TITULO: INTERNET DE LAS COSAS: BENEFICIOS Y PRIVACIDAD, UN DIFÍCIL EQUILIBRIO.

AUTOR: ESTHER MARIA NODA CAMACHO

"***A medida que casa vez más dispositivos se vuelven más inteligentes, es esencial que sepamos tanto de ellos como ellos de nosotros-que entendamos qué información recogen y cómo esta siendo usada o compartida". EDITH RAMIREZ, Presidenta FTC (Federal Trade Comission, Noviembre 2013).***

El llamado "**Internet de las cosas**" es una de las revoluciones tecnológicas que empieza ya a ser una realidad en nuestras vidas cotidianas. ¡Y ha llegado para quedarse!

La revolución de internet supuso la interconexión de las personas, a través de instrumentos inteligentes, redes sociales, etc. Ahora entramos una nueva ola de internet: el internet de las cosas, donde además de las personas, los objetos y las cosas están interconectados.

El también conocido como IoT (Internet of Things) es un término nacido en el Instituto Tecnológico de Massachusetts en 1999 y se refiere a la interconexión de objetos físicos en la red, programados para que ejerzan una función determinada, con la finalidad de controlar y optimizar su uso, reportando con ello un sinfín de beneficios y nuevos servicios para hacernos la vida más fácil.

¿Cómo funciona? Estos objetos inteligentes están conectados entre sí a través de internet y están programados para que generen información, interactúen entre ellos y con el mundo físico, ejecutando acciones y comunicándose con otros objetos.

Algunos dispositivos ya disponibles y más habituales se encuentran en la industria del automóvil (GPS, Wi-Fi, entre otros) en los Wearables (relojes, pulseras y zapatillas deportivas que nos facilitan datos de nuestro ejercicio físico, etc) y en los electrodomésticos de nuestras casas,

Y ejemplos ya familiares para muchos pueden ser el poder encender la calefacción a través del móvil antes de llegar a casa o frigoríficos inteligentes que detectan cuando se ha acabado un producto y conectan con la tienda/distribuidor para solicitar el pedido de reposición.

Seguramente todos hemos tenido contacto con algunos de estos objetos, ya que el ámbito de actuación puede ser tan amplio que abarca sectores como la salud, energía, infraestructuras, medio ambiente, electrodomésticos, automoción, servicios públicos, etc.

Otro ejemplo habitual lo podemos ver en aplicaciones como la monitorización de pacientes fuera del hospital o en cualquier lugar donde un enlace de comunicaciones pueda ser establecido. Los médicos pueden monitorizar las condiciones de un paciente y diagnosticar problemas o recibir alertas de eventos potencialmente letales.

Hay numerosos estudios que prevén que en el año 2020 el 75% de los coches estarán conectados a internet. Si tenemos en cuenta que sólo el año pasado el 14% de los coches vendidos tenía algún tipo de conectividad, la evolución de la industria se está desarrollando a ritmo vertiginoso.

Este futuro, curiosamente, ya lo veíamos en series y películas que pensábamos inalcanzable. Las primeras apariciones de la tecnología de los relojes inteligentes en el mundo del cine y las series se remontan muchas décadas atrás. Así podemos recordar la serie de **Knight Rider** (**El Coche Fantástico**), donde **Michael Knight** utilizaba su reloj para contactar con su coche.

Ahora muchos relojes inteligentes incorporan un micrófono, e incluso algunos relojes ya son capaces de permitirnos mantener conversaciones sin necesidad de utilizar en ningún momento nuestro móvil.

Al mismo tiempo, se prevé que vivamos en "ciudades inteligentes", creando ecosistemas urbanos, con grandes beneficios económicos, sociales y ecológicos: semáforos inteligentes, aparcamientos automatizados,…

El panorama actual del IoT sólo es una muestra de lo que deparará la innovación para los siguientes años. Y no tendremos que esperar mucho para ver nuevos objetos-dispositivos y, mejor aún, adoptarlos como una herramienta cotidiana.

Conforme las empresas creen nuevos objetos conectados a precios competitivos que favorezcan su penetración en el mercado, se podrá entender mejor su potencial para mejorar la calidad de vida de los usuarios.

Por parte de los gobiernos hay políticas de ayuda para incentivar esta economía. De hecho se publicó recientemente la noticia de que el Senado de EEUU había presentado un proyecto de Ley para impulsar el internet de la cosas.

El futuro, por tanto, es poder conectar e interconectarlo todo, tanto dispositivos como todo tipo de objetos. Según algunos estudios, para el año 2020 se estima que habrán entre 25.000 millones y 50.000 millones de objetos conectados a internet, lo que significa una progresiva digitalización del mundo físico, que cambiará completamente nuestras vidas cotidianas y el escenario socioeconómico actual.

Es ineludible, por tanto, una profunda reflexión sobre las implicaciones de estos avances y el tratamiento de grandes masas de datos que conlleva esta nueva era digital. Los dilemas éticos que representan y la necesidad de equilibrar, los beneficios que puede aportar el internet de las cosas y el derecho fundamental a la privacidad.

Como ciudadanos y profesionales especializados en protección de datos debemos preguntarnos si esta revolución tecnológica significará el próximo gran problema de la privacidad y seguridad. Cada vez es más complicado para los entes gubernamentales controlar si éstos dispositivos cumplen o no con sus políticas de privacidad, además, es necesario que se apruebe una ley especifica para proteger este derecho fundamental.

El nuevo Reglamento Europeo de Protección de Datos, que se ha aprobado el pasado mes de abril, recoge los principios primordiales para dar respuesta a estas innovaciones tecnológicas, como los principios de información y de transparencia, que dotaran al individuo del control sobre sus datos, así como los principios de finalidad, la privacidad desde el diseño y las evaluaciones del impacto.

El Reglamento Europeo establece preceptos de protección de datos que deberán integrarse desde el principio en cualquier proyecto, producto o servicio que requiera gestión de datos personales (privacidad desde el diseño), con la obligación añadida de que en su configuración automática por defecto sólo recopile y gestione aquellos datos que sean estrictamente necesarios (privacidad por defecto).

Asimismo, en el 2014 las autoridades europeas de protección de datos, conocidas como **Grupo de Trabajo del Artículo 29 (GT29**), aprobaron el primer Dictamen conjunto sobre internet de las cosas catalogado como la **Opinión 8/2014**, de 16 de septiembre. El documento, cuya elaboración ha sido liderada por la Agencia Española de Protección de Datos (AEPD) junto con la Autoridad francesa (CNIL), contempla tanto las perspectivas de beneficios económicos y sociales que puede aportar esta tecnología, como identifica y alerta de los riesgos que estos productos y servicios emergentes pueden suponer para la privacidad de las personas, definiendo un marco de responsabilidades.

El documento está dirigido a fabricantes de dispositivos, desarrolladores de aplicaciones y gestores de redes sociales, por un lado, y a usuarios que van a utilizar estos equipos conectados, por otro. Igualmente, contiene recomendaciones de utilidad en el desarrollo de estándares tecnológicos en el ámbito del internet de las cosas. El objetivo de este documento era identificar los riesgos que pueden surgir de esta tecnología si no se desarrolla desde un **enfoque ético y respetuoso**.

Las Autoridades alertan de que **el usuario puede perder el control sobre la difusión de sus datos** en función de si la recogida y el tratamiento de los mismos se realizan de manera transparente o no.

Al aumento de la cantidad de datos generados hay que sumar las posibilidades que existen para combinarlos y analizarlos de forma cruzada, obtener nuevos datos sobre los originalmente solicitados y utilizarlos para usos secundarios, afines o no al tratamiento inicial.

En cuanto a la **seguridad**, la opinión 8/2014, de 16 de septiembre, especifica que el internet de las cosas amplifica los riesgos asociados a una seguridad inadecuada en el diseño de los sistemas, no sólo por los datos recogidos y las inferencias que se pueden hacer de ellos sino por la tecnología que utilizan, que debería basarse en sistemas seguros y diseñados de acuerdo a los riesgos potenciales.

Las Autoridades recuerdan en el dictamen que el marco jurídico aplicable a cualquier sistema dirigido a usuarios europeos es la Directiva de Protección de Datos 95/46/CE, que será derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y entrará en vigor a los veinte días de su publicación en el DOUE y será aplicable a partir del 25 de mayo de 2018, en combinación con la Directiva 2002/58/CE de Privacidad y Comunicaciones Electrónicas, y que los beneficios de esta protección no dependen de que las organizaciones estén establecidas en territorio europeo.

En este sentido y desde una perspectiva estrictamente de carácter territorial, procede traer a colación los recientes pronunciamientos contenidos en la Sentencia del Tribunal de Justicia de las Comunidades Europeas de 13 de mayo de 2014, -ciertamente referida a los motores o buscadores de Internet-, pero cuya doctrina tiene un efecto expansivo que debe tomarse en consideración, y en la que se indicó expresamente, que en el Considerando 19 de la Directiva se afirma que «*el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable*», y «*que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante*». Para cumplir el requisito establecido en dicha disposición, es necesario, además, que el tratamiento de datos personales por parte del responsable del tratamiento se «*lleve a cabo en el marco de las actividades*» de un establecimiento de dicho responsable situado en territorio de un Estado miembro. Pronunciamiento que, si cabe, refuerza de una manera más poderosa los criterios de aplicación de la normativa Comunitaria a todos los

operadores jurídicos en Internet, entre los que, de manera obvia, se encuentran los que lo sean en el ámbito de Internet de las cosas.

Asimismo la Comisión Europea y el Gobierno de estados Unidos han acordado un nuevo marco, denominado "privacy shield" o "Escudo de privacidad", que entrará en vigor, aproximadamente, en unos tres meses y podrá ser revisado anualmente. Este acuerdo ayudará a lograr parte de la seguridad cuando dichos sistemas estén alojados en la nube. Según la Comisión, implica más obligaciones para las empresas estadounidenses a la hora de proteger los datos de ciudadanos europeos -como plazos obligatorios para responder a las reclamaciones- y una mayor colaboración con las autoridades de protección de datos, cuyas decisiones serán de obligado cumplimiento para dichas empresas. A partir de ahora, según la UE, "los problemas se resolverán con carácter inmediato"Las empresas tendrán que publicar las reglas de tratamiento de los datos que recopilan, algo que supervisará el Departamento de Comercio. Esas reglas serán compromisos de cuyo incumplimiento responderán ante los tribunales. Asimismo, el acuerdo incluiría un compromiso por parte del Gobierno de EE UU de que el acceso a los datos personales por parte de la administración estadounidense estará limitado, se realizará con todas las garantías y no será generalizado. Sólo se llevará a cabo cuando sea necesario y de forma proporcionada; no estará permitida, en ningún caso, la vigilancia indiscriminada.

Pero la preocupación por la seguridad no queda aquí. Organizaciones como Horizon 2020 Framework de la Unión Europea y la NSE de Estados Unidos están definiendo normas y buenas prácticas para proteger el sistema del internet de las cosas.

Entre las soluciones que se proponen está la seguridad basada en el hardware. La tecnología Intel EPID ofrece una “rampa” diseñada para ayudar a que los dispositivos se conecten en forma segura con la plataforma IoT. “La integridad de Intel EPID, aplicada mediante hardware, ofrece una identidad de dispositivo fija, de manera que sea compatible con las normas ISO TCG existentes y ayuda a proteger la identidad con tecnología de anonimato sofisticada”, se apunta en una nota oficial de Intel, que destaca que la ampliación del uso de EPID en la industria ayudará a hacer que las soluciones de IoT sean más seguras, independientemente de la opción del vendedor.

Un punto clave que no debe obviarse al desarrollar productos IoT: las entidades deben asegurarse de que la persona haya dado su **consentimiento de manera efectiva** después de haberle proporcionado **información clara y completa** sobre, entre otros aspectos, qué datos se recogen, cómo se recopilan y con qué fin se van a tratar, además de cómo pueden ejercer los derechos que les asisten.

Esos datos personales deben ser **recogidos de manera leal y lícita**, por lo que no deben ser recogidos y tratados sin que la persona sea consciente de ello. Este requisito es especialmente importante en un sector en el que los sensores son diseñados para ser tan invisibles como sea posible.

Las Autoridades insisten en que la información personal sólo puede ser recogida para unos fines determinados, explícitos y legítimos. Este principio permite a los usuarios conocer **cómo y con qué fines se están utilizando sus datos** y decidir en consecuencia.

Además, los datos recogidos deben **limitarse a los estrictamente necesarios** para la finalidad definida previamente. El dictamen puntualiza que "los datos que son innecesarios para tal fin no deben ser recogidos y almacenados por si acaso o porque podrían ser útiles más adelante".

Por último, según **Grupo de Trabajo del Artículo 29 (GT29**), los datos personales recogidos y tratados en el marco del internet de las cosas no deben mantenerse durante un período superior al necesario para los fines para los que fueron recogidos. El documento del GT29 especifica que, por ejemplo, los datos facilitados por un usuario cuando se suscribe a un servicio se deben eliminar tan pronto como el usuario pone fin a su suscripción. Del mismo modo, la información borrada por el usuario en su cuenta no debe mantenerse y, cuando un usuario no utiliza un servicio o aplicación, el perfil debe establecerse como inactivo hasta que pasado un tiempo se eliminen esos datos, proporcionando una información clara en todos los casos.

Por otro lado, el 1 de marzo de este año, varios senadores norteamericanos iniciaron el trámite un proyecto de Ley de regulación del Internet de las cosas. Bajo el título Developing Innovation nd Growing the Internet of Things (DIGIT) Act, el proyecto pretende abordar el desafío del internet de las cosas, centrándose inicialmente en los siguientes elementos:

- Necesidades de espectro radioeléctrico.
- Entorno regulatorio, subvenciones gubernamentales y retos presupuestarios y competenciales.
- Protección de los consumidores.
- Privacidad y seguridad.
- Uso de la IoT por las agencias gubernamentales y su estado de preparación para adoptarla en el futuro.

Según publicó el pasado 1 de marzo *The Information Technology and Innovation Foundation's Center for Data Innovation*, el Digit Act se desarrolla con el objetivo de establecer una estrategia nacional de los EEUU ante el desafío del Internet de las cosas. Para ello se creará un grupo de trabajo comprometido para que los Estados Unidos puedan aprovechar los cuantiosos beneficios que puede ofrecer el Internet de las cosas. En este sentido, se manifiesta como parte

de la estrategia nacional la consulta con las partes interesadas no gubernamentales, incluyendo expertos de la industria, los fabricantes de tecnología, negocios y grupos de consumidores así como representantes de los organismos que pueden ayudar a maximizar todas oportunidades, tales como el Departamento de Salud y Servicios Humanos, la Departamento de Vivienda y Desarrollo Urbano, y el Departamento de Agricultura.

Todas estas normativas e iniciativas legales intentan regular toda una revolución tecnológica. El Internet de las Cosas (IoT) nos está brindado una realidad nueva y conectada que hace años sólo se soñaba como ciencia ficción. Esta tercera ola del Internet ha alcanzado a más dispositivos u objetos que nunca y está transformando la forma en que las personas viven, trabajan, compran, se divierten… Es un cambio en todos los aspectos de la vida cotidiana.

Actualmente estamos ante noticias cotidianas donde los fallos de seguridad suceden en dispositivos, servidores Web, servidores de autenticación, bibliotecas de lenguajes de programación que afectan a decenas de miles de aplicaciones.

Hace poco, lograron tomar el control de un coche inteligente de forma remota y el conductor terminó asustado. Por este motivo, el fabricante, Fiat Chrysler, se vió obligado a retirar del mercado 1,4 millones de coches de sus marcas para revisar su software.

Dadas las condiciones de seguridad informáticas actuales, el caldo de cultivo que se cocinaría con la IoT es alarmante. No importa el sistema operativo, no importa la aplicación, todo lo digital es vulnerable a ataques. Si además de recolectar y transmitir la información, el internet de las cosas obtiene permiso para hacer algo, entonces un ataque sobre objetos peligrosos (un coche, por ejemplo) podría costar vidas. Es una de las conclusiones del Instituto de Ingenieros eléctricos y Electrónicos (IEEE).

Otro riesgo en seguridad que lesiona la privacidad son los datos que se transmiten sin cifrar la información. En este punto debemos tener en cuenta que aunque se implemente una cultura de cumplimiento sobre privacidad, exigiendo la privacidad desde el diseño a los fabricantes, dichos sistemas no dejan de ser vulnerables a los hackers.

Una cosa inteligente podría suponer erróneamente el lugar donde está, habiendo sido intervenida por un pirata informático, y tomar en consecuencia una decisión imprudente, decisión que podría comunicarle a terceros, con resultados todavía más peligrosos o comprometedores.

El problema de seguridad se encuentra en conseguir **proteger correctamente la información almacenada**, en la inteligencia que se pueda obtener de ella y, en definitiva, en el beneficio económico que grupos maliciosos puedan lograr. Palabras mayores son cuando nos

referimos a **ciberterrorismo**: generadores de *malware*, expertos en intrusión de sistemas y, en definitiva, equipos organizados con mayor capacidad de actuación cuyos ataques pueden ir dirigidos contra redes de distribución de energía, cuencas hidrográficas e instalaciones gubernamentales.

Pero la seguridad no es el único tema que preocupa, también la privacidad. "Las mentiras socialmente aceptables de antes serán más difíciles o casi imposibles porque estarás constantemente acechado y bajo monitoreo a través de Internet", asegura **Pamela Wright,** presidente de innovación para los Archivos Nacionales de EE.UU. "Oye, tú dijiste que te fuiste de fin de semana, pero tu cama dice que dormiste bien ocho horas el sábado por la noche. Y lo confirmó tu botella de vino…". Sabremos mucho más sobre nuestra sociedad con base en datos estadísticos que surgen de los dispositivos de la informática de vestir y del Internet de las cosas".

Todo este nuevo entorno que supone la revolución tecnológica del Internet de las cosas nos obliga a buscar el equilibrio entre los beneficios tanto económicos como sociales y la defensa de la privacidad para preservar el control y la libre disposición de los datos personales de los usuarios y de la sociedad en general.

Pero estamos viviendo una verdadera revolución donde los objetos conectados llegan primero que los acuerdos legales. Si bien es cierto que hace escasos dos meses la Comisión Europea y el Departamento de Comercio de EEUU han encontrado un sustituto al " SAFE HARBOUR" con el denominado "ESCUDO DE PRIVACIDAD", que conlleva más obligaciones para las empresas estadounidenses en la tarea de proteger los datos de los ciudadanos europeos.

Sin embargo, según publicó el pasado 10 de Febrero el diario británico The Guardian, el director de la Inteligencia de EEUU, James Clapper, declaró en el Senado "**En el futuro, los servicios de inteligencia podrán usar el (Internet de las Cosas) para identificación, vigilancia, monitorización, localización** y seguimiento para reclutar u **obtener acceso a redes o credenciales de usuari**o", como parte de una declaración sobre las amenazas a las que se enfrenta EEUU.

En conclusión, nos esperan tiempos interesantes, como ciudadanos, como sociedad y como profesionales de la protección de datos. Los objetos, las cosas, se están volviendo cada vez más inteligentes y nuestro reto es buscar el equilibrio entre privacidad y seguridad de la información y los beneficios del Internet de las cosas. Son muchas las cuestiones a debatir: ¿Cómo persuadir a los fabricantes para construir protocolos de comunicación estándar para los objetos cotidianos?, ¿cómo mantener los datos generados en servidores privados?, ¿de qué manera

pueden ofrecer modelos de negocio donde los datos obtenidos se puedan compartir y así poder compaginar los beneficios de los sitemas IoT con la privacidad y seguridad?, etc…

Sea como fuere, es importante que la seguridad y privacidad adquiera la relevancia que merece en el entorno tecnológico actual**.** La tecnología es, sin duda, una ayuda pero el eslabón más delicado no son las cosas, sino las personas.