Centro de Estudios de Consumo

www.uclm.es/centro/cesco

WEARABLES: QUÉ SON, CÓMO FUNCIONAN Y QUE PELIGROS ENTRAÑAN PARA NUESTRA PRIVACIDAD

Lourdes García Montoro
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

Fecha de publicación: 23 de enero de 2015

Algunos de los productos a los que mayor publicidad se dio durante la pasada campaña de navidad fueron los relojes, gafas o pulseras inteligentes, los "*wearables*" o tecnología que se lleva puesta. La acelerada evolución tecnológica que vivimos ha convertido internet en una herramienta indispensable en nuestra vida diaria, necesitamos estar permanentemente conectados a través del teléfono, email, redes sociales, etc. Ya no sólo se trata de sentarnos frente al ordenador o llevar a cualquier parte nuestro Smartphone, sino que la tecnología pone todas esas prestaciones a nuestro alcance a través de aparatos más ligeros como relojes o pulseras que podemos llevar puestos en diversidad de ocasiones como, por ejemplo, cuando hacemos deporte.

De hecho, la tecnología para llevar puesta ha ido ganando adeptos entre los deportistas. Aplicaciones para Smartphone como "Endomondo", que registra la actividad física de sus usuarios (pulsómetro, distancia que recorren, velocidad, recorrido…), fueron las primeras en ponerse de moda. En el caso concreto de Endomondo, da la posibilidad a sus usuarios de hacer pública esta información deportiva en las *redes* sociales, desvelando con ello de forma inintencionada su lugar de residencia, que suele coincidir con el lugar de inicio del recorrido, además de informar de la franja horaria en la que practica deporte habitualmente y se ausenta de su domicilio[1]. Son muchas las empresas relacionadas con el sector del deporte que ya han diseñado su pulsera para mantenerse en forma (Fitbit, Jawbone, Runtastic, Nike), aparato que medirá los datos biomédicos del usuario y, se supone, le ayudará a alcanzar sus objetivos de salud.

Pero el mercado de los *wearables* no es sólo para deportistas. Por ejemplo, el reloj inteligente o Smartwatch diseñado por Samsung (modelo Samsung Gear S)[2] ofrece

[1] Testimonio en http://www.elladodelmal.com/2014/07/robame-que-estoy-haciendo-deporte-y.html

[2] http://www.samsung.com/es/consumer/mobile-phone/wearables/

todas las prestaciones que cabría esperar del típico Smartphone: teléfono, agenda, email, redes sociales, tiempo o registro de actividad física, entre otras. El reloj incorpora una tarjeta SIM como la del teléfono y transfiere los datos a éste mediante Bluetooth y a través de la red WiFi.

Diseño y funcionalidad son las características que atraen a los compradores de *wearables*, pero estos aparatos tienen un riesgo añadido y es la posibilidad de que terceros como la propia empresa que fabrica o diseña el producto o los desarrolladores de las aplicaciones que instalamos en nuestro dispositivo tengan acceso a nuestros datos personales. Las empresas pueden usar el registro de actividad física para conocer los hábitos y preferencias del usuario y diseñar estrategias de venta, por pensar en un uso benévolo de los mismos.

Estos dispositivos inteligentes incorporan una serie de sensores que recopilan datos continuamente sin que el usuario, en muchas ocasiones, sea consciente de ello y no tenga control sobre los datos que pone a disposición de su dispositivo y, por ende, del fabricante del mismo o de los desarrolladores de aplicaciones a los que ha dado (o ha dejado de configurar en sentido contrario) acceso a sus datos personales. Datos que en muchas ocasiones pueden ser datos sensibles cuya pérdida o transmisión a terceros puede conllevar un menoscabo de la intimidad del usuario.

¿Por qué los *wearables* recogen y tratan nuestros datos personales sin que apenas seamos conscientes de ello? Fabricantes, diseñadores y desarrolladores de aplicaciones suelen configurar por defecto el dispositivo y las aplicaciones con todos los permisos del usuario activados, siendo éste quien debe realizar una configuración personal para limitar el acceso a sus datos. Sin embargo, la realidad legal es que los agentes que actúan en el mercado con la finalidad de tratamiento de datos, ya sean fabricantes, diseñadores o desarrolladores de aplicaciones, están obligados a obtener el consentimiento del usuario para tener acceso al tratamiento de sus datos, no pudiendo entenderse concedido el mismo porque el dispositivo venga configurado así por defecto, sino que el consentimiento del usuario debe facilitarse de forma libre, informada e inequívoca.

Los agentes que actúan en el mercado de los dispositivos inteligentes (el internet de las cosas del que más adelante trataremos) tienen que tomar cartas en el asunto para no vulnerar la normativa europea y nacional sobre protección de datos personales; para lo cual pueden servir de ayuda las directrices adoptadas por las Autoridades europeas de protección de datos (grupo de trabajo del Artículo 29) en el primer Dictamen conjunto

sobre internet de las cosas[3], cuya elaboración ha sido liderada por la Agencia Española de Protección de Datos junto con la autoridad francesa (CNIL).

Tomando como referencia este documento, analizaremos los riesgos que para la protección de los datos personales conlleva el uso de *wearables* y cómo se pueden evitar las intromisiones ilegítimas en los datos personales.

1. El internet de las cosas y los *wearables*

a) *El "internet de las cosas"*

El concepto "internet de las cosas" se refiere, tal y como lo define el Dictamen de la autoridad europea, a una infraestructura en la que billones de sensores instalados en dispositivos interconectados (cosas o cosas conectadas a otros objetos o individuos) están diseñados para recoger, procesar, almacenar y transferir datos e interactuar con otros dispositivos o sistemas usando las redes.

Los agentes que actúan en este mercado tienen como objetivo ofrecer nuevas aplicaciones y servicios a través de la recogida y posterior combinación de estos datos de los individuos, ya sea sólo para medir los datos del usuario o para observar y analizar sus hábitos. Una vez que los datos están almacenados de forma remota pueden ser compartidos con terceros, a veces sin que el usuario sea consciente de ello. En estos casos, la transmisión de sus datos es casi imperativa, pues el usuario no puede impedirlo sino cambiando la configuración del producto y perdiendo gran parte de su funcionalidad. Ello conlleva que los fabricantes y sus socios comerciales puedan tener acceso a detalles particulares de los perfiles de los usuarios a los que éstos, de otro modo, probablemente no les darían acceso.

b) *Wearable computing o tecnología para llevar puesta*

Aunque el Dictamen analiza tres tipos distintos de bienes en relación a la protección de datos en el "internet de las cosas" (*wearables*, dispositivos que registran información relacionada con la actividad física, y domótica), nos centraremos exclusivamente en el estudio del *wearable computing* o tecnología para llevar puesta.

Tal y como lo describe el grupo de trabajo que elabora el Dictamen, deben entenderse por "*wearables*" los objetos y ropa diaria, tales como relojes o gafas, en los que se instalan sensores para ampliar su funcionalidad. Pueden incluir

[3] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

cámaras, micrófonos y sensores que pueden grabar y transferir datos al fabricante. Además, la disponibilidad de un interfaz de programación de aplicaciones (API) en los dispositivos para llevar puestos (Android Wear[4]) propicia la creación de aplicaciones por terceros que pueden tener acceso a los datos recogidos por estos dispositivos.

Otros autores[5] han definido el *Wearable computing* como el estudio del invento, diseño, producción o el uso de miniaturas informáticas o dispositivos que incorporan sensores; la tecnología para llevar puesta suele formar parte de la vestimenta habitual del usuario o se trata de ropa propiamente dicha. También podrían los *wearables* colocarse en el cuerpo y formar parte de él. El dispositivo siempre "va junto al propietario y lo sigue a cualquier parte", no debiendo resultar sencillo (incluso en ocasiones imposible) retirarlo. Los *wearables* están funcionando constantemente o, al menos, están listos para ponerse en funcionamiento de inmediato. La tecnología para llevar puesta está diseñada no sólo para recoger, registrar y procesar datos, sino también para interpretar dichos datos y tomar decisiones en nombre del usuario; mientras que esta autonomía decisoria puede aumentar el confort del usuario, también puede implicar una pérdida del control de sus datos.

2. Tratamiento de datos de carácter personal por los *wearables*

a) Falta de transparencia al obtener el consentimiento del usuario

En muchos casos, pasa inadvertida para el usuario la recogida de datos que llevan a cabo algunos dispositivos electrónicos. Esta falta de información constituye una barrera importante para demostrar la válida prestación del consentimiento a esta finalidad ante el Derecho de la Unión Europea.

Los mecanismos clásicos para obtener el consentimiento del usuario podrían resultar difíciles de implantar en los *wearables*, obteniendo un consentimiento de baja calidad basado en la falta de información. En la práctica, hoy en día los dispositivos que incluyen sensores ni están diseñados para facilitar información por sí mismos ni disponen de un mecanismo válido para obtener el consentimiento del individuo. De ahí que sea recomendable que los distintos agentes del mercado establezcan nuevas vías para obtener el consentimiento del

[4] https://developer.android.com/wear/index.html

[5] R. Mathys, "*Legal challenges of wearable computing*", págs. 5-7, 2014, http://www.swlegal.ch/getdoc/5ff2741a-6e1e-4108-99c7-8dc1566f21b2/140731_Roland-Mathys_Paper-Legal-Challenges-of-Wea.aspx

usuario, incluyendo la instalación de mecanismos para obtener el consentimiento en el propio dispositivo.

b) *Uso de datos con fines distintos a aquellos para los cuales se recogieron*

El incremento de la cantidad de datos procesados por los dispositivos inteligentes en combinación con las nuevas técnicas de análisis de datos y el intercambio de los mismos podría permitir un uso secundario de dichos datos, relacionado o no con la finalidad inicialmente prevista. Los terceros que solicitan acceso a los datos almacenados por otros agentes podrían querer hacer un uso de los datos para propósitos diferentes de aquellos para los cuales el usuario prestó su consentimiento.

A pesar de la aparente irrelevancia de los datos recopilados en bruto, por ejemplo, la multitud de datos biomédicos que recoge la pulsera para mantenerse en forma, analizados en conjunto pueden permitir obtener información potencialmente sensible sobre el usuario final, como su forma física. Mientras el usuario comparte tranquilamente esta información con una finalidad concreta, podría no querer compartirla con terceros que pudieran usarla con un propósito muy distinto. El análisis de la información recogida por un dispositivo inteligente permitiría obtener una información detallada de la vida del individuo y de sus patrones de comportamiento. Por eso, es importante que los agentes del mercado (fabricantes, diseñadores, desarrolladores de aplicaciones…) se aseguren de que los datos se usen con el propósito para el que fueron obtenidos y que esta finalidad sea conocida por el usuario.

c) *Riesgos de seguridad: ¿implica una pérdida de eficiencia del dispositivo el aumento de los requisitos de seguridad?*

Los *wearables* adolecen de un problema de limitación de espacio y de autonomía energética evidentes y aún se desconoce cómo pretenden los fabricantes equilibrar el cumplimiento de los deberes de protección de datos con la necesidad de optimizar los recursos del dispositivo. Menos seguridad en los *wearables* conllevaría nuevas formas potenciales y eficaces de ataque, incluyendo datos personales robados o comprometidos que pueden perjudicar los derechos de los usuarios y menoscabar la imagen de seguridad de internet.

La mayoría de los sensores que se encuentran actualmente en el mercado no son capaces de encriptar el acceso de las comunicaciones puesto que los requisitos informáticos tienen un impacto limitado en el dispositivo por su batería de baja potencia. En relación con la seguridad de principio a fin en la cadena de suministro, el resultado de la integración de diferentes componentes

proporcionados por distintos agentes sólo garantiza el nivel de seguridad previsto en el componente más débil.

3. Marco legal en la Unión Europea

El tratamiento de datos personales y la libre circulación de los mismos en la Unión Europea deberá atenerse a lo dispuesto en la Directiva 95/46/CE[6] y en la Directiva 2002/58/CE[7]. Los responsables del tratamiento de datos con sede en Europa cumplirán esta normativa, pero muchos de ellos son de países no comunitarios (China, USA...) y en ocasiones prescinden de preparar sus dispositivos para que cumplan los requisitos de confidencialidad previstos en la normativa europea y en la de cada Estado miembro en particular.

Estas previsiones serán de aplicaciones a los diferentes agentes que actúan en el mercado: fabricantes, gestores de redes sociales y desarrolladores de aplicaciones, en la medida en que todos ellos intervienen como responsables del tratamiento de datos de carácter personal al participar en alguna de las fases del proceso.

a) Confidencialidad de las comunicaciones

El uso de las redes con fines de almacenamiento de información o de acceso a la información almacenada en el terminal de un usuario sólo se permitirá, en el sentido del artículo 5 (3) de la Directiva 2002/58/CE, cuando se facilite al usuario información clara y completa sobre la finalidad del tratamiento de los datos y siempre que el responsable de dicho tratamiento le ofrezca el derecho a oponerse a ello. Se entiende permitido el almacenamiento en la medida de lo estrictamente necesario a fin de proporcionar a una empresa un servicio expresamente solicitado por el usuario.

b) Legitimidad del tratamiento de datos

El tratamiento de datos estará legitimado cuando se cumplan los requisitos previstos en el artículo 7 de la Directiva 95/46/CE. En la práctica, desempeñan un papel esencial tres de ellos:

---

6 https://www.agpd.es/portalwebAGPD/internacional/textosynormas/textos_union_europea/textos_directivas/common/pdfs/B.4_Directiva_95-46-CE.pdf

7 http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.6-cp--Directiva-2002-58-CE-protecci-oo-n-e-intimidad-en-comunicaciones-electronicas.pdf

- Consentimiento: cuando el interesado haya dado su consentimiento de forma inequívoca.

- Ejecución de un contrato en el que el interesado sea parte: el ámbito de aplicación de este motivo está delimitado por el concepto de "necesidad", que requiere una conexión directa y objetiva entre el tratamiento de datos y la finalidad de la ejecución contractual esperada por el interesado.

- Satisfacción del interés legítimo perseguido por el responsable del tratamiento o por los terceros a quienes se comuniquen los datos: siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado[8].

c) Calidad de los datos

Entran en juego aquí las previsiones contenidas en el artículo 6 de la Directiva 95/46/CE.

En primer lugar, los datos deben ser tratados de manera leal y lícita. El principio de lealtad requiere que los datos personales nunca sean tratados sin que el individuo sea consciente de ello. Los agentes implicados en el tratamiento de datos (principalmente los fabricantes) deben informar a todos los usuarios cuando se recopilen sus datos o los relacionados con su entorno.

El segundo requisito es que los datos sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines. El objetivo de este requisito es permitir a los usuarios saber cómo y con qué finalidad se usarán sus datos y decidir si confiar el tratamiento de los mismos al agente que se lo requiere.

El tratamiento de datos también debe ser adecuado, pertinente y no excesivo con relación a los fines para los que se recogen y para los que se traten posteriormente. El principio de "minimización de datos" implica que los datos innecesarios a la finalidad perseguida por el agente no podrán ser recogidos y almacenados sólo porque pudieran resultar útiles con posterioridad.

d) Tratamiento de datos especiales o "sensibles"

Las aplicaciones diseñadas para instalarse en dispositivos inteligentes pueden procesar datos personales que revelen el origen étnico o racial del individuo, sus

[8] Sobre la extensión de esta legitimación, Judgment of the court (Grand Chamber), 13 May 2014, Case C-131/12, Google Spain.

opiniones políticas, creencias religiosas o filosóficas, pertenencia a sindicatos, salud o vida sexual[9]; datos que deben calificarse como "sensibles" y que merecen la especial protección prevista en el artículo 8 Directiva 95/46/CE. Para considerar legítimo el tratamiento de datos de este tipo será necesario obtener el consentimiento explícito del usuario, a no ser que el tratamiento se refiera a datos que él mismo haya hecho voluntariamente públicos.

e) Seguridad del tratamiento

El artículo 17 de la Directiva 95/46/CE obliga al responsable del tratamiento de datos a "*aplicar las medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados […]".* Requiere, además, que el responsable del tratamiento elija un encargado que reúna las garantías suficientes en relación con las medidas de seguridad técnica y organización de los tratamientos que deben realizarse.

Las medidas de seguridad deben hacerse efectivas teniendo en cuenta las restricciones operativas específicas de cada dispositivo. Hoy en día la mayoría de los sensores no son capaces de establecer una conexión encriptada como consecuencia de la prioridad otorgada a la autonomía física del dispositivo. En tanto sus componentes se sirven normalmente de las redes de comunicaciones WiFi y se caracterizan por tener unos recursos limitados en cuanto a energía e informática, los dispositivos son vulnerables a los ataques físicos, espionaje o ataques proxy. El internet de las cosas implica una compleja cadena de suministro con multitud de agentes que asumen diferentes grados de responsabilidad, pudiendo la falta de seguridad provenir de cualquiera de ellos.

f) Derechos del interesado en el tratamiento: derecho de acceso y oposición

Los interesados tienen derecho a conocer los datos objeto de tratamiento, la finalidad y los destinatarios a quienes se comunican; tienen derecho a la rectificación, supresión o bloqueo de los datos cuyo tratamiento no proceda y a que se informe a los terceros que tengan estos datos en su poder de las modificaciones pertinentes.

Así mismo, los interesados tienen la posibilidad de revocar cualquier consentimiento prestado previamente y oponerse al tratamiento de datos

[9] En el mismo sentido, R. Mathys, "*Legal challenges of wearable computing*", págs. 15-16, 2014, http://www.swlegal.ch/getdoc/5ff2741a-6e1e-4108-99c7-8dc1566f21b2/140731_Roland-Mathys_Paper-Legal-Challenges-of-Wea.aspx

relacionados con su persona. Estos derechos deben poder ejercerse sin restricciones ni obstáculos, y las herramientas previstas para ejercitar la oposición deben ser accesibles y eficaces.

4. Recomendaciones

El Dictamen de la autoridad europea de protección de datos tiene como objetivo proporcionar una serie de recomendaciones a los distintos agentes que intervienen en el mercado del internet de las cosas con la finalidad de que respeten, desde el origen, el marco legal de protección de datos vigente en la Unión Europea.

La vulneración de esta normativa así como de la vigente a nivel nacional podría implicar la comisión de una infracción y la consecuente imposición de sanciones. De ahí que sea recomendable para los agentes que intervienen en cualquier momento del proceso de tratamiento de datos tener en cuenta una serie de recomendaciones (recogemos a continuación las más relevantes) para evitar incurrir en irregularidades.

a) Recomendaciones comunes a todos los agentes que intervienen en el mercado

- Evaluación sobre el impacto de la privacidad (PIA – Privacy Impact Assesment): sería recomendable que los responsables del tratamiento de datos realizasen un PIA antes de la comercialización de sus productos. Una evaluación de impacto es un proceso que permite identificar los riesgos que un producto o servicio puede implicar para la protección de datos antes de que se materialicen. La metodología a seguir puede basarse en lo ya dispuesto por el grupo de trabajo del artículo 29 en su documento de 12 enero 2011[10] y, en el caso particular de España, en lo previsto en la Guía para una evaluación de impacto en la protección de datos personales[11].

- Muchos agentes solo necesitan datos globales y no todos los datos en bruto recogidos por el dispositivo. Los responsables del tratamiento deberían borrar estos datos en bruto tan pronto hayan extraído los que necesiten para su procesamiento.

- Todos los agentes que actúan en el mercado del internet de las cosas deben aplicar los principios de intimidad por diseño (*Privacy by design*) e intimidad por defecto (*Privacy by default*).

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

[11] http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

- La autorización del usuario es esencial. Los usuarios deben ser capaces de ejercitar sus derechos y de controlar sus datos en cualquier momento de acuerdo con el principio de autodeterminación.

- Sería deseable que las vías previstas para manifestar el consentimiento, obtener información u oponerse al tratamiento de datos resulten fáciles de usar por el interesado. En particular, las políticas de información y consentimiento deben centrarse en lo que es comprensible para el usuario y no limitarse a una política general de privacidad publicada en la web del responsable del tratamiento.

b) Recomendaciones específicas para los fabricantes

- Informar a los usuarios del tipo de datos que recogen los sensores instalados en el dispositivo y que serán posteriormente tratados, cómo serán procesados y combinados.

- Notificación al resto de agentes implicados en el tratamiento de datos de la revocación del consentimiento del interesado o de la oposición al tratamiento de sus datos tan pronto como tenga constancia de ello.

- Facilitar varias opciones para garantizar el acceso a las aplicaciones. La variedad no debe referirse exclusivamente a los datos que se recogen, sino también al tiempo y la frecuencia con que se realiza esta tarea, permitiendo al usuario deshabilitar la aplicación e impedir la recogida continua de datos.

- Para prevenir el seguimiento de la ubicación, los fabricantes de dispositivos deberían ofrecer la posibilidad de deshabilitar el interfaz WiFi cuando no se está usando para evitar que el identificador permanente pueda ser usado para el seguimiento de la ubicación.

- Los usuarios están legitimados para ejercitar el derecho de acceso a sus datos personales. Se les deberían proporcionar herramientas sencillas que les permitieran exportar fácilmente sus datos a un formato más habitual e incluso editarlos antes de que sean transferidos.

- Los fabricantes se servirán de herramientas simples para notificar a los usuarios y para actualizar los dispositivos cuando se descubran peligros para la seguridad. Cuando un dispositivo deviene obsoleto y no es susceptible de más actualizaciones, el fabricante debe informar al usuario y asegurarse de que está advertido de que el dispositivo no volverá a ser actualizado.

- Los fabricantes deben impedir en la medida de lo posible la pérdida de datos del dispositivo mediante la transformación de los datos en bruto en datos globales almacenados directamente en el dispositivo.

- Los fabricantes deberían disponer de entidades de control y procesamiento local (personal privacy proxies) que permitan a los usuarios tener una idea clara de los datos recogidos por su dispositivo y facilitar un procesamiento y almacenamiento local sin tener que transmitir los datos del dispositivo al fabricante.

c) Recomendaciones dirigidas a los desarrolladores de aplicaciones

- Diseño de sistemas de alertas y advertencias que recuerden con relativa frecuencia a los usuarios que los sensores están recogiendo datos.

- Las aplicaciones deberían facilitar el ejercicio de los derechos de acceso, rectificación y oposición del usuario respecto de los datos recogidos por el dispositivo.

- Aplicación del principio de "minimización de datos". Cuando la finalidad pueda ser alcanzada usando datos globales, los desarrolladores no deberán acceder a los datos en bruto. Los desarrolladores deberían seguir una política de intimidad mediante el diseño (*Privacy by design*) y minimizar la cantidad de datos recogidos a los necesarios para prestar el servicio.

d) Gestores de redes sociales

- Los ajustes por defecto de las aplicaciones de redes sociales deberían preguntar a los usuarios si desean revisar, editar o decidir sobre la información generada por su dispositivo antes de que se publique en la red.

- La información publicada por el dispositivo en las redes sociales debería, por defecto, no hacerse pública ni poder indexarse por motores de búsqueda.

e) Usuarios del dispositivo

- El consentimiento para el uso de un dispositivo interconectado y el tratamiento de datos recogidos por éste debe ser manifestado de forma voluntaria. Los usuarios no deberían ser económicamente penalizados o tener un acceso degradado a las capacidades de su dispositivo si deciden no usarlo o prescindir de un servicio específico.