

RETOS DE LA PROTECCIÓN DE DATOS EN LA INTERNET DE LOS OBJETOS PARA LAS PERSONAS MAYORES

Isidro Gómez-Juárez Sidera

Experto en Protección de Datos y Privacidad

Este trabajo ha obtenido el **Accésit Premio Estudios Financieros 2013** en la modalidad de **Derecho Constitucional-Administrativo**.

El Jurado ha estado compuesto por: don FRANCISCO MONTERDE FERRER, don JOSÉ LUIS MARTÍNEZ MORALES, don JOSÉ MANUEL PALAU NAVARRO, doña Remedio SÁNCHEZ FERRIZ y don RICARDO DE VICENTE DOMINGO.

Los trabajos se presentan con seudónimo y la selección se efectúa garantizando el anonimato del autor.

EXTRACTO

La expresión «Internet de los objetos» (IO) hace referencia al concepto general de objetos (tanto artefactos electrónicos como objetos de uso cotidiano) que se pueden leer, reconocer, dirigir, localizar o controlar a distancia a través de Internet. La Unión Europea (UE) ha subrayado que el alumbramiento de la IO no solo anticipa la Internet del futuro, sino que además permitirá responder a muchos retos actuales, como el envejecimiento de la población. No en vano, la propia UE ha resaltado la importancia de estudiar las implicaciones sociales, éticas y culturales de la IO, de cara a la posible gran transformación que experimentará la civilización a causa de dichas tecnologías. En este complejo escenario se plantean retos de gran calado para la protección de los derechos de las personas mayores, no debiendo entenderse dichos desafíos como una cuestión baladí que responda meramente a una visión futurista de la realidad, sino como la garantía de determinados derechos de tercera generación de este colectivo social especialmente vulnerable en el actual mundo desarrollado y tecnológicamente avanzado. En este sentido, hogares, residencias y ciudades inteligentes se perfilan como el nuevo ecosistema de las personas mayores en el mundo tecnológico del siglo XXI. Asimismo, la Comisión Europea espera que las aplicaciones de IO contribuyan en gran medida a responder a algunos de los desafíos de la sociedad de hoy, citando por caso los sistemas de vigilancia sanitaria que ayuden a entender las necesidades de una sociedad en proceso de envejecimiento. No en vano, la aparición de nuevos tipos de dispositivos móviles integrados, los avances en tecnologías inalámbricas y sensores inteligentes o la evolución de las tecnologías biométricas multiplican las oportunidades para el desarrollo de la innovación tecnológica orientada a las personas mayores y que, al margen de sus innegables ventajas para el fomento de su autonomía personal y la mejora de su calidad de vida, también conlleva nuevos riesgos para sus derechos. En dicho contexto, el presente trabajo tratará de resolver las principales cuestiones teórico-prácticas que giran en torno a la salvaguardia de uno de los derechos de tercera generación más significativos en el ámbito de Internet: el derecho fundamental a la protección de datos.

Palabras claves: protección de datos, Internet de los objetos (IO) y personas mayores.

Fecha de entrada: 03-05-2013 / *Fecha de aceptación:* 09-07-2013

THE INTERNET OF THINGS FOR THE ELDERLY AND THE CHALLENGES OF DATA PROTECTION

Isidro Gómez-Juárez Sidera

ABSTRACT

The term «Internet of Things» (IoT) refers to the general concept of objects (both electronic devices and everyday objects) that can be read, recognized, managed, located or remotely controlled via the Internet. The European Union (EU) has stressed that the introduction of IoT not only anticipates the Internet of the future, but will also be able to deal with many current challenges, such as the aging population. Not surprisingly, the EU itself has highlighted the importance of studying the social, ethical and cultural aspects of the IoT, to face the possible great transformation that civilization will experience because of these technologies. In this complex scenario, there are major challenges to protect the human rights of the elderly, these challenges should not be dealt with as a trivial matter merely responding to a futuristic vision of reality, but as a guarantee of certain third generation rights that are particularly vulnerable in today's developed and technologically advanced world. Therefore, homes, retirement homes and smart cities are emerging as a new ecosystem for the elderly in the technological world of the 21st century. Also, the European Commission expects IoT applications to contribute greatly in addressing some of the challenges of today's society, for example surveillance systems to help understand the needs of an aging society. Not surprisingly, the emergence of new types of integrated mobile devices, advances in wireless technologies and smart sensors or the evolution of biometric technologies, multiply the opportunities for the development of technological innovation aimed at the elderly but, apart from its undeniable advantages for the promotion of personal autonomy and improving their quality of life, it also brings about new risks for their rights. In this context, this study will try to resolve the major theoretical and practical issues that are related to safeguarding one of the third generation rights and most significantly in the field of the Internet: the fundamental right to data protection.

Keywords: data protection, Internet of Things (IoT) and elderly people.

Sumario

- I. La Internet de los objetos para las personas mayores
 - II. Sistemas de vigilancia sanitaria
 - 1. Dispositivos inteligentes para personas mayores en el ámbito de la salud
 - 2. Garantías para la protección de datos, dignidad e integridad física de las personas mayores
 - III. Sistemas de vigilancia en hogares, residencias y ciudades inteligentes
 - IV. Modulación de los principios de la protección de datos en la Internet de los objetos para las personas mayores
 - 1. Proporcionalidad, finalidad y minimización de datos
 - 2. Deber de información
 - 3. Consentimiento del interesado
 - V. Conclusiones: una nueva protección de datos para un nuevo paradigma
- Bibliografía

I. LA INTERNET DE LOS OBJETOS PARA LAS PERSONAS MAYORES

Tal y como reconoce la Exposición de Motivos de la Ley 39/2006, de 14 de diciembre, de promoción de la autonomía personal y atención a las personas en situación de dependencia, la atención a las personas en situación de dependencia y la promoción de su autonomía personal constituye uno de los principales retos de la política social de los países desarrollados. El reto no es otro que atender las necesidades de aquellas personas que, por encontrarse en situación de especial vulnerabilidad, requieren apoyos para desarrollar las actividades esenciales de la vida diaria, alcanzar una mayor autonomía personal y poder ejercer plenamente sus derechos de ciudadanía.

En España, los cambios demográficos y sociales están produciendo un incremento progresivo de la población en situación de dependencia. Por una parte, es necesario considerar el importante crecimiento de la población de más de 65 años, que se ha duplicado en los últimos treinta años, para pasar de 3,3 millones de personas en 1970 (un 9,7% de la población total) a más de 6,6 millones en 2000 (16,6%). A ello hay que añadir el fenómeno demográfico denominado «envejecimiento del envejecimiento», es decir, el aumento del colectivo de población con edad superior a 80 años, que se ha duplicado en solo veinte años¹.

Ambas cuestiones conforman una nueva realidad de la población mayor que conlleva problemas de dependencia en las últimas etapas de la vida para un colectivo de personas cada vez más amplio. Asimismo, diversos estudios ponen de manifiesto la clara correlación existente entre la edad y las situaciones de discapacidad, como muestra el hecho de que más del 32% de las personas mayores de 65 años tengan algún tipo de discapacidad, mientras que este porcentaje se reduce a un 5% para el resto de la población².

A nivel europeo, el Grupo Europeo de Ética en Ciencia y Nuevas Tecnologías (en adelante, EGE)³ ha señalado –con motivo de su Dictamen n.º 26, de 22 de febrero de 2012, titulado «Ética de

¹ Exposición de Motivos de la Ley 39/2006, de 14 de diciembre, de promoción de la autonomía personal y atención a las personas en situación de dependencia.

² *Ibidem*.

³ European Group on Ethics in Science and New Technologies. El Grupo, independiente y multidisciplinar, fue creado con el propósito de asesorar a la Comisión Europea sobre los aspectos éticos de la ciencia y las nuevas tecnologías en relación con la preparación e implementación de la legislación y política comunitarias. En la actualidad, está integrado por 15 miembros, provenientes de diferentes países y expertos en disciplinas diversas como la biología y la genética, la medicina, la informática, la filosofía o el derecho.

las Tecnologías de la Información y la Comunicación»⁴— que, según las proyecciones estimadas por el EUROSTAT⁵, para el año 2060 el 30% de los ciudadanos de la Unión Europea serán mayores de 65 años y el número de personas mayores de 80 serán más del doble —del 5 al 12%— alrededor del mismo periodo. Como consecuencia del envejecimiento de la población, se estima que el gasto sanitario crecerá entre un 1 y un 2% del Producto Interior Bruto (PIB) en la mayoría de los Estados miembros en el periodo 2008-2060; un incremento de aproximadamente el 25% de los actuales niveles de gasto. De tal manera, muchos Gobiernos de la Unión Europea se muestran proclives a apoyar el desarrollo de la innovación tecnológica para contribuir a la prestación de unos servicios de salud y asistencia social singularizados por una relación «calidad-coste del servicio» optimizada.

En el caso español, el Informe de la Fundación Vodafone, de 31 de mayo de 2011, titulado «Innovación TIC para las personas mayores. Situación, requerimientos y soluciones en la atención integral de la cronicidad y la dependencia», ha puesto de manifiesto que la principal preocupación de las personas mayores es la salud, y lo es por sus consecuencias en términos de dependencia, causa fundamental de sufrimiento y de mala autopercepción de salud⁶. En tal sentido, la variedad y dificultad en la provisión de la asistencia sanitaria y el soporte social necesarios para atender de forma idealmente correcta a las personas mayores según sea su estado de salud y función, hacen de la atención integral a estos pacientes un reto complejo y difícil de alcanzar en la práctica de los actuales escenarios de asistencia sanitaria y social. Según se desprende del citado Informe, muchas cosas han de cambiar en el actual contexto sociosanitario, y los materiales a utilizar y los métodos a seguir en ese camino del cambio no están en muchos casos definidos: se entra de lleno, pues, en el terreno de la innovación⁷.

De tal modo, hogares, residencias y ciudades inteligentes se perfilan como el nuevo ecosistema de las personas mayores en el mundo tecnológico del siglo XXI. En efecto, la aparición de nuevos tipos de dispositivos móviles integrados, los avances en tecnologías inalámbricas y sensores inteligentes, o la evolución de las tecnologías biométricas multiplican las oportunidades para el desarrollo de la innovación tecnológica orientada a las personas mayores y que, al margen de sus innegables ventajas para el fomento de su autonomía personal y la mejora de su calidad de vida, también conlleva nuevos riesgos para sus derechos.

A este respecto, interesa subrayar el desarrollo de sistemas basados en la tecnología de redes de sensores inalámbricas que permiten, a través de una serie de sensores de movimiento instalados en varias ubicaciones de la vivienda de la persona mayor, que sus familiares y cuidadores super-

⁴ Opinion of the European Group on Ethics in Science and New Technologies to the European Commission n.º 26, 22/02/2012, «Ethics of Information and Communication Technologies».

⁵ EUROSTAT es la oficina de estadística de la Unión Europea, situada en Luxemburgo. Su misión es proporcionar a la Unión Europea las estadísticas a nivel europeo que permitan comparaciones entre países y regiones.

⁶ VV. AA. (coord. HERNÁNDEZ SALVADOR, C.): *Innovación TIC para las personas mayores. Situación, requerimientos y soluciones en la atención integral de la cronicidad y la dependencia*, Fundación Vodafone, Madrid, 2011, pág. 9.

⁷ *Ibidem*, pág. 32.

visen determinadas actividades de su vida diaria, tales como cuándo se acuesta o se levanta de la cama, permanece sentada en el sillón, abre la nevera o el botiquín donde guarda los medicamentos, usa el inodoro, se ducha o sale de casa, así como otra serie de dispositivos inteligentes que permiten la supervisión y control de ciertos aspectos relacionados con su salud y bienestar físico, como su peso, presión arterial, pulso o niveles de glucosa⁸. Un caso ejemplar de la utilización de las nuevas tecnologías para un fin tan plausible como la mejora de la autonomía y la calidad de vida de las personas mayores, si bien condicionado a la necesidad de vivir en una orwelliana «casa de cristal», con todas sus consecuencias adversas.

De igual manera, la adopción de altos niveles de tecnología en las instituciones dedicadas al cuidado de las personas mayores plantea nuevos retos jurídicos. En este sentido, algunos ejemplos de la tecnología puesta al servicio de los mayores en las llamadas «residencias inteligentes» son los sistemas de seguimiento y control de errantes, desarrollados a partir de dispositivos de identificación por radiofrecuencia (RFID) y dispositivos basados en la tecnología GPS, o la utilización de sistemas de videovigilancia a fin de controlar y proteger a las personas mayores de riesgos como agresiones entre residentes, autolesiones, etc.⁹

Las ciudades inteligentes también tienen un espacio reservado para las personas mayores¹⁰. A título de ejemplo, podemos citar el desarrollo de aplicaciones digitales para la localización de enfermos de Alzheimer o afectados de demencia senil extraviados o desorientados, o las «experiencias *Smart City*» relacionadas con la movilidad y la utilización de transportes públicos por parte de personas invidentes (entre las cuales se encuentra un cierto número de **personas mayores como consecuencia del progresivo deterioro visual propio de la edad avanzada**).

De otro lado, el cuerpo humano constituye el siguiente horizonte del cibercrimen en relación con los dispositivos inteligentes para personas de edad avanzada en el ámbito de la salud (v. gr., enfermos de diabetes o insuficiencia cardiaca). En este sentido, numerosos expertos a nivel internacional han puesto de manifiesto los riesgos que entrañan para la vida de sus portadores los posibles ataques informáticos a las redes inalámbricas de comunicaciones electrónicas a través de las cuales se transmiten los datos relacionados con la salud del paciente que son necesarios para su monitorización por los correspondientes profesionales sanitarios y para el correcto funcionamiento del propio dispositivo tecnológico implantado en su cuerpo¹¹. En otros casos, los citados

⁸ Cfr. GÓMEZ-JUÁREZ SIDERA, I.: «Sistemas de vigilancia y personas mayores: un análisis desde la protección de datos», en *Revista Aranzadi de Derecho y Nuevas Tecnologías (RdNT)*, editorial Aranzadi, SA, Cizur Menor (Navarra), 2012, núm. 28, pág. 96.

⁹ *Ibidem*, pág. 89.

¹⁰ Cfr. Autoritat Catalana de Protecció de Dades (APDCAT): *La protecció de dades de caràcter personal en les ciutats intel·ligents («smart cities»)* –Document per al debat–, Barcelona, febrero de 2013, pág. 35.

¹¹ BBC News technology: «Warning over medical implant attacks» [en línea], 9 de abril de 2012. <http://www.bbc.com/news/technology-17623948> [consulta: 12 de octubre de 2012].

dispositivos no están implantados en el propio cuerpo de la persona mayor, sino que los porta en su ropa: en lo tocante a este particular, interesa señalar el desarrollo de prendas *e-wearable* que permiten adquirir parámetros biométricos, ritmo cardíaco y de respiración, temperatura corporal, posición del paciente o la actividad desarrollada por el mismo¹².

No en vano, la sociedad digital plantea retos de gran calado para la protección de los derechos de las personas mayores, no debiendo entenderse dichos desafíos como una cuestión baladí que responda meramente a una visión futurista de la realidad, sino como la garantía de determinados derechos de tercera generación¹³ de este colectivo social especialmente vulnerable en el mundo desarrollado y tecnológicamente avanzado. Prueba de ello es la notable preocupación de las instituciones y organismos europeos en lo tocante a la protección de datos de carácter personal y otros derechos estrechamente vinculados con la dignidad humana en el entorno digital.

En este sentido, el Supervisor Europeo de Protección de Datos (en adelante, SEPD)¹⁴ ha indicado que con las oportunidades y ventajas que acompañan al desarrollo de las tecnologías de la información y la comunicación (en adelante, TIC) llegan también nuevos riesgos, especialmente en lo relativo a la privacidad y la protección de los datos personales¹⁵. A juicio del SEPD, «las TIC suelen ayudar a que aumente (con bastante frecuencia, de maneras que no están a la vista de las personas) la cantidad de información que se recopila, clasifica, filtra, transfiere o posee de algún otro modo, con lo que los riesgos que conllevan estos datos se multiplican»¹⁶.

De otra parte, el EGE ha señalado que las cuestiones éticas relativas a la privacidad y la dignidad de las personas mayores han de ser, en todo caso, tenidas en cuenta en el marco de la innovación tecnológica. Mientras que la monitorización continua de los hogares y la actividad humana pueden ofrecer un entorno más seguro para las personas mayores, muchas de ellas recelan de una vigilancia constante y de la falta de control sobre sus propios datos. Situación que es más compleja, a juicio del propio EGE, en el supuesto del cuidado de personas mayores con deficiencias cognitivas que les impiden participar en la toma de decisiones en torno a la configuración de su privacidad¹⁷.

¹² ASINTEC - Centro Tecnológico de Confección: «INTELIGENTEX. Sistema de control y apoyo para residencias de mayores» [en línea], <http://www.asintec.org/pdf/inteligentex.pdf> [consulta: 18 de febrero de 2013].

¹³ Así como de otros derechos respecto de los cuáles determinados derechos de tercera generación tienen un valor instrumental.

¹⁴ La figura del SEPD se creó en 2001. El SEPD tiene la responsabilidad de garantizar que las instituciones y organismos de la Unión Europea respeten el derecho de las personas a la intimidad en el tratamiento de sus datos personales.

¹⁵ Dictamen del SEPD acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad (2010/C 280/01). Hecho en Bruselas, el 18 de marzo de 2010.

¹⁶ *Ibidem*.

¹⁷ *Cfr.* Opinion of the European Group on Ethics in Science and New Technologies to the European Commission n.º 26..., *op. cit.*

Finalmente, interesa señalar la gestación de un nuevo mercado de productos y servicios basados en la tecnología digital en torno a los fallecidos¹⁸ y que tiene cierta trascendencia sobre la protección de la memoria de los difuntos y los derechos e intereses legítimos de las personas vinculadas al mismo¹⁹. A título de ejemplo, cabe citar la integración de las nuevas tecnologías para la preservación de la memoria de los fallecidos a través de un servicio que permite incorporar a las lápidas tradicionales un código de barras bidimensional, un código QR (acrónimo del inglés *Quick Response*), para que cualquier usuario pueda descargarse información del difunto a través de un dispositivo móvil de forma gratuita, conociendo su biografía a través de texto e imágenes²⁰. En España, el Cementerio de Poblenou, situado en el barrio del mismo nombre al noreste de la ciudad de Barcelona, ha sido el primero en utilizar esta tecnología²¹.

En este escenario tecnológicamente complejo, se ha forjado la expresión «Internet de los objetos» (en adelante, IO) para hacer referencia al concepto general de objetos (tanto artefactos electrónicos como objetos de uso cotidiano) que se pueden leer, reconocer, dirigir, localizar o controlar a distancia a través de Internet²². A este respecto, el Parlamento Europeo ha resaltado la importancia de estudiar las implicaciones sociales, éticas y culturales de la IO, de cara a la posible gran transformación que experimentará la civilización a causa de dichas tecnologías²³.

A juicio del Parlamento Europeo, tanto el respeto de la privacidad y la protección de los datos personales como la apertura y la interoperabilidad son la única forma de que la IO adquiera una mayor aceptación social²⁴. Asimismo, cree firmemente que la protección de la privacidad constituye un valor básico y que todos los usuarios deben tener el control de sus datos

¹⁸ En este sentido, hacemos referencia a fallecidos o difuntos, en lugar de a «personas fallecidas», pues seguimos, en lo tocante al particular, la corriente doctrinal favorable a entender que, a efectos civiles, no hay persona tras el fallecimiento: «persona viva» es una redundancia, «persona fallecida» es una contradicción. *Cfr.* CASAS VALLÉS, R.: «Derecho a la imagen: el consentimiento y su revocación (nota a una sentencia de la AT de Barcelona de 19 de junio de 1988)», en *Revista del Poder Judicial*, núm. 14, 1989, pág. 133, pie de página 7.

¹⁹ GÓMEZ-JUÁREZ SIDERA, I.: «Protección de datos post mórtem en las redes sociales online», en el II Forum de Expertos y Jóvenes Investigadores en Derecho y Nuevas Tecnologías (FODERTICS), Universidad de Salamanca (USAL), marzo de 2013.

²⁰ Europa Press: *Lápidas con códigos QR permitirán conocer al difunto a través de la descarga de textos e imágenes* [en línea], 22 de octubre de 2012. <http://www.europapress.es/nacional/noticia-lapid-as-codigos-qr-permitiran-conocer-difunto-traves-descarga-textos-imagenes-20121022142005.html> [consulta: 3 de enero de 2013].

²¹ *Cfr.* Antena3.com: *Conoce la vida de un difunto con solo pasar el móvil sobre su tumba* [en línea], 11 de septiembre de 2012. http://www.antena3.com/noticias/tecnologia/conoce-vida-difunto-solo-pasar-movil-tumba_2012091100085.html [consulta: 20 de febrero de 2013].

²² Resolución del Parlamento Europeo, de 15 de junio de 2010, sobre la Internet de los objetos [2009/2224(INI)], considerando E.

²³ *Ibidem*, apdo. 14.

²⁴ *Ibidem*, apdo. 3.

personales²⁵. De tal manera, insiste sobre el hecho de que una de las condiciones previas para la promoción de la tecnología es la de establecer normas jurídicas que refuercen el respeto de los valores fundamentales, así como la protección de los datos personales y de la vida privada²⁶.

En un sentido similar, la Comisión Europea ha señalado que «[l]a aceptación social de la IO dependerá en gran medida del respeto de la privacidad y la protección de los datos personales, dos derechos fundamentales de la UE [Unión Europea]. Por una parte, la protección de la privacidad y de los datos personales influirá en cómo se conciba la IO. Por ejemplo, una casa equipada con un sistema de control de la salud podría procesar datos íntimos sobre algunos de sus habitantes. Un requisito previo para la confianza en estos sistemas y su aceptación es que se apliquen las medidas apropiadas de protección de datos contra posibles abusos y otros riesgos relativos a los datos personales»²⁷.

II. SISTEMAS DE VIGILANCIA SANITARIA

1. DISPOSITIVOS INTELIGENTES PARA PERSONAS MAYORES EN EL ÁMBITO DE LA SALUD

La Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 18 de junio de 2009, titulada «Internet de los objetos-Un plan de acción para Europa» [COM(2009)0278], presenta las perspectivas y los desafíos del desarrollo de la denominada «Internet de los objetos». En este sentido, la Comisión Europea espera que las aplicaciones de IO contribuyan en gran medida a responder a algunos de los desafíos de la sociedad de hoy, citando por caso los sistemas de vigilancia sanitaria que ayuden a entender las necesidades de una sociedad en proceso de envejecimiento.

En lo tocante a este particular, interesa señalar el desarrollo de dispositivos inteligentes para personas mayores en el ámbito de la salud (v. gr., enfermos de diabetes o insuficiencia cardíaca). Así por ejemplo, cabe citar la existencia de sistemas que permiten, a través de un sensor inalámbrico insertado en el tejido subcutáneo, enviar datos sobre el nivel de azúcar en la sangre del paciente a un dispositivo de control remoto: es lo que se conoce como medidor de glucosa continuo (CGM, acrónimo del inglés *continuous glucose meter*)²⁸. Asimismo, en el caso de pa-

²⁵ *Ibidem*, apdo. 4.

²⁶ *Ibidem*, apdo. 6.

²⁷ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 18 de junio de 2009, titulada «Internet de los objetos-Un plan de acción para Europa» [COM(2009)0278].

²⁸ RT Actualidad/Ciencia: «Un "hacker" estadounidense reclama más seguridad para los dispositivos de salud» [en línea], 8 de agosto de 2011. <http://actualidad.rt.com/ciencias/view/31046-Un-hacker-estadounidense-reclama-mas-seguridad-para-dispositivos-de-salud> [consulta: 18 de febrero de 2013].

cientes con insuficiencia cardiaca, se han desarrollado marcapasos inteligentes y dispositivos de desfibrilación²⁹ automática implantables en el cuerpo humano³⁰ que son controlados mediante una señal de radiofrecuencia³¹.

En un estadio tecnológico más avanzado, cabe citar el reciente desarrollo de dispositivos para tratar o evaluar determinadas patologías asociadas a las personas de edad avanzada (v. gr., dispositivos de neuroestimulación para el tratamiento de enfermedades como el Parkinson o el Alzheimer), que permiten insertar simultáneamente microelectrodos y canales para liberar fármacos. No en vano, las enfermedades relacionadas con el cerebro y el sistema nervioso son las más prevalentes en el mundo desarrollado. Asimismo, se está estudiando la posibilidad de recoger los datos relativos a la actividad cerebral del paciente a través de sistemas de telemetría mediante radiofrecuencia para dispositivos implantables en el cuerpo humano³².

En tal sentido, expertos en seguridad informática internacionalmente reconocidos sostienen que los homicidios cometidos a través de Internet serán una realidad a partir de 2014³³, reclamando mayores medidas de seguridad para los dispositivos inteligentes en el ámbito de la salud³⁴. Así por ejemplo, se ha puesto de manifiesto la existencia de importantes brechas de seguridad en los dispositivos inteligentes que suministran insulina a los enfermos de diabetes a través de un tubo subcutáneo y un medidor de glucosa continuo. De tal manera, la manipulación de los datos relativos a los niveles de glucosa que son objeto de transmisión a través de las redes inalámbricas de comunicaciones electrónicas podría condicionar el grado de suministro de la bomba de insulina, poniendo en riesgo la vida del paciente³⁵. De igual modo, la manipulación de las señales de radiofrecuencia que controlan los marcapasos inteligentes y desfibriladores automáticos implantables para pacientes con insuficiencia cardiaca podría poner en riesgo su propia vida. En este sentido, investigadores especialistas en seguridad informática han probado la vulnerabilidad de algunos de los citados dispositivos, siendo posible, mediante procesos de ingeniería inversa, realizar descargas eléctricas de elevada potencia (sobre unos 830 voltios) que podrían causar el

²⁹ Un desfibrilador es un aparato que aplica descargas eléctricas para restablecer el ritmo cardiaco normal.

³⁰ Desfibrilador automático implantable (en adelante, DAI).

³¹ BBC news technology: «Warning over...», *op. cit.*

³² El Mundo.es: «Una herramienta microscópica para analizar el cerebro» [en línea], 13 de marzo de 2013. <http://www.elmundo.es/elmundosalud/2013/03/12/neurociencia/1363114911.html> [consulta: 13 de marzo de 2013].

³³ IID (internet identity)/NEWS: «IID says 2013 cyberthreats are so 2012; predicts two years ahead: ubiquitous Internet connections will allow death by device and massive over-the-air theft by 2014» [en línea], 18 de diciembre de 2012. <http://www.internetidentity.com/news/?id=203> [consulta: 19 de febrero de 2013].

³⁴ Welivesecurity: «Malware and medical devices: hospitals really are unhealthy places...» [en línea], 18 de octubre de 2012. <http://www.welivesecurity.com/2012/10/18/malware-and-medical-devices-hospitals-really-are-unhealthy-places/> [consulta: 27 de febrero de 2013].

³⁵ RT Actualidad/Ciencia: «Un "hacker" estadounidense...», *op. cit.*

fallecimiento de sus portadores³⁶. En una línea similar, expertos de la University of Massachusetts Amherst (UMass) han puesto el acento sobre la necesidad de la utilización de sistemas de cifrado que garanticen que las señales de radiofrecuencia que controlan los mencionados dispositivos no sean manipuladas por terceros³⁷. Inclusive se ha estudiado la posibilidad de que el código malicioso (*malware*)³⁸ causante de la descarga eléctrica se propague de dispositivo en dispositivo —a modo de gusano informático— si estos se encuentran en un radio de acción lo suficientemente cercano (aproximadamente de unos nueve metros)³⁹, pudiendo causar el fallecimiento en cadena de sus portadores.

No en vano, el propio Parlamento Europeo ha observado que la información proporcionada por las tecnologías de la IO debe ser susceptible de ser trazada, verificada y corregida en caso de avería —en nuestro caso objeto de estudio, sustitúyase «avería» por «manipulación»— de un sistema que se base en ella, puesto que en determinados casos los errores en la información pueden poner vidas en peligro⁴⁰.

De otro lado, también ha de tenerse presente el desarrollo de prendas textiles inteligentes para la vigilancia sanitaria de las personas mayores. En el caso español, cabe referir la existencia de un programa pionero de telemedicina, liderado por el Centro Tecnológico de Confección de Talavera de la Reina (ASINTEC) y cofinanciado por el Fondo Europeo de Desarrollo Regional, basado en el desarrollo de prendas textiles inteligentes para la monitorización de las diferentes constantes vitales del paciente. En el seno del citado programa tuvo alumbramiento, bajo la denominación INTELIGENTEX⁴¹, un sistema de control y apoyo para residencias de mayores a partir de los siguientes elementos técnicos⁴²:

- Prendas *e-wearable* que permiten adquirir parámetros biométricos, ritmo cardiaco y de respiración, temperatura corporal, posición del paciente y actividad desarrollada.
- Dispositivos de control de presión arterial y glucosa.
- Elementos portátiles de recepción de datos mediante protocolos Bluetooth.

³⁶ Laboratorio Ontinet.Com: «Virus informáticos y marcapasos: una combinación de alto voltaje» [en línea], 19 de octubre de 2012. <http://blogs.protegerse.com/laboratorio/2012/10/19/virus-informaticos-y-marcapasos-una-combinacion-de-alto-voltaje/> [consulta: 27 de febrero de 2013].

³⁷ BBC news technology: «Warning over...», *op. cit.*

³⁸ Del inglés, *malicious software*.

³⁹ Laboratorio Ontinet.com: «Virus informáticos y marcapasos...», *op. cit.*

⁴⁰ Resolución del Parlamento Europeo, de 15 de junio de 2010..., *op. cit.*, apdo. 50.

⁴¹ Cfr. ASINTEC-Centro Tecnológico de Confección: «INTELIGENTEX: experiencia piloto apoyada en prendas inteligentes para asistencia a personas en situación de dependencia», en *Revista de Química e Industria Textil*, Asociación Española de Químicos y Coloristas Textiles, núm. 198, Barcelona, julio-agosto 2010, págs. 56-58.

⁴² Cfr. ASINTEC-Centro Tecnológico de Confección: «INTELIGENTEX. Sistema de control...», *op. cit.*

- Programas informáticos de almacenamiento de datos, histogramas, control de variables y agenda de actividades/actuaciones médicas en función de los resultados obtenidos, a través de una arquitectura de multidispositivos accesible en cualquier momento y desde cualquier lugar donde se disponga de conexión a Internet.

Dicho programa tuvo como experiencia piloto la residencia geriátrica de Belvís de la Jara (Toledo), a través de la utilización de prendas textiles inteligentes que medían las constantes vitales de los residentes y enviaban esta información, mediante Bluetooth, al sanitario, que de esta forma podía controlar al paciente desde cualquier lugar⁴³.

Citar finalmente el reciente nacimiento de un sistema de ayuda para enfermos de Alzheimer, consistente en la utilización de una sencilla chapa metálica, de unos cuatro centímetros de diámetro, que puede engancharse a la ropa de la persona mayor e incorpora un código QR⁴⁴ a través del cual puede tenerse acceso a determinada información personal, como los datos de carácter identificativo del portador de la chapa y del familiar responsable (v. gr., nombre y apellidos, dirección, teléfono, etc.), así como a otra serie de datos relacionados con la salud del enfermo (v. gr., grupo sanguíneo, patología, medicación, necesidades específicas, etc.). Para tener acceso a la citada información únicamente es necesario disponer de un teléfono móvil inteligente –*smartphone*– con lector de códigos QR integrado⁴⁵. De tal manera, cualquier persona que posea un teléfono móvil con la citada funcionalidad puede ayudar y orientar con altas probabilidades de éxito a un enfermo de Alzheimer extraviado que porte su chapa⁴⁶. El citado sistema de ayuda ha sido puesto en práctica por entes asociativos relacionados con dicha enfermedad, tales como la Asociación Alzheimer Asturias (AFA Asturias)⁴⁷ o la Asociación de Familiares, Enfermos y Colaboradores de Alzheimer de la Marina Baixa (AFA Marina Baixa)⁴⁸.

2. GARANTÍAS PARA LA PROTECCIÓN DE DATOS, DIGNIDAD E INTEGRIDAD FÍSICA DE LAS PERSONAS MAYORES

Con motivo de su Informe 0292/2010, el Gabinete Jurídico de la Unidad de Apoyo al Director de la Agencia Española de Protección de Datos (en adelante, AEPD) ha tenido ocasión de valorar

⁴³ Cfr. Agencia EFE: «Llevarse al médico puesto en la camiseta» [en línea], 15 de noviembre de 2010. <http://www.youtube.com/watch?v=bx8-d9wKKgI> [consulta: 18 de febrero de 2013].

⁴⁴ Vid. *supra*.

⁴⁵ Cfr. Elcomercio.es: «Los enfermos de alzhéimer portarán una chapa en la que irán encriptados sus datos personales» [en línea], 18 de marzo de 2013. <http://www.elcomercio.es/v/20130318/asturias/enfermos-alzheimer-portaran-chapa-20130318.html> [consulta: 18 de marzo de 2013].

⁴⁶ Cfr. Antena3.com «Las personas con alzhéimer llevarán un código identificativo para no perderse» [en línea], 21 de febrero de 2013. http://www.antena3.com/noticias/salud/personas-alzheimer-llevaran-codigo-identificativo-perderse_2013022100305.html [consulta: 15 de marzo de 2013].

⁴⁷ Cfr. Elcomercio.es: «Los enfermos de alzhéimer...», *op. cit.*

⁴⁸ Cfr. Antena3.com: «Las personas con alzhéimer...», *op. cit.*

el impacto de la utilización de dispositivos inteligentes implantables en el cuerpo humano sobre el derecho fundamental a la protección de datos. De tal manera, la garantía de este derecho en el citado contexto pivota, a juicio de nuestra autoridad, en torno a los siguientes ejes fundamentales: el consentimiento del interesado –que debería ser expreso cuando se trate de datos de carácter personal relacionados con la salud–, la adopción de las medidas de seguridad necesarias para evitar el acceso a la información por parte de personas no autorizadas, y el respeto escrupuloso de los principios de calidad, proporcionalidad y finalidad del tratamiento. Un criterio, en nuestra opinión, extrapolable a la utilización de dispositivos inteligentes en el ámbito de la salud que no sean implantables en el cuerpo humano pero recojan igualmente información sobre su portador (prendas *e-wearable*, elementos portátiles que incorporen un código QR con datos de salud, etc.)⁴⁹.

De tal manera, a juicio de la AEPD, con carácter general y salvo supuestos excepcionales, el criterio legitimador del tratamiento de datos de carácter personal a través de dispositivos inteligentes radica en la existencia del consentimiento libre, específico, informado e inequívoco del interesado. Además, cuando se trate de datos de carácter personal relacionados con la salud, dicho consentimiento deberá ser expreso, «derivándose necesariamente de una específica manifestación de voluntad mediante la que el interesado consienta y que revele una acción por su parte en tal sentido».

De igual modo, el consentimiento no solo debería verificarse en el momento de la implantación del dispositivo, sino que además debería concurrir en cada tratamiento relacionado con la lectura de los datos que el mismo pudiera contener, dado que dicha lectura podría llevarse a efecto por distintos sujetos. A criterio de nuestra autoridad de protección de datos, el cumplimiento de la citada exigencia puede plantear serias dificultades en el supuesto de que la información contenida en el dispositivo pueda ser leída a través de sistemas de identificación por radiofrecuencia (RFID): en tal sentido, la AEPD entiende que la información del dispositivo debería ser objeto de procedimientos que impidiesen lecturas no permitidas por el interesado, o su representante legal cuando se tratase de un incapacitado (v. gr., enfermos de Alzheimer o afectados de demencia senil)⁵⁰. Ello implica, siempre a juicio de la Agencia, la necesaria implantación en el propio dispositivo de las medidas de seguridad necesarias que garanticen el cifrado de toda la información contenida en el mismo para evitar su lectura en aquellos supuestos en los que no concurra el consentimiento del interesado.

Finalmente, la AEPD señala que, aún en el supuesto de que concurriese el consentimiento del interesado para la implantación y lectura de la información contenida en el dispositivo y que este reúna los requisitos de seguridad que se han indicado, sería preciso que el tratamiento resulte, además, respetuoso con los restantes principios de la protección de datos. De tal modo, si se contase con el consentimiento para tal tratamiento pero no resultase coherente con los citados principios, debería entenderse que aquel no se encuentra amparado por la Ley Orgánica 15/1999.

⁴⁹ *Vid. supra.*

⁵⁰ Sobre la prestación del consentimiento para el tratamiento de sus datos por parte de personas mayores que tengan afectada su capacidad de entender y querer volveremos más adelante.

En particular, debe tenerse en cuenta lo dispuesto en los artículos 4.1 y 4.2 de la Ley Orgánica 15/1999. Según el primero de ellos, «[l]os datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido». A su vez, el artículo 4.2 añade que «[l]os datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos».

Asimismo, y al margen del cumplimiento de los principios de la protección de datos, interesa subrayar la mención expresa que la propia AEPD realiza sobre el respeto a la dignidad de la persona y a su integridad física en relación con la utilización de dispositivos inteligentes implantables en el cuerpo humano: «[l]a implantación de la técnica descrita en la consulta resulta, lógicamente y como consecuencia de su propia naturaleza, invasiva, por cuanto el chip se implantaría bajo la piel del sujeto y previa realización de una pequeña intervención. Este hecho podría plantear serias implicaciones desde el punto de vista del derecho a la dignidad de la persona⁵¹ y a su integridad física, consagrado por la Constitución, que en principio escaparían a las competencias de esta Agencia pero podrían plantar problemas de índole legal en ámbitos distintos al de la actuación de aquella».

El EGE también se ha pronunciado en lo tocante a este particular con motivo de su Dictamen n.º 20, de 16 de marzo de 2005, titulado «Aspectos éticos de los implantes TIC en el cuerpo humano»⁵². En tal sentido, el EGE hace referencia a la posibilidad de exigir, con carácter adicional al consentimiento expreso del interesado, una autorización ad hoc de la autoridad de protección de datos como salvaguardia de la parte más sensible del «cuerpo electrónico» (*cf.*, a este respecto, la actual normativa italiana de protección de datos)⁵³. Ello para prevenir a los propios interesados de hacer accesibles determinadas partes de su cuerpo electrónico (v. gr., marcapasos y dispositivos de desfibrilación automática, medidores de glucosa continuos, etc.), de manera que pongan en peligro su propia integridad. Es por ello que, a juicio del citado Grupo de Trabajo,

⁵¹ A nuestro juicio, la dignidad de la persona no tiene la consideración de derecho desde un punto de vista formal, sino de valor jurídico fundamental. En este sentido, la importante Sentencia 53/1985, de 11 de abril, del Tribunal Constitucional, señala en su fundamento jurídico tercero que «[i]ndisolublemente relacionado con el derecho a la vida en su dimensión humana se encuentra el valor jurídico fundamental de la dignidad de la persona, reconocido en el artículo 10 como germen o núcleo de unos derechos "que le son inherentes". La relevancia y la significación superior de uno y otro valor y de los derechos que los encarnan se manifiesta en su colocación misma en el texto constitucional, ya que el artículo 10 es situado a la cabeza del título destinado a tratar de los derechos y deberes fundamentales, y el artículo 15 a la cabeza del capítulo donde se concretan estos derechos, lo que muestra que dentro del sistema constitucional son considerados como el punto de arranque, como el *prius* lógico y ontológico para la existencia y especificación de los demás derechos».

⁵² Opinion of the European Group on Ethics in Science and New Technologies to the European Commission N.º 20, 16/03/2005, «Ethical aspects of ICT implants in the human body».

⁵³ Artículo 26 del Decreto Legislativo 30 giugno 2003, n. 196, «Codice in materia di protezione dei dati personali».

cualquier tipo de implante TIC requiere de una valoración preliminar estricta a fin de evaluar el impacto sobre el derecho fundamental a la protección de datos del afectado o interesado. Asimismo, el EGE subraya la necesidad de respetar, en este contexto, los principios de minimización de datos, especificación de la finalidad, proporcionalidad y pertinencia: de tal manera, una determinada tecnología solo podrá ser legalmente aplicada si es indubitadamente idónea y necesaria en función de las circunstancias aplicables a cada caso concreto. Ello con la finalidad de evitar usos excesivos o inapropiados de las innovaciones tecnológicas disponibles.

En último lugar, interesa señalar la reflexión que el propio EGE realiza sobre el control externo de los portadores de dispositivos inteligentes implantables en el cuerpo humano en relación con su autonomía de la voluntad. De tal manera, el EGE entiende que la autonomía de la voluntad del individuo adquiere una singular trascendencia con la finalidad de impedir que su conducta pueda verse determinada o influenciada por las entidades responsables del control externo de los citados dispositivos. Incluso cuando no exista un control permanente del citado dispositivo, el respeto de la voluntad de su portador, en conjunción con otras salvaguardias (v. gr., adopción de las medidas de seguridad necesarias), se configura en un elemento clave en orden a impedir que la información contenida en el mismo no pueda ser modificada de manera remota sin su conocimiento.

III. SISTEMAS DE VIGILANCIA EN HOGARES, RESIDENCIAS Y CIUDADES INTELIGENTES

Como hemos tenido ocasión de señalar, la aparición de nuevos tipos de dispositivos móviles integrados, los avances en tecnologías inalámbricas y sensores inteligentes, o la evolución de las tecnologías biométricas multiplican las oportunidades para el desarrollo de la innovación tecnológica orientada a las personas mayores para el fomento de su autonomía personal y la mejora de su calidad de vida. En este sentido, las tecnologías de la IO han desembarcado en dos entornos esenciales de las personas mayores, tales como su propio hogar y las instituciones dedicadas a su cuidado. Asimismo, las llamadas ciudades inteligentes y las nuevas tecnologías inherentes a las mismas también contemplan entre sus beneficiarios a este colectivo social especialmente sensible.

De tal manera, un ejemplo de la tecnología puesta al servicio de los mayores son los sistemas de seguimiento y control de errantes en instituciones dedicadas al cuidado de las personas mayores. En lo tocante a este particular, debemos recordar la pérdida de la capacidad de orientación y déficit de la memoria propios del progresivo deterioro físico, sensorial, mental y cognitivo que, con carácter general, afecta a las personas mayores y en especial al colectivo que podríamos denominar «cuarta edad» o mayores ancianos (v. gr. enfermos de Alzheimer, afectados de demencia senil, etc.). En este sentido, se han desarrollado una serie de dispositivos —entre los cuales cabe citar los RFID y los dispositivos basados en la tecnología GPS— que permiten conocer la ubicación y movimientos de las personas que los portan, pudiendo, por ejemplo, localizar con

facilidad a una persona mayor que se haya extraviado o desorientado y evitar riesgos asociados como posibles caídas que puedan poner en peligro su propia integridad física⁵⁴.

Asimismo, interesa señalar que las instituciones dedicadas al cuidado de las personas mayores no dejan de ser un reflejo de la sociedad misma, en donde existen problemas de agresiones entre residentes, autolesiones, etc. En este sentido, cabe citar la utilización de sistemas de video-vigilancia a fin de controlar y proteger a los mayores de los riesgos expuestos⁵⁵.

En estrecha vinculación con las cuestiones relativas a los sistemas de vigilancia en instituciones dedicadas al cuidado de las personas mayores, surgen las relacionadas con la implementación de sistemas de vigilancia en su propio hogar con el propósito de prolongar la permanencia del mayor en su entorno habitual en unas condiciones adecuadas de autonomía y seguridad⁵⁶.

A este respecto, cabe volver a citar el desarrollo de sistemas basados en la tecnología de redes de sensores inalámbricas (*Wireless Sensor Networks*), que permiten, a través de una serie de sensores de movimiento instalados en varias ubicaciones de la vivienda del mayor, que sus familiares y cuidadores supervisen determinadas actividades de su vida diaria, tales como cuándo se acuesta o se levanta de la cama, permanece sentado en el sillón, abre la nevera o el botiquín donde guarda los medicamentos, usa el inodoro, se ducha o sale de casa, así como otra serie de dispositivos inteligentes que permiten la supervisión y control de ciertos aspectos relacionados con su salud y bienestar físico, como su peso, presión arterial, pulso o niveles de glucosa⁵⁷. Dicha información es enviada a los familiares y cuidadores de la persona mayor mediante un sistema de notificaciones personalizadas para la recepción de alertas a través de mensajes de correo electrónico, mensajes de texto dirigidos a su terminal de telefonía móvil o llamadas telefónicas, existiendo, además, la posibilidad de configurar el sistema para que la información sea accesible para el familiar, cuidador o incluso su médico a través de Internet, facilitando una instantánea de las actividades, rutinas diarias y otros aspectos relacionados con la salud del mayor que ayude a detectar posibles problemas (estado de salud, malestar físico, incumplimiento de la medicación, alimentación incorrecta, accidentes y caídas, pérdidas de orientación, etc.)⁵⁸.

Otro ejemplo de sistemas similares son los que podríamos denominar «pastilleros digitales», que avisan al familiar o cuidador, a través de una llamada telefónica, mensaje de texto o de correo electrónico, en aquellos casos en que la persona mayor olvide tomar su medicación. Igualmente,

⁵⁴ GÓMEZ-JUÁREZ SIDERA, I.: «Sistemas de vigilancia y personas mayores...», *op. cit.*, pág. 89.

⁵⁵ *Ibidem*.

⁵⁶ *Ibidem*, pág. 96.

⁵⁷ *Vid. supra*.

⁵⁸ *Cfr.*, sitios web de GrandCare Systems, Inc. y BeClose, Inc. [en línea]. <http://www.grandcare.com/> y <http://www.beclose.com/>.

los citados sistemas son configurables para que la información relativa a la toma de la medicación por parte del mayor sea accesible para el familiar, cuidador o su médico a través de Internet⁵⁹.

Junto a estas, señalar la existencia de otras tecnologías en fase de experimentación, tales como la instalación de sistemas de reconocimiento facial en el hogar de la persona mayor para la detección de su estado de ánimo a fin de mantener informados a sus familiares y cuidadores, que plantean importantes retos jurídicos a corto y medio plazo⁶⁰.

En último lugar, las llamadas ciudades inteligentes o *Smart Cities* plantean nuevos desafíos para la protección de datos de las personas mayores en el ámbito de la IO. Si bien no se dispone de una definición cerrada o uniforme de ciudad inteligente, algunos autores definen como *smart* aquella ciudad en la que las inversiones en capital humano y social y las infraestructuras de comunicación (con especial referencia a las TIC) están enfocadas al desarrollo económico sostenible, y en las que hay –o se persigue– una alta calidad de vida, una gestión inteligente de los recursos naturales y una gobernanza participativa a nivel social y cultural⁶¹.

En este sentido, resulta singularmente interesante la afirmación del Parlamento Europeo según la cual la IO comporta muchas ventajas para las personas con discapacidad y puede ser una forma de satisfacer las necesidades de una población que envejece, así como de ofrecer servicios de atención más sólidos⁶². De tal manera, en el entorno de las ciudades inteligentes, cabe citar el desarrollo de aplicaciones digitales para la localización de enfermos de Alzheimer o afectados de demencia senil extraviados o desorientados; así como el impulso de «experiencias *Smart City*» relacionadas con la movilidad y la utilización de transportes públicos por parte de personas invidentes o con dificultades visuales⁶³ (entre las cuales se encuentra un cierto número de **personas mayores como consecuencia del progresivo deterioro visual propio de la edad avanzada**)⁶⁴, que pueden experimentar mejor su entorno con ayuda de las tecnologías de la IO mediante dispositivos

⁵⁹ Cfr., sitio web de Medminder Systems, Inc. [en línea]. <https://www.medminder.com/>.

⁶⁰ GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M.: «La protección de datos de las personas mayores, necesidad y reto para una innovación tecnológica de calidad», en el Congreso de la Red Derecho TIC: la privacidad, ¿un lastre para la innovación tecnológica?, Universidad de Murcia, 22-23 de noviembre de 2012.

⁶¹ Autoritat catalana de protecció de dades (APDCAT): *La protecció de dades de caràcter personal... op. cit.*, pág. 5.

⁶² Resolución del Parlamento Europeo, de 15 de junio de 2010..., *op. cit.*, apdo. 31.

⁶³ A través de sensores de geolocalización y una brújula, una aplicación permite a las personas invidentes saber dónde se encuentran y les facilita el acceso en el transporte público.

⁶⁴ A juicio de SERRANO GARJO y RAMÍREZ SEBASTIÁN, «es claro que la edad es el marcador de riesgo más importante en relación con el deterioro sensorial, tanto auditivo como visual, multiplicándose enormemente la frecuencia del mismo con los años, hasta alcanzar una curva claramente exponencial en el caso de la visión». Cfr. SERRANO GARJO, P. y RAMÍREZ SEBASTIÁN, J. M.: «Edad, salud y deterioro de la visión: la disminución visual como síndrome geriátrico», en *Integración. Revista sobre ceguera y deficiencia visual*, Dirección General de la Organización Nacional de Ciegos Españoles, núm. 55 (Monográfico: Envejecimiento y discapacidad visual), diciembre de 2008, págs. 9-19.

auxiliares electrónicos⁶⁵. No obstante lo anterior, el propio Parlamento Europeo ha resaltado que, en dicho ámbito, deben tomarse medidas para garantizar la protección de la privacidad, facilitar la instalación y la gestión y proporcionar a los consumidores información sobre los servicios⁶⁶.

Como breve adelanto a nuestras conclusiones, la clave de la garantía del derecho fundamental a la protección de datos de las personas mayores en hogares, residencias y ciudades inteligentes estriba, a nuestro juicio, en el seguimiento sin fisuras de una línea de respeto a la autonomía de la voluntad de las personas mayores, siempre que ello sea legal y fácticamente posible, así como en una exquisita ponderación de los bienes jurídicos objeto de protección a la luz de las circunstancias concurrentes en cada caso concreto, de manera consecuente con el principio de proporcionalidad que debe regir cualquier medida restrictiva de derechos fundamentales. Completarían este juego de garantías los siguientes elementos: el respeto del contexto y una total transparencia en la información que se facilite a las personas mayores sobre el tratamiento de sus datos; la validez del consentimiento del interesado a efectos civiles; el respeto escrupuloso de los principios de finalidad y minimización de datos como límite infranqueable para los responsables del tratamiento; así como el sometimiento a unos criterios de seguridad singularmente rigurosos basados en el principio de privacidad desde el diseño (en adelante, PdD)⁶⁷.

IV. MODULACIÓN DE LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS EN LA INTERNET DE LOS OBJETOS PARA LAS PERSONAS MAYORES

1. PROPORCIONALIDAD, FINALIDAD Y MINIMIZACIÓN DE DATOS

El derecho a la protección de datos fue consagrado como un verdadero derecho fundamental autónomo e independiente del derecho a la intimidad en la trascendental Sentencia 292/2000, de 30 de noviembre, del Tribunal Constitucional, que supuso un punto de inflexión sin parangón hasta la fecha en la construcción jurisprudencial del mismo. Un reconocimiento que también le ha sido conferido en la Carta de Derechos Fundamentales de la Unión Europea, cuyo artículo 8.1 establece que «[t]oda persona tiene derecho a la protección de los datos de carácter personal que la conciernan».

Este derecho fundamental de tercera generación se halla estrechamente vinculado con el valor jurídico fundamental de la dignidad de la persona, proclamado en el artículo 10.1 de nuestra Constitución. No en vano, el derecho fundamental a la protección de datos de carácter personal persigue garantizar a la persona «un poder de control sobre sus datos personales, sobre su uso y destino, con

⁶⁵ Resolución del Parlamento Europeo, de 15 de junio de 2010..., *op. cit.*, apdo. 31.

⁶⁶ *Ibidem*.

⁶⁷ El término «Privacidad desde el Diseño» es traducción del anglosajón «*Privacy by Design*» (PbD).

el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado» (STC 292/2000, FJ 6). De tal manera, «el derecho fundamental a la protección de datos extiende su garantía no solo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 de la CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (STC 170/1987, de 30 de octubre, FJ 4), como el derecho al honor, citado expresamente en el artículo 18.4 de la CE, e igualmente, en expresión bien amplia del propio artículo 18.4 de la CE, al pleno ejercicio de los derechos de la persona» (STC 292/2000, FJ 6).

Indicar en este sentido que la AEPD ha venido tradicionalmente poniendo de manifiesto que el derecho fundamental a la protección de datos de carácter personal forma parte de los jurídico-civilmente identificados como «derechos de la personalidad»⁶⁸, derechos subjetivos cuyo objeto viene constituido por los diversos bienes o facetas que integran el mundo corporal o anímico de la persona, de forma que esta, sujeto de derecho, resulta ser al mismo tiempo objeto del mismo⁶⁹: de ahí su íntima vinculación con el valor jurídico fundamental de la dignidad de la persona⁷⁰.

De lo antepuesto se colige que el valor jurídico fundamental de la dignidad de la persona es el germen o fundamento último del derecho fundamental a la protección de datos de carácter personal consagrado en la STC 292/2000, en tanto en cuanto este derecho se configura como un derecho fundamental inherente a la persona. Y, a su vez, el derecho fundamental a la protección de datos de carácter personal constituye una manifestación o cristalización del valor jurídico fundamental de la dignidad de la persona⁷¹.

Por todo lo cual, desde el entendimiento por la jurisprudencia constitucional del derecho a la protección de datos como un derecho de la personalidad consustancial a la dignidad humana, concebimos el respeto a la protección de los datos de las personas mayores como el respeto a su propia dignidad personal⁷².

⁶⁸ Este razonamiento ha venido amparándose en la vinculación existente entre el derecho a la protección de datos y la intimidad de las personas, si bien debe seguir considerándose aplicable tras la configuración otorgada a la protección de datos como un derecho fundamental de la persona por la Sentencia 292/2000, de 30 de noviembre, del Tribunal Constitucional. *Cfr.* Informes 365/2006 y 0278/2009 del Gabinete Jurídico de la Unidad de Apoyo al Director de la AEPD.

⁶⁹ CARRASCO PERERA, A. (director); CORDERO LOBATO, E., *et al.*: *Derecho Civil (Introducción. Derecho de la persona. Derecho subjetivo. Derecho de propiedad)*, Editorial Tecnos, SA, 2.ª edición, Madrid, 2004, pág. 82.

⁷⁰ GÓMEZ-JUÁREZ SIDERA, I. y LARA YUSTE, F.: «Personas mayores en la sociedad de las nuevas tecnologías: la necesidad de navegar hacia un horizonte donde el derecho a la protección de sus datos sea plenamente respetado», en la revista digital *Datospersonales.org* [en línea], Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), 31 de julio de 2009, Madrid, núm. 40. http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142560422023&esArticulo=true&idRevistaElegida=1142557356539&language=es&pagename=RevistaDatosPersonales%2FPagae%2Fhome_RDP&siteName=RevistaDatosPersonales [consulta: 10 de octubre de 2012].

⁷¹ *Ibidem*.

⁷² Véase nota anterior.

A nivel supranacional, el Grupo de Protección de Datos del artículo 29 (en adelante, GT 29)⁷³, en su Opinión 3/2012, sobre la evolución de las tecnologías biométricas, adoptada el 27 de abril de 2012, ha reconocido la condición de las personas mayores como un colectivo social de especial fragilidad, así como el significativo impacto sobre su propia dignidad de determinados tratamientos de datos que podrían conducir a su estigmatización o discriminación. De tal manera, el GT 29 aboga por la adopción de salvaguardias específicas en relación con determinados tratamientos de datos de las personas mayores, a fin de garantizar el respeto de su dignidad humana y sus libertades fundamentales. Entre otras, señala la necesidad de establecer criterios más estrictos en el proceso de evaluación del impacto de las operaciones de tratamiento de datos que puedan afectar a la dignidad de las personas mayores, ello tanto en términos de necesidad y proporcionalidad como de posibilidad real de los afectados de ejercer de manera efectiva su derecho a la protección de datos.

Asimismo, el Parlamento Europeo ha acentuado la importancia de garantizar la protección de todos los derechos fundamentales –no solo el derecho a la protección de datos de carácter personal– en el proceso de desarrollo de la IO⁷⁴.

En este sentido, el derecho fundamental a la protección de datos, dotado de determinación, autonomía y contenido propios desde su consagración en la STC 292/2000 y en la propia Carta de Derechos Fundamentales de la Unión Europea, tiene, a su vez, un importante valor como instrumento para la efectividad de otros derechos estrechamente vinculados con la dignidad de la persona. Un valor instrumental que adquiere una singular relevancia para el desarrollo efectivo de determinados derechos de las personas mayores, entendidas estas como un colectivo social especialmente vulnerable⁷⁵. En tal sentido, cabe citar, entre otros, el derecho de las personas mayores a llevar una vida digna e independiente, el derecho a la igualdad y no discriminación por razones de edad, el derecho a la libre circulación e incluso el derecho a la vida y a la integridad física⁷⁶.

Así por ejemplo, el respeto del derecho fundamental a la protección de datos, en su vertiente de seguridad de los datos, se presenta como una exigencia consustancial al diseño de implantes TIC para personas mayores que sufran enfermedades crónicas, con el objeto de impedir el acceso no autorizado o la alteración de los datos relacionados con la salud del paciente y que pudieran

⁷³ Grupo de protección de las personas en lo que respecta al tratamiento de datos personales. Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo europeo, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

⁷⁴ Resolución del Parlamento Europeo, de 15 de junio de 2010..., *op. cit.*, apdo. 56.

⁷⁵ Si bien los datos de las personas mayores no tienen, conforme a lo establecido en nuestra normativa, la consideración jurídica de «datos especialmente protegidos» per se, estos forman parte, a nuestro juicio, de una categoría sui generis que podríamos denominar «datos de personas especialmente vulnerables», basada en un criterio subjetivo en función de las personas titulares de los datos y las especiales circunstancias que les caracterizan.

⁷⁶ GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M.: «La protección de datos de las personas mayores...», *op. cit.*

entrañar un riesgo para su vida o su integridad física como consecuencia de un funcionamiento anómalo del dispositivo tecnológico implantado en su cuerpo⁷⁷.

De igual modo, el derecho fundamental a la protección de datos –en sus múltiples manifestaciones de información, consentimiento, calidad, proporcionalidad y seguridad– actúa como garante de determinados derechos íntimamente relacionados con la dignidad de las personas mayores en supuestos tales como la implantación de sistemas de vigilancia en el hogar de la persona mayor y en instituciones dedicadas a su cuidado o el desarrollo de «experiencias *Smart City*» específicamente orientadas a este colectivo social de especial sensibilidad. En tal sentido, cabe citar el derecho «a llevar una vida digna e independiente», consagrado en el artículo 25⁷⁸ de la Carta de los Derechos Fundamentales de la Unión Europea, o el no menos trascendente derecho a la libre circulación de las personas, recogido en el artículo 2 del Protocolo Adicional n.º 4 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. A este respecto, el Dictamen 4/2004 del GT 29 recoge que «dicha libertad de circulación solo puede estar sujeta a restricciones necesarias en una sociedad democrática y proporcionales a la consecución de fines específicos»⁷⁹. De tal manera, «los interesados tienen derecho a ejercer su derecho a la libre circulación sin verse sometidos a un condicionamiento psicológico excesivo en cuanto a sus movimientos y su conducta y sin ser objeto de un control detallado, como la posibilidad de que se sigan sus movimientos...»⁸⁰.

Sentado lo anterior, interesa puntualizar que, de conformidad con la doctrina del Tribunal Constitucional, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan, basta con recordar que (como sintetizan las SSTC 66/1995, de 8 de mayo [RTC 1995\66], F.5; 55/1996, de 28 de marzo [RTC 1996\55], FF. 6, 7, 8 y 9; 207/1996, de 16 de diciembre [RTC1996\207], F.4.e) y 37/1998, de 17 de febrero [RTC 1998\37], F.8) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)⁸¹.

⁷⁷ *Ibidem*.

⁷⁸ «Artículo 25. Derechos de las personas mayores.

La Unión reconoce y respeta el derecho de las personas mayores a llevar una vida digna e independiente y a participar en la vida social y cultural».

⁷⁹ Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, adoptado el 11 de febrero de 2004.

⁸⁰ *Ibidem*.

⁸¹ *Cfr.* Sentencia del Tribunal Constitucional 186/2000, de 10 de julio, Fundamento Jurídico 6.

A este respecto, tanto la propia AEPD⁸² como el GT 29⁸³ y el EGE⁸⁴ preconizan un respeto exquisito del principio de proporcionalidad en las múltiples manifestaciones de la «IO para las personas mayores». De tal manera, entendemos necesario que, con carácter previo a la adopción de cualquier medida restrictiva del derecho fundamental a la protección de datos en este concreto ámbito, el responsable del tratamiento elabore un «Informe de proporcionalidad», en el cual examine detalladamente, desde una óptica técnico-jurídica, los siguientes extremos:

- Juicio de idoneidad: si la medida es adecuada y apropiada para conseguir el objetivo que se pretende.
- Juicio de necesidad: la inexistencia de otras medidas menos lesivas para el derecho fundamental a la protección de datos de las personas mayores que demuestren ser eficaces para la consecución del propósito perseguido. En lo tocante a este particular, el responsable del fichero o del tratamiento debería justificar la ineficacia, previamente contrastada y verificada, de otras medidas menos lesivas para el derecho fundamental a la protección de datos de las personas mayores.
- Juicio de proporcionalidad en sentido estricto: si la medida es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para las personas mayores –en términos de seguridad, salud, autonomía personal y calidad de vida– que perjuicios sobre su derecho fundamental a la protección de datos y otros derechos íntimamente relacionados con su dignidad personal.

De igual manera, nos gustaría hacer mención del denominado «principio de minimización de datos» contenido en la Directiva 95/46/CE –de la cual nuestra actual normativa es transposición–, según el cual los datos han de ser adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente [art. 6.1 c)]. Idea sobre la que profundiza la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)⁸⁵, según la cual los datos personales deberán ser «adecuados, pertinentes y limitados al mínimo necesario en relación con los fines para los que se traten; solo se tratarán si y siempre que estos fines no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales» [art. 5 c)]. En este sentido, entendemos que los principios de proporcionalidad y minimización de datos han de ir de la mano en la «IO para las personas mayores», evitando este último un tratamiento ex-

⁸² Vid., Informe 0292/2010 del Gabinete Jurídico de la Unidad de Apoyo al Director de la AEPD.

⁸³ Vid., Opinión 3/2012 sobre la evolución de las tecnologías biométricas, adoptada el 27 de abril de 2012.

⁸⁴ Vid., Dictamen n.º 20, de 16 de marzo de 2005, titulado «Aspectos éticos de los implantes TIC en el cuerpo humano».

⁸⁵ COM (2012) 11 final. Bruselas, 25 de enero de 2012.

cesivo, no pertinente o inadecuado de sus datos personales. No podemos ni debemos ignorar la extraordinaria potencialidad de las tecnologías de la IO: a modo de ejemplo, nos gustaría poner el acento sobre los posibles efectos indeseados del acceso por parte de terceros malintencionados a conjuntos de datos de carácter personal que ofrezcan un perfil de los hábitos, conductas, comportamientos o estado de salud de la persona mayor.

Finalmente, una aplicación rigurosa del subprincipio de finalidad –enmarcado en el principio general de calidad de los datos– se configura como el tercer elemento esencial de una «IO para las personas mayores» caracterizada por el respeto de sus derechos fundamentales. El citado principio pivota sobre la idea de que los datos de carácter personal únicamente pueden ser tratados para las finalidades determinadas, específicas y legítimas que justifican su tratamiento y no para otras finalidades distintas de aquellas. A este respecto, la Autoridad Catalana de Protección de Datos (en adelante, APDCAT) ha señalado, con manifiesto acierto, que la legitimidad que permite un determinado tratamiento no supone la legitimidad «en cascada» para tratamientos secundarios que quizás no son necesarios o que, simplemente, el interesado no desea⁸⁶. A nuestro juicio, el principio de finalidad ha de ser un límite infranqueable para los responsables de tratamientos específicamente vinculados a personas mayores en la IO.

Todo ello, en suma, con la finalidad de evitar un uso abusivo o torticero de las tecnologías inherentes a la IO en menoscabo del derecho fundamental a la protección de datos y otros derechos estrechamente vinculados con la dignidad de las personas mayores respecto de los cuales el primero tiene un valor instrumental. En este sentido, nuestra autoridad de protección de datos ha considerado desde fechas tempranas que las personas mayores precisan una especial protección, ya que en muchas ocasiones se encuentran en una situación que les impide conocer y ejercitar sus derechos en igualdad de condiciones⁸⁷. De ahí la necesidad de un respeto singularmente escrupuloso de los principios de proporcionalidad, finalidad y minimización de datos para el desarrollo de una IO de calidad para las personas mayores.

2. DEBER DE INFORMACIÓN

Según señala la jurisprudencia del Tribunal Constitucional (*vid.* STC 292/2000), el derecho fundamental a la protección de datos persigue garantizar a la persona un poder de control sobre sus datos personales, sobre su uso y destino⁸⁸. De tal manera, el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre sus datos, si bien «ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son

⁸⁶ Autoritat catalana de protecció de dades (APDCAT): *La protecció de dades de caràcter personal...*, *op. cit.*, págs. 39 y 40.

⁸⁷ *Cfr.* Memoria de la AEPD correspondiente al año 2004, pág. 148.

⁸⁸ *Vid. supra.*

los que se poseen por terceros, quiénes los poseen, y con qué fin» (FJ 6). Y profundiza el Tribunal Constitucional: «El derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales (STC 254/1993, FJ 7)» (FJ 6).

En su consecuencia, «el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular» (FJ 7). Y «ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos» (FJ 7). En fin, «son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos» (FJ 7).

De tal modo, concluye el Tribunal Constitucional, «sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD [Ley Orgánica de Protección de Datos]) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia» (FJ 13).

De otra parte, el Dictamen 15/2011 sobre la definición del consentimiento, adoptado el 13 de julio de 2011 por el GT 29, indica que «si se utiliza correctamente, el consentimiento es un instrumento que permite al interesado controlar el tratamiento de sus datos», pero «si se utiliza de forma incorrecta, el control por el interesado resulta ilusorio y el consentimiento deja de ser una base adecuada del tratamiento». En lo tocante a este particular, la AEPD ha subrayado, con motivo del Informe de su Gabinete Jurídico número 0340/2010, que «[l]a información en la recogida de datos personales constituye uno de los principios de la protección de datos, un derecho del afectado y un complemento previo de la prestación del consentimiento, cuya omisión puede determinar un vicio del consentimiento para el posterior tratamiento de datos de carácter

personal que origine la nulidad del mismo, siendo necesario para que el afectado pueda ejercer otros derechos que la LOPD le reconoce. Así se desprende del texto del artículo 5 al establecer la exigencia de que el mismo sea expreso, preciso e inequívoco».

En una línea argumental similar, la autoridad autonómica de control de Cataluña ha señalado, a colación de su Documento de Trabajo sobre la protección de datos de carácter personal en las ciudades inteligentes, que «[e]l deber de información es otro de los ejes fundamentales de la protección de datos. Este principio implica que el responsable de un fichero o tratamiento de datos tiene la obligación de informar a la persona física titular de los datos, entre otros, de qué tratamiento se hará y qué implica este tratamiento, a quién se cederán los datos, para qué finalidad, dónde tiene que dirigirse para obtener información sobre el tratamiento y, si procede, ejercer los derechos que otorga la normativa de protección de datos (acceso, rectificación, cancelación y oposición, derechos ARCO). Así, el principio de información es clave en el contexto de la autodeterminación informativa para ejercer los derechos ARCO. En esto radica buena parte de la trascendencia del dicho principio»⁸⁹.

De todo lo antedicho podemos colegir que el principio de información, dotado de una manifiesta significación, identidad y contenido propios, tiene, a su vez, un importante valor instrumental respecto del principio del consentimiento, eje vertebrador en torno al cual se estructura y cohesionan nuestro sistema normativo de protección de datos. Así, el principio de información se constituye en un medio para hacer efectivo el principio del consentimiento, sin el cual este difícilmente podría existir, careciendo de sentido y eficacia. Información y consentimiento son, en suma, principios íntimamente relacionados, completando y perfeccionando el primero al segundo, de manera que entre los caracteres que definen el propio contenido esencial del principio del consentimiento se encuentra la cualidad de «informado», siendo necesaria la concurrencia de este requisito para que el consentimiento pueda ser considerado conforme a derecho. De ahí la trascendental importancia del principio de información como pilar básico en la configuración jurídica del derecho fundamental a la protección de datos, cuyo fin último es la facultad de la persona de controlar la información concerniente a sí misma y la capacidad de disponer sobre ella.

Una idea compartida por el propio GT 29, que en su Dictamen 15/2011 puntualiza que la obligación de informar es diferente del consentimiento, aunque en muchos casos está obviamente vinculada a este. De tal manera, «mientras que el consentimiento no siempre sigue al suministro de información, la información siempre es necesaria antes del consentimiento». Esto significa en la práctica «que el consentimiento debe ser con conocimiento de causa: un consentimiento «informado» por parte del interesado supone un consentimiento basado en la apreciación y comprensión de los hechos y consecuencias de una acción. El individuo afectado debe contar con información exacta y completa, dada de forma clara y comprensible, sobre todas las cuestiones pertinentes, tal

⁸⁹ Autoritat Catalana de Protecció de Dades (APDCAT): *La protecció de dades de caràcter personal...*, op. cit., págs. 48 y 49.

como la naturaleza de los datos tratados, los fines del tratamiento de que van a ser objeto los datos, los destinatarios de los mismos y los derechos del interesado. Esto incluye también el conocimiento de las consecuencias de no consentir el tratamiento de los datos en cuestión».

Un valor instrumental (el del principio de información) no solo predicable respecto del principio del consentimiento, sino, como también se ha apuntado anteriormente, respecto del resto del «haz de facultades» que sirven para garantizar a la persona un poder de control sobre sus datos personales y, en particular, su derecho a acceder, rectificar, cancelar u oponerse al uso de los mismos. De tal manera, solo una información completa y de calidad, redactada en un lenguaje sencillo, claro y adaptado a la realidad sociocultural de sus destinatarios, puede garantizar su plena comprensión y, por ende, servir de vehículo para el ejercicio efectivo de sus derechos en un entorno de extraordinaria complejidad tecnológica.

En este sentido, la Comunicación de la Comisión Europea sobre «Un enfoque global de la protección de los datos personales en la Unión Europea»⁹⁰, señala que «[I]a transparencia es una condición fundamental indispensable para permitir a las personas efectuar un control sobre sus propios datos y para garantizar la protección efectiva de los datos personales. Es pues primordial que los responsables del tratamiento informen a los ciudadanos correcta y claramente, con toda transparencia, para que sepan quién recogerá y tratará sus datos, de qué manera, por qué motivos y durante cuánto tiempo, y cuáles son sus derechos a efectos de acceder, rectificar o suprimir sus datos». La transparencia se basa, a juicio de la Comisión, «en elementos fundamentales, como un acceso fácil a la información, que debe ser fácil de entender, y la utilización de un lenguaje claro y sencillo».

Asimismo, el artículo 11⁹¹ de la Propuesta de Reglamento general de protección de datos⁹² introduce la obligación para los responsables del tratamiento de ofrecer a los interesados información transparente y de fácil acceso y comprensión sobre el tratamiento de sus datos personales. De tal modo, el principio de transparencia, recogido en el citado artículo, exige que toda información dirigida al público o al interesado sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro⁹³. La propia Comisión Europea entiende que ello es

⁹⁰ Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 4 de noviembre de 2010, titulada «Un enfoque global de la protección de los datos personales en la Unión Europea» [COM(2010) 609 final].

⁹¹ «Artículo 11. Transparencia de la información y la comunicación.

1. El responsable del tratamiento aplicará políticas transparentes y fácilmente accesibles por lo que respecta al tratamiento de datos personales y al ejercicio de los derechos de los interesados.
2. El responsable del tratamiento facilitará al interesado cualquier información y comunicación relativa al tratamiento de datos personales, en forma inteligible, utilizando un lenguaje sencillo, claro y adaptado al interesado, en particular para cualquier información dirigida específicamente a los niños.»

⁹² *Vid. supra.*

⁹³ Considerando 46.

especialmente pertinente cuando, por mor de la complejidad tecnológica propia de la práctica de la recogida de información, resulte difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, los datos personales que le conciernen⁹⁴.

No en vano, el propio GT 29, en su veterano Dictamen 10/2004, sobre una mayor armonización de las disposiciones relativas a la información, adoptado el 25 de noviembre de 2004, ya manifestó expresamente su apoyo al principio de que la información proporcionada a los interesados debería utilizar un lenguaje y una presentación fáciles de entender. A juicio del GT 29, «[l]a comprensión por parte de los interesados constituye un objetivo importante, de manera que puedan adoptar decisiones con conocimiento de causa y dispongan del conocimiento y la comprensión necesarios para influir en las prácticas de los responsables del tratamiento de datos y de los encargados del mismo. En este contexto, es importante garantizar que la información se proporciona de manera adecuada a las personas con necesidades específicas».

Consideraciones estas de singular relevancia en la «IO para las personas mayores», como consecuencia de la brecha generacional existente con respecto a la asimilación y utilización de las TIC. En este sentido, los efectos negativos de la denominada «brecha generacional digital», unidos a la natural fragilidad de las personas mayores, hace de las mismas un colectivo social de riesgo en materia de protección de datos.

Así, por ejemplo, la APDCAT ha señalado, en relación con las tecnologías que conforman el ecosistema de las ciudades inteligentes, que «algunas de estas tecnologías pueden ser bastante desconocidas por el titular de los datos (geolocalización, trazabilidad, RFID, tarjetas *contactless*, NFC [*near field communication*]...). Así, nos tendremos que plantear si un usuario, un ciudadano sin especiales conocimientos técnicos, tendrá facilidad para comprender el tratamiento de datos que su uso puede comportar»⁹⁵. A juicio de la citada autoridad, incluso podría considerarse, dado que el uso de las citadas tecnologías podría presentar especiales riesgos para la seguridad de los datos de carácter personal, que el deber de información comprendiese, con carácter adicional a los aspectos tradicionalmente recogidos en la normativa de protección de datos, el facilitar a los interesados una serie de recomendaciones o consejos de índole práctica en materia de seguridad de datos, con la finalidad de evitar el acceso, tratamiento o alteración de la información por parte de personas no autorizadas. Observación que compartimos y que consideramos de especial interés en relación con la «IO para las personas mayores», con base en las razones aducidas con anterioridad. Huelga decir que determinados conceptos tecnológicos e informáticos como dirección IP, Bluetooth, RFID, geolocalización, código QR o cifrado (por citar algunos ejemplos significativos) son, hasta el momento, completamente ajenos a las personas mayores. En tal sentido, la incorporación de las exigencias planteadas por la APDCAT contribuiría de manera notable tanto a generar confianza en el sistema como a garantizar un tratamiento

⁹⁴ *Ibidem*.

⁹⁵ Autoritat Catalana de Protecció de Dades (APDCAT): *La protecció de dades de caràcter personal...*, *op. cit.*, pág. 53.

de datos leal⁹⁶ respecto de un colectivo social de riesgo singularmente importante en este temprano avance de la Internet del futuro.

A este respecto, no podemos olvidar la apreciación del Parlamento Europeo según la cual para lograr un uso pleno de la IO, tanto para beneficio individual como colectivo, los usuarios deben adquirir las habilidades necesarias para comprender estas nuevas tecnologías, estar motivados y ser capaces de utilizarlas de forma adecuada⁹⁷.

La autoridad autonómica de control de Cataluña recurre al ejemplo de «experiencias *Smart City*» que utilizan aplicaciones de geolocalización para ilustrar la problemática anteriormente expuesta: «Es muy improbable que los usuarios de aplicaciones *Smart City* que utilizan esta tecnología sean conscientes de su grado de control sobre la propia geolocalización, y de los derechos que les asisten y que les otorga la legislación de protección de datos. Para tener capacidad real de ejercer derechos ARCO, es necesario que el usuario haya recibido suficiente información sobre las consecuencias de este tratamiento»⁹⁸. De tal manera, a criterio de la APDCAT, el responsable de tratamientos de datos aparejados a aplicaciones de geolocalización «tiene que dar al usuario una información clara y comprensible sobre estos tratamientos. Podría ser exigible (además de lo que en cualquier tratamiento exige el art. 5 de la LOPD) que el usuario conozca qué datos de localización se recogen y tratan, que se le informe de cómo puede elegir el nivel y alcance de la geolocalización (limitar, bloquear, activar o desactivar la geolocalización), o de cómo puede eliminar datos de localización almacenados»⁹⁹.

No obstante, la trascendencia de una información previa, completa y de calidad en el ámbito de la «IO para las personas mayores» adquiere su máximo significado en supuestos ciertamente extremos como el de los dispositivos inteligentes implantables en el cuerpo humano con carácter irreversible, so pena de causar graves daños sobre la salud de su portador e incluso poner en riesgo su vida. En lo tocante a este particular, el propio EGE ha subrayado la importancia de una estricta observancia de los requisitos en materia de consentimiento informado y protección de datos (en particular, privacidad y confidencialidad de los datos), dado el carácter «irremovible» de los citados dispositivos inteligentes¹⁰⁰. Unas consideraciones que deben hacernos reflexionar en profundidad acerca de los riesgos de implantar en el cuerpo humano un dispositivo a través del cual la persona pueda ser «monitorizada» o «localizada» durante el resto de su vida, con la perversa

⁹⁶ El tratamiento leal de datos «supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención» (Directiva 95/46/CE, Considerando 38).

⁹⁷ Resolución del Parlamento Europeo, de 15 de junio de 2010... *op. cit.*, apdo. 33.

⁹⁸ Autoritat Catalana de Protecció de Dades (APDCAT): *La protecció de dades de caràcter personal...*, *op. cit.*, pág. 51.

⁹⁹ *Ibidem*, pág. 51.

¹⁰⁰ *Cfr.* Opinion of the European Group on Ethics in Science and New Technologies to the European Commission n.º 20..., *op. cit.*

posibilidad de que el funcionamiento e información contenida en el citado dispositivo escapen del control de su portador o de sus cuidadores a merced de terceros malintencionados, máxime teniendo en cuenta la especial fragilidad y vulnerabilidad de las personas mayores.

Incluso en ocasiones el tratamiento de datos puede resultar «invisible» para el interesado, facilitando una vigilancia constante e imperceptible de sus hábitos, movimientos y conductas. En el concreto ámbito de la IO, la APDCAT ha señalado cómo el usuario puede convertirse en un portador y distribuidor de su propia información personal, haciéndola accesible a terceros a veces con cierto riesgo y desconocimiento¹⁰¹; la APDCAT considera interesante plantearse a este respecto si el responsable del tratamiento tiene que explicar con cierto detalle (y de manera clara y adaptada a la capacidad de comprensión del usuario) qué datos, una vez tratados en el contexto de la finalidad principal, pueden ser objeto de anonimización o tratamiento agregado¹⁰².

La propia Comisión Europea ha puesto de manifiesto cómo diversos estudios han demostrado que dar a los usuarios un nivel suficiente de control mejora su nivel de confianza y desempeña un papel importante en la implantación de la tecnología¹⁰³. Un mensaje que no debe caer en el olvido cuando se trata de personas mayores en la IO, especialmente desde su entendimiento como un perfil de consumidor singularmente exigente y, en gran medida, renuente a las nuevas tecnologías.

El conjunto de consideraciones hasta aquí expuestas abocan a la necesidad de afrontar el deber de información en la «IO para las personas mayores» desde el «respeto del contexto», a fin de que el citado principio despliegue toda su eficacia y alcance en un entorno de gran complejidad tecnológica. En este sentido, el referido Dictamen 15/2011 del GT 29 recoge que la forma en que se facilite la información al interesado deberá estar condicionada al contexto en que se produce la recogida de los datos de carácter personal, debiendo aquel ser capaz de entenderla. De tal manera, el Grupo de Trabajo considera que cuanto más difícil resulte para el interesado supervisar y comprender todos los elementos del tratamiento de datos, mayor debe ser el esfuerzo del responsable para obtener un consentimiento basado en información específica y comprensible. De lo cual se colige la exigencia de un mayor grado de diligencia a los responsables de tratamientos específicamente vinculados a personas mayores en el ámbito de la IO. En este sentido, entendemos que la información que se facilite a la persona mayor deberá acomodarse a las circunstancias aplicables a cada caso concreto, de manera que la misma sea lo suficientemente clara y completa para que, con independencia de su edad y de la complejidad de la tecnología empleada para el tratamiento de sus datos, el interesado pueda adoptar una decisión acerca del mismo con pleno conocimiento de causa.

¹⁰¹ Autoritat Catalana de Protecció de Dades (APDCAT): *La protecció de dades de caràcter personal...*, op. cit., pág. 62.

¹⁰² *Ibidem*, pág. 52.

¹⁰³ *Cfr.* Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 18 de junio de 2009..., op. cit.

Así por ejemplo, en el supuesto de un dispositivo inteligente implantable en el cuerpo humano, existe determinada información consustancial a la adopción de una decisión consciente por parte de su futuro portador: si la implantación del mismo tiene o no carácter irreversible, qué personas tendrán acceso autorizado a la información contenida en el mismo, así como las medidas de seguridad previstas para evitar el acceso, tratamiento o alteración de la misma por parte de terceros malintencionados. En el caso de sistemas de geolocalización, interesa conocer aspectos tales como el radio de alcance del dispositivo, el procedimiento para su activación y desactivación o cómo limitar el acceso a los datos de localización registrados en el mismo o poder eliminarlos. Y como tercer ejemplo, la información necesaria para que la persona mayor pueda adoptar una decisión con pleno conocimiento de causa en relación con la instalación de sensores inteligentes en su vivienda debería incluir elementos de valoración como cuál será la ubicación de los citados dispositivos o qué personas tendrán acceso a la información que de los mismos se desprenda, de qué manera, con qué fines y durante cuánto tiempo.

Para finalizar, reiteramos la necesidad de atender, junto al respeto del contexto, al principio de transparencia, con la finalidad de convergir a una información completa y de calidad. En todo caso, entendemos que la información que se facilite a las personas mayores ha de ser fácilmente accesible y claramente visible (ubicación, tipo y tamaño de los caracteres, etc.), debiendo utilizarse un lenguaje sencillo, claro y adaptado a la realidad sociocultural de sus destinatarios, así como complementarse el texto con imágenes o gráficos cuando ello facilite la comprensión del mismo. Asimismo, la utilización de conceptos jurídicos abstrusos no debería tener cabida en una información que aspire a ser fácilmente comprensible para un usuario medio, con independencia de su edad. En último lugar, entendemos que sería oportuno facilitar a los interesados un medio de contacto sencillo y gratuito (v. gr., una dirección de correo electrónico o un número de teléfono gratuito), a fin de poder formular cuantas preguntas fuesen necesarias en orden a decidir de manera informada y consciente sobre el tratamiento de sus datos.

3. CONSENTIMIENTO DEL INTERESADO

Como hemos tenido ocasión de señalar, el principio del consentimiento es el eje vertebrador en torno al cual se estructura y cohesiona nuestro actual sistema normativo de protección de datos, cuyo fin último es la facultad de la persona de controlar la información concerniente a sí misma y la capacidad de disponer sobre ella. Dan fe de dicha afirmación los fundamentos jurídicos Sexto y Séptimo de la Sentencia del Tribunal Constitucional 292/2000, anteriormente transcritos.

En este sentido, el Grupo de Protección de Datos del artículo 29, en su Dictamen 15/2011 sobre la definición del consentimiento, ha puesto de manifiesto que «por lo general, el concepto de consentimiento está vinculado a la idea de que el interesado debe controlar el uso que se hace de sus datos. Desde la perspectiva de los derechos fundamentales, el control ejercido a través del consentimiento es un concepto importante. Al mismo tiempo y desde el mismo punto de vista, la decisión por la que una persona acepta una operación de tratamiento de datos debe estar sujeta a requisitos estrictos, teniendo en cuenta que dicha decisión puede implicar la renuncia a un derecho fundamental».

De tal manera, en opinión del GT 29, «el consentimiento está relacionado con el concepto de autodeterminación. La autonomía del interesado es a la vez una condición previa y una consecuencia del consentimiento: permite al interesado influir sobre el tratamiento de los datos». Este es un matiz muy importante en el ámbito específico de las personas mayores, considerando el progresivo deterioro físico, sensorial, mental y cognitivo que, con carácter general, afecta a las personas de edad¹⁰⁴.

A este respecto, TORRES VIGUERA y GALÁN SOLDEVILLA¹⁰⁵ distinguen tres posibles situaciones en las que puede encontrarse la persona mayor: 1. La persona mayor plenamente capaz, únicamente afectada por los procesos degenerativos propios de la edad, que no le impiden gobernarse por sí misma; 2. La persona mayor judicialmente incapacitada; y 3. La persona mayor afectada de un proceso de degeneración mental (v. gr., Alzheimer o demencia senil) o un proceso orgánico degenerativo, que no se encuentra judicialmente incapacitada pero puede tener limitadas sus facultades de autogobierno.

Esta multiplicidad de situaciones en las que pueden encontrarse las personas mayores es un factor determinante de la existencia real y efectiva de las facultades de disposición y control sobre sus datos personales¹⁰⁶. No en vano, el propio GT 29 cuestiona la validez del consentimiento como criterio legitimador para el tratamiento de los datos de carácter personal en determinadas circunstancias: «[a]lgunas veces el consentimiento constituye una débil base para justificar el tratamiento de datos personales y pierde valor si se amplía o ajusta para adaptarlo a situaciones en las que nunca debería utilizarse. Es fundamental utilizar el consentimiento "en el contexto adecuado". Si se utiliza en circunstancias inadecuadas, debido a que los elementos que le confieren validez pueden faltar, se puede producir una situación de gran vulnerabilidad y, en la práctica, la posición de los interesados puede resultar debilitada».

Interesa recordar aquí que, según lo señalado en el Fundamento Jurídico Décimo de la STC 292/2000, de tanta cita, «las facultades legalmente atribuidas a los sujetos concernidos y las consiguientes posibilidades de actuación de estos son necesarias para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos. Asimismo, esas facultades o posibilidades de actuación son absolutamente necesarias para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos». De tal manera, «privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos», puesto que, como concluyó en este punto la STC 11/1981, de 8 de abril (FJ 8), «se re-

¹⁰⁴ GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M.: «La protección de datos de las personas mayores...», *op. cit.*

¹⁰⁵ TORRES VIGUERA, A. y GALÁN SOLDEVILLA, L.: «Ética médica y tercera edad. Confidencialidad de los datos clínicos y consentimiento informado», en VV. AA. (coord. GONZÁLEZ PORRAS, J. M. y GALLEGO DOMÍNGUEZ, I.): *Actas de las Primeras Jornadas de Problemas legales sobre tutela, asistencia y protección a las personas mayores, Córdoba, 17 y 18 de noviembre de 2000*. Publicaciones Obra Social y Cultural CajaSur, Córdoba, 2001, pág. 319.

¹⁰⁶ GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M.: «La protección de datos de las personas mayores...», *op. cit.*

basa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección».

Es por ello que entendemos que la admisión del tratamiento de los datos de aquellas personas mayores que se encuentren en total ausencia de sus facultades de disposición y control sobre los mismos, como consecuencia de un deterioro mental y cognitivo fruto de su avanzada edad que anule su capacidad de entender y querer, comportaría la privación de su derecho fundamental a la protección de datos en condiciones de igualdad sustantiva, real y efectiva al resto de los ciudadanos, recibiendo, por ende, un trato discriminatorio y contrario a su propia dignidad personal. En resumen, la persona mayor quedaría posicionada en una situación de grave riesgo de desprotección y vulneración de su derecho fundamental a la protección de datos¹⁰⁷.

En relación con el consentimiento de las personas sin capacidad jurídica, el GT 29 realiza una remisión a las condiciones generales de validez del consentimiento en el ámbito del Derecho civil, pues se trata de una cuestión que, con carácter general, excede de la protección de datos¹⁰⁸. Ello obliga a acudir a nuestra doctrina jurídico-civil, con la finalidad de determinar las condiciones de validez del consentimiento en relación con las personas mayores.

En este sentido, CARRASCO PERERA señala que «en nuestro Derecho, la capacidad de obrar general se adquiere con la mayoría de edad, pues el artículo 322 del CC [Código Civil] se encarga de aclarar que el mayor de edad «es capaz para todos los actos de la vida civil, salvo los exceptuados». Una vez alcanzada la mayoría, la persona solo puede ver suprimida o limitada su capacidad de obrar mediante una sentencia que la incapacite, por alguna de las causas previstas en el artículo 200 del CC»¹⁰⁹.

Siguiendo una misma línea argumental, ZURITA MARTÍN entiende que «desde los dieciocho años y hasta la muerte, somos titulares de la plena capacidad de obrar, esto es, de la aptitud para ejercitar con eficacia actos jurídicos, dado que desde el mismo momento del nacimiento toda persona goza de idéntica capacidad jurídica (art. 29 CC), o idoneidad para ser titular de derechos y obligaciones. La mayoría de edad viene, por tanto, a marcar la frontera entre la capacidad de obrar plena y la incapacidad, presumiéndose que, a partir de los dieciocho años, somos plenamente capaces»¹¹⁰.

TORRES VIGUERA y GALÁN SOLDEVILLA¹¹¹ también se alinean con esta corriente doctrinal, bajo la consideración de que la persona mayor no es en sí misma incapaz. Para estos autores, la

¹⁰⁷ *Ibidem*.

¹⁰⁸ *Cfr.* Dictamen 15/2011 del Grupo de Protección de Datos del artículo 29, sobre la definición del consentimiento, adoptado el 13 de julio de 2011.

¹⁰⁹ CARRASCO PERERA, A. (director); CORDERO LOBATO, E., *et al.*: *Derecho Civil...*, *op. cit.*, pág. 63.

¹¹⁰ ZURITA MARTÍN, I.: *Protección civil de la ancianidad*, editorial Dykinson, S.L., Madrid, 2004, pág. 55.

¹¹¹ TORRES VIGUERA, A. y GALÁN SOLDEVILLA, L.: «Ética médica y tercera edad...», *op. cit.*, pág. 325.

vejez no es una enfermedad y toda actuación en relación con la persona mayor debe ser tenida sobre la base de la presunción de capacidad que nuestro ordenamiento jurídico establece y se deduce del artículo 322 del Código Civil.

Idea asimismo compartida por ZURITA MARTÍN, para quien «la edad por sí misma, no modifica la capacidad del hombre, por muy avanzada que aquella sea; el anciano cronológico no sufrirá, por ello, limitación alguna en sus derechos, ni perderá un ápice de su dignidad de persona, ni de los derechos inviolables que son inherentes a dicha condición, todo ello fundamento del orden público y la paz social a la luz del artículo 10 de la Constitución»¹¹². Por tanto, en el ámbito civil, «una vez cumplidos los dieciocho años, no existe diferencia de trato en razón de la edad de las personas (...), ni puede ser esta tomada como argumento diferenciador o discriminatorio en el ejercicio de los derechos civiles del individuo»¹¹³.

Sintetizando, nuestro Código Civil establece, en su artículo 322, una presunción de capacidad de obrar que se adquiere con la mayoría de edad y que subsiste hasta el fallecimiento de la persona, mientras no sea declarada judicialmente su incapacidad por alguna de las causas previstas en el artículo 200 del Código Civil¹¹⁴. En este sentido, la sentencia de incapacitación destruye la presunción legal de plena capacidad del mayor de edad, que ve limitada dicha capacidad a los márgenes que se describan en la resolución judicial¹¹⁵.

En su consecuencia, abogamos por el seguimiento de una línea de respeto a la autonomía de la voluntad de las personas mayores, siempre que ello sea legal y fácticamente posible, basada en el consentimiento previo, libre e informado del propio interesado para el tratamiento de los datos que le conciernen en la IO. Asimismo, pero a contrario sensu, rechazamos cualquier patrón de índole paternalista tendente a la infantilización o negación de la autonomía de la voluntad de las personas mayores sobre el tratamiento de sus datos en dicho ámbito. Y, en tercer lugar, entendemos que debería estudiarse la facultad, en el supuesto de que la persona mayor judicialmente incapacitada sea capaz de entender, de que su opinión en relación con el tratamiento de sus datos sea al menos escuchada, especialmente en aquellos casos en que aquel afecte singularmente a otros derechos estrechamente vinculados con su dignidad personal (v. gr., implantes TIC, sistemas de seguimiento y control, tratamientos de datos biométricos, etc.)¹¹⁶.

Ahora bien, la propia doctrina se ha encargado de subrayar la problemática existente en relación con la persona mayor que padezca enfermedades o deficiencias de carácter físico o psíquico,

¹¹² ZURITA MARTÍN, I.: *Protección civil...*, op. cit., pág. 17.

¹¹³ *Ibidem*.

¹¹⁴ Según el artículo 200 del Código Civil, son causas de incapacitación «las enfermedades o deficiencias persistentes de carácter físico o psíquico, que impidan a la persona gobernarse por sí misma».

¹¹⁵ ZURITA MARTÍN, I.: *Protección civil...*, op. cit., pág. 55.

¹¹⁶ GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M.: «La protección de datos de las personas mayores...», op. cit.

que le impidan gobernarse por sí misma, y no existir en ella una situación de incapacitación por no haber sido declarada por una sentencia o resolución judicial¹¹⁷, lo que se ha convenido denominar «incapacidad natural». A juicio de RETUERTO BUADES, «es una realidad que no podemos desconocer la de aquellas personas mayores de edad que son plenamente capaces y lo han sido toda su vida pero que pueden perder facultades con el paso de los años y llegarse a convertir en discapacitados o incapaces totales o parciales»¹¹⁸.

A juicio de la doctrina jurídico-civil, se puede decir que, en estos casos, confluyen en la persona la presunción legal de capacidad por su mayoría de edad y la incapacidad natural del individuo, por concurrir algún defecto físico o psíquico que le impide autogobernarse¹¹⁹. En este sentido, el incapaz natural puede actuar jurídicamente con una voluntad viciada, debiendo demostrarse su incapacidad para impugnar aquellas actuaciones jurídicas llevadas a cabo por él¹²⁰. MARTÍN JIMÉNEZ y MARTÍN JIMÉNEZ¹²¹ señalan que sería preciso demostrar que cuando la persona prestó su consentimiento se encontraba en una situación de incapacidad, dado que la jurisprudencia ha instituido la presunción de que a todas las personas se les presume capaces mientras no se demuestre de forma evidente la perturbación de sus facultades mentales o sea declarada judicialmente su incapacidad¹²².

En tal sentido, consideramos que debería explorarse la posibilidad de que, con carácter adicional a las condiciones generales de validez del consentimiento en el ámbito del Derecho civil, la normativa de protección de datos establezca determinadas disposiciones específicas sobre la recogida y tratamiento de datos de las personas presuntamente capaces que puedan tener afectadas algunas de sus facultades como consecuencia de su avanzada edad, al entender que dicha circunstancia les sitúa en una especial situación de riesgo de violación de su derecho a la protección de datos¹²³, muy especialmente en el entorno de las nuevas tecnologías en general y de la IO en particular.

Como corolario de este epígrafe, traer a colación la consideración del Parlamento Europeo, el cual advierte que la confianza que los consumidores depositen en la IO debe basarse en un marco jurídico claro que incluya normas sobre el control, la recogida, el procesamiento y el uso de los

¹¹⁷ Cfr. CARRASCO PERERA, A. (director); CORDERO LOBATO, E., et al.: *Derecho Civil... op. cit.*, pág. 123; ZURITA MARTÍN, I.: *Protección civil...*, *op. cit.*, pág. 55.

¹¹⁸ RETUERTO BUADES, M.: «Discapacidad y tuición: las limitaciones a la capacidad de obrar por razón de la edad y de la salud. Los derechos del impedido» en VV. AA. (coord. GONZÁLEZ PORRAS, J. M. y GALLEGO DOMÍNGUEZ, I.): *Actas de las Primeras Jornadas de Problemas legales sobre tutela, asistencia y protección a las personas mayores, Córdoba, 17 y 18 de noviembre de 2000*. Publicaciones Obra Social y Cultural CajaSur, Córdoba, 2001, pág. 64.

¹¹⁹ ZURITA MARTÍN, I.: *Protección civil...*, *op. cit.*, pág. 55.

¹²⁰ *Ibidem*.

¹²¹ MARTÍN JIMÉNEZ, C. M. y MARTÍN JIMÉNEZ, J. J.: *Teoría y práctica del ejercicio de las acciones civiles. Comentarios y formularios*, Lex Nova, S.A.U., Valladolid, 2010, pág. 788.

¹²² En lo tocante a este particular, resulta singularmente ilustrativo lo señalado en la Sentencia de fecha 28 de abril de 2009, de la Sección 20.ª de la Audiencia Provincial de Madrid, a cuya lectura remitimos.

¹²³ GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M.: «La protección de datos de las personas mayores...», *op. cit.*

datos recogidos y transmitidos mediante las tecnologías de la IO, así como acerca de los tipos de autorización que deben conceder los consumidores¹²⁴. De ahí la necesidad de adoptar las medidas apropiadas que cubran las actuales lagunas legales existentes en materia de consentimiento para el tratamiento de los datos de las personas mayores y fortalezcan la confianza de este colectivo social de especial sensibilidad en el desarrollo de la Internet del futuro.

V. CONCLUSIONES: UNA NUEVA PROTECCIÓN DE DATOS PARA UN NUEVO PARADIGMA

Tal y como se ha encargado de subrayar la propia Comisión Europea, la IO llega a un entorno informático en el que influyen varias tendencias fundamentales. Una de ellas es la «escala»: el número de dispositivos conectados está aumentando, mientras su tamaño se reduce por debajo del umbral de visibilidad para el ojo humano. Otra es la «movilidad»: los objetos están cada vez más conectados de manera inalámbrica, son transportados permanentemente por las personas y son geolocalizables. Una tercera tendencia es la de «heterogeneidad y complejidad»: la IO se desarrollará en un entorno ya abarrotado de aplicaciones, lo cual genera cada vez más dificultades de interoperabilidad¹²⁵. Este nuevo paradigma exige un enfoque renovado del derecho fundamental a la protección de datos, de cara a la posible gran transformación que experimentará la civilización a causa de las tecnologías de la IO.

De tal manera, y ante los riesgos asociados al «tsunami tecnológico» propio de la IO, el Parlamento Europeo ha acentuado la necesidad de incluir en todas las tecnologías de la IO los sistemas de transmisión más seguros y más protegidos, haciendo especial hincapié sobre la adopción de medidas de seguridad que garanticen que solo los usuarios autorizados puedan acceder a los datos¹²⁶. En este sentido, el propio Parlamento considera que la privacidad y la seguridad deben tenerse en cuenta desde la etapa más temprana posible del proceso de desarrollo e implantación de las tecnologías de la IO¹²⁷. A este respecto, interesa apuntar que el desarrollo de nuevas aplicaciones y el propio funcionamiento y el potencial comercial de la IO están estrechamente ligados a la confianza que los consumidores depositen en el sistema; una confianza que se obtiene cuando se aclaran las dudas sobre las posibles amenazas para la intimidad y la salud¹²⁸.

En una línea similar, el Supervisor Europeo de Protección de Datos ha indicado que, «[e]n la práctica, las ventajas potenciales de las TIC solo se pueden disfrutar si estas tecnologías son

¹²⁴ Resolución del Parlamento Europeo, de 15 de junio de 2010... *op. cit.*, apdo. 30.

¹²⁵ «Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 18 de junio de 2009...», *op. cit.*

¹²⁶ «Resolución del Parlamento Europeo, de 15 de junio de 2010...», *op. cit.*, apdo. 23.

¹²⁷ *Ibidem*, apdo. 16.

¹²⁸ *Ibidem*, apdo. 29.

capaces de generar confianza, o dicho con otras palabras, si pueden garantizar la voluntad del usuario de depender de las TIC por sus características y ventajas»¹²⁹. Y esta confianza solo se generará «si las TIC son fiables y seguras, están bajo el control de las personas y se garantiza la protección de los datos personales y la privacidad de estas»¹³⁰.

No en vano, el propio Grupo de Protección de Datos del artículo 29, en su Dictamen 3/2010 sobre el principio de responsabilidad, adoptado el 13 de julio de 2010, ha puesto de manifiesto cómo, desde un punto de vista sociológico, hay un reconocimiento creciente de la protección de datos como valor social. De tal manera, a medida que la información personal se hace más valiosa para los responsables del tratamiento de datos de todos los sectores, los ciudadanos, los consumidores y la sociedad en su conjunto adquieren una conciencia creciente de su significación. Esto a su vez refuerza la necesidad de aplicar medidas estrictas para salvaguardarla.

Las personas mayores configuran un perfil de consumidor singularmente exigente –incluso desconfiado– resultado de la experiencia acumulada a lo largo de su vida, máxime en un territorio para muchos de ellos «hostil» como consecuencia de la brecha generacional existente con respecto a la asimilación y utilización de las TIC. De ahí que surja la necesidad de redoblar esfuerzos en lo que a generar confianza en el colectivo social de las personas mayores respecta. En lo tocante a este particular, GONZÁLEZ VEGA, KÄMÄRÄINEN y KALLA¹³¹ han puesto de manifiesto cómo los productos y servicios TIC orientados a las personas mayores y que no cumplan con unos determinados principios éticos pueden no ser aceptados por sus destinatarios. De igual manera, pero en sentido contrario, el cumplimiento de los citados principios puede contribuir significativamente a su aceptación y, por ende, a su éxito en el mercado, especialmente cuando se trate de sistemas que afecten a la dignidad, a la privacidad y a la libertad de la persona mayor. En este sentido, recomiendan la consideración del diseño de cualquier innovación tecnológica orientada a las personas mayores desde un punto de vista ético que tenga en cuenta sus derechos y libertades (v. gr., el derecho fundamental a la protección de datos, entendido este como uno de los llamados derechos de tercera generación más significativos en la sociedad digital). En opinión de los citados autores, esto podría marcar la diferencia entre los productos y servicios TIC exitosos y los no exitosos¹³².

En un mismo sentido, el SEPD ha subrayado que las garantías efectivas relativas a la protección de los datos, la privacidad y todas las dimensiones éticas asociadas son cruciales para

¹²⁹ Dictamen del Supervisor Europeo de Protección de Datos acerca de la promoción de la confianza... *op. cit.*

¹³⁰ *Ibidem.*

¹³¹ GONZÁLEZ VEGA, N., KÄMÄRÄINEN, A. y KALLA, O.: «Ethical Aspects in ICT Research and Development: The Case of the Confidence Project», en CUNNINGHAM, P. y CUNNINGHAM, M. (eds.): *eChallenges e-2010 Conference Proceedings*, IIMC International Information Management Corporation, Dublín, 2010.

¹³² GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M.: «El reto de la protección de datos de las personas mayores en la sociedad del ocio digital», en CERRILLO I MARTÍNEZ, A.; PEGUERA, M.; PEÑA-LÓPEZ, I.; PIFARRÉ DE MONER, M. J. y VILASAU SOLANA, M. (coords.): *Retos y oportunidades del entretenimiento en línea. Actas del VIII Congreso Internacional, Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona 9-10 Julio, 2012*, UOC-Huygens Editorial, Barcelona, 2012, págs. 380 y ss.

que el público confíe en la IO. Solo entonces podrá la tecnología dar sus numerosos beneficios económicos y sociales¹³³.

Volviendo al aspecto de la seguridad de los datos, la Comunicación de la Comisión Europa titulada «Internet de los objetos-Un plan de acción para Europa» ha puesto de manifiesto que la seguridad de la información es un requisito imprescindible y, para la mayoría de las partes interesadas, una de las preocupaciones más importantes en relación con la IO. Huelga decir que la seguridad de la información está estrechamente vinculada a cuestiones como la confianza y la privacidad. En este sentido, «[l]a experiencia del desarrollo de las tecnologías de la información y las comunicaciones enseña que estas características a veces se descuidan durante la fase de diseño, y que integrar funciones para protegerlas en una fase posterior crea dificultades, es caro y puede reducir considerablemente la calidad de los sistemas. Por consiguiente, es crucial que los componentes de la IO estén diseñados desde el comienzo con una mentalidad de privacidad y seguridad inherentes al diseño e incorporen integralmente los requisitos de los usuarios».

Una cuestión sobre la que también ha entendido oportuno pronunciarse el Supervisor Europeo de Protección de Datos, señalando que «[l]as tecnologías de la información y la comunicación son cada vez más complejas y entrañan mayores riesgos para la privacidad y la protección de los datos»¹³⁴. A su juicio, «a medida que avancemos hacia las redes de objetos interconectados, los riesgos aumentarán»¹³⁵ y, en este sentido, «cuanto mayores sean los riesgos a los que se expongan la privacidad y la protección de los datos, mayor será la demanda de mejores salvaguardias»¹³⁶. De ahí que los argumentos favorables a la necesidad de implementar la privacidad desde el diseño tengan un mayor peso específico en el ámbito de la «IO para las personas mayores», de manera que la privacidad y la protección de los datos se integren en todo el ciclo de vida de las tecnologías asociadas a la misma, desde la primera fase del diseño hasta su uso y su eliminación.

De otro lado, el progresivo deterioro físico, sensorial, mental y cognitivo que afecta a las personas de edad, unido a los efectos negativos de la citada «brecha generacional digital», aconseja una modulación de los principios «tradicionales» de la protección de datos en la «IO para las personas mayores». En tal sentido, abogamos por el seguimiento sin fisuras de una línea de respeto a la autonomía de la voluntad de las personas mayores, siempre que ello sea legal y fácticamente posible, así como una exquisita ponderación de los bienes jurídicos objeto de protección a la luz de las circunstancias concurrentes en cada caso concreto, de manera consecuente con el principio de proporcionalidad que debe regir cualquier medida restrictiva de derechos fundamentales. Completarían este juego de garantías los siguientes elementos: el respeto del contexto y una total transparencia en la información que se facilite a las personas mayores sobre el tratamiento de sus datos; la validez del consentimiento del interesado a efectos civiles; así como el respeto

¹³³ Dictamen del Supervisor Europeo de Protección de Datos acerca de la promoción de la confianza..., *op. cit.*

¹³⁴ Véase nota anterior.

¹³⁵ *Ibidem.*

¹³⁶ Véase nota anterior.

escrupuloso de los principios de finalidad y minimización de datos como límite infranqueable para los responsables del tratamiento.

Finalmente, desde el entendimiento por la jurisprudencia constitucional del derecho a la protección de datos como un derecho de la personalidad consustancial a la dignidad humana, concebimos el respeto a la protección de los datos de las personas mayores como el respeto a su propia dignidad personal. Las personas mayores son, en todo caso, dignas merecedoras del disfrute del derecho fundamental a la protección de datos en condiciones de igualdad sustantiva, real y efectiva al resto de los ciudadanos, significando la privación o menoscabo del mismo un trato discriminatorio y contrario a su propia dignidad personal.

Asimismo, recordar que el derecho fundamental a la protección de datos, dotado de determinación, autonomía y contenido propios desde su consagración en la STC 292/2000 y en la propia Carta de Derechos Fundamentales de la Unión Europea, tiene, a su vez, un importante valor como instrumento para la efectividad de otros derechos estrechamente vinculados con la dignidad de la persona. Un valor instrumental que adquiere una singular relevancia para el desarrollo efectivo de determinados derechos de las personas mayores, entendidas estas como un colectivo social especialmente vulnerable. En tal sentido, cabe citar, entre otros, el derecho de las personas mayores a llevar una vida digna e independiente, el derecho a la igualdad y no discriminación por razones de edad, el derecho a la libre circulación e incluso el derecho a la vida y a la integridad física.

En su consecuencia, un respeto exquisito del derecho fundamental a la protección de datos por parte de todos los agentes implicados en su desarrollo es sinónimo de una IO de calidad para las personas mayores, entendida esta como un temprano avance de la Internet del futuro singularmente respetuoso con los derechos y libertades fundamentales de los ciudadanos en general y de los colectivos sociales más vulnerables en particular. Esta es, a nuestro juicio, la dirección correcta en pos de un mundo desarrollado y tecnológicamente avanzado concebido para la mejora de la calidad de vida de todas las personas.

Bibliografía

AGENCIA EFE [2010]: «Llevarse al médico puesto en la camiseta» [en línea], 15 de noviembre, <http://www.youtube.com/watch?v=bx8-d9wKKgI>.

ANTENA3.COM [2012]: «Conoce la vida de un difunto con solo pasar el móvil sobre su tumba» [en línea], 11 de septiembre, http://www.antena3.com/noticias/tecnologia/conoce-vida-difunto-solo-pasar-movil-tumba_2012091100085.html.

– [2013]: «Las personas con alzhéimer llevarán un código identificativo para no perderse» [en línea], 21 de febrero, http://www.antena3.com/noticias/salud/personas-alzheimer-llevaran-codigo-identificativo-perderse_2013022100305.html.

ASINTEC-CENTRO TECNOLÓGICO DE CONFECCIÓN [2010]: «INTELIGENTEX: experiencia piloto apoyada en prendas inteligentes para asistencia a personas en situación de dependencia», en *Revista de Química e Industria Textil*, Asociación Española de Químicos y Coloristas Textiles, núm. 198, Barcelona, julio-agosto, págs. 56-58.

- «INTELIGENTEX. Sistema de control y apoyo para residencias de mayores» [en línea], <http://www.asintec.org/pdf/inteligentex.pdf>.

AUTORITAT CATALANA DE PROTECCIÓ DE DADES (APDCAT) [2013]: *La protecció de dades de caràcter personal en les ciutats intel·ligents («smart cities») –Document per al debat–*, Barcelona, febrero.

BBC NEWS TECHNOLOGY [2012]: «Warning over medical implant attacks» [en línea], 9 de abril, <http://www.bbc.com/news/technology-17623948>.

CARRASCO PERERA, A. (director); CORDERO LOBATO, E.; et ál. [2004]: *Derecho Civil (Introducción. Derecho de la persona. Derecho subjetivo. Derecho de propiedad)*, Editorial Tecnos, SA, 2.ª edición, Madrid.

CASAS VALLÉS, R. [1989]: «Derecho a la imagen: el consentimiento y su revocación (nota a una sentencia de la AT de Barcelona de 19 de junio de 1988)», en *Revista del Poder Judicial*, núm. 14.

EL MUNDO.ES [2013]: «Una herramienta microscópica para analizar el cerebro» [en línea], 13 de marzo, <http://www.elmundo.es/elmundosalud/2013/03/12/neurociencia/1363114911.html>.

ELCOMERCIO.ES [2013]: «Los enfermos de alzhéimer portarán una chapa en la que irán encriptados sus datos personales» [en línea], 18 de marzo, <http://www.elcomercio.es/v/20130318/asturias/enfermos-alzheimer-portaran-chapa-20130318.html>.

EUROPA PRESS [2012]: «Lápidas con códigos QR permitirán conocer al difunto a través de la descarga de textos e imágenes» [en línea], 22 de octubre, <http://www.europapress.es/nacional/noticia-lapidas-codigos-qr-permitiran-conocer-difunto-traves-descarga-textos-imagenes-20121022142005.html>.

GÓMEZ-JUÁREZ SIDERA, I. [2012]: «Sistemas de vigilancia y personas mayores: un análisis desde la protección de datos», en *Revista Aranzadi de Derecho y Nuevas Tecnologías (RdNT)*, Editorial Aranzadi, SA, Cizur Menor (Navarra), núm. 28.

- [2013]: «Protección de datos post mortem en las redes sociales online», en el II Forum de Expertos y Jóvenes Investigadores en Derecho y Nuevas Tecnologías (FODERTICS), Universidad de Salamanca (USAL), marzo.

GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M. [2012]: «El reto de la protección de datos de las personas mayores en la sociedad del ocio digital», en CERRILLO I MARTÍNEZ, A.; PEGUERA, M.; PEÑA-LÓPEZ, I.; PIFARRÉ DE MONER, M. J. y VILASAU SOLANA, M. (coords.): *Retos y oportunidades del entretenimiento en línea, actas del VIII Congreso Internacional, Internet, Derecho y Política*, Universitat Oberta de Catalunya, Barcelona, 9-10 julio, UOC, Huygens Editorial, Barcelona.

- [2012]: «La protección de datos de las personas mayores, necesidad y reto para una innovación tecnológica de calidad», en el Congreso de la Red Derecho TIC: la privacidad, ¿un lastre para la innovación tecnológica?, Universidad de Murcia, 22-23 de noviembre.

GÓMEZ-JUÁREZ SIDERA, I. y LARA YUSTE, F. [2009]: «Personas mayores en la sociedad de las nuevas tecnologías: la necesidad de navegar hacia un horizonte donde el derecho a la protección de sus datos sea plenamente respetado», en la revista digital *Datospersonales.org* [en línea], Agencia de Protección de Datos de la Comunidad de Madrid (APDCM), 31 de julio, Madrid, núm. 40, http://www.madrid.org/cs/Satellite?c=CM_Revisita_FP&cid=1142560422023&esArticulo=true&idRevistaElegida=1142557356539&language=es&pagina=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales.

GONZÁLEZ VEGA, N.; KÄMÄRÄINEN, A. y KALLA, O. [2010]: «Ethical aspects in ICT research and development: the case of the confidence project», en CUNNINGHAM, P. y CUNNINGHAM, M. (eds.): *eChallenges e-2010 Conference Proceedings*, IIMC International Information Management Corporation, Dublín.

IID (INTERNET IDENTITY)/NEWS [2012]: «IID says 2013 cyberthreats are so 2012; predicts two years ahead: ubiquitous Internet connections will allow death by device and massive over-the-air theft by 2014» [en línea], 18 de diciembre, <http://www.internetidentity.com/news/?id=203>.

LABORATORIO ONTINET.COM [2012]: «Virus informáticos y marcapasos: una combinación de alto voltaje» [en línea], 19 de octubre, <http://blogs.protegerse.com/laboratorio/2012/10/19/virus-informaticos-y-marcapasos-una-combinacion-de-alto-voltaje/>.

MARTÍN JIMÉNEZ, C. M. y MARTÍN JIMÉNEZ, J. J. [2010]: *Teoría y práctica del ejercicio de las acciones civiles. Comentarios y formularios*, Lex Nova, SAU, Valladolid.

RETUERTO BUADES, M. [2001]: «Discapacidad y tuición: las limitaciones a la capacidad de obrar por razón de la edad y de la salud. Los derechos del impedido», en VV. AA. (coord. GONZÁLEZ PORRAS, J. M. y GALLEGO DOMÍNGUEZ, I.): *Actas de las Primeras Jornadas de Problemas legales sobre tutela, asistencia y protección a las personas mayores, Córdoba, 17 y 18 de noviembre de 2000*, Publicaciones Obra Social y Cultural CajaSur, Córdoba.

RT ACTUALIDAD/CIENCIA [2011]: «Un "hacker" estadounidense reclama más seguridad para los dispositivos de salud» [en línea], 8 de agosto, <http://actualidad.rt.com/ciencias/view/31046-Un-hacker-estadounidense-reclama-mas-seguridad-para-dispositivos-de-salud>.

SERRANO GARIJO, P. y RAMÍREZ SEBASTIÁN, J. M. [2008]: «Edad, salud y deterioro de la visión: la disminución visual como síndrome geriátrico», en *Integración. Revista sobre ceguera y deficiencia visual*, Dirección General de la Organización Nacional de Ciegos Españoles, núm. 55 (monográfico: Envejecimiento y discapacidad visual), diciembre, págs. 9-19.

SITIO WEB DE BECLOSE, INC. [en línea], <http://www.beclose.com/>.

SITIO WEB DE GRANDCARE SYSTEMS, INC. [en línea], <http://www.grandcare.com/>.

SITIO WEB DE MEDMINDER SYSTEMS, INC. [en línea], <http://www.medminder.com/>.

TORRES VIGUERA, A. y GALÁN SOLDEVILLA, L. [2001]: «Ética médica y tercera edad. Confidencialidad de los datos clínicos y consentimiento informado», en VV. AA. (coord. GONZÁLEZ PORRAS, J. M. y GALLEGO DOMÍNGUEZ, I.): *Actas de las Primeras Jornadas de Problemas legales sobre tutela, asistencia y protección a las personas mayores, Córdoba, 17 y 18 de noviembre de 2000*, Publicaciones Obra Social y Cultural CajaSur, Córdoba.

VV. AA. (coord. HERNÁNDEZ SALVADOR, C.) [2011]: *Innovación TIC para las personas mayores. Situación, requerimientos y soluciones en la atención integral de la cronicidad y la dependencia*, Fundación Vodafone, Madrid.

WELIVSECURITY [2012]: «Malware and medical devices: hospitals really are unhealthy places...» [en línea], 18 de octubre, <http://www.welivesecurity.com/2012/10/18/malware-and-medical-devices-hospitals-really-are-unhealthy-places/>.

ZURITA MARTÍN, I. [2004]: *Protección civil de la ancianidad*, Editorial Dykinson, SL, Madrid.