Nota informativa

Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre internet de las cosas

- **El documento analiza tres escenarios: la tecnología para llevar puesta (*wearable computing*), los dispositivos capaces de registrar información relacionada con la actividad física de las personas y la domótica**
- **El Dictamen identifica y alerta de los riesgos que estos productos y servicios pueden plantear para la privacidad de las personas, definiendo un marco de responsabilidades y realizando recomendaciones**
- **A pesar de que los objetos que conforman la internet de las cosas recogen piezas aisladas de información, los datos recogidos de diferentes fuentes y analizados de otra forma o en conjunción con otros pueden revelar auténticos patrones de la vida de las personas**
- **Un ejemplo destacado en el Dictamen es la información recogida por el acelerómetro y el giroscopio de un smartphone, que podría ser utilizada para obtener información sobre los hábitos de conducción del individuo**

(Madrid, 24 de septiembre de 2014). Las Autoridades europeas de protección de datos (Grupo de Trabajo del Artículo 29) han aprobado el primer Dictamen conjunto sobre internet de las cosas. El documento, **cuya elaboración ha sido liderada por la Agencia Española de Protección de Datos junto con la Autoridad francesa (CNIL)**, acoge con satisfacción las perspectivas de beneficios económicos y sociales que puede suponer esta tecnología, pero también identifica y alerta de los riesgos que estos productos y servicios emergentes pueden plantear para la privacidad de las personas, definiendo un marco de responsabilidades.

Las Autoridades subrayan las obligaciones en cuanto a protección de datos de los diversos actores que participan en la internet de las cosas y recuerdan los derechos que amparan a los ciudadanos, con ejemplos específicos en cada caso. Además, el documento ofrece un amplio conjunto de recomendaciones prácticas dirigidas a cada uno de los grupos involucrados en el desarrollo de esta tecnología. Estas recomendaciones pretenden ayudar a los responsables a cumplir con la legislación sobre protección de datos y, en consecuencia, contribuir a que **esta tecnología se desarrolle en un marco positivo de respeto a los derechos fundamentales**. En opinión de las Autoridades europeas de protección de datos, los proyectos que cumplan con estas expectativas obtendrán **una fuerte ventaja competitiva**.

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 de la internet de las cosas. Para identificar los riesgos que pueden surgir de esta tecnología si no se desarrolla desde un **enfoque ético y respetuoso**, el Dictamen plantea **tres escenarios**: la conocida como tecnología para

llevar puesta (*wearable computing*), los dispositivos capaces de registrar información relacionada con la actividad física de las personas y la domótica.

Patrones de comportamiento y perfiles

La **tecnología para llevar puesta** incluye relojes o gafas a las que se añaden sensores, cámaras o micrófonos que registran y transfieren datos al fabricante del dispositivo, y que pueden permitir la instalación de aplicaciones de terceros. En cuanto a los objetos que registran la información sobre los **hábitos y estilo de vida** de sus usuarios, el Dictamen se centra en aquellos que recogen datos relacionados con la actividad física de la persona, en especial, relativos a la salud. En este sentido, el Dictamen alerta de que en principio, pese a que los dispositivos pertenecientes a esta categoría no recojan datos especialmente protegidos –un podómetro, por ejemplo- pueden acabar proporcionando a terceros información inferida acerca de la salud del individuo. Por último, el documento analiza la internet de las cosas aplicada a la **domótica**, con oficinas y hogares con detectores, termostatos y sensores conectados cuyos patrones de uso pueden revelar detalles de la forma de vida y los hábitos personales y familiares.

El Dictamen subraya que, a pesar de que los diferentes objetos que conforman la internet de las cosas recogen piezas aisladas de información, los datos recogidos de diferentes fuentes y analizados de otra forma o en conjunción con otros pueden revelar aspectos específicos de hábitos, comportamientos y preferencias, configurando **auténticos patrones de la vida de las personas**. El Dictamen advierte de que, de hecho, si esta vigilancia potencial llegara a producirse, podría condicionar la forma en la que las personas se comportan en la vida real.

La 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 realiza 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. Un ejemplo destacado en el Dictamen es la información recogida por **el acelerómetro y el giroscopio** de un teléfono inteligente, que podría ser utilizada para deducir información con un significado muy diferente al inicial, como los **hábitos de conducción del individuo**.

En cuanto a la **seguridad**, el documento especifica que la 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.

Derechos de los ciudadanos

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, 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.

Así, las entidades que participan en el ecosistema de la internet de las cosas 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, los datos personales recogidos y tratados en el marco de la 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.

El Dictamen íntegro (en inglés), que incluye un análisis completo de los posibles riesgos incluyendo ejemplos y recomendaciones, puede consultarse en:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Grupo de trabajo del Artículo 29
El Grupo de Autoridades europeas de protección de datos -Grupo de Trabajo del Artículo 29- es el grupo consultivo compuesto por representantes de las autoridades nacionales de protección de datos de los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea. Sus funciones están descritas en el Artículo 30 de la Directiva 95/46/EC y el Artículo 15 de la Directiva 2002/58/EC. El Grupo de Trabajo del Artículo 29 está facultado para examinar cualquier cuestión que esté relacionada con la aplicación de las directivas en materia de protección de datos para contribuir a la aplicación uniforme de las mismas. Desempeña sus funciones emitiendo recomendaciones, dictámenes y documentos de trabajo sobre todas aquellas cuestiones relevantes que afectan a la protección de datos personales.