*Carlos Enrile D'Outreligne**

INTERNET DE LAS COSAS
Todo un mundo por regular

Una nueva tecnología de captación de datos está emergiendo y va a tener en los próximos años un impacto en las relaciones humanas y empresariales. Ese impacto puede incidir en los derechos fundamentales del individuo por lo que el legislador debe asegurar la protección de esos derechos ante las nuevas situaciones.

Asimismo es necesario garantizar la protección de los datos recopilados ante los ataques de la ciberdelincuencia. Por otra parte, las grandes empresas de Internet tienen diseñada su estrategia para ser líderes en las novedades que creará el «Internet de las cosas».

Palabras clave: tecnología, Internet, derechos fundamentales, ciberdelincuencia, comercio electrónico.
Clasificación JEL: K14, K42.

1. Introducción

Hasta hace relativamente poco tiempo, el mundo de los drones era un mundo de juguetes, en algunos casos de juguetes caros, pero en todo caso no más que meros juguetes.

Con el tiempo han evolucionado y se han ido perfeccionando de modo que ahora son verdaderos mini-helicópteros o mini-aviones que tienen muchas utilidades en campos muy diversos; como, por ejemplo, el uso para la fotografía y el vídeo aéreos, la vigilancia aérea o también están siendo utilizados como sistemas de monitorización en el mundo de la agricultura.

Con esta novedad tecnológica surgió el problema de la invasión en la vida cotidiana de las personas. Los drones comenzaron a sobrevolar cerca de los aeropuertos; por encima de las viviendas, por encima de espacios que por tierra estaban restringidos, tales como las infraestructuras críticas; sobrevolando las centrales nucleares.

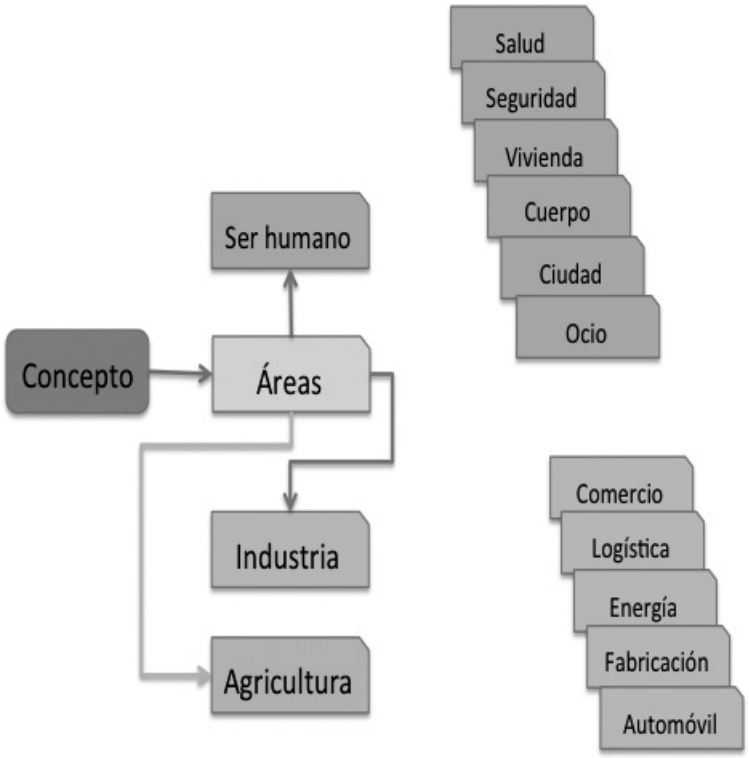
Como consecuencia de todo esto, la aparición de estos aparatos en el cielo ha obligado al legislador a tener que intervenir, por un lado, para controlar el acceso al espacio aéreo que tiene el piloto de dron y, por otro, para restringir el acceso en el espacio siempre y cuando colisione con otro tipo de derechos y servicios; tales como el derecho a la intimidad o el servicio de tráfico aéreo.

El tema que nos ocupa hoy es que el Internet de las cosas va a crear nuevos problemas. Aquí también el legislador, en defensa del ciudadano y, en concreto, de su privacidad y de su seguridad, deberá legislar para que este nuevo mundo no colisione con los derechos del ciudadano y de modo especial con aquellos protegidos como derechos fundamentales.

Para terminar esta breve historia, recordamos que la Unión Europea tiene previsto imponer en 2016 una legislación unificada respecto a la operación de drones para mantener la unidad de mercado. En ▷

* Consultor y formador en Internet para la empresa exportadora.
Versión de noviembre de 2015.

ESQUEMA 1
ESBOZO DE CLASIFICACIÓN NO EXHAUSTIVA DE LAS ÁREAS AFECTADAS POR EL INTERNET DE LAS COSAS



Fuente: elaboración propia.

este artículo vamos a sugerir el mismo tratamiento para el Internet de las cosas.

2. Concepto de «Internet de las cosas»

El concepto de «Internet de las cosas» en realidad hace referencia al concepto de monitorización remota con detectores adaptados al efecto. Recibe este nombre porque el detector puede estar identificado con una dirección IP y la transmisión de los datos monitorizados puede hacerse por la infraestructura de Internet.

Ponemos un ejemplo: un termostato instalado en una vivienda transmite al propietario y a un tercero datos sobre temperatura, y tanto el propietario como el tercero pueden dar órdenes al termostato por control remoto para modificar la temperatura, en este ejemplo el termostato es de la marca Nest[1] que a su vez es propiedad de Google, y permite al propietario de la vivienda conocer y modificar la temperatura a través del móvil. Por su parte, los datos pueden llegar a Google que es quien envía al móvil del propietario resúmenes estadísticos y propuestas para el ahorro en el consumo de calefacción. Pero podemos ampliar el concepto a todo aquel aparato detector que monitoriza unos datos que serán enviados a una entidad o usuario para su gestión y análisis.

Y en esta definición más amplia entrarían otros ejemplos:

- El sistema de geolocalización de un teléfono móvil *(#FindMyIphone*, Administrador de dispositivos Android, etcétera).
- El sistema de alarma del hogar, comercio o fábrica.
- El contador digital de telegestión de la electricidad.

3. Clasificación

Si bien las áreas que abarca el Internet de las cosas es enorme, nos vamos a ceñir a aquellas ▷

[1] *www.nest.com*

situaciones que afectan directamente al ser humano como portador de derechos fundamentales.

3.1. Internet de las cosas y el ser humano

Hay una serie de soluciones que se están planteando que van a permitir obtener más datos del individuo, datos de todo tipo que necesitan ser regulados.

Salud

Nos referimos a todo tipo de aplicaciones que monitoricen remotamente la salud del individuo sea por ejemplo el nivel de azúcar, el ritmo cardíaco, etcétera.

Esos datos se envían al centro de salud y los responsables sanitarios realizan las actuaciones necesarias según las medidas recibidas del paciente.

Seguridad

Control de presencia, control de accesos, incidencias. El ejemplo típico es la alarma que muchas familias tiene instalada en su casa.

Vivienda

Concepto conocido como domótica: los sensores controlan múltiples aspectos del hogar entre los que están la temperatura, apertura y cierre de puertas, suministro de insumos necesarios, etcétera.

Cuerpo humano

Aquí incluimos un concepto anglosajón conocido como *wearables*, es decir, aquella ropa o instrumentos en contacto con el ser humano y que sirven para mejorar su confort o su salud desde un aspecto no médico. Estarían incluidos en esta categoría los relojes y pulseras que se utilizan para monitorizar el ejercicio físico, la ropa de moda que contiene algunos de estos sensores, las gafas de realidad aumentada como las que están desarrollando Google y que venderán el grupo Luxottica[2], o las gafas de sol que no se pierden al estar geoposicionadas, de *Tzukuri.com*. También se incluyen en esta categoría las aplicaciones para teléfono móvil que monitorizan a los deportistas o a aquellos que están siguiendo una dieta.

Ciudad

Las *smartcities* o ciudades conectadas recogen datos de utilidad para la gestión de la ciudad y para el confort del ciudadano, tales como la ubicación de plazas de aparcamiento libre, gestión de flotas de transporte público o predicción de zonas potencialmente delictivas.

Ocio

Dentro de esta categoría están una gran variedad de situaciones que van desde los videojuegos en red hasta gafas de realidad virtual para interactuar con otras personas.

Industria y agricultura

Debido a las limitaciones de espacio de este artículo no podemos entrar en las áreas del Internet de las cosas orientados a la agricultura y a la industria. En ambos casos los cambios que puede generar esta nueva tecnología son impresionantes y animamos al lector a continuar investigando. Señalar, por lo menos, que aparece un nuevo y emocionante campo en el cual las máquinas se comunican entre sí (M2M, Machine to Machine communications). Solo un pequeño apunte como ejemplo: en tiempos recientes está apareciendo en televisión un anuncio de un automóvil que tiene un accidente y que por vía telemática el fabricante conoce el hecho, conoce la ubicación y envía una ambulancia para socorrer a los accidentados. Todo ello es posible gracias al Internet de las cosas. ▷

[2] *http://www.luxottica.com/en/luxottica-google-glass*

4. Medios para la transmisión de los datos generados

Como después comentaremos los posibles problemas legales que aparecen con el Internet de las cosas, es interesante indicar los distintos medios que existen para la transmisión de los datos.

Transmisión de los datos por Internet

Un medio de transmisión obvio va a ser el sistema de telecomunicaciones existente en Internet. Así cuando un sensor de temperatura avisa al propietario y al gestor de la información acerca de cambios en la misma, estos datos normalmente van a viajar por la infraestructura de Internet: el sensor, que está identificado con un número IP único, utilizará la red wifi de la vivienda para transmitir los datos a los respectivos destinatarios. Es por ello que en un principio a este conjunto de tecnologías de monitorización remota se le llamó el Internet de las cosas (*Internet of Things*). Más adelante valoraremos el papel que juega la empresa transmisora de datos en el control de los mismos.

Pero existen otras tecnologías que permiten la transmisión de estos datos. El paquete de información enviado por el sensor es muy pequeño, por lo que prácticamente su consumo de ancho de banda es ínfimo. Por ello existen otro tipo de soluciones para transmitir los datos. Veamos algunas.

Transmisión por la red de telefonía móvil

Esta solución es usada por defecto en las alarmas de hogar. En caso de inhibición maliciosa se activan otros sistemas.

Transmisión por la red eléctrica

Esta red de transmisiones es obviamente utilizada por las compañías eléctricas para recibir la medida de consumo de los contadores digitales con telemedición. En el caso de España el legislador tiene previsto que todo el parque de contadores sea digital en el año 2018. Nada impide que las compañías eléctricas puedan ofrecer su red a empresas que aporten soluciones relacionadas con el Internet de las cosas, o que incluso las mismas compañías eléctricas ofrezcan estos servicios.

Transmisión en muy baja frecuencia (*VLF, Very Low Frequency*)

Como los datos a transmitir ocupan muy poco espacio estos pueden ser enviados en muy baja frecuencia con las ventajas que ello supone. Estas frecuencias son libres, es decir, no necesitan de autorización administrativa ni compra de licencia para su uso. La empresa Sigfox[3] es pionera en esta solución.

5. Propiedad, gestión y protección de los datos

Hasta ahora hemos descrito qué es, para qué sirve y cómo funciona el Internet de las cosas. Ahora vamos a ver qué problemas puede plantear con respecto a la protección de derechos del ciudadano.

El proceso completo de recogida de datos comienza con la medida de estos en el punto de origen, sea este el cuerpo humano, una vivienda o el sistema de reconocimiento de matrículas de automóvil de un ayuntamiento.

Luego continúa con el transporte de estos datos hasta destino y, por último, en destino una entidad se va a encargar de gestionar y analizar esos datos y obtener de ellos unos resultados que tendrán determinadas consecuencias.

En resumen tenemos tres momentos diferenciados:

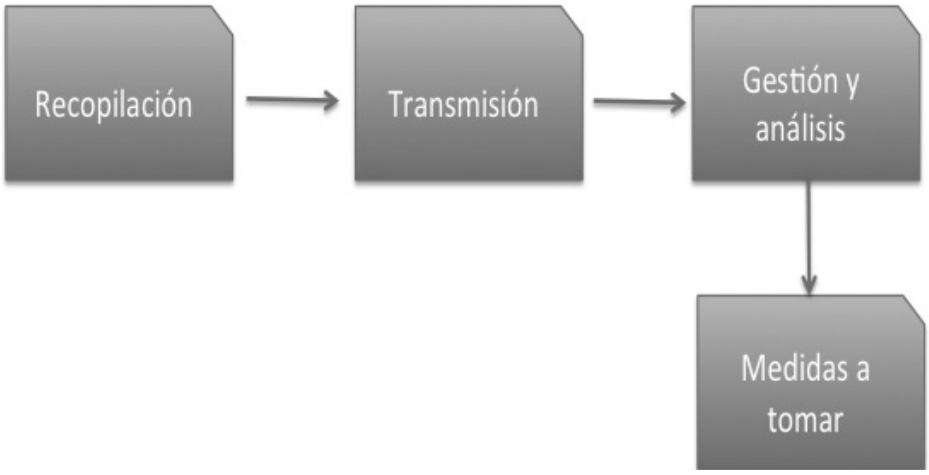
Obtención de datos.

Transporte de los datos.

Gestión y análisis de los datos. ▷

[3] *www.sigfox.com*

ESQUEMA 2
PROCESO



Fuente: elaboración propia.

Tenemos que tener en cuenta a varios intervinientes en todo el proceso, desde el origen al destino de los datos emitidos por el Internet de las cosas. La portadora o transmisora, empresa titular por la cual van a pasar los datos que generalmente va a ser una empresa de telecomunicaciones. La receptora que va a gestionar los datos los va a utilizar, en principio, en provecho del interesado.Y ,en su caso, el interesado.

Desde el punto de vista legal, aparecen las primeras preguntas:

¿La portadora debe permanecer neutra o tiene derecho al acceso a los datos?

¿Sería responsable la portadora por la rotura de la confidencialidad de las transmisiones?

¿La receptora debe o no compartir los datos con el usuario?

¿La receptora puede o no diseminar de manera gratuita o mediante pago los datos del usuario?

¿Qué datos del usuario se consideran confidenciales y protegidos y cuales no?

Algunos supuestos serían:

El destino de los datos tiene otros usos además del definido:

1. Las mediciones de consumo de energía recopiladas por las compañías eléctricas contienen información sobre aquellos horarios en los que el cliente se encuentra en su domicilio, ya que en ese momento suele realizarse un mayor consumo. En este caso la compañía eléctrica es propietaria del aparato que toma la medida, de la señal portadora de la transmisión (que es la propia red eléctrica) y del sistema de gestión y análisis de la información (análisis que será compartido con el cliente, con menor o mayor grado de detalle).

¿Puede la compañía eléctrica ceder a terceros los datos de cuándo está el cliente en casa u otros datos que se puedan obtener? Las empresas de *telemarketing* posiblemente pagarían por esa información.

2. El cliente dispone de un termostato con medición remota de la marca Nest. Al igual que en el caso anterior Google recoge las pautas de comportamiento del cliente y también sabe cuando éste está en casa.

¿Puede Google ceder a terceros los datos de cuándo está el cliente en casa? ¿Puede Google ceder a terceros información sobre el consumo para que estos hagan propuestas de ahorro?

3. El cliente utiliza *weareables* o su teléfono móvil para monitorizar su ejercicio físico. Estos datos se envían a la empresa que vendió el sistema para su gestión y análisis, de modo que el cliente conoce su rendimiento y cómo progresa. ▷

¿Puede la empresa vender a terceros datos de usuarios con una masa corporal o estilo de vida para que estos ofrezcan sus productos y servicios?

¿Durante cuánto tiempo puede la empresa almacenar esos datos?

4. Las empresas de Internet de las cosas relacionadas con la monitorización de la salud se ven obligadas a ceder al Estado los datos de los individuos para realizar perfiles de riesgo con objeto de modular el copago o las contribuciones al sistema nacional de salud.

¿Puede el Estado forzar esta cesión de datos?

5. Una empresa gestiona y analiza datos sobre la salud de un paciente gracias a un sensor instalado en este. ¿Quién es propietario de los datos? ¿quién y cómo puede ceder datos a terceros?¿el paciente?¿la empresa?¿puede ésta ceder los datos sin revelar la identidad del paciente?

El gestor de los datos es atacado por ciberdelincuentes que sustraen los mismos

En abril de 2014 los datos de 77 millones de usuarios de *Sony PlayStation* fueron sustraídos, incluyendo números de tarjetas de crédito. ¿Cuál es la responsabilidad del custodio de los datos?

5.1. Marco regulador en la Unión Europea

La protección de datos de carácter personal está regulada por la Directiva 95/46/CE y su transposición en el ordenamiento jurídico español con la Ley Orgánica 15/1999.

Asimismo está la Directiva sobre la privacidad y las comunicaciones electrónicas 2002/58/CE.

Es posible que a la luz de su articulado algunas de estas situaciones estén protegidas por la ley, pero es posible que otras no, ya que en el momento de su redacción alguno de los supuestos arriba mencionados no se contemplaban.

Además, la Directiva y la Ley Orgánica no serían de aplicación efectiva si los datos estuvieran físicamente ubicados fuera de la Unión Europea. La famosa «nube» no es más que una serie de centros de proceso de datos en los que se apilan miles de ordenadores, y si estos no están en territorio de la UE escaparían a su control.

La Comisión Europea está elaborando un proyecto de directiva de reforma y actualización de la protección de datos de carácter personal. Esta directiva deberá solucionar los problemas que genera el Internet de las cosas.

6. Ciberdelito

Como hemos visto, los datos se generan en el cuerpo o domicilio del usuario, se transfieren a través de una portadora y se entregan a la entidad gestora, que es quien va a realizar el análisis de los datos y quien va a tomar una serie de medidas en consecuencia.

La vulnerabilidad del proceso se encuentra en todos los pasos.

Quiebra de la protección de los contenidos en origen

El ciberdelincuente puede acceder a través de la red al dispositivo de medida y modificarlo, bien para recibir copia de sus lecturas, bien para enviar lecturas erróneas. En el área del Internet de las cosas industrial estas actuaciones son muy peligrosas ya que pueden afectar y comprometer a instalaciones críticas como generación y transporte de energía.

Con respecto al individuo, el ciberdelincuente puede comprometer su privacidad.

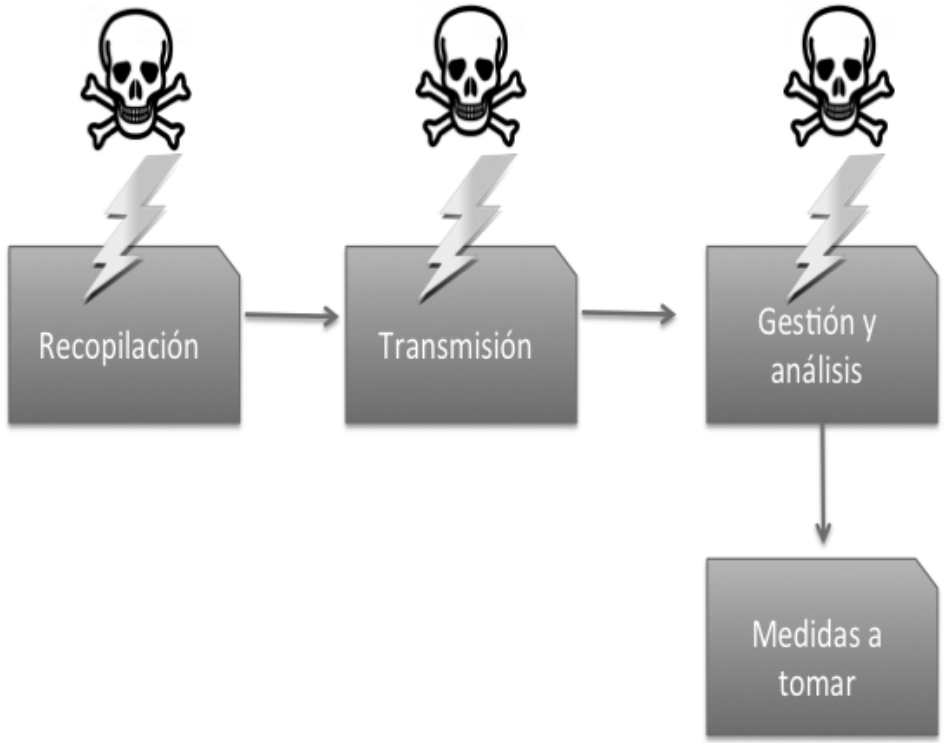
Quiebra de la protección de los contenidos durante la transmisión

El ciberdelincuente accede a la red de transmisión de datos y bien clona los contenidos y se aprovecha de ellos, bien los modifica con intenciones dañinas.

Quiebra de la protección de los contenidos en el destino

El ciberdelincuente accede a la base de datos y sustrae o modifica los mismos. ▷

ESQUEMA 3
VULNERABILIDAD DEL PROCESO



Fuente: elaboración propia.

De todo esto se desprende que es necesaria cierta formación en el usuario, así como una gran inversión por parte de los propietarios de las transmisiones y de los gestores de datos para intentar evitar los ataques de la ciberdelincuencia.

7. Estrategia de Google, Facebook y Amazon con respecto al Internet de las cosas

Como se puede inferir del artículo, el mundo del Internet de las cosas va a mover mucho dinero en los próximos años y además va a tener una importancia capital para el conocimiento de los parámetros de comportamiento de los usuarios.

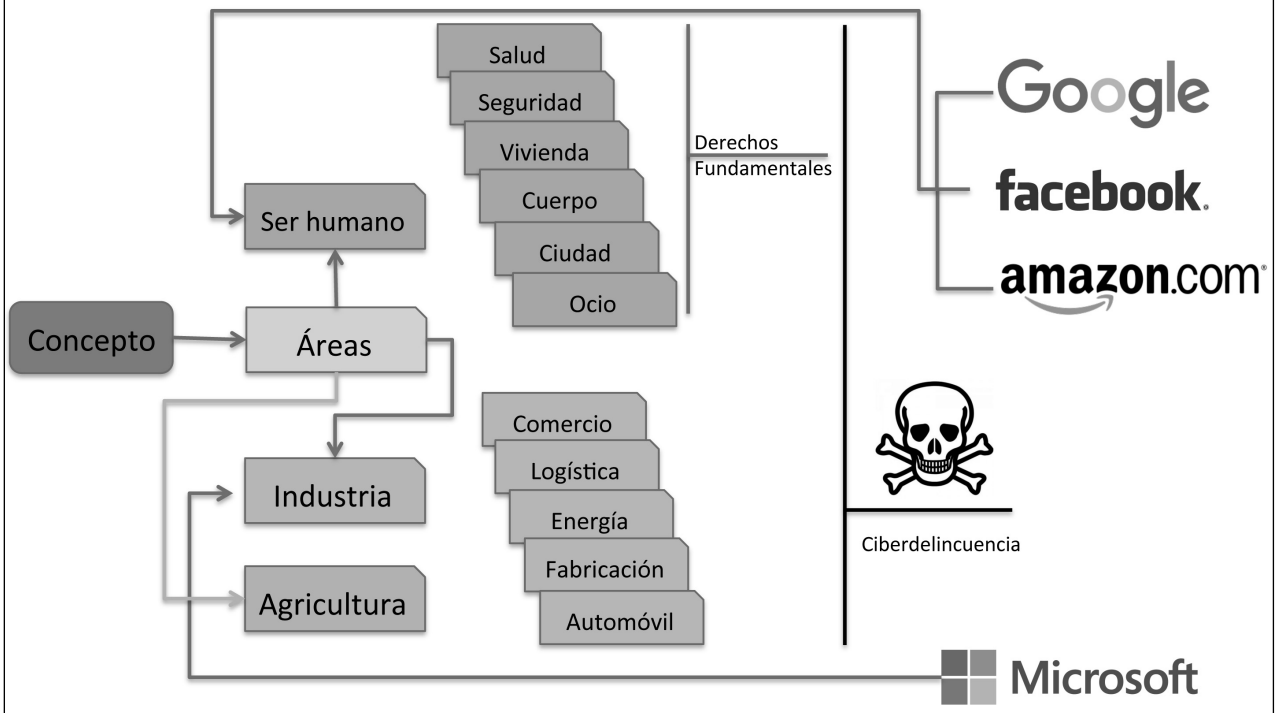
Por ello las grandes empresas de Internet ya han elaborado una estrategia para incorporar el Internet de las cosas a su evolución en el futuro próximo. En este artículo vamos a ver la estrategia de Google, de Facebook y de Amazon. Por falta de tiempo y espacio no trataremos de otras empresas con una visión interesante sobre el Internet de las cosas. Entre ellas está Microsoft que apuesta fuertemente por el Internet de las cosas dentro del mundo de la industria.

7.1. Google

Nest

Google tiene una visión muy ambiciosa. Ha comprado una empresa llamada Nest por 3.200 millones de dólares, luego la apuesta es fuerte. El producto estrella de Nest es un termostato que puede ser controlado a distancia desde el teléfono móvil. Así el usuario puede indicar al termostato remoto de Nest que debe ir incrementando la temperatura de la vivienda para cuando sus ocupantes lleguen a ella. Imaginemos que si cientos de miles de hogares tienen instalado este aparato Google puede saber si el propietario está ▷

ESQUEMA 4
ESTRATEGIAS DE GOOGLE, FACEBOOK Y AMAZON CON RESPECTO A INTERNET DE LAS COSAS



Fuente: elaboración propia.

o no en la vivienda según la temperatura programada, y ese dato tiene un valor comercial. Por ejemplo, es un dato que podría venderse a empresas de *telemarketing*. Estas empresas solo llamarían al hogar para ofrecer sus servicios siempre y cuando el propietario estuviera en él.

En la propia publicidad de la página de Nest presumen que el termostato sabe cuándo el usuario no está en casa. Obviamente este dato puede ser de interés para los ciberdelincuentes, ya que podrían interceptar las comunicaciones.

Google Glass

Podemos decir que el proyecto Google Glass también pertenece al Internet de las cosas, dentro de la categoría de *wearables.* En este caso, las gafas recogen datos ya que nos están geolocalizando continuamente y conocen nuestro ángulo de visión, por lo que nos van a mostrar contenidos contextuales con el alcance de nuestra vista. Google ha decidido parar el desarrollo del *hardware* pero continúa desarrollando el sistema operativo con el que quiere que las gafas de realidad virtual funcionen. Al ser las gafas un producto de moda, Google ha firmado un acuerdo con la multinacional italiana Luxottica, que es propietaria de las principales marcas de gafas. Con este acuerdo Luxottica pone la moda y Google pone la tecnología.

Google Brillo

Es el proyecto de Google de sistema operativo basado en Android para ser utilizado en el Internet de las cosas.

Facebook

Esta empresa ha conseguido conectar a miles de personas entre sí. Su nuevo reto consiste en conectar estas miles de personas con los objetos ▷

que los rodean y que pertenecen al Internet de las cosas.

Parse

Se trata de una plataforma de *«software* como servicio*»* (SaaS, Software as a Service) que permite a terceros desarrollar aplicaciones para distintas soluciones, incluidas aquellas para el Internet de las cosas. Parse ofrece kits de desarrollo de *software* para que terceros creen aplicaciones que funcionen en los microcontroladores que toman los datos. Parse funciona en la «nube» de Amazon, Amazon Web Service, que veremos más adelante.

Protogeo

Empresa de origen finlandés adquirida en 2014 y que se dedica a la generación de aplicaciones para móviles utilizadas para mejorar la forma física (*fitness*).

Amazon Echo

Esta herramienta es un asistente virtual que funciona por medio de comandos de voz. Este asistente, llamado *Alexa*, está conectado a Internet y contesta a todas aquellas preguntas con datos de los que obtiene respuesta en Internet; tales como el tiempo, las noticias, datos enciclopédicos, etcétera. La estrategia de Amazon consiste en que los usuarios que tengan este aparato en su casa y lo utilicen, además, para hacer pedidos a Amazon.

Así, por ejemplo, si es necesario un insumo, como puede ser una bombilla o un producto de cocina, se le puede ordenar al asistente virtual que lo incluya en la lista de pedidos para realizar a Amazon. Como es obvio, según Amazon ofrezca nuevos servicios, estos podrán solicitarse a través de este asistente virtual. Uno de los atractivos que tiene consiste en que se puede conectar a soluciones del Internet de las cosas, con lo que se le podría solicitar mediante comandos de voz que encienda o apague las luces o que abra o cierre las puertas automáticas.

Amazon Dash Button

Esta utilidad consiste en un pequeño botón que lleva el logotipo de un proveedor. Pongamos, por ejemplo, que el proveedor es un fabricante de jabón para lavadoras e instalamos el botón en nuestra lavadora. Cada vez que necesitemos jabón de lavadora bastará con pulsar una vez el botón para que Amazon tome nota del pedido. Por un lado, Amazon consigue fidelizar al cliente ya que el pedido se va a realizar con ellos y, por otro lado, invita a las marcas a participar y a tener sus propios botones para asegurarse que el pedido sea siempre de la misma marca.

AWS-IoT, Amazon Web Services Internet of Things

Consiste en una plataforma con una serie de servicios de software, almacenamiento y gestión de datos instalados en la infraestructura de Amazon y conocido como *software* en la nube o *cloud computing*. Amazon ofrece su infraestructura y su tecnología para que terceros gestionen en ella su Internet de las cosas.

En resumen, al igual que pasó con los drones, el Internet de las cosas puede aportar soluciones muy interesantes pero que, en todo caso, deberán someterse a un futuro marco normativo que ciña su utilización dentro del respeto a la privacidad y seguridad.

Bibliografía

[1] CONSTINE, J. (2014). *Visualizing 15 Years Of Acquisitions By Apple, Google, Yahoo, Amazon, And Facebook.* Disponible en*: http://techcrunch.com/2014/02/25/the-age-of-acquisitions/*

[2] G. CARR, N. (2011). *Superficiales: ¿qué está haciendo Internet con nuestras mentes?* Editorial Taurus.

[3] GREENGARD, S. (2013). *The Internet of Things*. Editorial The Mit Press Essential Knowledge. ▷

[4] MADISETTI, V. (2015). *Internet of Things. A Hands-On Approach*. Editorial Arshdeep Bahga.

[5] MC EWEN, A. y CASSIMALLY, H. (2015). *Internet de las cosas*. Editorial Anaya Multimedia

[6] SCHMIDT, E. (2014). *El Futuro Digita*l. Editorial Anaya Multimedia.

[7] SCOTT PEÑA, P. (2013). *Internet de las Cosas*. Editorial Anaya Multimedia.

[8] PEIRANO, M. (2014). *El pequeño libro rojo del activista en la red*. Editorial Roca.

[9] ROSE, D. (2015). *Enchanted Objects. The Future of Technology*. Editorial Tech Insider.