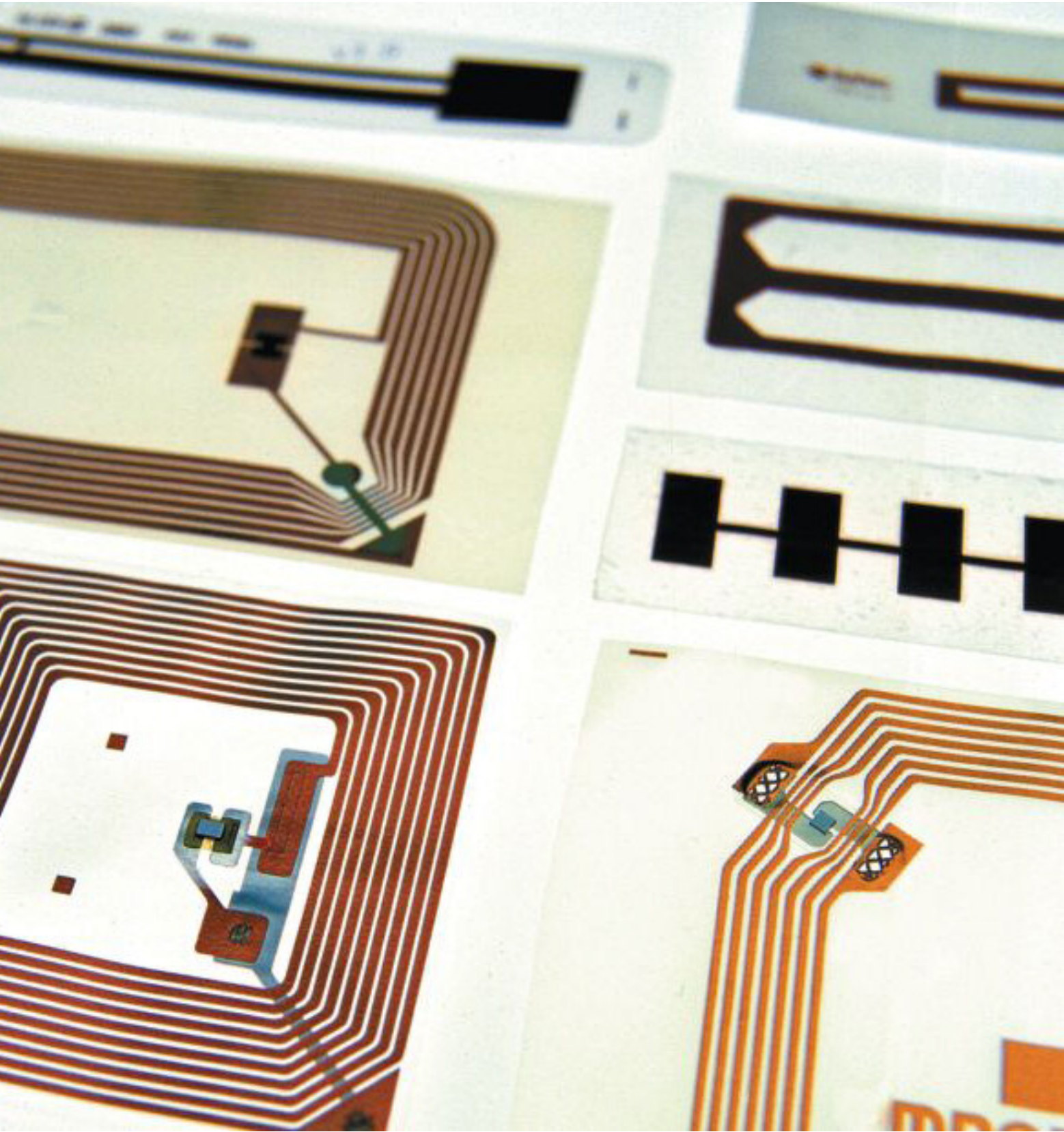
deportes

Raúl llega a Alemania como símbolo de casta



revista

La hora de Rihm en el festival de Salzburgo



tes” de las etiquetas RFID. Aunque ambos dispositivos se basan en los sistemas de radiofrecuencia, según esta asociación, el chip antirrobo no identifica en modo alguno el artículo, con lo que no compromete la privacidad del consumidor.

El sistema RFID —al que los expertos denominan el *Internet de las cosas*— permite vincular los objetos que se mueven, identificarlos y controlarlos. Pueden llegar a dar información suficiente para la localización de una persona. “Entre las empresas españolas, el uso es todavía incipiente, pero las previsiones apuntan a un crecimiento exponencial en los próximos años”.

Aunque también pueden ser de uso personal. Los padres, por ejemplo, pueden instalar estos dispositivos en pulseras o en prendas de ropa o bajo la piel para tener localizados minuto a minuto a sus hijos. Algunos hospitales, como el Clínic de Barcelo-

Las compras de una persona dicen mucho de su perfil y aficiones

Los expertos definen esta nueva red como el ‘Internet de las cosas’

na, han puesto en marcha un sistema de identificación y seguimiento de sus pacientes por radiofrecuencia. Con esta fórmula persiguen mejorar la seguridad y calidad asistenciales de los pacientes.

Como todo, la tecnología tiene dos caras. Pablo Sancho, director comercial de Asís Consultores —que se encarga de implantar estas etiquetas, por ejemplo, en la-

vanderías industriales— destaca que la identificación y la preparación logística de una sola prenda con código de barras tarda 16 segundos, mientras que con *tags* se gestionan hasta 150 prendas en unos 10 segundos. “El RFID es el futuro”, asegura Sancho, y su uso no supondrá un problema siempre que “no se grabe nada en el *tag*, sino en una base de datos local que solo las personas autorizadas puedan consultar”. Además, recalca que “a nivel de privacidad de la información, quizá está en una posición más vulnerable el usuario que entra a ver cualquier información vía Bluetooth en su móvil” puesto que la información en el RFID va “encriptada y codificada”.

¿Pueden estos dispositivos transmitir algún tipo de información personal? “Solamente podrían hacerlo, quizá, los de tipo activo. Y en caso de que lo hicieran los pasivos, siempre transmitirían información que

El RFID se ve como el futuro porque es más eficaz que el código de barras

Los padres podrían utilizar las etiquetas para seguir a sus hijos

tú hayas autorizado. Además, previamente esa información está codificada y almacenada en una base de datos. No tengo ningún cliente que haya grabado información relevante en el *tag*”, asegura Sancho.

Para Protección de Datos, el principal ataque que puede sufrir la privacidad del usuario es el intento de lectura de la información personal y privada alma-

cenada en estos dispositivos. Y pone como ejemplo las pegatinas adheridas a la ropa: “Pueden ofrecer información capaz de elaborar un perfil con los gustos o aficiones de una persona a partir de sus compras”.

Aun con un mal uso, la información delicada “no está específicamente en la tarjeta, se necesitaría acceder a un sistema de información”, replica Cardona.

Daniel Alguacil, editor del portal especializado RFID-Spain, añade que reunir datos que puedan llegar a identificar a un consumidor “requeriría una extraordinaria universalización, una implementación a nivel global que a día de hoy no existe”. Además, asegura que los “hipotéticos” riesgos para la intimidad que según algunos implica el RFID no son comparables a las ventajas del sistema: “Posibilita la reducción de precios, genera muchísimos puestos de trabajo, aumenta la competitividad de las empresas...”.

Existen interminables debates entre defensores y detractores. Fuentes de la industria descartan que la distancia de lectura de las tarjetas pueda suponer un factor de riesgo (“hay que estar bastante cerca” para leer una tarjeta pasiva, según Sergi Cardona), mientras que la percepción generalizada se inclina porque “pueden ser leídas a distintas distancias y eso puede suponer un problema”, según Llaneza. Además, para la abogada, el problema principal se encuentra en el “tipo de información que llevan dentro y en la combinación que se pueda hacer con otro tipo de etiquetas”.

Además, señala Llaneza, los lectores de etiquetas pueden estar en cualquier parte. “Imagínate que llevas una cartera que has comprado en una gran superficie. En ella llevas el nuevo pasaporte europeo —que lleva una etiqueta RFID dentro—, y una medicación identificada con este mismo sistema. Al pasar por el lector de la gran superficie, o por un lector pirata, alguien podría leer todo lo que llevas en el bolso y saber así si quieren robarte o no”. En cuanto al uso no delictivo, los expertos alertan de que los comercios podrían llegar a averiguar el perfil del cliente que entra por la puerta: ¿está enfermo? ¿qué productos compra?.

“La gran cuestión, según Llaneza”, es “qué información va incluida en la etiqueta RFID”. ¿Datos personales, información sobre los hábitos de consumo y estilo de vida pero sin nombre ni apellidos...?”. Los expertos exigen que se asegure la codificación de la información, que se asegure que las redes de comunicación estén totalmente protegidas para evitar el pirateo y que las etiquetas no identifiquen al usuario final.



CENTRO DE ALTOS
ESTUDIOS UNIVERSITARIOS
CENTRO DE ALTOS
ESTUDOS UNIVERSITÁRIOS



Agencia Española
de Cooperación
Internacional
para el Desarrollo

Proyecto Iberoamericano de Divulgación Científica
Comunidad de Educadores Iberoamericanos para la Cultura Científica

Ficha de catalogación

Título:	Esta etiqueta inteligente sigue todos sus pasos	
Autor:	Raquel Seco / Rosario G. Gómez	
Fuente:	<i>El País</i> (España)	
Resumen:	Las redes digitales plantean a veces problemas en relación con la privacidad de los hábitos de las personas. Pero también los propios objetos que consumimos pueden servir para rastrear nuestros comportamientos. Las etiquetas de identificación por radiofrecuencia que llevan incorporados muchos productos como sistema de protección antirrobo constituyen una verdadera Internet de las cosas que permite obtener información más allá del lugar en el que un producto es adquirido. Las ventajas de poder conocer dónde están las cosas pueden tener como contrapartida los inconvenientes del control sobre lo que las personas hacen con ellas.	
Fecha de publicación:	29/07/10	
Formato	☐	Noticia
	☒	Reportaje
	☐	Entrevista
	☐	Artículo de opinión
Contenedor:	☐	1. Los retos de la salud y la alimentación
	☐	2. Los desafíos ambientales
	☐	3. Las nuevas fronteras de la materia y la energía
	☐	4. La conquista del espacio
	☐	5. El hábitat humano
	☒	6. La sociedad digital
	☐	7. Otros temas de cultura científica
Referencia:	6MMG115	



CENTRO DE ALTOS
ESTUDIOS UNIVERSITARIOS
CENTRO DE ALTOS
ESTUDIOS UNIVERSITÁRIOS



Agencia Española
de Cooperación
Internacional
para el Desarrollo

Proyecto Iberoamericano de Divulgación Científica
Comunidad de Educadores Iberoamericanos para la Cultura Científica

Propuesta didáctica

Actividades para el alumnado

1. Señala cuáles de las siguientes afirmaciones son verdaderas y cuáles falsas teniendo en cuenta lo que se dice en el texto sobre las etiquetas digitales y la privacidad:

1. Los chips de radiofrecuencia insertados en los objetos tienen más usos que prevenir los robos.	V	F
2. La tecnología RFID permite que los objetos lleven incorporada una microemisora de radio.	V	F
3. Las etiquetas pasivas sólo dan información cuando entran en el campo de acción de un lector, mientras que las etiquetas activas emiten su señal continuamente.	V	F
4. En las empresas dedicadas al transporte y almacenamiento no llega al 3% el uso de este tipo de dispositivos.	V	F
5. La jaula de Faraday impide el intercambio de información entre el lector y la tarjeta.	V	F
6. Usando técnicas de minería de datos es posible orientar las estrategias publicitarias de las empresas.	V	F
7. Se conoce como Internet de las cosas a los sistemas que permiten enviar objetos por correo electrónico utilizando redes RFID.	V	F
8. La información en RFID resulta más vulnerable y accesible que la que se envía vía bluetooth.	V	F
9. Al no llevar información sobre la identidad del comprador, la información de las etiquetas RFID no plantea ningún problema para la privacidad de las personas.	V	F
10. Es técnicamente posible obtener información personal incluida en objetos que están dentro de un bolso sin tener que abrirlo.	V	F

2. ¿En qué consiste la tecnología RFID?

3. ¿En que se diferencian las etiquetas pasivas y las activas?

4. ¿Haz una lista sobre los contextos o situaciones en los que se utilizan etiquetas RFID? Selecciona algunas de ellas y comenta qué efectos tendría la repentina desaparición de estos sistemas.

5. Selecciona tres de los riesgos para los consumidores derivados del uso de estos sistemas de control y comenta, poniendo algunos ejemplos, los problemas que plantean.

6. ¿Qué es la Internet de las cosas? ¿Qué ventajas tiene? ¿Debería tener limitaciones en algunos casos o con algunas cosas?

7. ¿Crees que los padres deberían poder usar sistemas RFID para saber en todo momento dónde se encuentran sus hijos? Hazte esta misma pregunta sobre otros posibles usuarios de estas tecnologías: empresarios y trabajadores, directores de centros educativos y alumnos, policía y personas en libertad condicional, etc.

8. Sobre cada frase de la siguiente quiniela señala tu postura de acuerdo, desacuerdo o duda. Selecciona dos o tres frases de la quiniela que te parezcan destacables (estés o no de acuerdo con lo que dicen) y redacta un comentario sobre ellas.

Quiniela sobre la privacidad y las etiquetas digitales			
1. El control y la vigilancia siempre son positivos.	1	X	2
2. No merece la pena que la garantía de la seguridad de las personas sea a costa de su libertad.	1	X	2
3. Estaría bien que la administración de la hacienda pública tuviera sistemas para conocer en todo momento todo el dinero que ingresan y gastan las personas, así nadie podría defraudar impuestos.	1	X	2
4. Las tecnologías RFID hacen que haya menos trabajo porque son necesarios menos trabajadores para controlar los productos.	1	X	2
5. Me gustaría tener todas mis cosas controladas con tecnologías RFID para saber en todo momento dónde están.	1	X	2
6. Me gustaría tener a todos mis amigos controlados con tecnologías RFID para saber en todo momento dónde están.	1	X	2
7. Sería bueno que los matrimonios o las parejas sentimentales estables contaran con pulseras provistas de este tipo de tecnologías para que cada uno pudiera controlar en todo momento lo que hace el otro.	1	X	2
8. Si no hay limitaciones a la Internet de las palabras y las ideas no hay motivos para que las tenga la Internet de las cosas.	1	X	2
9. Me parece bien que haya en distintos lugares cámaras que graven todo lo que hacen las personas fuera de sus casas.	1	X	2
10. La privacidad es un mito, todo lo que hacen las personas debería ser público y publicable.	1	X	2

1: De acuerdo; **X:** En duda; **2:** En desacuerdo



CENTRO DE ALTOS
ESTUDIOS UNIVERSITARIOS
CENTRO DE ALTOS
ESTUDIOS UNIVERSITÁRIOS



Proyecto Iberoamericano de Divulgación Científica
Comunidad de Educadores Iberoamericanos para la Cultura Científica

Propuesta didáctica
Sugerencias para el profesorado

- De entre las actividades propuestas conviene elegir cuáles se adaptan mejor al grupo y a sus intereses. En todo caso, antes de proponer la realización de las actividades se recomienda una lectura atenta del texto.
- La actividad 1 facilita el análisis del contenido del texto. Su revisión permitirá aclararlo y resolver posibles dudas. Las actividades 2 y 3 piden que se expliquen algunos de los conceptos principales que aparecen en el reportaje. La actividad 4 sugiere enumerar situaciones en las que se utilizan tecnologías RFID valorando, a partir de las consecuencias de su hipotética desaparición, su importancia en esos ámbitos. La actividad 5 propone comentar algunos de los riesgos que pudieran plantear este tipo de sistemas. La actividad 6 se centra en la Internet de las cosas, pidiendo una caracterización de ese concepto y una valoración sobre sus ventajas y los límites que, eventualmente, debería tener. En la actividad 7 se plantea un conflicto de derechos entre personas que se encuentran en situaciones de relación asimétrica a propósito del uso de ese tipo de sistemas y los límites que el mismo debería tener. La actividad 8 plantea diversas cuestiones valorativas que podrán generar cierta controversia en relación con esos temas.
- Aunque las actividades propuestas están redactadas para ser realizadas individualmente, varias de ellas son especialmente propicias para ser desarrolladas en equipo o incluso en debate abierto con toda la clase. Es especialmente interesante, en este sentido, compartir los trabajos sobre las actividades 4, 7 y 8.
- Podría ser oportuno registrar algunos de los comentarios y las respuestas que aparecen en el aula en torno a las actividades 7 y 8. Tales apreciaciones pueden ser útiles para entender las percepciones que los jóvenes tienen acerca de las ventajas y límites de los sistemas tecnológicos de control y sobre el valor que asignan a la privacidad.