GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

1471/14/ES
WP 223

Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos

Adoptado el 16 de septiembre de 2014

EL GRUPO DE TRABAJO SORE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

Vistos los artículos 29 y 30 de dicha Directiva,

Visto su Reglamento interno,

HA ADOPTADO EL PRESENTE DICTAMEN:

RESUMEN

La Internet de los objetos (IO) se encuentra en el umbral de integración en las vidas de los ciudadanos europeos. La viabilidad de muchos de los proyectos de la IO aún está por confirmar, pero ya existen «objetos inteligentes» que controlan nuestros hogares, automóviles, entornos de trabajo y actividades físicas y se comunican con ellos. Hoy en día, los dispositivos conectados satisfacen adecuadamente las necesidades de los ciudadanos de la UE en los mercados a gran escala del «Yo cuantificado» y la domótica. La IO presenta, por tanto, buenas perspectivas de crecimiento para un número importante de empresas de la UE innovadoras y creativas, tanto grandes como pequeñas, que operan en estos mercados.

El Grupo de trabajo del artículo 29 desea que estas expectativas se cumplan, en interés tanto de los ciudadanos como de la industria de la UE. Sin embargo, los beneficios que se esperan deben también respetar los numerosos retos a la intimidad y a la seguridad que se pueden asociar a la IO. Surgen muchas cuestiones en torno a la vulnerabilidad de dichos dispositivos, que a menudo se utilizan al margen de la estructura tradicional de las TI y no ofrecen suficiente seguridad. Las pérdidas de datos, la infección por programas maliciosos, así como el acceso no autorizado a datos personales, el uso invasor de dispositivos corporales y la vigilancia ilegal, suponen riesgos que las partes interesadas en la IO han de abordar para atraer a los usuarios finales potenciales de sus productos o servicios.

Más allá del cumplimiento de las condiciones jurídicas y técnicas, lo que está en juego su posible repercusión en la sociedad. Las organizaciones que colocan la intimidad y la protección de los datos en la primera línea del desarrollo de los productos estarán bien situadas para garantizar que sus productos y servicios respetan los principios de la intimidad desde el diseño y están equipados por defecto con los elementos respetuosos de la intimidad que los ciudadanos de la UE esperan.

De momento, este análisis solo ha sido formulado en términos muy generales por algunos organismos reguladores y partes interesadas, tanto en la UE como fuera de ella. El Grupo de trabajo del artículo 29 ha decidido ir más allá en esta cuestión adoptando el presente Dictamen. De esta manera, pretende contribuir a la aplicación uniforme del marco jurídico de protección de datos en la IO, así como al desarrollo de un elevado nivel de protección en lo que respecta a la protección de los datos personales en la UE. El cumplimiento de este marco es clave para abordar los retos jurídicos y técnicos, así como los sociales, pues se basa en la cualificación de la protección de los datos como un derecho humano fundamental.

Así pues, el presente Dictamen identifica los principales riesgos de la protección de datos que radican en el ecosistema de la IO, antes de proporcionar orientaciones sobre cómo se debería aplicar el marco jurídico de la UE en este contexto. El Grupo de trabajo respalda la incorporación por las partes interesadas pertinentes de las máximas garantías para los usuarios individuales en el núcleo de los proyectos. En particular, los usuarios deben tener siempre el control completo de sus datos personales a lo largo de todo el ciclo de vida del producto, y cuando las organizaciones se basen en el consentimiento como base del tratamiento, este deberá ser específico y los usuarios deberán darlo libremente y tras haber sido plenamente informados. Para que puedan cumplir este objetivo, el Grupo de trabajo elaboró un conjunto exhaustivo de recomendaciones prácticas dirigido a las diferentes partes interesadas afectadas (fabricantes de dispositivos, creadores de aplicaciones, plataformas sociales, destinatarios posteriores de los datos, plataformas de datos y organismos de normalización) que les ayudará a respetar la intimidad y la protección de datos en sus productos.

En efecto, la clave para respaldar la confianza y la innovación, y, por lo tanto, el éxito en esos mercados, es capacitar a las personas manteniéndolas informadas, libres y seguras. El Grupo de trabajo

cree firmemente que las partes interesadas que cumplan estas expectativas conseguirán una ventaja competitiva excepcionalmente fuerte sobre otros actores cuyos modelos empresariales se basen en no informar a sus clientes de la medida en que sus datos personales se tratan y se comparten y en encerrarlos en sus ecosistemas.

Teniendo en cuenta los importantes retos que la IO plantea en materia de protección de datos, el Grupo de trabajo del artículo 29 seguirá supervisando las novedades que se produzcan en este ámbito. A tal fin, está abierto a la cooperación en estas cuestiones con otros reguladores y legisladores nacionales e internacionales. También está abierto al debate con los representantes de la sociedad civil y de la industria, en particular cuando estas partes interesadas operan como responsables o encargados del tratamiento de datos en la UE.

INTRODUCCIÓN

El concepto de Internet de los objetos (IO) se refiere a una infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos («objetos» como tales, u objetos vinculados a otros objetos o individuos) registran, someten a tratamiento, almacenan y transfieren datos y, al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red. Dado que la IO se basa en el principio del tratamiento amplio de los datos mediante estos sensores diseñados para comunicar datos de manera inadvertida e intercambiarlos de manera fluida, está estrechamente relacionada con las nociones de informática «generalizada» y «ubicua».

Las partes interesadas en la IO desean ofrecer nuevas aplicaciones y servicios mediante la recopilación y posterior combinación de estos datos acerca de las personas, ya sea «únicamente» para medir los datos del usuario específicos del entorno, ya para observar y analizar sus hábitos de manera específica. Es decir, por lo general la IO implica el tratamiento de datos relacionados con personas físicas identificadas o identificables, por lo que se consideran datos personales en el sentido del artículo 2 de la Directiva sobre protección de datos de la UE.

El tratamiento de tales datos en este contexto se basa en la intervención coordinada de un número considerable de partes interesadas, como los fabricantes de dispositivos (que en ocasiones también actúan como plataformas de datos), agregadores o corredores de datos, creadores de aplicaciones, plataformas sociales, prestadores o arrendadores de dispositivos, etc.). Las funciones de cada una de estas partes interesadas se analizarán más adelante en el presente Dictamen. La implicación de las diferentes partes interesadas puede obedecer a razones diversas, a saber, proporcionar funcionalidades adicionales o interfaces de control fáciles de usar que permitan la gestión de los ajustes técnicos o relativos a la intimidad, o el acceso habitual del usuario a sus datos por medio de una interfaz web diferente. Por otra parte, una vez se ha procedido al almacenamiento remoto de los datos, estos se pueden compartir con otras partes, en algunos casos sin que lo sepa la persona afectada[1]. Cuando esto sucede, se impone al usuario la transmisión posterior de sus datos, y este no la puede evitar sin desactivar la mayor parte de las funcionalidades el dispositivo. A resultas de esta cadena de acciones, la IO puede poner a los fabricantes de los dispositivos y sus socios comerciales en condiciones de construir perfiles de usuario muy detallados o de tener acceso a ellos.

[1] http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

A la luz de lo anterior, el desarrollo de la IO plantea claramente retos nuevos y significativos en el ámbito de la protección de los datos personales y de la intimidad[2]. De hecho, una IO no sometida a controles podría evolucionar hacia el desarrollo de una forma de vigilancia de las personas que cabría considerar ilegal en el marco del Derecho de la UE. La IO suscita también grandes inquietudes, pues los fallos de seguridad pueden conllevar importantes riesgos para la intimidad de las personas cuyos datos son objeto de tratamiento en estos contextos.

Por consiguiente, el Grupo de trabajo del artículo 29 ha decidido emitir el presente Dictamen a fin de contribuir a la identificación y el seguimiento de los riesgos derivados de estas actividades en los casos en los que están en juego los derechos fundamentales de los ciudadanos de la UE.

[2] El presente informe deberá leerse conjuntamente con los dictámenes previos adoptados por el Grupo de trabajo en 2014 sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas (WP 211) y sobre la vigilancia de las comunicaciones electrónicas a efectos de inteligencia y seguridad nacional (WP 215).

1. Alcance del Dictamen: atención especial a tres aspectos del desarrollo de IO

En este momento resulta imposible prever las posibles evoluciones de la IO. Ello se debe en parte a que la cuestión de cómo transformar todos los datos que se puedan recoger en la IO en algo útil, y, por tanto, viable desde el punto de vista comercial, sigue, en gran medida, abierta. Tampoco están claras las posibles convergencias y sinergias de la IO con otros aspectos del desarrollo tecnológico, como la informática en la nube y el análisis predictivo, que, de momento, solo afectan a los avances de los nuevos mercados.

Por consiguiente, el Grupo de trabajo del artículo 29 ha decidido que el presente Dictamen se centre fundamentalmente en tres aspectos concretos del desarrollo de la IO (ordenadores corporales, «Yo cuantificado» y domótica), que, (1) se conectan al usuario mediante una interfaz directa y (2) corresponden a dispositivos y servicios que están realmente en uso, por lo que se prestan al análisis en virtud de las leyes de protección de datos. El presente Dictamen no se ocupa expresamente de las aplicaciones B2B ni de cuestiones más globales como las «ciudades inteligentes» o los «transportes inteligentes», ni tampoco de los entornos M2M (máquina a máquina). Sin embargo, los principios y recomendaciones formulados en el presente Dictamen se pueden aplicar más allá de su ámbito estricto y también cubren estos otros avances de la IO.

1.1 **Ordenadores corporales**

Los ordenadores corporales son objetos y prendas de ropa cotidianos, como relojes y gafas, que tienen sensores incorporados para ampliar sus funcionalidades. Es probable que los objetos corporales se adopten rápidamente, pues amplían la utilidad de objetos cotidianos conocidos por el usuario y resultan difíciles de diferenciar de sus análogos que no están conectados. Estos dispositivos pueden llevar integrados cámaras, micrófonos y sensores capaces de registrar y transferir datos a su fabricante. Por otra parte, la disponibilidad de API para dispositivos corporales (por ejemplo, Android Wear[3]) admite también la creación de aplicaciones por terceros que, de esta manera, pueden acceder a los datos recogidos por los dispositivos.

1.2 **«Yo cuantificado»**

Los dispositivos orientados al «Yo cuantificado» están diseñados para el uso regular por personas que desean registrar información sobre sus propios hábitos y estilos de vida. Por ejemplo, a una persona le puede interesar llevar por la noche un seguidor de sueño para tener una visión amplia de sus patrones de sueño. Otros dispositivos se centran en el movimiento; tal es el caso de los contadores de actividad, que elaboran de manera continua indicadores relacionados con la actividad física del usuario, como las calorías quemadas, las distancias recorridas u otros.

También hay dispositivos que miden el peso, el pulso y otros indicadores de salud. Mediante la observación de tendencias y cambios de comportamiento a lo largo del tiempo, los datos recogidos se pueden analizar para deducir información cualitativa relacionada con la salud, como evaluaciones de la calidad y los efectos de la actividad física, basándose en umbrales previamente definidos y en la presencia probable de síntomas de enfermedad, en cierta medida.

A menudo, para que los sensores de «Yo cuantificado» obtengan información pertinente, es necesario utilizarlos en unas condiciones determinadas. Por ejemplo, con los algoritmos adecuados, un acelerómetro situado en el cinturón del interesado podría medir los movimientos del abdomen («datos primarios»), extraer información sobre el ritmo respiratorio («datos agregados e información

[3] http://developer.android.com/wear/index.html

extraída») y mostrar el nivel de estrés del interesado («datos visualizables»). Algunos dispositivos solo comunican al usuario esta última información, pero el fabricante del aparato o el proveedor del servicio pueden tener acceso a otros muchos datos que se pueden analizar más adelante.

El «Yo cuantificado» supone un reto en cuanto a los tipos de datos recogidos que están relacionados con la salud, y por tanto pueden ser sensibles, así como respecto de su recogida extensiva. De hecho, dado que este movimiento se centra en motivar a los usuarios para que se mantengan sanos, está muy relacionado con el ecosistema de la eSalud. Sin embargo, investigaciones recientes han puesto en entredicho la precisión real de las mediciones y de las deducciones realizadas a partir de ellas[4].

1.3 **Automatización de viviendas («domótica»)**

También en las oficinas y en los hogares se pueden encontrar en la actualidad dispositivos de la IO, en forma de bombillas, termostatos, alarmas de incendio, estaciones meteorológicas, lavadoras u hornos «conectados» que se pueden controlar a distancia por Internet. Por ejemplo, los objetos que contienen sensores de movimiento pueden detectar y registrar que un usuario está en casa y cuáles son sus pautas de movimiento, y en algunos casos pueden desencadenar determinadas actuaciones previamente identificadas (como encender una luz o modificar la temperatura de una habitación). La mayoría de los dispositivos de automatización están conectados de manera constante y pueden enviar datos al fabricante.

Es evidente que la domótica plantea retos concretos en materia de protección de datos y de la intimidad, como un análisis de si las pautas de uso en tal contexto pueden revelar detalles del estilo de vida, las costumbres y las elecciones de los habitantes, o simplemente su presencia en casa.

Las tres categorías de dispositivos presentadas más arriba ilustran la mayor parte de las cuestiones sobre la intimidad relativas a la IO en su estado actual. Conviene señalar, no obstante, que esas categorías no son exclusivas: por ejemplo, un dispositivo «corporal», como un reloj inteligente, se puede utilizar para controlar el ritmo cardiaco, de cara, por ejemplo, a una evaluación del «Yo cuantificado».

2. Problemas de intimidad y protección de datos relacionados con la Internet de los objetos

El Grupo de trabajo del artículo 29 decidió emitir este Dictamen por considerar que la IO plantea diversos retos importantes relativos a la intimidad y la protección de los datos, algunos nuevos, otros más tradicionales, pero amplificados por el aumento exponencial del tratamiento de datos que conlleva la evolución de este fenómeno. La importancia de la aplicación del marco jurídico de protección de los datos de la UE y las correspondientes recomendaciones que se presentan más abajo se deben contemplar a la luz de estos retos.

2.1 **Falta de control y asimetría de la información**

Como consecuencia de la necesidad de prestar servicios generalizados de manera inadvertida, los usuarios podrían en la práctica acabar bajo el control de terceros. Ello puede dar lugar a situaciones de pérdida por el usuario del control de la difusión de sus datos, dependiendo de si la recogida y el tratamiento de esos datos se hacen o no con transparencia.

De manera más general, la interacción entre objetos, entre objetos y dispositivos personales, entre personas y otros objetos y entre objetos y sistemas *back-end* dará lugar a la generación de flujos de

[4] http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results

datos que difícilmente se podrán controlar con las herramientas clásicas utilizadas para garantizar la protección adecuada de los intereses y derechos de los afectados. Por ejemplo, a diferencia de otros tipos de contenido, es posible que los datos enviados por la IO no puedan ser adecuadamente revisados por el interesado antes de su publicación, lo que sin duda genera un riesgo de falta de control y exposición excesiva del usuario. Además, la comunicación entre objetos se puede desencadenar automáticamente o por defecto, sin que la persona afectada sea consciente de ello. Si no es posible controlar de manera efectiva cómo interactúan los objetos o definir límites virtuales que establezcan zonas activas o no activas para objetos concretos, resultará extremadamente difícil controlar el flujo de datos generado. Y aún será más difícil controlar el uso posterior de los datos y, por consiguiente, evitar una desviación de su uso. Esta cuestión de la falta de control, que afecta también a otros progresos técnicos, como la informática en la nube y los grandes datos, se revela aún más problemática si se piensa en las posibilidades de combinación de estas nuevas tecnologías.

2.2 **Calidad del consentimiento del usuario**

En muchos casos, es posible que el usuario no esté al corriente del tratamiento de los datos que realizan determinados objetos. Esta falta de información supone una barrera importante a la hora de demostrar el consentimiento válido regulado por el Derecho de la UE, pues el interesado debe estar informado. En estas circunstancias, no se puede confiar en el consentimiento como base jurídica para el correspondiente tratamiento de los datos con arreglo al Derecho de la UE.

Por otra parte, dispositivos corporales como los relojes inteligentes pasan desapercibidos[5]: la mayor parte de los observadores no podrían distinguir un reloj normal de uno conectado, y este podría llevar incorporados cámaras, micrófonos y sensores de movimiento capaces de registrar y transferir datos sin que las personas lo sepan o incluso con su consentimiento. Esto plantea la cuestión de la identificación del tratamiento de datos mediante ordenadores corporales, que se podría resolver con una señalización apropiada realmente visible para los interesados.

Además, al menos en algunos casos, la posibilidad de renunciar a ciertos servicios o características de un dispositivo de la IO es más un concepto teórico que una alternativa real. Así surge la pregunta de si el consentimiento del usuario al tratamiento de los datos subyacentes se puede considerar libre y, por lo tanto, válido según el Derecho de la UE.

Por otra parte, los mecanismos clásicos utilizados para obtener el consentimiento de las personas pueden resultar difíciles de aplicar en la IO, lo que da lugar a un consentimiento de baja calidad basado en la falta de información o en la imposibilidad objetiva de dar un consentimiento ajustado en línea con las preferencias expresadas por los interesados. En la práctica, actualmente parece que por lo general los sensores no están diseñados para proporcionar información por sí mismos ni para proporcionar un mecanismo válido para obtener el consentimiento del interesado. Sin embargo, las partes interesadas deberían plantearse nuevas maneras de obtener el consentimiento válido de los usuarios, incluida la implementación de mecanismos de consentimiento en los propios dispositivos. En este documento, más adelante, se comentan ejemplos concretos como los *privacy proxies* y las *sticky policies*.

[5] Como se describe en el Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, los ordenadores corporales también sacan a la luz retos derivados de la recogida continua de datos de otras personas que se encuentran a escasa distancia y durante periodos prolongados.

2.3 **Conclusiones extraídas de los datos y readaptación del tratamiento original**

El aumento de la cantidad de datos generados por la IO, en combinación con las técnicas modernas de análisis y cotejo de datos, puede prestar esos datos a usos secundarios, relacionados o no con el propósito asignado al tratamiento original. Es posible que los terceros que piden acceso a datos recogidos por otras partes quieran usar esos datos con fines totalmente diferentes.

Datos aparentemente insignificantes recogidos mediante un dispositivo (por ejemplo, el acelerómetro y el giroscopio de un teléfono inteligente) se pueden utilizar para deducir otra información con un significado totalmente distinto (por ejemplo, los hábitos de conducción del interesado). Esta posibilidad de extraer conclusiones de información «primaria» se ha de combinar con los riesgos clásicos analizados en relación con la fusión de datos de sensores, fenómeno bien conocido en el ámbito de la informática[6].

El «Yo cuantificado» ilustra también cuánta información se puede deducir de los sensores de movimiento mediante la agregación y un análisis avanzado. Estos dispositivos suelen utilizar sensores elementales para captar datos primarios (por ejemplo, los movimientos del interesado) y utilizan algoritmos sofisticados para extraer la información sensible (por ejemplo, el número de pasos) y deducir información potencialmente sensible que se mostrará a los usuarios finales (por ejemplo, su condición física).

Tal tendencia plantea unos retos concretos. De hecho, aunque el usuario se sienta cómodo compartiendo la información original para un fin determinado, es posible que no quiera compartir esa información secundaria que se podría utilizar con fines totalmente diferentes. Por consiguiente, es importante que las partes interesadas en la IO se aseguren en cada nivel (datos primarios, extraídos o visualizados) de que todos los fines para los que se utilizan los datos son compatibles con el fin original del tratamiento y de que el usuario está enterado de tales fines.

2.4 **Revelación invasiva de pautas de comportamiento y perfiles**

Aunque los diferentes objetos recogerán diferentes informaciones aisladas, una cantidad suficiente de datos recogidos y posteriormente analizados puede revelar determinados aspectos de los hábitos, comportamientos y preferencias de una persona. Como se ha visto más arriba, la generación de conocimiento a partir de datos triviales, o incluso anónimos, resultará más fácil con un mayor número de sensores e impulsará importantes capacidades de creación de perfiles.

Por otra parte, los análisis basados en información captada en un entorno de IO podrían hacer posible la detección de pautas de vida y comportamiento de una persona aún más detalladas y completas.

En realidad, es probable que esta tendencia influya en el comportamiento real del individuo, de la misma manera que, según se ha demostrado, el uso intensivo de circuitos cerrados de televisión ha influido en el comportamiento de los ciudadanos en los espacios abiertos. Con la IO, esta vigilancia potencial podría llegar ahora a alcanzar la esfera más privada de la vida de las personas, incluso en el hogar. Esto supondría una presión para evitar comportamientos no habituales con el fin de impedir la detección de lo que se podría considerar anómalo. Esta tendencia sería muy invasiva de la vida privada y la intimidad de las personas y se debe controlar muy estrechamente.

[6] La fusión de datos de sensores consiste en combinar datos de diferentes sensores o procedentes de diferentes fuentes para obtener información mejor y más precisa que la que se podría conseguir de esas fuentes por separado.

2.5 **Limitaciones de la posibilidad de permanecer en el anonimato cuando se hace uso de estos servicios**

El desarrollo pleno de las capacidades de la IO puede suponer una presión excesiva sobre las posibilidades actuales de uso anónimo de estos servicios, y generalmente limita las posibilidades de pasar desapercibido.

Por ejemplo, los objetos corporales que se mantienen muy cercanos al interesado hacen posible la disponibilidad de otros identificadores, como las direcciones MAC u otros dispositivos que podrían ser útiles para generar una huella digital que permita rastrear la localización del interesado. La recogida de múltiples direcciones MAC de múltiples sensores ayudará a crear huellas digitales únicas e identificadores más estables que las partes interesadas en la IO podrán atribuir a determinadas personas. Estos identificadores y huellas digitales se podrían usar para diferentes fines, incluido el análisis de la localización[7] o el análisis de las pautas de movimiento de grupos y de personas.

Esta tendencia se debe conjugar con la posibilidad de combinar esos datos más adelante con otros procedentes de otros sistemas (por ejemplo, televisión en circuito cerrado o registros de Internet).

En tales circunstancias, algunos de los datos obtenidos mediante sensores resultan especialmente vulnerables a los ataques de reidentificación.

A la luz de lo anterior, está claro que permanecer en el anonimato y proteger la intimidad en la IO será cada vez más difícil. El desarrollo de la IO suscita grandes preocupaciones relacionadas con la protección de datos y de la intimidad en este contexto.

2.6 **Riesgos para la seguridad: seguridad frente a eficiencia**

La IO plantea diversos problemas relacionados con la seguridad, pues las limitaciones impuestas por la seguridad y los recursos fuerzan a los fabricantes de los dispositivos a equilibrar la eficiencia de la batería y la seguridad del dispositivo. En particular, aún no está claro cómo equilibrarán los fabricantes de dispositivos la aplicación de las medidas de confidencialidad, integridad y disponibilidad a todos los niveles de la secuencia de tratamiento con la necesidad de optimizar el uso de los recursos informáticos (y la energía) en los objetos y los sensores.

Por consiguiente, se corre el riesgo de que la IO llegue a convertir un objeto de uso cotidiano en un objetivo potencial de intimidad y seguridad de la información a la vez que distribuye esos objetivos de una manera mucho más amplia que la versión actual de Internet. Los dispositivos conectados menos seguros constituyen nuevas maneras de ataque potencialmente eficientes entre las que se cuentan la facilidad de las prácticas de vigilancia y las violaciones de los datos personales, que pueden tener efectos generalizados en los derechos de consumidor y en la percepción que las personas tienen de la seguridad de la IO.

También se espera que los dispositivos y plataformas de la IO intercambien datos y los almacenen en las infraestructuras de los proveedores de servicios. Por tanto, al enfocar la cuestión de la seguridad de la IO no se ha de pensar únicamente en la seguridad de los dispositivos, sino también en la de los enlaces de comunicación, la infraestructura de almacenamiento y otros elementos de este ecosistema.

[7] El análisis de la localización es el análisis de cuántas personas se encuentran en un lugar determinado en un momento determinado y cuánto tiempo permanecen en él.

De la misma manera, la existencia de diferentes niveles de tratamiento de cuyos diseño técnico y aplicación se encargan diferentes partes interesadas no garantiza la adecuada coordinación entre todos ellos y puede dar lugar a la aparición de puntos débiles susceptibles de ser aprovechados.

Por ejemplo, en su mayor parte, los sensores que en la actualidad están presentes en el mercado no son capaces de establecer un enlace encriptado para las comunicaciones, pues los requisitos informáticos influyen en un dispositivo limitado por baterías de poca potencia. Respecto de la seguridad extremo a extremo, el resultado de la integración de los componentes físicos y lógicos aportados por un conjunto de diferentes partes interesadas solo garantiza el nivel de seguridad proporcionado por el componente más débil.

3. Aplicabilidad del Derecho de la UE al tratamiento de los datos personales en IO

3.1 **Normativa aplicable**

El marco jurídico pertinente para evaluar las cuestiones de intimidad y protección de datos planteadas por la IO en la UE está formado por la Directiva 95/46/CE y por determinadas disposiciones de la Directiva 2002/58/CE, en su versión modificada por la Directiva 2009/136/CE.

Este marco se aplica cuando se cumplen las condiciones necesarias, establecidas en el artículo 4 de la Directiva 95/46/CE. El Grupo de trabajo ha presentado amplias orientaciones sobre la interpretación de las disposiciones del artículo 4, concretamente en su Dictamen 8/2010[8] sobre el Derecho aplicable.

En particular, de conformidad con el artículo 4, apartado 1, letra a), de la Directiva, la legislación nacional de un Estado miembro es aplicable a todo tratamiento de datos personales efectuado «en el marco de las actividades de un establecimiento» del responsable en el territorio de dicho Estado miembro. La noción de «establecimiento» en la economía basada en Internet ha sido interpretada recientemente de una manera muy amplia por el Tribunal de Justicia Europeo[9].

También es aplicable la legislación nacional de un Estado miembro en los casos en los que el responsable del tratamiento no está establecido en el territorio de la Comunidad pero hace uso de «medios» situados en el territorio de un Estado miembro [artículo 4, apartado 1, letra c)]. Por tanto, incluso cuando una parte interesada en la IO considerada un responsable del tratamiento de datos con arreglo a la Directiva 95/46/CE no está establecida en la UE en el sentido del artículo 4, apartado 1, letra a) (independientemente de si interviene en la creación, la distribución o el funcionamiento de los dispositivos de la IO), probablemente estará sujeta al Derecho de la UE en tanto se sometan a tratamiento datos recogidos con «medios» de usuarios situados en la UE.

De hecho, todos los objetos que se utilizan para recoger y, posteriormente, someter a tratamiento los datos de las personas en el contexto de la prestación de servicios en la IO se consideran medios en el sentido de la Directiva. Evidentemente, esta calificación se aplica a los propios dispositivos (cuentapasos, seguidores de sueño, dispositivos domésticos conectados como termostatos, alarmas de incendios, gafas o relojes conectados, etc.). También se aplica a los dispositivos terminales de los usuarios (por ejemplo, teléfonos inteligentes o tabletas) en los que haya programas o aplicaciones previamente instalados tanto para controlar el entorno del usuario mediante sensores integrados o interfaces de red como para, posteriormente, enviar los datos recogidos por esos aparatos a los diferentes responsables del tratamiento de los datos implicados.

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf
[9] Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, asunto C-131/12 (apartados 45 a 60).

La identificación de la función de las diferentes partes interesadas implicadas en la IO será esencial para calificar su estatuto jurídico como responsables del tratamiento de datos, y de esta manera identificar la legislación nacional aplicable al tratamiento que realizan, así como las responsabilidades correspondientes. La identificación de la función de las partes implicadas en la IO se analizará más adelante, en la sección 3.3.

3.2 **La noción de datos personales**

El Derecho de la UE se aplica al tratamiento de los datos personales según la definición del artículo 2 de la Directiva 95/46/CE. El Grupo de trabajo ha presentado amplias orientaciones sobre la interpretación de esta noción, concretamente en su Dictamen 4/2007 sobre el concepto de datos personales[10].

En el contexto de la IO, sucede a menudo que una persona puede ser identificada a partir de datos procedentes de «objetos». Esos datos pueden servir para conocer el modelo de vida de una persona o una familia determinadas (por ejemplo, datos generados por el control centralizado de la iluminación, la calefacción, la ventilación y el aire acondicionado).

Además, incluso los datos relativos a las personas que se deberían someter a tratamiento haciendo uso de un seudónimo o con carácter anónimo se pueden considerar datos personales. De hecho, la gran cantidad de datos sometidos automáticamente a tratamiento en el contexto de la IO conlleva riesgos de reidentificación. A este respecto, el Grupo de trabajo remite a las novedades descritas en su reciente Dictamen sobre técnicas de anonimización, que ayuda a detectar esos riesgos y formula recomendaciones para la aplicación de estas técnicas[11].

3.3 **Partes interesadas en la IO como responsables del tratamiento de datos establecidos en la UE**

El concepto de responsable del tratamiento de datos y su interacción con el concepto de encargado del tratamiento de datos son esenciales en la aplicación de la Directiva 95/46/C, pues condicionan las respectivas responsabilidades de las diferentes organizaciones que intervienen en la aplicación del tratamiento de datos en relación con la normativa de protección de datos de la UE. Las partes interesadas pueden consultar el Dictamen 1/2010 del Grupo de trabajo del artículo 29 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»[12], que aportan orientaciones sobre la aplicación de este concepto a sistemas complejos con múltiples actores, en los que los responsables y los encargados del tratamiento intervienen, conjuntamente o por separado, en numerosos escenarios y con diferentes grados de autonomía y responsabilidad.

Casualmente, la aplicación de la IO implica la intervención combinada de múltiples partes interesadas, como fabricantes de dispositivos, plataformas sociales, aplicaciones de terceros, prestadores o arrendadores de dispositivos, corredores de datos[13] o plataformas de datos.

---

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[11] Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[12] Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», adoptado el 16 de febrero de 2010 (WP 169), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[13] Los corredores de datos compran datos mediante empresas para confeccionar listas de personas que pertenecen a una misma categoría o grupo. Estas categorías y grupos son establecidas por los corredores de datos, pero pueden reflejar atributos demográficos, ingresos o intereses manifiestos por determinados asuntos o productos.

El complejo entramado de partes interesadas exige e implica la necesidad de una asignación precisa de responsabilidades jurídicas entre ellos, en relación con el tratamiento de los datos personales, basándose en las especificidades de sus respectivas intervenciones.

3.3.1 Fabricantes de dispositivos

Los fabricantes de dispositivos de la IO no se limitan a vender objetos materiales a sus clientes o productos de marca blanca a otras organizaciones. Algunos de ellos también modifican el sistema operativo del «objeto» o instalan programas informáticos que determinan su funcionalidad general, lo que incluye los datos y su frecuencia de recogida, así como cuándo y a quién se transmiten los datos y con qué fines (por ejemplo, las empresas pueden valorar los seguros de sus empleados basándose en los datos registrados por los rastreadores que les hacen llevar[14]). De hecho, la mayoría recogen y someten a tratamiento datos personales generados por el dispositivo, con fines y medios establecidos únicamente por ellos. Así pues, los fabricantes de dispositivos se consideran responsables del tratamiento de datos con arreglo al Derecho de la UE.

3.3.2 Plataformas sociales

Probablemente, el interesado hará más uso de objetos conectados si puede compartir sus datos públicamente o con otros usuarios. En particular, los usuarios de dispositivos del «Yo cuantificado» tienden a compartir sus datos con otras personas en las redes sociales para potenciar una competencia positiva dentro del grupo.

En muchos casos, esta puesta común en las redes sociales de los datos recogidos y agregados por objetos tiene lugar de manera automática, una vez que el usuario ha configurado la aplicación para que así sea. Normalmente, la función de puesta en común viene establecida en los parámetros por defecto de las aplicaciones que proporciona el fabricante.

La responsabilidad específica de la protección de los datos corresponde a las plataformas sociales, pues es en ellas donde se agregan estos informes. Como es el propio usuario el que introduce los datos en las plataformas, cuando las redes sociales los someten a tratamiento con diferentes fines determinados por ellas mismas pasan a considerarse a todos los efectos responsables del tratamiento de datos en el sentido del Derecho de la UE. Por ejemplo, una red social puede utilizar información recogida por un podómetro para deducir que determinada usuaria práctica regularmente la marcha y mostrarle anuncios de calzado deportivo adecuado. Las consecuencias de esta calificación se detallan en el Dictamen del Grupo de trabajo del artículo 29 sobre las redes sociales en línea.[15]

3.3.3 Terceros creadores de aplicaciones

Muchos sensores exponen API para facilitar el desarrollo de aplicaciones. Para utilizar estas aplicaciones, el interesado ha de instalar aplicaciones de terceros que permiten a estos acceder a los datos que el fabricante del dispositivo ha guardado. La instalación de estas aplicaciones suele consistir en dar acceso a los datos al creador de la aplicación a través de API.

Algunas aplicaciones recompensan a los usuarios de determinados objetos; por ejemplo, una aplicación de una compañía de seguros sanitarios puede recompensar a los usuarios de objetos del «Yo cuantificado», o una compañía de seguros puede crear una aplicación específica para asegurarse de

[14] Con dispositivos apropiados, los empresarios pueden llevar el seguimiento de la salud de los empleados, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

[15] Dictamen 5/2009 sobre las redes sociales en línea, adoptado el 12 de junio de 2009 (WP 163), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

que el cliente ha conectado la alarma de incendios correctamente configurada. A menos que los datos se anonimicen, este acceso constituye un tratamiento con arreglo al artículo 2 de la Directiva 95/46/CE, de manera que el creador de la aplicación que ha establecido ese acceso a los datos se debe considerar un responsable del tratamiento de datos según lo dispuesto en el Derecho de la UE.

Por lo general, para que estas aplicaciones se instalen es necesario que el usuario se dé de alta explícitamente en ellas. De hecho, dado que este acceso está sujeto al requisito de obtener el consentimiento previo del usuario, ese consentimiento ha de ser claro y específico y el usuario lo debe dar tras haber sido plenamente informado. Sin embargo, en la práctica estas solicitudes de autorización realizadas por terceros creadores de aplicaciones no suelen mostrar información suficiente para que se pueda considerar que el usuario ha dado su consentimiento de manera específica, tras haber sido plenamente informado, y de forma válida de acuerdo con el Derecho de la UE (véase más abajo).

3.3.4 Otros terceros

Los terceros que no son fabricantes de dispositivos ni creadores de aplicaciones pueden utilizar los dispositivos de la IO para recoger información sobre personas y someterla a tratamiento. Por ejemplo, a las compañías de seguros les puede convenir regalar podómetros a sus clientes para controlar con qué frecuencia hacen ejercicio[16] y adaptar sus primas de seguro a esta información.

A diferencia de los fabricantes de dispositivos, estos terceros no tienen control sobre el tipo de datos que recoge el objeto. Sin embargo, se consideran responsables del tratamiento de datos, pues recogen y almacenan los datos generados por esos dispositivos de la IO para fines específicos que ellos mismos han determinado.

Ejemplo: Una compañía de seguros organiza una nueva campaña y ofrece un podómetro a los abonados que deseen solicitar tarifas más reducidas. Los abonados que aceptan la oferta reciben un podómetro configurado y registrado por la compañía. Aunque los abonados pueden acceder a los datos registrados por su podómetro, los dispositivos son propiedad de «FeelGood», que también tiene acceso a los datos de los abonados. En este contexto, los abonados se deben considerar interesados y se les debe dar acceso a su cuenta en la aplicación del podómetro, mientras que la compañía de seguros se considera un responsable del tratamiento de datos.

3.3.5 Plataformas de datos de IO

Por falta de normalización e interoperabilidad, la Internet de los objetos se ve en ocasiones como una «Intranet de los objetos» en la que cada fabricante ha definido el formato de su propio conjunto de interfaces y de sus datos. Los datos se alojan a continuación en entornos amurallados que impiden eficazmente a los usuarios transferir sus datos de un dispositivo a otro (o incluso combinarlos).

Sin embargo, los teléfonos inteligentes y las tabletas se han convertido en las pasarelas naturales de entrada a Internet de los datos recogidos mediante numerosos dispositivos de la IO. A resultas de ello, los fabricantes han ido desarrollando de manera progresiva plataformas cuyo objetivo es alojar los datos recogidos con los diferentes dispositivos, a fin de centralizar y simplificar su gestión.

[16] Con dispositivos apropiados, los empresarios pueden llevar un seguimiento de la salud de los empleados, http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

Cuando el desarrollo de estos servicios implica realmente la recogida de los datos de los usuarios para sus propios fines, esas plataformas también se pueden considerar responsables del tratamiento de datos con arreglo a la legislación de protección de datos de la UE.

3.4 Las personas como interesados: abonados, usuarios y no usuarios

El Derecho de la UE considera a los abonados y, de manera más general, a los usuarios de la IO, interesados. Si utilizan los datos que recogen y almacenan exclusivamente para fines personales o domésticos, quedan incluidos en la «exención doméstica» de la Directiva 95/46/CE[17]. Sin embargo, en la práctica, el modelo empresarial de la IO implica que los datos del usuario se transfieran sistemáticamente a los fabricantes de dispositivos, creadores de aplicaciones y otros terceros considerados responsables del tratamiento de datos. Por consiguiente, la «exención doméstica» será de aplicación limitada en el contexto de la IO.

El tratamiento de datos en la IO puede afectar también a personas que no son abonados ni usuarios reales de la IO. Por ejemplo, los dispositivos corporales, como las gafas inteligentes, pueden recoger datos sobre otros interesados diferentes del propietario del dispositivo. Conviene hacer hincapié en que este factor no impide la aplicación del Derecho de la UE a esas situaciones. La aplicación de la normativa de protección de datos de la UE no está condicionada a la propiedad del dispositivo o terminal, sino al tratamiento de los datos personales, independientemente de quién sea la persona afectada por esos datos.

4. Obligaciones de las partes interesadas en IO

Las partes interesadas en la IO consideradas responsables del tratamiento de datos (ya sea independientemente o junto con otras) con arreglo al Derecho de la UE deben cumplir las diferentes obligaciones impuestas por la Directiva 95/46/CE y las disposiciones pertinentes de la Directiva 2002/58/CE, si procede. El presente Dictamen solo trata de las disposiciones que merecen una atención específica en este contexto, si bien este enfoque limitado no impide la aplicación de las demás disposiciones.

4.1 Aplicación del artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas

El artículo 5, apartado 3, de la Directiva 2002/58/CE es aplicable a las situaciones en las que una parte interesada en la IO almacena información ya almacenada en un dispositivo de la IO u obtiene acceso a ella, siempre y cuando los dispositivos de la IO se consideren un «equipo terminal» en el sentido de esta disposición[18]. Esta disposición exige que, para que tales acciones sean legítimas, el abonado o usuario afectado dé su consentimiento para el almacenamiento o acceso, salvo que sea «estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado»[19]. Este requisito resulta especialmente importante cuando partes interesadas diferentes del usuario o abonado pueden acceder a información sensible para la intimidad almacenada en dichos equipos terminales[20].

---

[17] Véase el Dictamen 5/2009 sobre las redes sociales en línea, adoptado el 12 de junio de 2009 (WP 163).

[18] La noción de «equipos terminales» del artículo 5, apartado 3, se debe entender de la misma manera que la de «medios» del artículo 4, apartado 1, letra c) de la Directiva 95/46/CE.

[19] Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[20] Véase el considerando 25 de la Directiva 2002/58/CE.

El requisito de consentimiento del artículo 5, apartado 3, afecta principalmente a los fabricantes de dispositivos, pero también a las partes interesadas que desean tener acceso a esos datos primarios agregados almacenados en esa infraestructura. También se aplica a cualquier responsable del tratamiento de datos que desee almacenar datos adicionales en el dispositivo de un usuario.

En tales circunstancias, las partes interesadas en la IO deben velar por que la persona afectada haya dado efectivamente su consentimiento para el almacenamiento o el acceso, tras obtener del responsable del tratamiento de datos información clara y completa de, *inter alia*, los fines del tratamiento.

Por tanto, el consentimiento del usuario se ha de obtener antes de acceder a información del dispositivo que se pueda utilizar para generar una huella digital de algún dispositivo (incluidos los corporales). El Grupo de trabajo ya publicó unas orientaciones sobre la noción de consentimiento para las *cookies* o tecnologías de seguimiento similares en su Documento de Trabajo 02/2013 (WP 208) y aportará más directrices sobre esta cuestión en su futuro dictamen sobre huellas digitales.

Ejemplo: Un podómetro registra el número de pasos que da su usuario y almacena esta información en su memoria interna. El usuario instala en su ordenador una aplicación para descargar directamente el número de pasos desde el dispositivo. Si el fabricante del dispositivo desea cargar los datos del podómetro en sus servidores, ha de obtener el consentimiento del usuario en virtud del artículo 5, apartado 3, de la Directiva 2002/58/CE.

Una vez cargados los datos en los servidores del fabricante del dispositivo, este solo guarda los datos agregados acerca del número de pasos por minuto. Una aplicación que requiera acceso a estos datos, en tanto estén almacenados en el servidor del fabricante del dispositivo, no estará sujeta al artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas, sino a las disposiciones de la Directiva 95/46/CE relativas a la legitimidad de este tratamiento.

Por otra parte, es posible que la persona cuyos datos se vayan a controlar (el interesado) no sea el propietario del dispositivo de IO. Esa situación puede conducir a una aplicación distribuida del artículo 5, apartado 3, de la Directiva 2002/58/CE y la Directiva 95/46/CE.

Ejemplo: Un servicio de alquiler de automóviles instala un dispositivo inteligente de seguimiento en los automóviles que alquila. Aunque se considerará que el servicio de alquiler de automóviles es el propietario o abonado del servicio de seguimiento, el usuario del dispositivo será la persona que alquila el automóvil. El artículo 5, apartado 3, exige que el fabricante del dispositivo obtenga (como mínimo) el consentimiento del usuario del dispositivo, que en este caso es la persona que alquila el automóvil. Además, la legitimidad del tratamiento de los datos personales relacionados con las personas que alquilan los automóviles estará sujeta a los requisitos recogidos en el artículo 7 de la Directiva 95/46/CE.

4.2 **Fundamento jurídico del tratamiento (artículo 7 de la Directiva 95/46/CE).**

Para que el tratamiento de datos personales sea legítimo, las partes interesadas en la IO consideradas responsables del tratamiento de datos (véase la sección 4.3) han de cumplir uno de los requisitos enumerados en el artículo 7 de esta Directiva. Estos requisitos se aplican a algunas de las partes interesadas además del artículo 5, apartado 3, cuando el tratamiento en cuestión va más allá del

almacenamiento de la información o de la obtención de acceso a la información almacenada en los equipos terminales del usuario o abonado[21].

En la práctica, en este contexto hay tres fundamentos jurídicos pertinentes.

El primer fundamento jurídico en el que los fabricantes de dispositivos, las plataformas sociales o de datos, los prestadores de dispositivos o los terceros creadores se han de basar principalmente en el contexto de la IO es el consentimiento [artículo 7, letra a)]. En diversas ocasiones, el Grupo de trabajo ha publicado también orientaciones sobre la aplicación simultánea de los requisitos del artículo 7, letra a), y el artículo 5, apartado 3, de la Directiva 2002/58/CE[22]. Las condiciones para que ese consentimiento sea válido con arreglo al Derecho de la UE se han especificado en un Dictamen previo del Grupo de trabajo[23].

El artículo 7, letra b), establece también que el tratamiento es legítimo cuando es necesario para la ejecución de un contrato en el que el interesado sea parte. El alcance de este fundamento jurídico se limita al criterio de necesidad, que requiere una relación directa y objetiva entre el propio tratamiento y los fines del cumplimiento contractual que se espera del interesado.

En tercer lugar, el artículo 7, letra f), permite el tratamiento de los datos personales cuando es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado (en particular, su derecho a la intimidad en relación con el tratamiento de datos personales) que requieran protección con arreglo al apartado 1 del artículo 1 de la Directiva.

Su sentencia en el asunto *Google Spain*[24], el Tribunal de Justicia Europeo ha aportado indicaciones notables sobre la interpretación de esta disposición, además de las que ya había facilitado en los asuntos conjuntos previos ASNEF y FECEMD (C-468/10 y C-469/10). En el contexto de la IO, es probable que el tratamiento de los datos de una persona afecte considerablemente a sus derechos fundamentales y a la protección de los datos personales en situaciones en las que, sin dispositivos de IO, la interconexión de los datos hubiera sido imposible o muy dificultosa. Estas situaciones se pueden producir cuando los datos recogidos están relacionados con el estado de salud de la persona, su hogar o su intimidad, su localización y otros muchos aspectos de su vida privada. A la luz de la posible gravedad de esta injerencia, está claro que el tratamiento difícilmente se podrá justificar por el interés económico que una parte interesada en la IO tenga en él. Deberán estar en juego otros intereses perseguidos por el responsable del tratamiento de datos o por el tercero o terceros a los que se comuniquen los datos[25].

---

[21] Sobre la articulación del artículo 5, apartado 3, y el artículo 7, letra a), véanse en particular el Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, adoptado el 27 de febrero de 2013 (WP 202), pp. 14 y ss. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf y el Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE (WP 217), pp. 26, 32, 46.

[22] Dictamen WP 202, pp.14 y ss.

[23] Dictamen 15/2011 sobre la definición del consentimiento, adoptado el 3 de julio de 2011 (WP 187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

[24] Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, asunto C-131/12 (apartados 74 y ss.).

[25] Dictamen WP 217

Ejemplo: En el marco de un plan para promover el uso del transporte público y reducir la contaminación, el Ayuntamiento desea regular el estacionamiento en el centro de la ciudad imponiendo restricciones al acceso y tarifas de estacionamiento. El importe del estacionamiento depende de varios parámetros, como el tipo de motor (de gasóleo, de gasolina o eléctrico) y la antigüedad del vehículo. Cuando el automóvil se aproxima a una plaza de estacionamiento libre, un sensor puede leer la matrícula para, tras consultar una base de datos, calcular el recargo o el descuento que se aplicará automáticamente con arreglo a unos criterios previamente definidos. En este caso, el tratamiento de la información de la matrícula para determinar la tarifa podría satisfacer el interés legítimo del responsable del tratamiento de datos. Para un tratamiento adicional, como la obtención de información (sin anonimizarla) sobre el movimiento de los automóviles por una zona restringida, se requeriría la aplicación de otro fundamento jurídico.

4.3 **Principios relativos a la calidad de los datos**

Conjuntamente, los principios consagrados en el artículo 6 de la Directiva 95/46/CE constituyen una de las piedras angulares de la legislación de la UE sobre protección de datos.

Los datos personales se han de recoger y tratar de manera leal y lícita. El principio de lealtad exige expresamente que los datos personales no se recojan ni sometan a tratamiento sin que el interesado sea realmente consciente de ello. Este requisito es de suma importancia en relación con la IO, pues los sensores están diseñados para pasar lo más desapercibidos posible. Sin embargo, los responsables del tratamiento de datos que actúan en la IO (principalmente, los fabricantes de dispositivos) deben informar a todas las personas que se encuentran en la vecindad geográfica o digital de dispositivos conectados de que se están recogiendo datos sobre ellos o sobre su entorno. El cumplimiento de esta disposición va más allá de un requisito jurídico estricto: la recogida leal es una de las expectativas más cruciales de la persona en relación con la IO, y en particular cuando se trata de ordenadores corporales.

Ejemplo: Un dispositivo relacionado con la salud utiliza una pequeña luz para controlar el flujo sanguíneo en las venas y deducir información sobre el latido cardiaco. El dispositivo incluye otro sensor que mide el nivel de oxígeno en la sangre, pero no hay información disponible sobre la recogida de este dato ni en el dispositivo ni en la interfaz del usuario. Aunque el sensor que mide el nivel de oxígeno en la sangre es plenamente funcional, no se debe activar sin avisar primero al usuario. Para activar ese sensor se precisará un consentimiento explícito.

Según el principio de limitación de los fines, los datos solo se pueden recoger con fines determinados, explícitos y legítimos. Cualquier otro tratamiento incompatible con esos fines originales sería ilícito con arreglo al Derecho de la UE. El objetivo de este principio es que los usuarios sepan cómo y con qué fines se utilizarán sus datos y decidan si desean confiarlos a un responsable del tratamiento de datos. Estos fines se deben definir *antes* del tratamiento de los datos, lo que excluye cambios repentinos en las condiciones esenciales del tratamiento. Para ello es necesario que las partes interesadas en la IO tengan una buena visión general de su negocio antes de empezar a recoger datos personales.

Por otra parte, los datos recogidos sobre el interesado deben ser los estrictamente necesarios para el fin específico previamente determinado por el responsable del tratamiento de datos (principio de minimización de datos). Los datos innecesarios para ese fin no se deberán recoger y almacenar «por si acaso» o «porque pueden ser útiles más adelante». Algunas partes interesadas consideran que el principio de minimización de datos puede limitar oportunidades potenciales de la IO y, por lo tanto,

ser una barrera a la innovación, basándose en la idea de que los posibles beneficios del tratamiento de los datos se obtendrán mediante un análisis exploratorio con el que se buscarán correlaciones y tendencias que no sean obvias. El Grupo de trabajo no puede compartir este punto de vista e insiste en que el principio de minimización de datos desempeña un papel fundamental en los derechos de protección de los datos que el Derecho de la UE garantiza a las personas, por lo que se ha de respetar[26]. Este principio implica expresamente que cuando los datos personales no son necesarios para prestar un servicio determinado en la IO, como mínimo se debe ofrecer al interesado la posibilidad de usar el servicio de manera anónima.

El artículo 6 también establece que los datos personales recogidos y sometidos a tratamiento en el contexto de la IO se deben conservar durante un periodo no superior al necesario para el fin para el que fueron recogidos o para el que se traten ulteriormente. Esta comprobación de la necesidad la debe llevar a cabo cada una de las partes interesadas en la prestación de un servicio determinado de la IO, pues, de hecho, los fines de sus respectivos tratamientos pueden ser diferentes. Por ejemplo, los datos personales comunicados por un usuario cuando se abona a un determinado servicio de la IO se deben eliminar tan pronto como el usuario se da de baja en ese servicio. De manera similar, la información que el usuario elimina de su cuenta no se debe conservar. Cuando un usuario no hace uso de un servicio o una aplicación durante un periodo de tiempo definido, su perfil se debe desactivar. Transcurrido un periodo adicional, los datos deben eliminarse. Antes de dar estos pasos, la parte interesada debe notificárselo al usuario con los medios pertinentes que tenga a su disposición.

4.4 **Tratamiento de datos sensibles (artículo 8)**

Las aplicaciones de la IO pueden someter a tratamiento datos personales capaces de revelar el origen racial o étnico del interesado, sus opiniones políticas, sus creencias religiosas o filosóficas, su afiliación a algún sindicato o información sobre su salud o su vida sexual, que se consideran «datos sensibles» y merecen una protección especial en el sentido del artículo 8 de la Directiva 95/46/CE. En la práctica, para aplicar el artículo 8 a los datos sensibles en la IO es necesario que los responsables del tratamiento de datos obtengan el consentimiento explícito del usuario, salvo que el propio interesado haya hecho públicos esos datos.

Esta situación suele surgir en contextos determinados como los dispositivos del «Yo cuantificado». En tales casos, los dispositivos registran en su mayor parte datos relacionados con el bienestar de la persona. No siempre se trata de datos relativos a la salud, pero pueden proporcionar rápidamente información sobre la salud de la persona, pues se registran en el tiempo, lo cual permite realizar deducciones de su variabilidad a lo largo de un periodo dado. Los responsables del tratamiento de datos deben adelantarse a ese posible cambio de calificación y tomar medidas adecuadas al respecto.

Ejemplo: La empresa X ha desarrollado una aplicación que, analizando los datos primarios de las señales de electrocardiograma generadas por unos sensores comerciales que suelen estar a disposición del consumidor, es capaz de detectar pautas de drogadicción. El motor de la aplicación puede extraer características específicas de los datos primarios de ECG que, de acuerdo con los resultados de investigaciones previas, están relacionados con el consumo de drogas. El producto, compatible con la mayor parte de los sensores del mercado, se podría utilizar como aplicación independiente o mediante

[26] En cualquier caso, en la práctica la investigación exploratoria nunca se realiza totalmente al azar: el fin general de cualquier investigación adopta una definición tradicional, como mínimo parcial, aunque solo sea por razones de organización y de presupuesto. Cuesta imaginar que el tratamiento de los datos para una investigación determinada sea compatible con el fin original de la recogida de datos, lo que topa con el Derecho de la UE.

una interfaz web en la que se hayan de cargar los datos. Para tal fin es necesario obtener el consentimiento explícito del usuario. El cumplimiento de este requisito de consentimiento se puede satisfacer en las mismas condiciones y a la vez que se obtiene el consentimiento del interesado previsto en el artículo 7, letra a).

4.5 **Requisitos de transparencia (artículos 10 y 11)**

Más allá del requisito de recogida leal de los datos establecido en el artículo 6, letra a), en aplicación de los artículos 10 y 11 los responsables del tratamiento de datos deben comunicar a los interesados información específica: la identidad del responsable del tratamiento de datos, los fines del tratamiento, los destinatarios de los datos y la existencia de derechos de acceso y oposición (lo que incluye información sobre cómo desconectar el objeto para evitar la comunicación de datos a terceros).

Dependiendo de las aplicaciones, esta información se podría proporcionar, por ejemplo, en el propio objeto, utilizando la conectividad inalámbrica para transmitir la información o haciendo uso de la localización por medio de pruebas de proximidad que preserven la intimidad realizadas por un servidor central para informar a los usuarios de que están cerca del sensor.

Además, esta información se debe facilitar de manera clara y comprensible, de acuerdo con el principio de tratamiento leal. Por ejemplo, el fabricante del dispositivo podría imprimir en los objetos equipados con sensores un código QR o un Flashcode que describa el tipo de sensores y la información que capta, así como los fines de estas recopilaciones de datos.

4.6 **Seguridad (artículo 17)**

El artículo 17 de la Directiva sobre protección de datos impone «la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales» y dispone que «el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse».

Por consiguiente, cualquier parte interesada considerada responsable del tratamiento de datos es plenamente responsable de la seguridad del tratamiento de los datos. Si, a consecuencia de un diseño o un mantenimiento inadecuados de los dispositivos utilizados, se producen fallos de seguridad que dan lugar a infracciones del principio de seguridad, la responsabilidad del responsable del tratamiento de datos se ve comprometida. En este sentido, es necesario que esos responsables del tratamiento de datos lleven a cabo evaluaciones de la seguridad de los sistemas en conjunto, incluso a nivel de los componentes, aplicando los principios de la seguridad componible. En la misma línea, a fin de mejorar la seguridad general del ecosistema de la IO, se deben utilizar certificados de dispositivos y se han de adoptar las normas de seguridad reconocidas internacionalmente.

En sentido estricto, los subcontratistas que diseñan y manufacturan componentes de *hardware* por cuenta de otras partes interesadas sin someter realmente a tratamiento ningún dato personal no se pueden considerar responsables, en virtud del artículo 17 de la Directiva 95/46/CE, en caso de que se infrinja la protección de datos a causa de un defecto de la seguridad de esos dispositivos. Sin embargo, esas partes interesadas desempeñan un papel fundamental en el mantenimiento de la seguridad del ecosistema de la IO. Las partes interesadas con responsabilidades directas en la protección de datos frente a los interesados deben asegurarse de que esos subcontratistas aplican unas normas de seguridad estrictas en relación con la intimidad cuando diseñan y fabrican sus productos.

Como ya se ha dicho, al aplicar las medidas de seguridad se han de tener en cuenta las limitaciones operativas específicas de los dispositivos de la IO. Por ejemplo, en la actualidad, la mayor parte de los sensores no son capaces de establecer un vínculo encriptado debido a la prioridad de que goza la autonomía física del dispositivo o al control de los costes.

Por otra parte, la seguridad de los dispositivos que operan en la IO también es difícil de garantizar, por razones de carácter tanto técnico como empresarial. Dado que sus componentes suelen hacer uso de infraestructuras de comunicación inalámbrica y se caracterizan por la escasez de recursos en términos de energía y potencia informática, los dispositivos son vulnerables a los ataques físicos, al espionaje y a los ataques por medio de *proxies*. Las tecnologías más corrientes actualmente en uso (es decir, las infraestructuras PKI) no se pueden trasladar a los dispositivos IO, pues en su mayor parte estos carecen de la potencia informática precisa para enfrentarse a las tareas de tratamiento necesarias. La IO conlleva una compleja cadena de suministros con múltiples partes interesadas y diferentes grados de responsabilidad. Un fallo de seguridad puede tener su origen en cualquiera de ellas, especialmente cuando se trata de entornos M2M basados en el intercambio de datos entre dispositivos. Por consiguiente, se ha de tener en cuenta la necesidad de utilizar protocolos seguros y ligeros que se puedan aplicar en entornos con pocos recursos.

En este contexto en el que la reducida capacidad informática puede poner en peligro una comunicación segura y eficiente, el Grupo de trabajo del artículo 29 hace hincapié en que es aún más importante cumplir el principio de minimización de datos y restringir al mínimo necesario el tratamiento de los datos personales, y en particular su almacenamiento en el dispositivo.

Además, no todos los dispositivos diseñados para el acceso directo a través de Internet están configurados por el usuario. Por lo tanto, si se mantienen en funcionamiento con los parámetros por defecto pueden proporcionar una vía de fácil acceso a los intrusos. Las prácticas de seguridad basadas en restricciones de red, la desactivación por defecto de las funcionalidades que no son críticas y la imposibilidad de utilizar fuentes de actualización de programas que no sean de confianza (con lo que se limitan los ataques de programas maliciosos basados en la alteración de códigos) podrían contribuir a reducir el impacto y el alcance de las posibles violaciones de datos. Estas protecciones de la intimidad se deberían incorporar desde el comienzo, en aplicación del principio de «la protección de la intimidad desde el diseño».

Por otra parte, la ausencia de actualizaciones automáticas provoca frecuentes vulnerabilidades sin parches que se pueden descubrir fácilmente con motores de búsqueda especializados. Aunque los usuarios sean conscientes de las vulnerabilidades de sus propios dispositivos, puede suceder que no tengan acceso a las actualizaciones del proveedor, ya sea por limitaciones del *hardware*, ya porque la obsolescencia de las tecnologías impida que el dispositivo admita actualizaciones de los programas. En caso de que un fabricante de dispositivos deje de dar soporte a un dispositivo, se deberán proporcionar soluciones alternativas (por ejemplo, apertura del programa a la comunidad de fuente abierta). Se debe comunicar a los usuarios que sus dispositivos pueden ser vulnerables a fallos indeterminados.

Algunos de los sistemas de seguimiento automático que se encuentran en el mercado (como los podómetros y los seguidores de sueño) también presentan fallos de seguridad que permiten a los atacantes manipular los valores observados que se comunican a las aplicaciones y a los fabricantes de dispositivos. Resulta esencial que esos dispositivos ofrezcan protección adecuada contra la

manipulación de datos, en particular si los valores comunicados por los sensores tienen un impacto indirecto en las decisiones relacionadas con la salud de los usuarios.

Por último, una adecuada política de notificación de las violaciones de los datos también puede ayudar a limitar los efectos negativos de las vulnerabilidades de los programas y el diseño difundiendo conocimientos y aportando orientación sobre estas cuestiones.

5. Derechos del interesado

Las partes interesadas en la IO deben respetar los derechos de los interesados de conformidad con lo dispuesto en los artículos 12 y 14 de la Directiva 95/46/CE y adoptar medidas organizativas en este sentido. Estos derechos no se limitan a los abonados a los servicios de IO ni a los propietarios de dispositivos y afectan a toda persona cuyos datos personales se sometan a tratamiento.

5.1 **Derecho de acceso**

El artículo 12, letra a), establece que los interesados tienen derecho a obtener de los responsables del tratamiento de datos la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos.

En la práctica, los usuarios de la IO suelen tener bloqueados determinados sistemas. Por lo general, primero los dispositivos envían los datos al fabricante del dispositivo, quien a continuación los pone a disposición del usuario mediante un portal web o una aplicación. Este diseño permite a los fabricantes prestar servicios en línea que potencian las funciones del dispositivo, pero puede impedir que los usuarios elijan libremente el servicio que interactúa con su dispositivo.

Además, en la actualidad los usuarios finales no suelen estar en condiciones de acceder a los datos primarios registrados por los dispositivos de la IO. Está claro que tienen un interés más inmediato en los datos interpretados que en los primarios, que pueden no significar nada para ellos. Sin embargo, acceder a esos datos puede resultar útil para que los usuarios finales entiendan qué puede deducir de ellos el fabricante del dispositivo. Por otra parte, disponer de estos datos primarios les puede dar capacidad para transferir sus datos a otro responsable del tratamiento de datos y optar por otros servicios (por ejemplo, si el responsable original cambia de política de protección de la intimidad y ya no les satisface). En la práctica, estas personas no tienen más posibilidad que dejar de usar sus dispositivos, pues la mayoría de los responsables del tratamiento de datos no proporcionan esta funcionalidad y solo dan acceso a una versión degradada de los datos primarios almacenados.

El Grupo de trabajo del artículo 29 considera que estas actitudes impiden el ejercicio efectivo del derecho de acceso previsto en el artículo 12, letra a), de la Directiva 95/46/CE. Al contrario, sostiene que las partes interesadas en la IO deben tomar medidas para que los usuarios puedan ejercer este derecho de manera efectiva y ofrezcan a los usuarios la posibilidad de elegir otro servicio que quizás el fabricante del dispositivo no proponga. A este fin puede ser conveniente que se desarrollen unas normas de interoperabilidad de los datos.

Estas medidas serían muy pertinentes, pues el llamado «derecho a la portabilidad», que probablemente se consagrará en el Reglamento general de protección de datos como variante del derecho de acceso, tiene por objetivo poner fin a las situaciones de «bloqueo» del usuario[27]. En este sentido, el legislador europeo desea desbloquear los impedimentos a la competencia y ayudar a nuevos agentes a innovar en este mercado.

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

5.2 **Posibilidad de retirar el consentimiento y oponerse**

Los interesados han de tener la posibilidad de revocar cualquier consentimiento previo a un tratamiento de datos determinado y a oponerse al tratamiento de sus datos. El ejercicio de tales derechos debe ser posible sin limitaciones ni impedimentos de carácter técnico u organizativo y las herramientas proporcionadas para registrar la retirada del consentimiento deben ser accesibles, visibles y eficientes.

Los planes de retirada del consentimiento deben estar desglosados y han de abarcar: (1) los datos recogidos por un objeto determinado (por ejemplo, la petición de que una estación meteorológica deje de recoger datos sobre humedad, temperatura y sonido); (2) un tipo determinado de datos recogidos por cualquier objeto (por ejemplo, el usuario ha de tener la posibilidad de interrumpir la recogida de datos mediante cualquier dispositivo que registre sonidos, ya sea un seguidor del sueño o una estación meteorológica); (3) un tratamiento de datos determinado (por ejemplo, un usuario puede pedir que tanto su podómetro como su reloj dejen de contar los pasos que da).

Asimismo, dada la posibilidad de que los «objetos conectados» corporales acaben sustituyendo a los artículos existentes que proporcionan funcionalidades habituales, los responsables del tratamiento de datos deben ofrecer la opción de desconectar el objeto y permitir que funcione como el artículo original, no conectado (es decir, desactivar la funcionalidad conectada del reloj o las gafas inteligentes). El Grupo de trabajo ya ha especificado que los interesados deben tener la posibilidad de «retirar su consentimiento en cualquier momento y sin tener que abandonar» el servicio prestado[28].

Ejemplo: Un usuario instala en su apartamento una alarma de incendios conectada. La alarma contiene un sensor de ocupación, un sensor de calor, un sensor ultrasónico y un sensor de luz. Algunos de estos sensores son necesarios para detectar el fuego, mientras que otros solo aportan características adicionales sobre las que ha sido informado previamente. El usuario debería ser capaz de desactivar esas características para hacer uso únicamente de la alarma de incendios, y por lo tanto de desconectar los sensores que las captan.

Es interesante señalar que, gracias a algunas novedades recientes en este ámbito, se está intentando capacitar a los interesados dándoles más control sobre las características de gestión del consentimiento, por ejemplo mediante el uso de *sticky policies*[29] o *privacy proxies*[30].

6. Conclusiones y recomendaciones

[28] Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, adoptado el16 de mayo de 2011 (WP 185) - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[29] A este respecto, el uso de un enfoque basado en las llamadas *sticky policies* puede respaldar el cumplimiento del marco de protección de los datos integrando en los propios datos la información sobre las condiciones y los límites de uso. Así pues, estas políticas podrían establecer el contexto de uso de los datos, los fines, las políticas sobre el acceso de terceros y una lista de usuarios de confianza.

[30] Una manera de ofrecer un control real del interesado sobre cómo se pueden tratar los datos cuando interactúan con sensores siendo capaz de expresar las preferencias, incluidas la obtención y la retirada del consentimiento y las elecciones sobre la limitación del fin, se podría basar en el uso de *privacy proxies*. Sobre la base de un dispositivo, las solicitudes de datos se enfrentan a políticas previamente definidas que rigen el acceso a los datos bajo control del interesado. Definiendo pares de sensores y medidas, las peticiones de recogida de datos de los sensores o de acceso a esos datos formuladas por terceros se autorizarían, se limitarían o, simplemente, se rechazarían.

A continuación se enumeran las recomendaciones que el Grupo de trabajo del artículo 29 ha considerado útil formular a fin de facilitar la aplicación de los requisitos jurídicos de la UE a la IO, presentados más arriba.

Las recomendaciones siguientes solo aportan unas orientaciones adicionales a los documentos previamente adoptados por el Grupo de trabajo del artículo 29.

A este respecto, el Grupo de trabajo desea insistir especialmente en sus recomendaciones previas sobre las aplicaciones de los dispositivos inteligentes[31]. Dado que los teléfonos inteligentes forman parte del entorno de la IO y que los conjuntos de partes interesadas de ambos ecosistemas son semejantes, estas recomendaciones son directamente aplicables a la IO. En particular, los creadores de aplicaciones y los fabricantes de dispositivos deben proporcionar un nivel adecuado de información a los usuarios y ofrecerles maneras sencillas de darse de baja o formas de consentimiento más desglosadas, cuando proceda. Por otra parte, si no se ha obtenido el consentimiento, el responsable del tratamiento de los datos debe anonimizarlos antes de modificar su finalidad o de compartirlos con otras partes.

6.1 **Recomendaciones comunes a todas las partes interesadas**

- Antes de lanzar una nueva aplicación en IO, se deben efectuar las correspondientes evaluaciones de impacto sobre la intimidad (PIA). La metodología de realización de las PIA se puede basar en el Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad para las aplicaciones RFID que el Grupo de trabajo del artículo 29 adoptó el 12 de junio de 2011[32]. En los casos en que es apropiado o viable, las partes interesadas deben plantearse la posibilidad de poner la PIA correspondiente a la disposición del público en general. Se podrían desarrollar marcos específicos de la PIA para determinados ecosistemas de la IO (por ejemplo, ciudades inteligentes).

- Muchas de las partes interesadas en la IO solo necesitan datos agregados, y no los datos primarios recogidos por los dispositivos de la IO. Las partes interesadas deben eliminar los datos primarios apenas hayan extraído los datos necesarios para el tratamiento. En principio, la eliminación debe realizarse en el punto más cercano a la recogida de los datos primarios (por ejemplo, en el mismo dispositivo, tras el tratamiento).

- Todas las partes interesadas en IO deben aplicar los principios de la intimidad desde el diseño y la intimidad por defecto.

- En el contexto de la IO, la capacitación del usuario resulta esencial. Los interesados y usuarios deben ser capaces de ejercer sus derechos y, de esta manera, controlar los datos en todo momento de acuerdo con el principio de autodeterminación de los datos.

- Los métodos utilizados para presentar la información, ofreciendo la posibilidad de pedir el consentimiento o de denegarlo, deben ser tan fáciles de aplicar para el usuario como sea posible. En particular, las políticas de información y consentimiento se deben centrar en información comprensible por el usuario y no se deben limitar a una política general de intimidad publicada en el sitio web del responsable del tratamiento de datos.

[31] Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes (WP 202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

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

- Además, los dispositivos y las aplicaciones se deben diseñar de manera que informen a los interesados, sean o no usuarios, por ejemplo mediante la interfaz física del dispositivo o difundiendo una señal en un canal inalámbrico.

6.2 **Fabricantes de sistemas operativos y dispositivos**

- Los fabricantes de dispositivos deben informar a los usuarios del tipo de datos que se recogen mediante los sensores y se someten a tratamiento, de los tipos de datos que se reciben y de cómo se someterán a tratamiento y se combinarán.

- Los fabricantes de dispositivos deben ser capaces de comunicar inmediatamente al resto de las partes interesadas implicadas la retirada o la oposición del interesado a que sus datos se sometan a tratamiento.

- Al dar acceso a las aplicaciones, los fabricantes de dispositivos deben ofrecer opciones desglosadas. El desglose no debe afectar únicamente a la categoría de los datos recogidos, sino también al momento en que los datos se recogen y a la frecuencia con la que se recogen. De manera similar a la opción de «no molestar» de los teléfonos inteligentes, los dispositivos de la IO deberían incluir una opción de «no recoger datos» para programar o desactivar rápidamente los sensores.

- Para evitar el seguimiento y la localización, los fabricantes de dispositivos deben limitar las huellas digitales de los dispositivos desactivando las interfaces inalámbricas cuando no las usan, o utilizar identificadores aleatorios (como direcciones MAC aleatorias para buscar redes WiFi) a fin de impedir el uso de identificadores persistentes para el seguimiento y la localización.

- Para imponer la transparencia y el control por el usuario, los fabricantes de dispositivos deben proporcionar herramientas que efectúen la lectura, la edición y la modificación locales de los datos antes de transferirlos a un responsable del tratamiento de datos. Por otra parte, los datos personales sometidos a tratamiento se deben almacenar en un formato que permita la portabilidad.

- Los usuarios han de tener derecho de acceso a sus datos personales. Se les deben proporcionar herramientas que les permitan exportar fácilmente sus datos con un formato estructurado y de uso habitual. Por consiguiente, los fabricantes de dispositivos deben proporcionar una interfaz fácil de usar a los usuarios que deseen obtener datos agregados o los datos primarios que tienen almacenados.

- Los fabricantes de dispositivos deben proporcionar herramientas sencillas para enviar notificaciones a los usuarios y actualizar los dispositivos cuando se descubran vulnerabilidades de seguridad. Cuando un dispositivo se queda anticuado y se deja de utilizar, su fabricante debe notificárselo al usuario y asegurarse de que es consciente de que el dispositivo no se seguirá actualizando. También se ha de informar a todas las partes interesadas que puedan verse afectadas por la vulnerabilidad.

- Los fabricantes de dispositivos deben seguir un proceso de seguridad desde el diseño y dedicar algunos componentes a las primitivas criptográficas clave.

- Los fabricantes de dispositivos deben limitar en la mayor medida posible la cantidad de datos que salen de los dispositivos transformando directamente en el dispositivo los datos primarios en datos agregados. Los datos se deben agregar en un formato normalizado.

- A diferencia de los teléfonos inteligentes, los dispositivos de la IO pueden ser compartidos entre varios interesados, o incluso se pueden alquilar (por ejemplo, las casas inteligentes). Debe haber una configuración disponible que permita distinguir entre los diferentes individuos que utilicen el mismo dispositivo, de manera que no puedan enterarse de las actividades de los demás.

- Los fabricantes de dispositivos deben trabajar con los organismos de normalización y las plataformas de datos para aplicar un protocolo común que exprese las preferencias relativas a la recogida y el tratamiento de los datos por los responsables del tratamiento de datos, especialmente cuando los datos se recojan mediante dispositivos discretos.

- Los fabricantes de dispositivos deben hacer posible que las entidades responsables y encargadas del tratamiento de datos (las llamadas *privacy proxies*) permitan a los usuarios hacerse una idea clara de los datos recogidos por sus dispositivos y faciliten el almacenamiento y el tratamiento locales sin tener que transmitir los datos al fabricante del dispositivo.

6.3 **Creadores de aplicaciones**

- Se deben elaborar avisos o advertencias para recordar frecuentemente a los usuarios que los sensores están recogiendo datos. Si el creador de la aplicación no tiene acceso directo al dispositivo, la aplicación debe enviar periódicamente al usuario una notificación para recordarle que sigue registrando datos.

- Las aplicaciones deben facilitar el ejercicio del derecho del interesado al acceso, la modificación y la eliminación de la información personal recogida por los dispositivos de IO.

- Los creadores de aplicaciones deben proporcionar herramientas para que los interesados exporten tanto los datos primarios como los agregados en un formato normalizado y fácil de utilizar.

- Los creadores deben prestar una atención especial a los tipos de datos que se someten a tratamiento y a la posibilidad de deducir de ellos datos personales sensibles.

- Los creadores de aplicaciones deben aplicar el principio de minimización de datos. Cuando los fines se puedan alcanzar mediante datos agregados, los creadores no deberán acceder a los datos primarios. De manera más general, los creadores deben seguir un enfoque de intimidad desde el diseño y reducir la cantidad de datos recogidos al mínimo necesario para la prestación del servicio.

6.4 **Plataformas sociales**

- Los parámetros por defecto de las aplicaciones sociales basadas en dispositivos de IO deben pedir a los usuarios que revisen y editen la información generada por su dispositivo y decidan sobre ella antes de publicarla en las plataformas sociales.

- Por defecto, la información publicada por los dispositivos de IO en las plataformas sociales no debe hacerse pública ni ser indexada por motores de búsqueda.

6.5 **Propietarios de dispositivos de IO y otros destinatarios**

- El consentimiento para el uso de un dispositivo conectado y el tratamiento de los datos resultantes se debe dar libremente y tras haber sido plenamente informado. No se deben imponer sanciones económicas a los usuarios, y el acceso a las funciones de sus dispositivos no se debe degradar porque hayan decidido no utilizar el dispositivo o un servicio determinado.

- El interesado cuyos datos se estén sometiendo a tratamiento en el contexto de una relación contractual con el usuario de un dispositivo conectado (por ejemplo, un hotel, una compañía de seguros o un servicio de alquiler de automóviles) debe estar en condiciones de administrar el dispositivo. Independientemente de la existencia de relaciones contractuales, cualquier interesado que no sea usuario debe ser capaz de ejercer sus derechos de acceso y oposición.

- Los usuarios de los dispositivos de IO deben informar de la presencia de dispositivos de IO y del tipo de los datos recogidos a los interesados cuyos datos se recogen pero que no son usuarios. También deben respetar las preferencias de los interesados de que sus datos no sean recogidos por el dispositivo.

6.6 **Organismos de normalización y plataformas de datos**

- Los organismos de normalización y las plataformas de datos deben promover formatos de datos que sean portables e interoperables, además de claros y autoexplicativos, a fin de facilitar tanto la transferencia de datos entre diferentes partes y de ayudar a los interesados a entender qué datos sobre ellos están recogiendo realmente los dispositivos de IO.

- Los organismos de normalización y las plataformas de datos no deben centrarse únicamente en el formato de los datos primarios, sino también en la aparición de nuevos formatos para los datos agregados.

- Los organismos de normalización y las plataformas de datos deben promover los formatos de datos que contengan el menor número posible de identificadores fuertes, a fin de garantizar la adecuada anonimización de los datos de la IO.

- Los organismos de normalización deben trabajar en normas certificadas que establezcan el punto de partida de las salvaguardas de la seguridad y la intimidad de los interesados.

- Los organismos de normalización deben desarrollar protocolos ligeros de encriptación y comunicación adaptados a las especificidades de la IO que garanticen la confidencialidad, la integridad, la autenticación y el control del acceso.