Proyecto PG E-Salud

EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN LAS APPS DE SALUD

Alumno: DAVID BENEDED BLÁZQUEZ

Director: Dr. ISIDRE FÀBREGUES ALADREN

Resumen

Constituidas como las más relevantes y prolíficas soluciones de la *mHealth*, las aplicaciones de salud para dispositivos móviles manejan gran cantidad de información sensible comprendiendo, entre otras funcionalidades, el acceso a sistemas de información interconectados, la comunicación con profesionales sanitarios y comunidades de pacientes o el registro de todo tipo de datos incluyendo los obtenidos de modo automático a través de técnicas como la geolocalización o la monitorización biomédica mediante sensores y wearables.

El presente trabajo tiene como finalidad el determinar si las *apps de salud* garantizan la confidencialidad y seguridad de la ingente cantidad de datos personales que pueden llegar a recabar de los usuarios que las utilizan. Y, estando sujetas al marco normativo en materia de protección de datos, se analizan los conceptos básicos y principios fundamentales por los que se rige el nuevo Reglamento General de Protección de Datos

Finalmente, se ofrecen a los desarrolladores una serie de recomendaciones y buenas prácticas que no sólo les pudiese ayudar a cumplir con la legislación sino también a que, aplicando los principios de responsabilidad activa y privacidad desde el diseño, puedan contribuir a crear mejores y más completas soluciones centradas en el usuario.

TÉRMINOS CLAVE

mHealth, apps de salud, privacidad, protección de datos, RGPD

Índice

Introducción

Las aplicaciones de salud para dispositivos móviles se han constituido como las más relevantes y prolíficas soluciones de la llamada salud móvil o *mHealth*, gracias a su ubicuidad, facilidad de uso, versatilidad, multifuncionalidad, interactividad, sensibilidad al entorno junto al bajo e, incluso, bajo o nulo coste de las mismas para quienes las adquieren.

El uso de las *apps* permite redimensionar el uso básico de los teléfonos móviles, incorporando funcionalidades mucho más avanzadas y complejas que comprenden "herramientas de comunicación, información y motivación, tales como los recordatorios de medicación o las herramientas que proporcionan recomendaciones dietéticas y para mantenerse en forma" además, de entre otras funciones, "medir diversidad de constantes vitales y permitir, junto a otros sensores, la recogida de un considerable número de datos médicos, fisiológicos y relativos al modo de vida, a la actividad diaria y al entorno" (COM, 2014).

Para ello, las *apps de salud* deben manejar gran cantidad de información sensible referente a los individuos que hacen uso de ellas. Ingentes cantidades de datos personales que, en muchos casos, son accesibles y tratados por diferentes y múltiples actores implicados en el desarrollo, publicación y mantenimiento de las mismas: desarrolladores, fabricantes de sistemas operativos y dispositivos, tiendas de aplicaciones, autoridades públicas, profesionales sanitarios y hasta otras terceras partes como proveedores de análisis y publicidad.

Las preguntas que rápidamente surgen es si estos datos, catalogados en su gran parte como sensibles al referirse a la salud, están adecuadamente protegidos y si las *apps* ofrecen garantías suficientes para la privacidad y confidencialidad de los mismos. Por estos motivos, el presente trabajo tiene los siguientes objetivos:

- Dar a conocer qué es la *mHealth*, especialmente las *apps de salud* como máximo exponente de la misma, analizando su estado actual, las categorizaciones, el variado ecosistema de *skateholders* y su compleja arquitectura.

- Examinar, a través de la revisión de la literatura científica, los beneficios y problemas que actualmente presentan las *apps de salud*, tratando de determinar los posibles riesgos en cuanto a la seguridad, privacidad, confidencialidad e integridad de los datos que se tratan a través de las mismas.

- Determinar el marco normativo que le son aplicables en materia de protección de datos así como qué otras leyes del ordenamiento jurídico español complementan dicha normativa a través de disposiciones específicas desarrolladas en el ámbito sanitario y de la administración pública.

- Analizar los conceptos jurídicos y principios fundamentales de la normativa vigente, en especial, el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) con efecto a partir del 25 de mayo de 2018.

- Concienciar a los desarrolladores de *apps* de la transcendencia de garantizar el cumplimiento de la normativa sobre privacidad y protección de datos y de la relevancia, incluso para el propio negocio, de transmitir confiabilidad en todo momento y a todo el mundo (tanto a los que ya son usuarios de una *app* como a los que en un futuro podrían serlo).

- Difundir una serie de buenas prácticas, basadas en el análisis de la legislación en materia de protección de datos, en la aplicación de los principios de responsabilidad proactiva y privacidad desde el diseño y en las recomendaciones y sugerencias emanadas desde las autoridades competentes como la Agencia de Protección de Datos Española o el "Grupo de Trabajo del artículo 29".

1. La *mHealth* y las aplicaciones móviles de salud

Los avances tecnológicos y la creciente prevalencia y asequibilidad de los dispositivos móviles ha llevado a que el número de éstos, estimado en casi ocho mil millones según el informe Ditrendia (2016), supere ya al de habitantes en el mundo.

De entre todos estos dispositivos, destacan sobremanera los llamados *teléfonos móviles inteligentes* o *smartphones*, término genérico acuñado para describir a aquellos teléfonos móviles que proporcionan una amplia variedad de funciones por encima de las asociadas a hacer llamadas telefónicas, tales como navegar por web o mantener una agenda (Ince, 2016).

La popularidad y la exitosa inmersión en nuestra sociedad de los *smartphones* es tal que, según el citado informe, en España ya representan el 87% del total de teléfonos móviles (lo que sitúa a nuestro país en la primera posición a nivel europeo) siendo con diferencia los dispositivos más utilizados para acceder a internet, por delante de ordenadores de escritorio y portátiles.

Y es que, desde que en el año 2007 la multinacional tecnológica Apple presentara su iPhone, el mundo de estos dispositivos daría un giro radical provocando que el resto de fabricantes de teléfonos comenzaran a fabricar terminales con características similares, llevando así a estandarizar un único dispositivo que, combinando los conceptos de teléfono móvil y ordenador *handheld*[1], se convertiría en una herramienta imprescindible que ya ha cambiado la forma en que las personas se comunican, se informan, pasan su tiempo de ocio y, también, cuidan su salud.

1.1 La *mHealth* o "salud móvil"

Si bien el uso de las Tecnologías de la Información y las Comunicaciones (TIC) ya estaba integrado en el sector sanitario en el contexto de la *eHealth*, definida por Eysenbach (2001) como "un campo emergente en la intersección de la informática médica, la salud pública y los negocios, referido a los servicios sanitarios y la información transmitida o mejorada a través de internet y las tecnologías relacionadas"[2], gracias al crecimiento de los servicios de redes móviles y a los elevados índices de penetración de los dispositivos móviles, han quedado revolucionados los pilares básicos de la sanidad en base a un modelo *everywhere*, *everytime*, *everyone*, es decir, llevando los servicios de atención sanitaria allá donde sean necesarios: en todas partes, en todo momento y para todas las personas.

[1] Según *Oxford Business Spanish Dictionary* término con el que se define a la "computadora u ordenador de mano", considerando "mano" como que se puede llevar en una mano mientras se utiliza.

[2] El Dr. Gunther Eysenbach, además, trataría de otorgar un sentido más amplio al término al considerar que representaba "no sólo un desarrollo técnico, sino también un estado mental, una forma de pensar, una actitud, y un compromiso con un pensamiento conectado, global, para mejorar la sanidad local, regional y globalmente a través del uso de las tecnologías de la información y la comunicación".

De esta manera, y como una evolución de los sistemas *eHealth* (o al menos como confluencia entre éstos y la tecnología de teléfonos inteligentes), surgiría el término *mHealth* o "salud móvil" empleado por vez primera por Istepanian y Lacal (2003) para referenciar la prestación de servicios de salud y al ejercicio de la telemedicina inalámbrica mediante el uso de las tecnologías emergentes de red y de comunicaciones móviles.

Un concepto académico que, en pocos años, acabaría transformándose en un fenómeno global de la tecnología de la salud, siendo la propia Organización Mundial de la Salud quien redefiniera la *mHealth* como "la práctica médica y de salud pública apoyada por dispositivos móviles, tales como teléfonos móviles, dispositivos de monitorización de pacientes, asistentes digitales personales (*PDA*) y otros dispositivos inalámbricos" (OMS, 2011).

Desde fases incipientes, la *mHealth* era poseedora de una serie de características intrínsecas que la diferenciaban del resto de tendencias: accesibilidad, al proporcionar ubicuidad y acceso universal para dar soluciones en cualquier momento; personalización, al ofrecer soluciones individualizadas para abordar las necesidades específicas de una persona concreta basándose en su perfil; inmediatez, al brindar servicios en el momento justo y centrarse en información pertinente, puntual y oportuna; interactividad, al promover la cocreación de valor mediante una interacción bidireccional intensa y a largo plazo; movilidad, al satisfacer las necesidades de movilidad temporal, espacial y contextual; y localización, al proporcionar servicios de información específicos del contexto mediante sistemas de posicionamiento global y de célula de origen (Akter, D'Ambra y Ray, 2013).

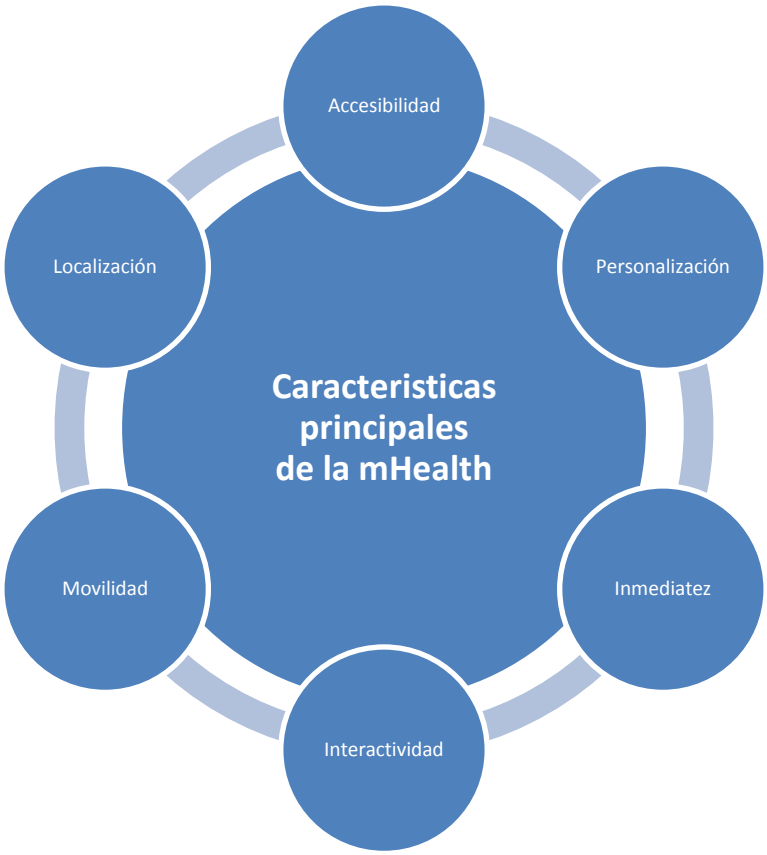

Ilustración 1. Características principales de la mHealth según Akter, D'Ambra y Ray (2013).

Y, aunque inicialmente estaba basada esencialmente en servicios de voz (centros de atención de llamadas sobre salud y números de emergencias) y mensajería de textos cortos (envío de SMS para el recordatorio de citas, seguimiento de tratamientos o sensibilización de temas de salud) pronto se incorporarían en los dispositivos tecnológicos "estrellas" (*tablets* y *smartphones)* funcionalidades más complejas a través de las *apps*, modo abreviado con el que se define a los "programas residentes en un smartphone que realiza alguna función útil" (Ince, 2016).

1.2. Las *apps*, máximo exponente de la *mHealth*

Gracias a su ubicuidad, facilidad de uso, versatilidad, multifuncionalidad, interactividad, sensibilidad al entorno e, incluso, su bajo o nulo coste para los usuarios, las conocidas *apps de salud* se han establecido como el máximo exponente de la *mHealth* al comprender "herramientas de comunicación, información y motivación, tales como los recordatorios de medicación o las herramientas que proporcionan recomendaciones dietéticas y para mantenerse en forma" además de, entre otras funciones, interconectarse con otros sistemas de información o recoger para su monitorización, en combinación con distintos sensores y dispositivos de *tecnología ponible*[3], constantes vitales (como la frecuencia cardíaca, el nivel de glucosa en la sangre, la presión arterial, la temperatura corporal y la actividad cerebral) y un largo número de datos médicos, fisiológicos, relativos al modo de vida y bienestar, a la actividad diaria y al entorno (COM, 2014).

Según el estudio sobre seguimiento de la salud y la forma física llevado a cabo en dieciséis países por GfK (2016), se estima que una de cada tres personas hace un seguimiento de su salud o de su forma física a través de algún dispositivo mediante una *app*, siendo los españoles los sextos del mundo que más seguimiento hacen con aplicaciones móviles al declarar el 24% de los encuestados que actualmente lo llevan a cabo y otro 17% que, aunque actualmente no lo hacen, si lo han hecho en el pasado.

Las *apps de salud* están a la vanguardia de la tecnología y su proliferación es tal que, según el último estudio anual de Research2Guidance, en 2016 se encontraban disponibles unas 259.000 *apps* publicadas en las principales tiendas de aplicaciones por 58.000 desarrolladores, habiéndose producido solo en el último año alrededor de 3.000 millones de descargas y previéndose que en 2020 haya 551 millones de usuarios que, al menos, hayan instalado y usado una de estas *apps* en sus dispositivos.

Como se apuntaba, las miles de *apps* abarcan diferentes áreas referentes a la salud y funcionalidades distintas tanto para profesionales sanitarios como para pacientes / ciudadanos y, si bien la mayoría de las *apps* están enfocadas al bienestar físico, estilo de vida y nutrición (el 65%), ya hay un 22% de *apps* centradas en manejo del tratamiento y gestión de la enfermedad (IMS Health Institute, 2015) pudiéndose efectuar una clasificación particular de las mismas en función de las condiciones de salud más prevalentes según la *Global Burden of Disease* (GBS) publicada desde 2004 por la OMS (Martínez-Pérez, de la Torre-Díez y López-Coronado, 2013) o basándose en la décima versión de la *Clasificación Internacional de Enfermedades*, como hicieran los investigadores de la Fundación iSYS para desarrollar un método automatizado de

[3] Término recomendado por la Fundación por el Español Urgente (Fundéu) como traducción al español de *wearable technology* con el que se hace referencia a aquellos dispositivos que se llevan sobre, debajo o incluidos en la ropa y que están siempre encendidos.

captura de *apps* (MACA) que les permitiera efectuar una amplia y objetiva selección para su proyecto índice iSYScore extrayendo palabras claves del citado CIE-10 y que, finalmente, acabarían por incluir estas categorías en su *Catálogo de Aplicaciones de la Salud*, por lo que los usuarios pueden acceder a la búsqueda de las *apps* mediante las mismas como herramienta adicional a su conocido y prestigioso *Top 20 iSYScore* (Grau et al., 2016).

Como se decía, es importante realizar una correcta clasificación de los distintos tipos de *apps* relacionadas con la salud, teniendo en cuenta que en las tiendas de aplicaciones todas se engloban en las manidas "medicina", "salud y bienestar" o "salud y forma física". Por este motivo, y aunque se puede llevar a cabo la categorización de diferentes formas, al no existir todavía un consenso sobre cómo proceder, resulta de interés la elaborada desde "la perspectiva de cómo las personas usan las aplicaciones de salud y su percepción del riesgo" por el Dr. Zoran Stančič en el prólogo del informe *The myhealthapps directory 2015-2016* publicado por la organización independiente británica PatientView, en donde estableció tres clases distintas:

- Aplicaciones para discapacidad: que posibilitan a las personas con discapacidad (ya sea física, mental y/o sensorial) hacer frente a su vida diaria y brindarles apoyo. Por ejemplo, formarían parte de esta clase, *apps* de conversión de texto a voz que ayudan a las personas que tienen dificultades de hablar o habilidades verbales limitadas, para aumentar sus habilidades de comunicación.

- Aplicaciones médicas: aquellas *apps de salud* que conducen a cualquier tipo de toma de decisiones clínicas, diagnóstico o tratamiento así como las que funcionan con dispositivos médicos. Concretamente, y bajo el criterio de la US Food and Drug Administration (FDA) estas *apps* deben ser evaluadas y reguladas[4] si están "destinadas a ser utilizadas como un accesorio para un dispositivo médico regulado", por ejemplo, una aplicación que permite a un profesional de la salud hacer un diagnóstico específico mediante la visualización de una imagen médica de un sistema de archivo y comunicación de imágenes (PACS en inglés) en un *smartphone* o una *tablet*, o si "se transforman en un dispositivo médico regulado", por ejemplo, una aplicación que convierte el smartphone en un electrocardiógrafo para detectar ritmos cardíacos anormales o determinar si un paciente está sufriendo un ataque al corazón.

- Aplicaciones para la salud, el bienestar y el cuidado en la comunidad: quedando encuadradas las *apps* referentes a estilo de vida (dieta, ejercicio, hábitos saludables) y las que contribuyen a la autogestión de la salud sin requerir, inicialmente, la intervención de un profesional sanitario.

Como esta última agrupación parece intentar abarcar demasiadas finalidades y funcionalidades que difieren enormemente entre sí, acudimos a otra categorización, la propuesta por *The App Date* en su *Informe 50 mejores apps de salud en español*, para realizar una sub-clasificación que permita una mayor representación:

- Información: aquellas *apps* cuya función principal es aportar información completa y detallada sobre alguna patología determinada, ya sea en formato texto, imagen o vídeo.

[4] De similar modo en Europa, como se describe más adelante, al ser consideradas "productos sanitarios"

- Educación y sensibilización: las que van más allá de aportar información, promoviendo la educación activa de los usuarios tratando de empoderar al paciente siguiendo la metodología de *paciente experto* emprendida por la Universidad de Stanford[5] y el concepto *e-paciente* propuesto por el Dr. Tom Ferguson[6].

- Registro y monitorización: las que realizan un seguimiento de tratamiento o para monitorizar diversos parámetros físicos y hacer el seguimiento de la actividad diaria o comportamiento, excepto cuando pudieran ser *productos sanitarios*, debiendo pasar a la categoría de aplicaciones médicas.

- Recordatorio y seguimiento de tratamiento: las que sirven de apoyo al paciente para mejorar su adherencia al tratamiento o tener un control sobre cómo está llevando el mismo (sin que requiera intervención médica), como recordatorios de cuándo y en cuánta dosis se deben tomar los medicamentos o la anotación de cada una de las administraciones llevadas a cabo.

- Gestión y utilidades: las que permiten realizar gestiones administrativas y otras utilidades (como citas, localización de centros y profesionales).

1.3. Beneficios y problemas de la *mHealth*

Las bonanzas de la *mHealth* han sido puestas de manifiesto en diversidad de estudios formales y evaluaciones de proyectos siendo indudable que pueden contribuir a mejorar la eficiencia de la prestación de asistencia sanitaria aumentando significativamente la disponibilidad y asequibilidad de la misma, especialmente en aquellos pacientes que residen en zonas rurales y remotas (Mirza, Norris y Stockdale, 2008); facilita la promoción de la salud y estilos de vida saludables mediante la comunicación de comportamientos de prevención de enfermedades agudas y crónicas (OMS, 2016); y posibilita el alcanzar una mayor eficacia de la atención sanitaria al aportar beneficios palpables en el cumplimiento de los regímenes de adherencia al tratamiento, los autocuidados y la gestión de la enfermedad (UNF & Vodafone, 2009).

La gestión de salud pública también se beneficia, puesto que la recopilación de grandes cantidades de datos provenientes de las soluciones de *mHealth* facilita la investigación epidemiológica y mejora la eficacia del cuidado de la salud al analizar patrones a gran escala. Y, en última instancia, también ayuda a abordar los problemas derivados de la falta de profesionales sanitarios contribuyendo, adicionalmente, a una considerable reducción de costes y a una mejora en la calidad de la atención médica tradicional "cara a cara" al permitir que los profesionales puedan dedicar más tiempo a los pacientes que realmente lo requieren (PWC, 2013).

Sin embargo, pese a todos los potenciales beneficios antes citados y las posibilidades de transformación de la prestación de asistencia sanitaria que en todos los sistemas sanitarios puede llegar a ofrecer, la *mHealth* y, consiguientemente, las *apps de salud* todavía presentan una serie de graves problemas y preocupaciones.

[5] http://patienteducation.stanford.edu/
[6] http://www.e-patients.net

Las administraciones e instituciones públicas, como pone de manifiesto en 2016 el Consejo Ejecutivo de la OMS, esgrimen que "les resulta difícil evaluar, ampliar e integrar las soluciones de *mHealth*" debido a cuatro factores principales: "la existencia de múltiples proyectos experimentales sin ningún plan ni proceso definido de ampliación; la falta de interconexión entre las diferentes aplicaciones y de integración con las estrategias nacionales de *cibersalud* y las estructuras de información sanitaria existentes; la ausencia de normas y herramientas para la evaluación comparativa de la funcionalidad, la posibilidad de ampliación y el valor comparativo de las soluciones de *salud móvil*, lo que da lugar a una falta de datos para articular la orientación normativa; y la falta de enfoque multisectorial dentro del gobierno […] y de recomendaciones normativas de colaboración con el sector privado" (OMS, 2016).

Los profesionales sanitarios, por su parte, todavía son reacios en su mayoría a recomendar aplicaciones a sus pacientes, siendo solamente el 7,5% de los médicos españoles los que lo hacen según el estudio de ONTSI (2016).

Y si bien no se puede ocultar que todavía conforma una barrera ese cierto "paternalismo médico" contrario a ceder el control a los pacientes por temor al autodiagnóstico y al autotratamiento (Telefónica, 2013), los profesionales se sienten perdidos ante la cantidad ingente de *apps* existentes sin saber cómo discriminar las de mayor utilidad y calidad científica, surgiendo también dudas sobre la responsabilidad que les atañería en caso de "prescribir" una determinada *app* que funcione incorrectamente.

En general, el colectivo médico argumenta una ausencia generalizada de resultado clínico (Singh et al., 2016) poniendo el foco directamente sobre los desarrolladores, a quienes acusan de falta de conocimientos y competencia (Akter, D'Ambra y Ray, 2013) así como de precipitarse en la publicación y de poner las *apps* en el mercado sin adherirse a la evidencia médica pertinente ni contar con la participación de expertos (Subhi et al., 2015) ni con la aportación previa y la evaluación crítica de los hipotéticos usuarios finales (Barton, 2012). Un razonamiento similar al que utiliza la Asociación Médica Mundial en su *Declaración sobre la salud móvil* donde subraya que muchas de las soluciones se han llevado a cabo solo por el estímulo del mercado en vez de por la "necesidad de eliminar las deficiencias en la prestación de atención médica o mejorar la calidad de la atención" añadiendo que tampoco se tenía "la consideración apropiada de los aspectos de la protección y seguridad de la información" ni se preocupaban sobre la seguridad del paciente, ya que "a menudo es imposible que los usuarios sepan si la información difundida a través de la salud móvil proviene de una fuente médica fiable".

Los desarrolladores, a su vez, aducen que aunque el mercado de *apps de salud* está en crecimiento, todavía no es un negocio rentable excepto para un número muy reducido de casos. De hecho, según el estudio de IMS Health Institute (2015), un grupo relativamente pequeño de *apps de salud* (el 12%) cuentan con más de 100.000 descargas (lo que representa el 90% del total de descargas) abundando lo que se denomina *apps zombies*, es decir, aplicaciones prácticamente invisibles y sin apenas descargas que, además, tras su publicación inicial permanecen desactualizadas y sin ningún tipo de mantenimiento. Consecuentemente, para rentabilizar la inversión deben buscar otras fuentes de ingresos alternativas a las tradicionales formas de monetización mediante *pay per download* (pago por descarga) o *in-app purchase* (compras dentro de la aplicación) por lo que deben recurrir a otorgar licenciamientos, el desarrollo a medida para terceros, patrocinios o a otras técnicas como el *in-app advertising* (R2G, 2016).

Finalmente, los pacientes y ciudadanos en general, al igual que los profesionales sanitarios (con el hándicap añadido de, en general, no tener conocimientos médicos), se ven desorientados a la hora de escoger las *apps* más adecuadas y discernir entre cuáles contribuirán a mejorar su salud de las que pueden provocar el efecto contrario (especialmente en aquellas que, por sus características, debían tener el certificado *CE producto sanitario* y no lo tienen). Además, también se enfrentan a problemas derivados de la brecha digital o a la deficiente usabilidad de algunas *apps* que presentan interfaces complejas que dificultan el que se puedan completar tareas básicas y críticas, careciendo muchas de ellas de funciones más automatizadas (Sarkar et. al, 2016). Y otra cuestión problemática es la económica puesto que, pese a que las *apps* son relativamente baratas (e incluso, gratuitas) éstas funcionan sobre costosos dispositivos, debiendo también que contratar las pertinentes líneas de telefonía móvil con tarifas para datos que no están al alcance de todos los colectivos (Patrick et al., 2008).

Pero si hay algo que preocupa por igual a todos los actores implicados y que se considera como la principal cuestión en juego en relación con el desarrollo de la mHealth, es como pone de manifiesto la Comisión Europea en su *Libro Verde sobre sanidad móvil* (en adelante, el *Libro Verde*), ese es sin duda "**la protección de datos, incluyendo la seguridad de los datos sanitarios**".

Como se desprende de las funcionalidades anteriormente citadas, la gran mayoría de las llamadas *apps de salud*, recopilan y procesan cantidades ingentes de datos referentes a los individuos que las instalan en sus dispositivos y hacen uso de ellas.

De hecho, el tráfico de información se inicia incluso con anterioridad al uso de la propia *app*, puesto que los usuarios deben acceder a las tiendas de aplicaciones previo registro para tener la posibilidad de descargar e instalar la *app* deseada, debiendo retornar la conexión periódicamente (aunque la mayoría de ocasiones, se haga ya de forma automática) para descargar actualizaciones. En caso de tener que efectuar pagos para la descarga o para acceder, por ejemplo, a determinadas funcionalidades (en los modelos *freemium*) también se pueden a llegar a efectuar conexiones con servidores de entidades bancarias para modo de pago como *paypal*.

Una vez instalada, la *app* comienza a registrar datos (muchos de ellos sensibles al pertenecer a la esferas íntimas como la salud) ya sea porque los introduce directamente el usuario o de forma automatizada mediante los sensores del propio dispositivo u otros dispositivos externos interconectados vía *Bluetooth* como *wearables* (ropa, pulseras, gafas) o dispositivos médicos (pulsímetro, tensiómetro, termómetro, glucómetro, etc.) que recogen parámetros fisiológicos, condiciones de salud, movimientos y ubicación.

Pero estos datos difícilmente quedan almacenados única y exclusivamente en el propio dispositivo o, a lo sumo, en una tarjeta de memoria externa, sino que lo hacen en servidores, por lo que se requiere una conexión cuasi permanente con ellos a través de internet vía Wifi, WiMAX o, principalmente, telecomunicaciones móviles de tercera y cuarta generación (3G y 4G). Y no sólo se utiliza un determinado servidor, sino que a su vez, se precisa la interconectividad con otras bases de datos y sistemas de información con los que comparte el acceso y la comunicación de datos, abarcando desde las entidades prestadoras de servicios sanitarios (acceso a la Historia Clínica Electrónica, receta electrónica o la tramitación de citas y otras gestiones) hasta sistemas de seguimiento de salud a través del uso de *APIs* (como Google Fit o Apple Healthkit).

También, las *apps* suelen permitir cargar, hacer copias de seguridad o sincronizar datos en servicios de almacenamiento en la nube así como compartir datos de forma programada y automatizada mediante un simple correo electrónico o a través de las redes sociales. Y es que, como señala el Grupo de Trabajo «artículo 29 sobre protección de datos» (en adelante, GT29), la multiplicidad de actores intervinientes en el ecosistema de las *apps de salud* incluye no pocos tratamientos adicionales de datos para proporcionar al usuario servicios distintos de la finalidad prevista y esperada de la *app* pero que si suelen conformar una fuente para generar ingresos, de forma desconocida o no deseada por el usuario, tales como servidores de publicidad o herramientas analíticas para realizar un seguimiento del comportamiento del usuario (WP202).

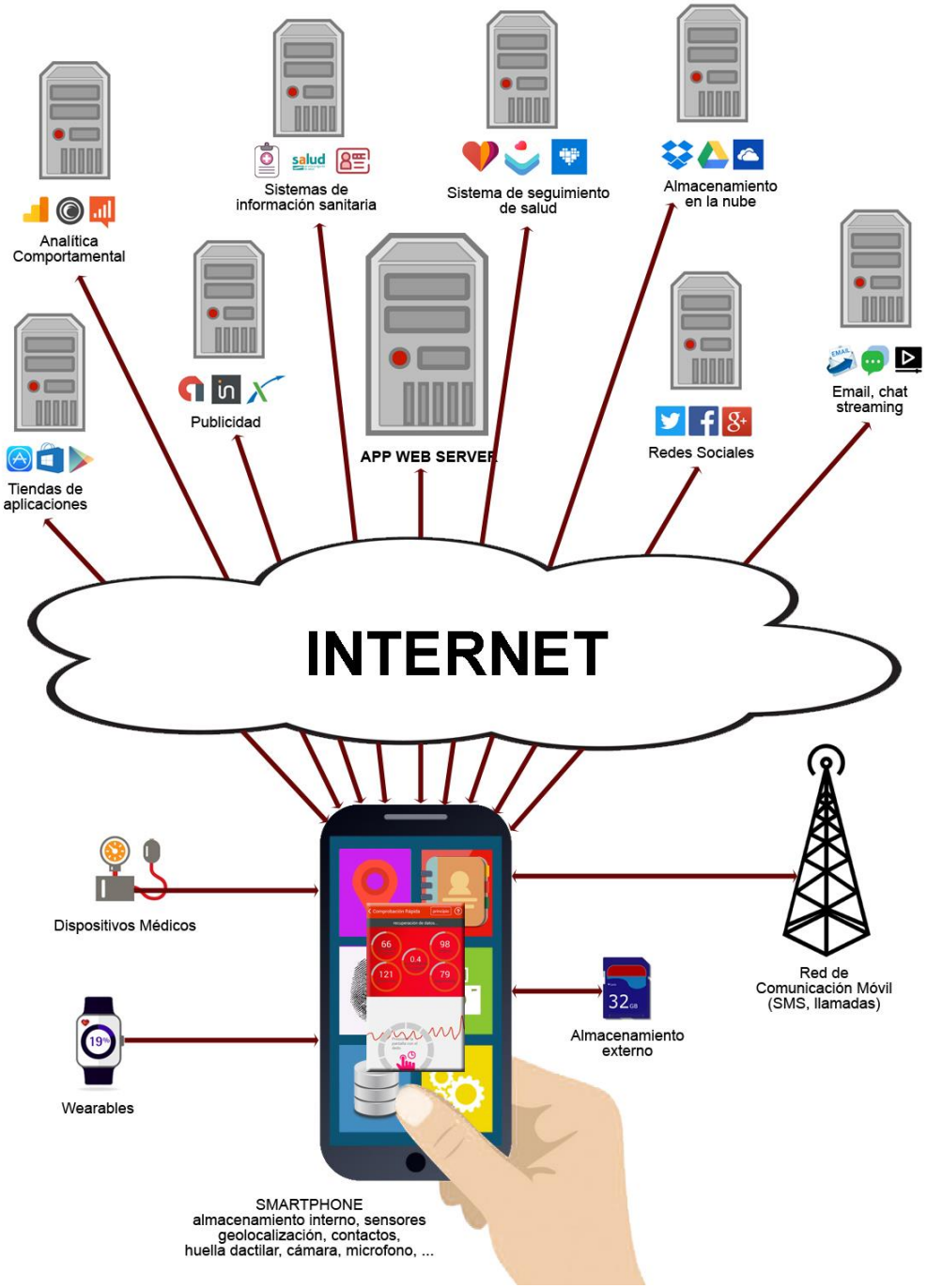

Ilustración 2. Arquitectura "tipo" de una *app de salud*.

1.4. Riesgos en el uso de *apps de salud* para la privacidad y la seguridad de los datos personales de los usuarios

Para poder determinar si las *apps de salud* tratan adecuadamente los datos de salud de los usuarios que las manejan o si suponen un riesgo significativo para la privacidad y la seguridad de dicha información, se realiza una revisión de la literatura científica:

Así, por ejemplo, encontramos que **Linda Ackerman (2013)** llevó a cabo una investigación para California Consumer Protection Foundation sobre 43 de las más populares aplicaciones de salud y fitness, concluyendo que el 26% de las aplicaciones gratuitas y un impactante 40% de las de pago no tenían ningún tipo de política de privacidad. Además, de las *apps* que si tenían, solamente el 43% de las gratuitas y el 25% de pago proporcionaban un acceso a sus políticas de privacidad desde la propia *app*, debiendo ser el usuario quien, en el resto de *apps*, tuviera que buscar por su cuenta las políticas de privacidad pertinentes. Además, la investigación también desveló que el 39% de las *apps* gratuitas y el 30% de las de pago enviaban datos sin que el usuario fuera informado de ello así como que solo el 13% de las *apps* gratuitas y el 10% de las de pago cifraban todas las conexiones de transmisión de datos.

A raíz de este estudio, el **Financial Times** realizó una investigación en la que ponía de manifiesto que 20 de las aplicaciones más populares relacionadas con la salud transmitían información a una red de casi 70 empresas, haciéndolo 9 de las cuales con una de las empresas dominantes de seguimiento de la información sobre el uso del teléfono móvil (Steel y Dembosky, 2013).

De modo similar, en el análisis de más de 1200 *apps* efectuado por la **Red Global de Control de la Privacidad** en la que participan las principales autoridades de protección de datos, también se comprobó que solo un 15% de las *apps* suministraban información clara a los usuarios sobre cómo van a ser recopilados, utilizados y divulgados sus datos personales y que el resto solo ofrecía "cierta información (31%), información inadecuada (24%), o no ofreció información alguna sobre privacidad aparte de los permisos (30%)". Además, el 31% de las *apps* analizadas solicitaban permisos excesivos en relación a las funciones previstas (GPEN, 2014).

Sunyaev et al. (2014) enfocaron su estudio sobre las 600 *apps de salud* más descargadas en las dos principales tiendas de aplicaciones, detectando que el 69,5% no tenían políticas de privacidad. Un resultado que todavía era mucho peor al encontrar que dos terceras partes del 30,5% que si tenían política de privacidad no hacían en ella referencia específica a la propia aplicación sino que su contenido derivaba en información genérica de varios servicios ofrecidos por el desarrollador. Y, en el mejor de los casos, concluían que las políticas encontradas eran largas (1755 palabras de longitud de media) y complejas de entender, requiriendo para ello conocimientos de nivel universitario.

Principios de calidad que también esperaban encontrar en su estudio **Huckvale et al. (2015)** en las *apps* incluidas en la *Health Apps Library*, la biblioteca de *apps de salud* recomendadas por el servicio sanitario público británico, el National Health Service (NHS). Y aunque los resultados fueron bastante positivos, ya que solo el 20% no tenían política de privacidad, otros aspectos analizados como que ninguna de las *apps* cifraba los datos personales almacenados "en local" o que el 66% enviaban información de

identificación a través de internet sin utilizar ningún tipo de cifrado, llevaría a tal escándalo que la NHS se vería obligada a cerrar en octubre de 2015 la, hasta entonces, prestigiosa biblioteca puesto que su acreditación se basada fundamentalmente en la autodeclaración de los desarrolladores y no en un método exhaustivo de evaluación (Satish Misra, 2015).

Por su parte, **He et al. (2015)** investigaron la seguridad y privacidad de las aplicaciones gratuitas de *mHealth* que se ofrecían en Google Play encontrando que el 42,9% de las *apps* usaban comunicación no cifrada para transferir la información sensible relacionada con la salud así como que el 33,3% ponían información sensible en mensajes de registro, revelando datos de coordenadas GPS, información de amigos de Facebook e, incluso, datos más sensibles como nombre o el historial de detección de enfermedades. Además también identificaron hasta siete superficies de ataque que potencialmente podían afectar la seguridad, tales como errores en las configuraciones de conexión con *wearables* y dispositivos de salud habilitados para *Bluetooth* (quedando expuesta la información registrada a ataques por *sniffing*, inyección de datos), almacenamiento de la información en archivos sin cifrar en la tarjeta SD o en servidores de terceros de los que se desconocía si usaban cifrado o no así como otros riesgos como que los componentes de la aplicación (*activities, services, content providers, broadcast receivers)* pese a estar destinados a ser privados, quedaban exportados siendo accesibles para otras aplicaciones instaladas en el dispositivo.

Knorr et al. (2015) investigaron sobre 154 *apps* para Android sobre diabetes e hipertensión, encontrando que muchas de ellas no proporcionan políticas de privacidad constatando que solo el 19% de las mismas tenía publicada la política de privacidad en la propia tienda de aplicaciones (en este caso, Google Play). Además tampoco utilizaban comunicaciones seguras (solo el 17% utilizaban el algoritmo de encriptación SHA-256) y que, en general, estaban "infestadas" de complementos publicitarios y analíticos que, por si fuera poco, transmitían datos en el encabezado HTTP siendo susceptibles de sufrir *eavesdropper*.

Similar estudio, también sobre *apps* para la diabetes en Android, llevaron a cabo **Blenner et al. (2016)**, concluyendo que el 81% de las mismas no tenía ningún tipo de política de privacidad. Y de las que tenían, apenas se alcanzaba el 10% de las que verdaderamente informaban que recogían datos de los usuarios o que los compartían con terceros. Además, llamaban la atención sobre la colocación de *cookies* de rastreo en el 86,2% de las *apps* y sobre la cantidad de permisos que los usuarios debían aceptar al descargar una aplicación, siendo en muchos casos totalmente injustificados como la activación de la cámara o del micrófono sin que existiese aparentemente una funcionalidad para la que fueran necesarios.

Por su parte, **Singh et al. (2016)**, tras evaluar las 137 *apps de salud* mejor valoradas por los usuarios en App Store y Google Play, determinaron que sólo dos tercios tenían una política de privacidad en la que se explicaba cómo se protegen o utilizan los datos proporcionados así como que únicamente el 60% de las *apps* utilizaban métodos seguros para compartir la información. Datos significativamente algo mejores que los estudios anteriores pero igual de alarmantes al haberse procedido a una selección de *apps* con supuesta calidad.

Y en la investigación de **Future of Privacy Forum**, asociación corporativamente apoyada por algunas de las mayores empresas tecnológicas del mundo, también se

detectaron que únicamente el 66% de las *apps* diseñadas para mejorar los patrones de sueño y un 80% de las destinadas a ayudar a las mujeres al seguimiento de sus ciclos de fertilidad tenían algún tipo de política de privacidad. Unos resultados que, si bien seguían una clara tendencia al alza respecto a similares estudios llevados a cabo por la misma asociación en años anteriores, seguían siendo igual de "inesperados y preocupantes" (FPF, 2016).

Con los resultados de estos estudios **se puede concluir que todavía las *apps de salud* no son particularmente seguras cuando se trata de proteger la privacidad de los usuarios**, quedando patentes una serie de graves problemas y deficiencias entre los que destacan:

a) La ausencia de información transparente a los usuarios

Como se ha visto en la revisión de la literatura científica, muchas aplicaciones carecen de política de privacidad o, si la tienen, no informan adecuadamente a los usuarios sobre el tipo de datos personales que van a procesarse, ni los fines por los que se recogen ni otros aspectos fundamentales que impiden al usuario ejercer el principio fundamental (que, seguidamente analizaremos) de otorgar su consentimiento de forma "libre, informada, específica e inequívoca".

Curiosamente en otras ocasiones, esta ausencia de información o la insuficiencia de la misma choca frontalmente con la circunstancia contrapuesta por la que los usuarios quedan desbordados con extensos, farragosos y complejos textos con condiciones plagadas de términos técnicos y jurídicos poco amigables para el usuario "de a pie" que, además, se presentan bajo un inadecuado diseño tipográfico sin cumplir los principios mínimos de accesibilidad y usabilidad o ni siquiera estar preparadas adecuadamente para el dispositivo que se está utilizando. Todo esto provoca que se otorguen los consentimientos sin haber leído las políticas (o, al menos, con la exhaustividad que se debiera) consiguiendo así la legitimación precisa para llevar a cabo prácticas éticamente dudosas como pueda ser la cesión retribuida de datos personales a terceros incluidos anunciantes, compañías aseguradoras y farmacéuticas (Armstrong, 2016).

Bien sea por haber "caído" en una estrategia premeditada del editor de la *app*, o por desconocimiento, mala costumbre o, simplemente, por las prisas de acceder cuanto antes a la *app* o servicio en cuestión sin importarles lo que puedan hacer con sus datos personales (seguramente, porque no se valoran) el hecho es que, según la encuesta del INE de 2016, solamente uno de cada tres usuarios españoles leen las políticas de privacidad antes de proporcionar información personal. Cifras que aún son peores según el Barómetro de febrero de 2017 del CIS, donde se apunta que solo el 14,6% de los usuarios que habitualmente utilizan páginas web o aplicaciones móviles leen con asiduidad las políticas de privacidad, alcanzando el 34,6% los que nunca las leen.

b) La maximización de los datos y multiplicidad de finalidades

La ausencia de información transparente ofrecida al usuario repercute en que éste no pueda conocer claramente qué datos personales realmente se están recogiendo, ni qué usos se les darán a los mismos ni por quiénes.

Es práctica habitual que los desarrolladores de aplicaciones de salud (hasta el 72%, según el informe de Research2guidance anteriormente citado) implementen en sus *apps*

herramientas que les permita analizar el comportamiento de los usuarios en la misma, su grado de fidelización así como conocer sus respuestas ante determinadas notificaciones, con objeto de medir el rendimiento de la *app* y poder ofrecer, llegado el caso, nuevas actualizaciones con interfaces y funcionalidades mejoradas. Pero también es recurrente su utilización para la llamada *publicidad comportamental* que estudia esos hábitos para desarrollar un perfil y ofrecer anuncios dirigidos y personalizados, por lo que muchos datos personales son recogidos sin ser totalmente necesarios para el funcionamiento previsto de la *app*, terminando ingentes cantidades de datos en manos distintas a la del propio desarrollador de la *app*, tales como redes publicitarias y empresas de análisis y medición.

El intercambio de datos también se puede producir con terceros a través del uso de APIs pudiendo también algunas de ellas "proporcionar información sobre el propio dispositivo mediante uno o varios identificadores únicos e información sobre otras aplicaciones instaladas", por lo que estas fuentes de datos "pueden ser objeto de un tratamiento adicional, normalmente para generar ingresos, de manera desconocida o no deseada por el usuario final" (WP202).

El que los desarrolladores incorporen en sus *apps* determinadas funcionalidades mediante el uso de los sensores y recursos del dispositivo, también deriva en un abuso sistemático en cuanto a los permisos que el usuario debe otorgar para poder utilizar la aplicación. Y es que, si bien es cierto que para garantizar su funcionamiento, las *apps* requieren que le sean otorgados permisos que le permitan acceder a determinados recursos básicos del dispositivo o interactuar con el hardware del mismo (lo que Google bautiza para su sistema Android como *permisos normales*, con un riesgo mínimo para la privacidad del usuario o el funcionamiento de otras *apps*, cubriendo acciones como, por ejemplo, el acceso a internet, la creación de iconos, conexión *Bluetooth* o el establecimiento del huso horario) es habitual encontrarse con *apps* que requieren ciertos permisos que "abarcan áreas en las cuales la *app* requiere datos o recursos que incluyen información privada del usuario, o bien que podrían afectar a los datos almacenados del usuario o el funcionamiento de otras *apps*", los llamados *permisos riesgosos* entre los que se encuentran el acceso a calendario, cámara, contactos, localización, micrófono, teléfono, sensores, SMS y almacenamiento externo[7].

Hasta la aparición de Android *6*, el régimen de permisos estaba limitado al "todo o nada" (en vez de en tiempo de ejecución, que posteriormente se comentará como "buena práctica") por lo que el usuario, si quería utilizar la *app*, debía otorgar todos los permisos de una única vez en la instalación. Tal como afirma **Panda Security (2015)**, estos permisos en muchos casos no responden a una necesidad real "sino que sirven para crear un entorno publicitario que se adapte a la ubicación y los intereses del usuario. De ahí que una linterna quiera acceder al GPS o un lector de códigos QR pida permisos para consultar tu historial de navegación y tus marcadores web".

También el crecimiento y la expansión global de la *Internet de las cosas*, manifestada en el contexto de la salud a través de la interconectividad de las *apps* con ordenadores corporales (objetos y prendas de ropa cotidianos, como relojes y gafas, provistas de sensores) y otros *wearables* orientados al fenómeno del *yo cuantificado* [8] con el que se

[7] https://developer.android.com/guide/topics/security/permissions.html#normal-dangerous

[8] Modo en el que ha quedado traducido el término *Quantified Self* acuñado en el año 2007 por Gary Wolf y Kevin Kelly para denominar al fenómeno de recoger series de datos cuantitativos procedentes de la monitorización del propio cuerpo o del comportamiento y actividades realizadas por uno mismo.

cuantifican cada una de las actividades que se realizan a lo largo del día o monitorizar una serie de parámetros como la presión arterial o la glucosa en sangre, supone "un reto en cuanto a los tipos de datos recogidos que están relacionados con la salud, y por tanto pueden ser sensibles, así como respecto de su recogida extensiva" (WP223). El GT29 advierte en dicho dictamen que, aunque "el usuario se sienta cómodo compartiendo la información original para un fin determinado, es posible que no quiera compartir esa información secundaria que se podría utilizar con fines totalmente diferentes" perdiendo así el control de la difusión de sus datos y dando lugar a la detección detallada de sus pautas de vida y comportamiento.

El problema de que gigantescas cantidades de datos vayan a parar a otra serie de terceras partes con fines indeterminados, distintos a los inicialmente previstos e informados al usuario y, en cualquier caso, lejanos a los meramente estadísticos o de investigación científica e histórica previstos legalmente, se ve potenciado por el avance tecnológico en el análisis de los mismos mediante el uso de algoritmos, lo que viene a denominarse la ciencia de los macrodatos o, más comúnmente por su voz inglesa, *big data*.

El *big data* permite analizar diversidad de tipos de datos (estructurados, semiestructurados o no estructurados) procedentes de diferentes fuentes a una gran velocidad y en un corto intervalo de tiempo (incluso en tiempo real) revelándose también como una herramienta eficaz y útil para la toma de decisiones e, incluso, para la realización de predicciones dando paso, en el ámbito de la salud y la atención sanitaria, a la bautizada como *Medicina 4P*[9]: personalizada, predictiva, preventiva y participativa.

Sin embargo, como concluía la 36ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Mauricio en 2014, el *big data* por su propia esencia puede ser percibido como "un desafío para los principios clave de privacidad, en particular los principios de limitación de la finalidad y la minimización de datos" (ICDPPC, 2014), al basar sus analíticas en el tratamiento posterior con finalidades adicionales a la finalidad original de tal manera que "puede llevar a situaciones en las que la finalidad inicial para la que se recogió el dato quede al menos 'difuminada' una vez el dato es explotado" lo que puede entrañar graves problemas ocasionados por el uso discriminatorio en la generación de perfiles de consumidores (*profiling*) o riesgos de reidentificación de datos en principio anonimizados al combinarlos con datos procedentes de otras fuentes tanto públicas como privadas (AEPD y ISMS Forum Spain, 2017).

c) Las insuficientes y, en muchos casos, deficientes medidas de seguridad

En la compleja arquitectura de las *apps de salud*, las vulnerabilidades en cuanto a la seguridad de la información pueden aparecer en cualquiera de sus capas por lo que unas medidas de seguridad insuficientes o deficientes pueden impedir el garantizar la confidencialidad, integridad y disponibilidad de la información.

Siguiendo la metodología OWASP Top 10 Mobile Risk (analizada más adelante), en 2016 la empresa estadounidense de seguridad móvil Arxan analizó 126 de las *apps* más populares de finanzas y salud, incluyendo aquellas aprobadas por la FDA y el NHS

[9] Más información en http://p4mi.org/p4medicine

británico, descubriendo que todas ellas eran vulnerables, por lo menos, a dos de esos diez principales riesgos, destacando sobremanera el que el 83% carecían de protección suficiente en la capa de transporte en las conexiones con los servidores así como que, nada menos que al 98% de las *apps* les faltaba protección a nivel binario haciéndoles susceptibles de ataques por ingeniería inversa.

Los ciberataques que aprovechan estas y otras vulnerabilidades para sustraer datos de salud están a la orden del día, tal y como confirma el **Informe ITRC** que analizaba el registro estadounidense de brechas de datos sucedidas en el año 2015 (año bautizado como "el año de las fugas de datos") y en donde se señalaba que el sector de la atención médica y de salud sufrió un 35,5% de las violaciones identificadas, afectando a más de cien millones de registros que suponían nada menos que el 66,7% del total de registros afectados[10].

Los datos de salud substraídos son valiosos, llegando a ascender en el mercado negro a 50 veces el valor de los datos de tarjetas de crédito, según se desprende de la investigación plasmada en el informe **The 2014 Bitglass Healthcare Breach Report**, porque la gran parte de los mismos no tienen caducidad, es decir, que mientras un número de tarjeta de crédito o una cuenta bancaria se puede cancelar, esto no se puede hacer con la fecha de nacimiento, los números de identificación o afiliación o las informaciones del historial médico, por lo que dichos datos pueden seguir siendo explotados para perpetrar diversidad de actos delictivos durante mucho tiempo después de que la víctima conozca el incidente. De ahí que **McAfee Labs (2016)** haya llegado más allá y hable sin tapujos de la transformación de la ciberdelincuencia en el sector de la asistencia sanitaria como servicio constatando, no solo que los datos médicos se venden "al por mayor", sino que verdaderamente existe demanda.

Lo que es evidente es que, en el ámbito de las *apps de salud*, las fugas de la información tratada pueden aumentar la probabilidad de ocasionar problemas a los usuarios por la publicación de la misma, tales como vergüenza, daño a la reputación, estigma social o la pérdida de afecto o respeto de los miembros de la comunidad. Además también puede conllevar el robo de identidad y acarrear repercusiones monetarias por fraudes (por ejemplo, facturación de tratamientos no prestados), provocar el encarecimiento o la indisponibilidad de una determinada cobertura de seguro o, incluso, provocar dificultades laborales disminuyendo las posibilidades de promoción o de superar procesos de selección (Dehling et al., 2015). Asimismo, las pérdidas o modificaciones de la información sufridas a consecuencia de errores técnicos o de ataques malintencionados pueden, adicionalmente, afectar gravemente a la calidad de atención sanitaria e incluso, en casos extremos, "pueden tener consecuencias que pongan en peligro la vida" (AMM, 2016).

[10] En el informe de la misma entidad correspondiente al año 2016, el número de registros afectados fue significativamente menor, alcanzado "sólo" los 16 millones si bien esta cifra suponía ya el 43,6% del total (http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf).

2. La normativa en materia de protección de datos aplicable a las *apps de salud*

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental reconocido en la *Carta de Derechos fundamentales de la Unión Europea* (art. 18.1) y por el Tribunal Constitucional ya que "persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado" (STC 292/2000).

El texto de referencia en materia de protección de datos personales y el marco regulador "destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea" lo constituye la *Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (en adelante, la Directiva), siendo adaptada al ordenamiento jurídico español mediante la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal* (en adelante, LOPD) y el *Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* (en adelante, RDLOPD).

Sin embargo, debido a los retos planteados para la protección de datos a causa de la evolución tecnológica y la globalización, se ha requerido, más de veinte años después, un marco más sólido y coherente desarrollándose el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE*.

El Reglamento General de Protección de Datos (en adelante, RGPD) entró en vigor en el mes de mayo de 2016 si bien no será aplicable hasta el 25 de mayo de 2018 cuando definitivamente quedarán derogadas tanto la Directiva como las normas nacionales que la transponen (la citada LOPD y el RDLOPD) las cuales, mientras y hasta entonces, seguirán siendo válidas y aplicables, habiéndose dejado este plazo de dos años para que estados, instituciones, organizaciones y empresas puedan ir preparándose y adaptándose a este nuevo marco regulador.

2.1. Conceptos básicos sobre la normativa de protección de datos personales

Puesto que para la aplicación a las *apps de salud* del citado marco normativo es condición *sine qua non* que éstas traten datos personales convendrá, en primer término, discernir sobre éste y otros conceptos básicos:

a) Dato de carácter personal

Se entiende como dato de carácter personal "cualquier información concerniente a personas físicas identificadas o identificables" (art. 2a de la Directiva).

Esta definición, tal y como manifestara el GT29, está basada en cuatro componentes: "cualquier información", abarcando tanto la información objetiva como la subjetiva, cualquiera que sea su amplitud (comprendiendo la vida privada y familiar así como cualquier tipo de información tanto de la actividad desarrollada como la referida a sus relaciones laborales o a la actividad económica o social) y con independencia del soporte técnico que la contenga; "sobre", referido a una persona concreta; "identificada o identificable", entendiendo como tal "toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social" siempre que dicha identificación no requiera actividades o plazos desproporcionados[11]; y "persona física", requiriendo que los datos personales se refieran a personas vivas excluyendo, por tanto, a las fallecidas. (WP136).

Desde el punto de vista del formato, el RDLOPD enumeraba que los datos personales podían ser "numéricos, alfabéticos, gráficos, fotográficos, acústicos o de cualquier otro tipo" (art. 5). Precisamente la ambigüedad de ese "otro tipo" es la que se ha ido esclareciendo a lo largo de los años a través de jurisprudencias, dictámenes e informes jurídicos emanados por las autoridades competentes en materia de protección de datos tanto en España (la Agencia Española de Protección de Datos, en adelante AEPD) como en Europa (el ya citado GT29) determinándose que datos personales son los que hacen referencia a la localización, direcciones IP tanto fijas como dinámicas, identificadores únicos del dispositivo y del cliente, identidad y número del teléfono, registros de llamadas, SMS y mensajería instantánea, historial de navegación, correo electrónico, credenciales de autenticación para los servicios de la sociedad de la información (en particular los servicios con características sociales), datos biométricos como modelos de reconocimiento facial y huellas dactilares, números de tarjetas de crédito, fotografías, vídeos y cualquiera de los "elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" (art. 4.1 RGPD).

De entre todos estos tipos de datos personales, y debido a que proporcionan una información sobre esferas íntimas del individuo, la Directiva ya establecía una especial protección a los que hacen referencia al "origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad" (art. 8.1) añadiéndose también por el nuevo RGPD "el tratamiento de datos genéticos[12], biométricos[13] dirigidos a identificar de manera unívoca a una persona física" (art. 9.1 RGPD).

[11] Esta condición, como se irá viendo a lo largo del trabajo, ha quedado en entredicho con el avance de la tecnología y el nacimiento del *big data* que incluso posibilita la re-identificación de personas física aun después de haber sometido a los datos a procesos de anonimización al combinar diferentes fuentes.

[12] En el art. 4.13 del RGPD quedan definidos como "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona".

[13] El art. 4.14 del RGPD los define como "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que

Para la normativa española, eran *datos de carácter personal relativos a la salud* "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética" (art. 5.g RDLOPD).

A este respecto cabe señalar el destacado avance propiciado por el RGPD donde, ya en su considerando 35, amplía la definición anteriormente dada añadiendo que se debe incluir "la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

b) Fichero

La Directiva definía fichero como "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica", manteniéndose intacta la definición de este término en el RGPD.

A este respecto, la LOPD hace distinción entre ficheros de titularidad pública y privada quedando definidos como públicos aquellos "de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades públicas" (art. 5.1.m RDLOPD) pudiendo solamente crearse, modificarse o suprimirse mediante disposición general publicada en el Boletín Oficial del Estado o Diario Oficial correspondiente incluyendo los boletines oficiales autonómicos (art. 21.1 LOPD y 52.1 RDLOPD).

Por su parte, los ficheros privados son aquellos "de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica" (art. 5.1.l RDLOPD) posibilitándose la creación de ficheros de titularidad privada cuando resultase necesario para el logro de la actividad u objeto legítimo de la persona, empresa o entidad titular y se respeten las garantías de la LOPD para la protección de las personas (art. 25 LOPD).

---

permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".

Sin embargo, el RGPD no hace esta distinción, y como ya anunciado la propia AEPD[14], hará también que se sustituya la actual obligatoriedad de inscribir o notificar los ficheros a la Agencia (prevista en el art. 18 de la Directiva) "por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas" (cdo. 89 RGPD).

c) Tratamiento

El RGPD, variando ligeramente lo señalado en la Directiva, lo define como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (art. 4.2).

Es relevante, por tanto, diferenciar este concepto del anterior puesto que, mientras que el fichero únicamente permite ordenar y facilitar el acceso y localización de la información, el tratamiento ofrece la posibilidad de explotar los datos, analizarlos, interpretarlos, reelaborarlos, obtener resultados de los mismos e, incluso, con el avance tecnológico, realizar predicciones, elaborar perfiles[15] y tomar decisiones individuales automatizadas basadas en algoritmos.

d) Los sujetos

Como se ha ido señalando, el ecosistema de las *apps de salud* está integrado por múltiples y variados actores que realizan diversidad de tratamientos con los datos personales de las personas físicas que utilizan dichas *apps*: desarrolladores de las aplicaciones, fabricantes de sistemas operativos y dispositivos, tiendas de aplicaciones, autoridades públicas, profesionales sanitarios y otras terceras partes como proveedores de análisis y publicidad.

Para determinar las responsabilidades y obligaciones que la legislación depara para cada una de las partes, es de vital importancia identificar los diferentes tipos de sujetos que ésta prevé, concretándose en la Directiva en tres: responsable del tratamiento, encargado del tratamiento y tercero.

El **responsable del tratamiento** se define como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario" (art. 2.d de la Directiva).

[14] http://www.agpd.es/blog/de-la-inscripcion-de-ficheros-al-registro-de-actividades-ides-idPhp.php

[15] Según define el RGPD, "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física" (art. 4.5).

En un entorno tan globalizado, donde cualquier usuario puede instalar y usar *apps* desarrolladas en cualquier punto del mundo, esta figura es esencial para establecer "quién debe ser responsable del cumplimiento de las normas de protección de datos y la manera en que los interesados pueden ejercer sus derechos en la práctica", sino también "a la hora de determinar la legislación nacional aplicable y para el ejercicio eficaz de las tareas de supervisión conferidas a las autoridades de protección de datos" tal y como señala el GT29 en su Dictamen 1/2010 (WP169).

Y puesto que como es quien determina los fines del tratamiento así como los datos que deban tratarse, la duración de su conservación, el acceso a los mismos, etc., también al responsable del tratamiento le corresponde, como ya emanaba la Directiva, la obligación "de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales" (art. 17.1).

Además, es relevante destacar una última consideración, tal y como indica el GT29, puesto que desde un punto de vista estratégico de la asignación de responsabilidades, "preferentemente debe considerarse responsable del tratamiento [extensible a los otros sujetos previstos] a la empresa o al organismo como tal, antes que a una persona concreta dentro de la empresa o el organismo" (WP136) por lo que no se consideran responsables a aquellas personas físicas que, aunque traten los datos personales, lo hagan en su condición de empleado dentro de una relación laboral mantenida con una persona jurídica que es quién debe asumir la responsabilidad.

En el caso de las *apps de salud*, generalmente el responsable del tratamiento corresponde con el desarrollador, no limitándose este término a los programadores de la misma sino que incluye, como recuerda el GT29, "a los propietarios, es decir, a las empresas y organizaciones que encargan su desarrollo y fijan sus objetivos" (WP202), pudiendo existir varios corresponsables cuando "dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento" (art. 26.1 RGPD).

Cuando el responsable del tratamiento adopta la decisión de delegar parte de las actividades de tratamiento a alguien externo de la organización, éste recibe la denominación de **encargado del tratamiento**, es decir, "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento" (art. 2.e de la Directiva).

Por lo tanto, para poder actuar como encargado del tratamiento tienen que darse dos condiciones básicas: la de ser una entidad jurídica independiente del responsable del tratamiento y la de realizar el tratamiento de datos personales por cuenta de éste (WP136). Y esta vinculación respecto al responsable sólo se puede regir mediante "un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros" donde se plasme "el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable" (art. 28.3 RGPD).

En las *apps de salud*, es relativamente frecuente que se ponga a disposición de los usuarios a equipos de personal sanitario para que les lleven a cabo un seguimiento o

para que puedan atender sus consultas, por lo que estos profesionales autónomos, empresas o instituciones determinadas (siempre que sean independientes del responsable del tratamiento) deberán actuar como encargados del tratamiento.

Aunque el caso más frecuente en el que aparece esta figura se produce con las empresas que ofrecen los servicios *hosting* y *cloud computing* y que necesitan las *apps* para el almacenamiento remoto de datos. Dichos proveedores se configuran como encargado de tratamiento "siempre que la empresa que presta el servicio de alojamiento no pueda en modo alguno decidir sobre el contenido, finalidad y uso del tratamiento y siempre que su actividad no le reporte otro beneficio que el derivado de albergar las bases de datos, sin utilizarlas en modo alguno en su provecho" (AEPD, Informe 0574/2009)

También actuarían como tales aquellas empresas que proporcionasen análisis dentro de la *app*, siempre y cuando también actuasen exclusivamente por encargo del responsable del tratamiento y no procesasen datos para sus propios fines ya que, en ese supuesto caso, se convertirían en nuevos responsables del tratamiento ajustándose al concepto de lo que la Directiva denomina **terceros**, es decir, "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento" (art. 2.f de la Directiva).

Como señala el GT29, la Directiva utiliza el concepto de terceros "de una forma que no es distinta de la forma que habitualmente se utiliza en Derecho civil, donde el tercero suele ser una persona que no es parte de una entidad o acuerdo. En el contexto de la protección de datos, este concepto debería interpretarse como referente a cualquier persona que no tenga legitimidad o autorización específica" (WP136).

De esta manera, en relación con las *apps de salud*, las empresas de publicidad, los proveedores de análisis y todos aquellas que ofrecen distintas infraestructuras con las que los desarrolladores suelen interconectar la *app*, recopilando directamente datos personales o siendo destinatarios[16] de datos cedidos, siempre que realicen tratamientos para sus propios fines en actividades que no estén a cuenta del responsable, deben ser considerados terceros quedando obligados a tener su propia legitimización (es decir, distinta a la del responsable y no derivada de la otorgada a éste) para poder convertirse en nuevos responsables de tratamiento y poder tratar los datos conforme a la legislación. Legitimización que, como se verá próximamente, solamente se podrá obtener a través de los casos previstos por el RGPD o mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado (el consentimiento).

Adicionalmente para estos sujetos, el RGPD ha creado una nueva figura, la de **representante**, definida como la "persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento […] represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento" (art. 4.17).

La designación del mismo es obligatoria para los responsables y encargados de tratamiento que no se encuentren establecidos en la Unión Europea "a menos que el

[16] "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero" (art. 2.g de la Directiva).

tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público" (cdo. 18 RGPD).

2.2. La normativa aplicable en materia de protección de datos a las *apps de salud*

Explicados los principales conceptos, ya se puede proceder al análisis del RGPD para discernir sobre sobre su ámbito de aplicación, determinándose en su artículo 2 que "se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".

Consecuentemente, la normativa en materia de protección de datos es aplicable a cualquiera de los sujetos implicados en la inmensa mayoría de *apps de salud* (con excepción, lógicamente, de la persona física a la que refieren los mismos) puesto que a través de las mismas se procede al registro, almacenamiento, acceso y tratamiento de datos de una persona física, directa o indirectamente, identificada o identificable.

Es decir, como señala el GT29 en su *Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes*, en la medida en que una *app* genera tráfico de datos personales con los responsables del tratamiento de datos ya le es aplicable la legislación con independencia de la naturaleza de éste ("sea una entidad de carácter público o privado, un programador individual o una gran corporación, un responsable del tratamiento de los datos, un encargado del tratamiento de datos o un tercero") y aunque no estuviera establecido en el territorio de la Unión Europea, puesto que utiliza para el tratamiento de datos medios situados en el territorio de cualquiera de los Estados miembros, lo que sucede con las *apps* que se ejecutan en los dispositivos de usuarios residentes en dichos lugares geográficos.

A tenor de estas premisas, el RGPD no resultaría aplicable a las *apps* que ni registran ni generan ni acceden ni comparten desde la misma ningún tipo de dato personal como, por ejemplo, aquellas que se limitan a proporcionar información o recomendaciones basadas en guías de práctica clínica. Únicamente, y en el caso de que el usuario tenga que registrarse en una determinada tienda de aplicaciones para proceder a su descarga, será ésta quien deberá cumplir con la normativa y no el *publicador* de la *app*.

Asimismo, tampoco es aplicable la legislación cuando, pese a tratar datos personales, no se procesen ninguno de ellos para los propios fines del desarrollador ni se permita el acceso a los datos por parte de terceros, resultando también muy limitadas las responsabilidades cuando los datos "no se distribuyen fuera del dispositivo, o si han adoptado las medidas técnicas y organizativas adecuadas para garantizar que los datos se hacen anónimos y se agregan de forma irreversible en el propio dispositivo, antes de extraerlos del mismo" (WP202).

Finalmente, tampoco es aplicable cuando concurran algunas de las excepciones previstas en el citado artículo 2 del RGPD, es decir cuando el tratamiento de los datos personales sea realizado "en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión" o en actividades de los Estados miembros comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de la Unión Europea (referente a las disposiciones específicas sobre la política exterior y de seguridad común) así como cuando sea "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas" o "por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención".

En este sentido, es relevante aclarar que la excepción referida al tratamiento llevado a cabo por una persona física en el ejercicio de actividades exclusivamente personales o domésticas, refiere únicamente a la no aplicación de la legislación en materia de protección de datos a una persona física cuando trate datos de otras personas físicas "en el ejercicio de actividades exclusivamente personales o domésticas y, por tanto, sin conexión alguna con una actividad profesional o comercial" como, por ejemplo, pudiera ser "la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades domésticas". Esto, como indica el considerando nº 18 del RGPD, no exime a quienes "proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas", siempre y cuando lleven a cabo cualquier tipo de tratamiento de datos personales para sus propios fines, pues se indica expresamente "a los responsables o encargados del tratamiento".

La legislación complementaria del ordenamiento jurídico español

A la hora de considerar el tratamiento normativo referente a la protección de datos de carácter personal hay que tener presente que los desarrolladores de *apps de salud* y/o aquellos que sean responsables o encargados de los tratamientos que se lleven a cabo con los datos recabados o manejados a través de la *app*, que lleven a cabo su actividad en España, adicionalmente están sujetos a diferentes leyes de nuestro ordenamiento jurídico, algunas de las cuales completarán y complementarán la citada normativa a través de disposiciones específicas desarrolladas en el ámbito sanitario y de la administración pública, pudiendo llegar a reforzar o incluso hacer variar sustancialmente aspectos concernientes a derechos de los usuarios, plazos de conservación, medidas de seguridad aplicables, etc.

Es el caso, por ejemplo, de la aplicación de la *Ley de Servicios de la Sociedad de la Información y Comercio Electrónico* (LSSICE), que incorpora en nuestro ordenamiento legislativo la Directiva 2000/31/CE del Consejo y del Parlamento Europeo en la que se regulan determinados aspectos jurídicos de los Servicios de la Sociedad de la Información, en particular los relativos al comercio electrónico, por lo que es aplicable si con la *app* se percibe cualquier tipo de ingresos directos (desde el pago por descarga o la venta de productos a través de la misma) o indirectos (por publicidad, patrocinio, etc.), incidiendo en aspectos sobre los términos y condiciones de uso, requerimiento de consentimiento previo.

Cuando la *app* permita el acceso de los ciudadanos a la información y al procedimiento administrativo con las Administraciones Públicas (entendiendo por tales la

"Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas"), lo que puede suceder cuando desde la *app* se posibilitan la tramitación de citas médicas o en los contactos de telemedicina con profesionales de centros sanitarios públicos (por poner solo unos ejemplos), también es aplicable la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.*

De similar manera, cuando los datos tratados por la *app* (los recopilados por la misma o a los que accede) son utilizados en el contexto de una actividad asistencial prestada por centros, servicios y profesionales sanitarios interconectándose con un determinado sistema de información sanitario o integrándose en la Historia Clínica Electrónica, también le son aplicables la *Ley General de Sanidad 14/1986, de 25 de abril*; la *Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de sus derechos y obligaciones en materia de información y documentación clínica* (en sucesivas ocasiones, LBAP) así como las diversas normas en relación con la sanidad dictadas por distintas comunidades autonómicas, algunas de ellas con rango de ley.

En último lugar, cuando una *app* esté destinada por su fabricante "a finalidades específicas de diagnóstico y/o terapia y que intervengan en su buen funcionamiento, destinado por el fabricante a ser utilizado en seres humanos con fines de diagnóstico, prevención, control, tratamiento o alivio de una enfermedad; diagnóstico, control, tratamiento, alivio o compensación de una lesión o de una deficiencia; investigación, sustitución o modificación de la anatomía o de un proceso fisiológico; o regulación de la concepción" deben quedar encuadradas dentro de la definición de *producto sanitario* y, por tanto, también les son aplicables la Directiva 2007/47/CE del Parlamento Europeo incorporada al derecho español mediante el *Real Decreto 1591/2009, de 16 de octubre, por el que se regulan los productos sanitarios*.

2.3. Principios fundamentales estipulados en el RGPD relativos al tratamiento de los datos personales

Determinado el ámbito de aplicación del RGPD, a continuación se analizan los principios fundamentales relativos al tratamiento de los datos personales en torno a los cuales se articula toda la normativa.

Según dispone el artículo 5, los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado; recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; serán exactos y, si fuera necesario, actualizados; serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; y tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

De esta manera, se pueden estipular hasta seis principios fundamentales, la mayoría de los cuales ya estaban previstos en la Directiva y en la LOPD.

1) Lealtad, transparencia y licitud

Cumplir con los principios de lealtad y transparencia supone que los interesados tienen que estar en condiciones de conocer la existencia de los tratamientos debiéndose, por tanto, ofrecer una información precisa y completa respecto a las circunstancias de dicha obtención y, en definitiva, siendo transparentes, entendiéndose este término (tal y como lo define el DRAE) como "claro, evidente, que se comprende sin duda ni ambigüedad", lo que implica no informar de forma ambigua, oscura, indeterminada, imprecisa, general o confusa (Pinedo, 2007) sino de una manera que al interesado le quede "totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que le conciernen, así como la medida en que dichos datos son o serán tratados" (cdo. 39, RGPD).

El RGPD impone que, "en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo en particular cualquier información dirigida específicamente a un niño" y "por escrito o por otros medios, inclusive, si procede, por medios electrónicos" (art. 12), se debe proporcionar a los interesados a los que se soliciten datos personales, "en el momento en que estos se obtengan", la siguiente información:

- la identidad y los datos de contacto del responsable y, en su caso, de su representante;

- los datos de contacto del delegado de protección de datos, en su caso;

- los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

- los intereses legítimos del responsable o de un tercero;

- los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

- la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en su caso, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

- cuando el tratamiento esté basado en la otorgación del consentimiento, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

- el derecho a presentar una reclamación ante una autoridad de control;

- si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

- la existencia de decisiones automatizas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

- y, llegado el caso, si se proyecta el tratamiento ulterior de datos personales para un fin que sea aquel para el que se recogieron, también se debe proporcionar información sobre ese fin con anterioridad a llevarlo a cabo

El deber de información queda conformado como uno de los principales fundamentos jurídicos de la protección de datos personales constituyendo, como señaló la Audiencia Nacional, "un derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos" (SAN 3888/2001).

Y es que, efectivamente, el derecho a ser informado se encuentra estrechamente vinculado con la obligatoriedad de obtener del interesado su consentimiento para cumplir con el principio de licitud, puesto que éste debe darse con conocimiento de causa pues, como señala el Tribunal Constitucional, "sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales 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" (STC 292/2000).

Por consiguiente, la licitud refiere a que los datos personales "deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato" (cdo. 40 RGPD).

El consentimiento se entiende, por tanto, como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". En esta definición, "libre" supone una decisión voluntaria de un individuo en posesión de todas sus facultades, tomada sin ningún tipo de coacción; "específico" refiere a una situación bien definida y concreta en que esté previsto el tratamiento de datos; "informado", como se decía, supone un consentimiento basado en la apreciación y comprensión de los hechos y consecuencias de una acción; y "explícito", porque el interesado debe ser consciente, dejando constancia de ello mediante una acción demostrable, no que acepta la protección sino que renuncia a ella.

En el caso concreto de los datos relativos a la salud, como aquellos otros que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, […] o datos relativos a la vida

sexual o las orientación sexuales de una persona física" queda prohibido su tratamiento salvo si el interesado otorga su consentimiento explícito o concurren algunas de las excepciones contempladas en el art. 9.2 del RGPD y que en este ámbito podrían ser:

- el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social;

- el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

- el tratamiento es necesario por razones de un interés público esencial;

- el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social;

- el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, y siempre teniendo particularmente presente el secreto profesional;

- el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, disponiéndose en tal caso de medidas técnicas y organizativas y respetando el principio de minimización de los datos personales.

2) Limitación de la finalidad

El segundo de los principios obliga a que los datos deben ser "recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines".

El GT29, en una extensa y clarificadora opinión sobre este principio, señala que la "limitación de la finalidad" constituye en sí misma un pre-requisito para el cumplimiento de otros principios contemplados en la normativa, tales como la calidad de los datos, la adecuación, la pertinencia, la proporcionalidad o la precisión de los datos recogidos junto con las reglas que rodean los periodos de retención (WP203).

Además, en el mismo documento explica los conceptos fundamentales de este principio considerando que "determinado" (o específico, como se dice que debe ser el consentimiento) referido a los propósitos requiere que antes (o como mucho, en el mismo momento) que se produzca la recogida de los datos personales, se deben establecer con precisión los fines, debiendo identificar claramente qué tratamientos están o no están incluidos dentro del propósito, de tal manera que pueda ser evaluado y aplicar las medidas y salvaguardias pertinentes; que "explícito", refiere que los objetivos deben ser revelados de forma que sean explicados y expresados claramente para que "todo el mundo" (con independencia de cualquier diversidad cultural o

lingüística) pueda comprender inequívocamente los efectos del procesamiento; y que "legítimo", interpela al requisito de disponer de un terreno legal para el procesamiento.

El otro aspecto fundamental del principio es el de la compatibilidad de los tratamientos ulteriores con los fines "determinados, explícitos y legítimos".

Los usos secundarios son especialmente relevantes en el ámbito de la salud "donde tienen una importante virtualidad para la mejora de la calidad de los servicios, en la investigación médica, en la planificación y administración sanitaria y en salud pública, entre otras muchas posibilidades" (Barbará i Fondevila, 2014) motivos por los cuales, el RGPD considera que no son incompatibles con los fines iniciales los tratamientos ulteriores de los datos personales con "fines de archivo en interés público, fines de investigación científica e histórico o fines estadísticos".

La minería de datos y el *big data* abren nuevas puertas a la explotación de los datos y no solo por su potencialidad sino también porque permite aprovechar los datos evitando los costes e inconvenientes de tener que volver a recabar la misma información. Sin embargo, la reutilización o los usos secundarios de los datos y las vinculaciones o combinaciones con diversas fuentes, pese a implicar nuevas oportunidades, pueden cambiar el contexto o la finalidad original al conllevar que los datos lleguen a adquirir sentidos y significados diferentes (Goodman, 2015) siendo este el motivo por el que, evidentemente, deba procederse a proporcionar nueva información a los interesados debiéndose asegurarse el responsable del tratamiento de la legitimidad (para lo cual, en muchos casos, deberá obtener un consentimiento del interesado para el nuevo fin).

3) Minimización de Datos

Este principio, claramente unido al anterior, hace referencia a que los datos personales deben ser "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados".

Como ya ha expresado el GT29, en el entorno de la *mHeatlh* en combinación con la *IO* y el *big data*, el principio es especialmente relevante dado que frecuentemente se da una recogida masiva de datos que no suelen se pertinentes para la finalidad del tratamiento. Sin embargo, no se deben recoger datos excesivos ni aquellos que sean innecesarios para la prestación del servicio determinado (WP221), es decir, no cabe de modo alguno el recoger datos "por si acaso" o "porque pueden ser útiles más adelante" y, si se llegase a hacer, como mínimo habrá que "ofrecer al interesado la posibilidad de usar el servicio de manera anónima" (WP223).

En oposición a este principio, muchos responsables de los tratamientos consideran que el mismo pone límites a las oportunidades potenciales de la tecnología conformándose en barrera a la innovación avalando la "idea de que los posibles beneficios del tratamiento de los datos se obtendrán mediante un análisis exploratorio con el que se buscarán correlaciones y tendencias que no sean obvias" (WP223).

Esta adquisición masiva de datos que, a la hora de la verdad y en el momento actual, no son usados para lograr conocimientos o para tomar decisiones, ya ha sido definida bajo el término de *Dark Data*. Para la consultora Gartner, estos "datos oscuros" serían todas aquellas informaciones que las organizaciones recogen, procesan y almacenan pero que normalmente no son de utilidad para ningún propósito, llegando a producirse por una

falta de análisis sobre lo que realmente se precisa recoger para una finalidad concreta (maximizándose los datos recogidos sin fundamento), por la naturaleza perecedera de la misma (datos que pierden su valor al poco de ser registrados, como los cientos de miles de datos en bruto que se pueden capturar con dispositivos wearables y que solamente pueden tener interés y significado cuando se presentan como "datos agregados") y datos recogidos sin estructurar, que son difícilmente procesables, explotables y ni siquiera interconectables con otros datos. Además, también habría que unir todos aquellos datos que se encuentran retenidos, principalmente por motivos de regulación legal (García Meixa, 2014).

En el ámbito de la salud, se suele ser proclive al exceso de información en pro de una futura e hipotética mejor atención sanitaria del paciente, de la salud pública y de la epidemiología. Sin embargo, el principio de minimización debe tenerse presente en el tratamiento ulterior de los datos personales aún con fines de "archivo en interés público, fines de investigación científica, histórica o fines estadísticos" (cdo. 156 RGPD) debiendo poner medidas como la seudonimización (que posteriormente se comentará).

4) Exactitud

Los datos deben ser "exactos y, si fuera necesario, actualizados", debiéndose adoptar "todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan".

Como señalaba el Tribunal Supremo, la normativa de protección de datos "descansa en principios de prudencia, ponderación y sobre todo, de veracidad, de modo que los datos objeto de tratamiento deben ser auténticos, exactos, veraces y deben estar siempre actualizados, y por ello el interesado tiene derecho a ser informado de los mismos y a obtener la oportuna rectificación o cancelación en caso de error o inexactitud" (STS 13/2013).

Los datos han de ser exactos y puestos al día, para responder, por tanto, con veracidad a la situación actual del interesado, por lo que la observancia de este principio responde a la necesidad por parte del responsable del tratamiento de tratar datos que revelen la situación presente y cierta del interesado de modo que no se transformen en información inservible por su falsedad o por su inexactitud. Causas ambas que podrían deslegitimar la recogida de los mismos además de poder llegar a provocar un perjuicio para el propio interesado (Rebollo y Serrano, 2008), por lo que se deben tomar todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos.

Esto todavía cobra mayor relevancia cuando se tratan datos de salud y, por ello, en la LBAP se obliga a los pacientes o usuarios al "deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria" (art. 2.5) exigiendo igualmente que en la "historia clínica consten todos aquellos datos que permitan el conocimiento veraz y actualizado del estado de salud del paciente" (art. 15.2).

5) Limitación del plazo de conservación

Los datos también deben ser "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales".

Esto implica que, como señala el cdo. 39 del RGPD, el responsable del tratamiento ha de ser quien establezca los plazos para su supresión o revisión periódica, si bien esta condición queda supeditada tanto a la determinación del tiempo de duración del tratamiento (que en el caso de una *app* puede ser todo aquel transcurrido entre la instalación y su desinstalación –con los matices que se explicarán más adelante–) y por el plazo de conservación estipulado para la defensa de reclamaciones (incluyendo las limitaciones que otras leyes del ordenamiento jurídico español puedan imponer).

En cualquier caso, hay que tener presente que esta limitación es aplicable únicamente a los datos personales que se conserven de una forma que permita la identificación de los interesados, por lo que el almacenamiento lícito por tiempo indefinido puede conseguirse mediante la anonimización o la seudoanonimización. En caso contrario, únicamente podrán conservarse durante periodos más prolongados en el tiempo aquellos datos personales que fueran a ser tratados "con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos" sin que ello suponga perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el RGPD a fin de proteger los derechos y libertades del interesado.

6) Integridad y Confidencialidad

Finalmente, el RGPD estipula que los datos personales serán "tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".

La integridad y la confidencialidad son, junto a la disponibilidad, los tres pilares fundamentales de la seguridad de la información.

Según ISO 27001, la integridad "es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada". Sin embargo no puede ser esta la única definición válida en el contexto de la protección de datos. Gelbstein (2011) señalaba que de los tres citados dominios de la seguridad de la información, la noción de integridad es quizás el más complejo precisamente "porque se trata de un concepto que puede tener distintas interpretaciones".

Y tal es así que daba diferentes definiciones dependiendo del rol de quién lo describiera. Así encontraba que, para un encargado de seguridad, la integridad de los datos podría definirse como "como la imposibilidad de que alguien modifique datos sin ser descubierto" por lo que desde la perspectiva de la seguridad de datos y redes era "la garantía de que nadie pueda acceder a la información ni modificarla sin contar con la autorización necesaria" concluyendo que "no solo alude a la integridad de los sistemas (protección mediante antivirus, ciclos de vida del desarrollo de sistemas estructurados, revisión de códigos fuente por expertos, pruebas exhaustivas), sino también a la integridad personal (responsabilidad, confianza, fiabilidad, etc.)".

Desde el punto de vista de un administrador de bases de datos, la integridad de los datos podía depender de que los datos registrados fuesen "precisos, válidos y coherentes", debiendo "analizar la integridad de las entidades, la integridad de los dominios y la integridad referencial". Para un arquitecto o modelador de datos, podría estar relacionada con el "mantenimiento de entidades primarias únicas y no nulas" refiriendo también a la ausencia de duplicados en el conjunto de datos y por la presencia de una clave que permita acceder de forma exclusiva a cada una de las entidades del conjunto. Y para un proveedor, la integridad está referida a la "exactitud y coherencia de los datos almacenados, evidenciada por la ausencia de datos alterados entre dos actualizaciones de un mismo registro", debiéndose establecer en la etapa del diseño y manteniéndose con el uso de rutinas de validación y verificación de errores.

Por su parte, la confidencialidad admite menos interpretaciones, pudiendo ser totalmente aplicable la definición dada por ISO 27001 como "la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados".

El deber de confidencialidad obliga no sólo al responsable del tratamiento sino a todos aquellos que intervengan en cualquier fase del tratamiento quedando, por tanto, estrechamente relacionado con el deber de secreto. Como señala la jurisprudencia de la AEPD en diversidad de ocasiones, este "deber de secreto comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido, teniendo el deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo" siendo este deber una "exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática" por lo que comporta "que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto".

El RGPD exige al responsable del tratamiento el garantizar la confidencialidad (así como los otros aspectos de la seguridad de la información) debiendo desarrollar la capacidad de resistir acontecimientos accidentales, acciones ilícitas o malintencionadas que comprometan los datos personales conservados o transmitidos, debiendo ir más allá puesto que también se debe garantizar la seguridad de las infraestructuras y de los servicios conexos ofrecidos a través de los sistemas de información y redes como, por ejemplo, el "impedir el acceso no autorizado a las redes de comunicación electrónicas y la distribución malintencionada de códigos, y frenar ataques de denegación de servicio y daños a los sistemas informáticos y de comunicaciones electrónicas" (cdo. 49).

No basta, pues, con solucionar los problemas sino, que como ahora se comentará al hablar sobre la responsabilidad proactiva, se deben "evaluar los riesgos inherentes al tratamiento" y, en consecuencia, aplicar la medidas para mitigarlos "que garanticen un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse" (cdo. 83).

2.4. La responsabilidad proactiva

La mayor innovación del RGPD con respecto a la anterior Directiva es la inclusión de este principio por el cual el responsable del tratamiento tiene que garantizar el cumplimiento de los principios anteriormente citados debiendo ser capaz de demostrarlo (art. 5.2).

Sin embargo, hay que señalar que este principio no es ni mucho menos nuevo ya que, como sucede con los otros principios, ya fue previsto en 1980 por la Organización de Cooperación y Desarrollo Económico (OCDE) en sus *Directrices relativas a la protección de la Intimidad y de la Circulación Transfronteriza de datos personales*, instando a todo responsable de datos "a ser responsable de cumplir con las medidas que hagan efectivos los principios expuestos [de limitación de la recogida, de calidad de los datos, de especificación de la finalidad, de limitación de uso, de salvaguardas de seguridad, de apertura, de participación individual]".

Es decir, que ya no basta sólo que el responsable del tratamiento no incumpla la normativa sino que existe la necesidad de que adopte las medidas adecuadas y eficaces para aplicar los principios de protección de datos y, además, debe demostrar que así lo hecho aportando pruebas fehacientes.

De este modo, aparece en el RGPD el concepto *accountability*, un término anglosajón complejo que en su uso cotidiano significa "responsabilidad" pudiendo ser traducido, como señala Fundéu BBVA, "por sistema o política de rendición de cuentas o, simplemente, por rendición de cuenta"[17]. De un modo general, señalaba el GT29 en su *Dictamen 3/2010 sobre el principio de responsabilidad*, que el término "apunta sobre todo al modo en que se ejercen las competencias y al modo en que esto puede comprobarse" puesto que "competencia y responsabilidad son dos caras de la misma moneda y sendos elementos esenciales de la gobernanza" y solamente "cuando la responsabilidad funciona en la práctica puede desarrollarse la confianza suficiente".

Más recientemente, ISMS Forum Spain y la AEPD (2017) han señalado que "la *accountability* constituye una filosofía que implica la procedencia de dar cumplimiento al régimen jurídico y las obligaciones derivadas de la protección de datos de carácter personal, con independencia de que exista una norma concreta de carácter imperativo que así lo exija" y que, por ello, las organizaciones se ven obligadas "a implicar a los grupos de interés para identificar, comprender y responder a los temas y preocupaciones existentes en este ámbito, a los efectos de poder garantizar adecuadamente la sostenibilidad jurídica y social de los tratamientos de datos, informando, explicando y dando repuesta al efecto al regulador, a los ciudadanos como titulares de los datos, y a la sociedad en general acerca de las decisiones, las acciones y el desempeño".

Para tratar de concretar materialmente este principio en medidas comunes de responsabilidad, el GT29 en el citado WP173 se incluyó la siguiente lista no exhaustiva:

1. Establecimiento de procedimientos internos previos a la creación de nuevas operaciones de tratamiento de datos personales (revisión interna, evaluación).

[17] http://www.fundeu.es/recomendacion/rendicionde-cuentas-y-norendimientomejor-que-accountability-1470/

2. Establecimiento de políticas escritas y vinculantes de protección de datos que se tengan en cuenta y se valoren en nuevas operaciones de tratamiento de datos (por ejemplo, el cumplimiento de los criterios de calidad de datos, notificación, principios de seguridad, acceso, etc.) que deben ponerse a disposición de las personas interesadas.

3. Cartografía de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de operaciones de tratamiento de datos.

4. Nombramiento de un funcionario (delegado) de protección de datos y otras personas responsables de la protección de datos.

5. Oferta adecuada de protección de datos y formación a los miembros del personal, debiendo incluir a los procesadores (o responsables del proceso) de datos personales (como los directores de recursos humanos) pero también a los administradores de tecnologías de la información, desarrolladores y directores de unidades comerciales.

6. Establecimiento de procedimientos de gestión del acceso y de las demandas de corrección y eliminación de datos con transparencia para las personas interesadas.

7. Establecimiento de un mecanismo interno de tratamiento de quejas.

8. Establecimiento de procedimientos internos de gestión y notificación eficaces de fallos de seguridad.

9. Realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas.

10. Aplicación y supervisión de procedimientos de verificación que garanticen que las medidas no sean solo nominales sino que se apliquen y funcionen en la práctica (auditorías internas o externas, etc.).

2.5. La privacidad desde el diseño y por defecto

La otra gran incorporación que hace el RGPD es la de considerar que el responsable del tratamiento "debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto" (cdo. 78).

El RGPD introduce, por tanto, la *privacidad desde el diseño*, un concepto que al igual que *accountability* (con el que se encuentra estrechamente relacionado) tampoco es novedoso pues fue ideado a principios de la década de los años noventa del siglo pasado, recibiendo su espaldarazo definitivo a raíz de la 32ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Jerusalén en octubre de 2010 en donde se adoptó una resolución por la cual se reconocía como un componente esencial y fundamental para la protección de la privacidad, se alentaba a adoptar sus principios fundamentales como guía para establecer la privacidad como modo de funcionamiento predeterminado y se invitaba a los comisionados y autoridades

de protección de datos de todo el mundo a promover y fomentar su implementación, a formular políticas basadas en el mismo, a promover la investigación sobre este tema e, incluso, a darlo a conocer públicamente (ICDPPC, 2010).

Concebido por Ann Cavoukian, comisionada de Información y Privacidad de Ontario, con el fin de promover que la privacidad no solamente pueda ser garantizada mediante el cumplimiento de los marcos regulatorios sino convirtiéndola "en el modo de operación predeterminado de una organización". Y aunque originalmente surgiría como desarrollo de las tecnologías de protección de la intimidad (conocidas por sus siglas en inglés, PET) finalmente acabaría evolucionando a una trilogía que engloba los sistemas TIC, las prácticas de negocio responsables y el diseño físico e infraestructura en red.

Tal y como explica su propia autora, *Privacy by Design* (también conocido por sus siglas en inglés, PbD) está basado en los siguientes siete principios fundamentales:

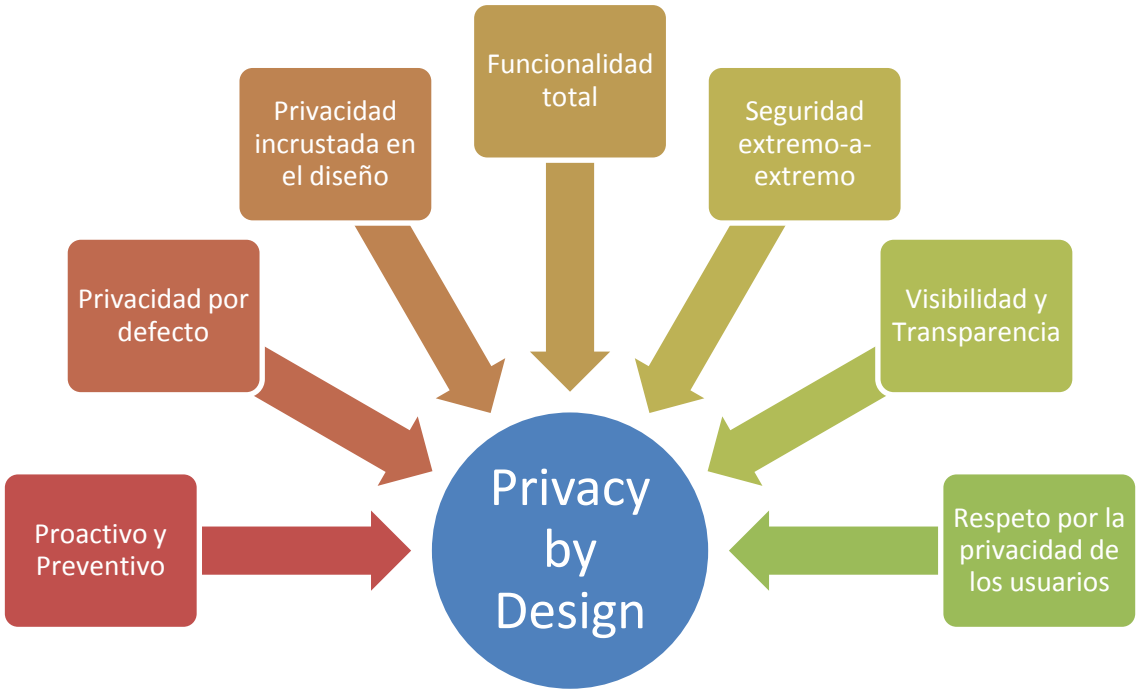

Ilustración 3: Los siete principios promovidos por Ann Cavoukian que llevan al *Privacy by Design*

1. Proactivo, no reactivo; preventivo, no correctivo.
El enfoque de PbD se caracteriza por la adopción de medidas proactivas, es decir, por anticipar y prevenir los riesgos y no esperar a que estos se materialicen en impactos para actuar entonces.

2. Privacidad como la configuración predeterminada.
PbD busca entregar el máximo grado de privacidad por defecto y de forma automática, tratando de que la privacidad se mantenga intacta sin que la persona implicada tenga que realizar ninguna acción.

3. Privacidad incrustada en el diseño.
La privacidad no puede ser un elemento suplementario al proceso de diseño y desarrollo de la arquitectura de los sistemas TIC, sino que se convierte en componente esencial integrándose en el sistema sin que por ello disminuya la funcionalidad.

4. Funcionalidad total.
PbD busca evitar dicotomías innecesarias y equilibrar los intereses y objetivos legítimos de las partes, de modo que "todos ganen" y, por tanto, huyendo del "si alguien gana es porque el otro pierde". Privacidad y seguridad no pueden estar contrapuestas sino que es posible tener ambas al mismo tiempo.

5. Seguridad extremo a extremo.
PbD se extiende, con seguridad y sin demoras, a través del ciclo de vida completo de los datos, desde antes de su recogida pasando por las fases de tratamiento y hasta su definitiva destrucción.

6. Visibilidad y transparencia.
PbD busca asegurar que toda la tecnología involucrada y las acciones que sean precisas para el tratamiento de los datos personales estén estructuradas y funcionando en conformidad con la información y los fines declarados, permaneciendo visibles y transparentes a los usuarios.

7. Respeto por la privacidad de los usuarios.
Se debe mantener el enfoque centrado, por encima de todo, en el usuario, situando a éste en el centro de las prioridades a la hora de diseñar y configurar los sistemas. De esta manera, se deben contemplar medidas tales como configuraciones predeterminadas, y sistemas apropiados de notificación así como promover la usabilidad para un manejo sencillo y amigable.

3. Difusión de buenas prácticas para desarrolladores de *apps de salud*

Los preocupantes datos proporcionados anteriormente no hacen más que confirmar lo que ya fue expresado en 2013 en la denominada *Declaración de Varsovia sobre la "appificación" de la sociedad*, y es que los creadores de aplicaciones "no son conscientes de las implicaciones de privacidad de su trabajo" por lo que aun siendo "los conductores del crecimiento de la economía digital y aportan facilidad en nuestro día a día, al mismo tiempo, tienen que garantizar el cumplimiento de la normativa sobre privacidad y protección de datos de todo el mundo" (ICDPPC, 2013).

Con el fin de contribuir a concienciar a desarrolladores y responsables de tratamiento de la importancia de cumplir la normativa en materia de protección de datos, a continuación se tratan de transmitir una serie de buenas prácticas y aspectos significativos del modo adecuado de hacerlo partiendo del análisis normativo previamente comentado y desde la revisión de directrices y recomendaciones emanadas por las autoridades competentes en esta materia, tratando de aplicar los principios anteriormente presentados *accountability* y *Privacy by Design*.

3.1 Tener presente la privacidad y el cumplimiento de los requerimientos de la normativa de protección de datos desde la propia conceptualización de la *app*

La adopción de los principios de la privacidad desde el diseño, implica desde que surge la idea el tener presente la protección de la privacidad de los que van a ser los usuarios de la *app* y el cumplimiento normativo en materia de protección de datos. Aspectos, ambos que los desarrolladores no deben ver como una carga administrativa impuesta para "complicarles la vida" sino como oportunidad para mejorar la calidad de su producto, de ser más competitivo en el mercado y de satisfacer a sus clientes que, al fin y al cabo, son el centro de su actividad.

De esta manera, ya no basta solamente con tener claro qué es lo que se quiere que haga la *app* o a quién está dirigida sino que se debe colocar al usuario en el centro, analizar los riesgos que puedan existir al tratar datos personales para poder implementar las medidas acordes y, por ende, cumplir la normativa de protección de datos.

Para iniciar "con buen pie" este proceso se deben observar para con la autoridad competente una serie de obligaciones (como la ya comentada designación de un representante en caso de que el responsable del tratamiento no se encuentre establecido en la Unión Europea) y otras totalmente nuevas que, seguidamente, se comentarán.

Teniendo presente que, en un ámbito como la *mHealth* todo se encuentra magnificado y globalizado siendo muy probable que se traten grandes cantidades de datos personales correspondientes a un también elevado número de personas (pues eso se desea, que la *app* tenga éxito y que sean muchos los usuarios que la descarguen y le den uso), antes de empezar el diseño de la *app* se debe llevar a cabo un exhaustivo análisis con el fin de determinar las categorías de los datos personales a tratar, identificar los responsables y encargos, documentar la base legal sobre la que se desarrollan los tratamientos.

Las *apps de salud*, precisamente son llamadas así porque, generalmente, van a tratar datos relacionados con la salud, excepto en casos muy concretos donde (aunque bajo esta temática) se ofrezcan informaciones sobre ciertas enfermedades (siendo incluso muy probable que no sea preciso registrar ningún dato personal y, por tanto, no le sea aplicable el RGPD) o para realizar gestiones administrativas (donde se recabarán datos personales pero no de naturaleza sensible en la mayoría de casos).

Datos personales, que como ya se ha indicado, están categorizados como especiales. A este respecto, hay que considerar que en el entorno del *yo cuantificado* si bien se registran datos en bruto o, en su mayor parte datos, relacionados con el bienestar de la persona no tratándose siempre de datos relativos a la salud, pueden cambiar rápidamente a este tipo de datos especialmente protegidos cuando, medidos a lo largo del tiempo y en combinación con la edad y el peso, pueden "utilizarse para determinar un aspecto significativo de la salud de un individuo, como los riesgos para la salud relacionados con la obesidad o una enfermedad que causa una pérdida significativa de peso" (Unión Europea, 2015).

Proceder a la exhaustiva selección de los encargados de tratamiento, estableciendo una relación contractual con los que se consideren más adecuados.

Como se especificaba en páginas anteriores, en las *apps de salud* es frecuente que actúen otros sujetos que serán considerados como encargados del tratamiento estipulando el RGPD que se debe proceder a una adecuada elección de entre aquellos que ofrezcan garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas (art. 28) y obligándose a que la relación deba regirse por un contrato u otro acto jurídico que vincule al encargado respecto al responsable y "establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable".

Para ayudar y facilitar a los responsables del tratamiento a la correcta preparación y redacción del citado contrato, la AEPD conjuntamente con la *Autoritat Catalana de Protecció de Dades* y la *Agencia Vasca de Protección de Datos*, ha preparado unas *Directrices para la elaboración de contratos entre responsables y encargados del tratamiento* que se pueden consultar online[18] y en las que se desglosan los diferentes epígrafes que debe contener e, incluso, un modelo de contrato que se puede seguir para cuando (en el más complejo de los casos) el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas.

La adecuada elección requerida cobra aún mayor relevancia en el caso de los proveedores de servicios *hosting* y *cloud computing* en cuyos servidores se almacenarán

[18] https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf

los datos gestionados por la *app* ya que, como se ha especificado en páginas anteriores, también se constituyen en encargados de tratamiento.

Y es que, a la hora de decantarse por la utilización de un servicio u otro, hay que considerar una serie de condicionantes, siendo quizás el más relevante el que se encuentren preferentemente localizados dentro del Espacio Económico Europeo (EEE) o, a lo sumo, en países que garanticen un nivel adecuado de protección de los datos de carácter personal, determinándose la localización no sólo referida a la sede del proveedor del servicio, sino también a la de cada uno de los recursos físicos que emplea para implementar el servicio.

A estos efectos, cualquier tratamiento de datos que suponga una transmisión de los mismos fuera del territorio del EEE, bien constituya una cesión o comunicación de datos o bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del tratamiento, se considera una transferencia internacional de datos. Y estas transferencias únicamente se puede llevar a cabo si el susodicho país u organización internacional, bajo el criterio de la Comisión Europea, "garantiza un nivel de protección adecuado", no requiriéndose entonces ninguna autorización específica (art. 44.1 RGPD).

En el caso de que el país no cumpla dichas garantías (se puede acceder a un listado actualizado en la web de la AEPD[19]) será necesaria la autorización previa de la Dirección de la Agencia Española de Protección de Datos pudiéndose también establecer la posibilidad de que, en determinadas circunstancias, medie el consentimiento explícito del interesado "si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores" (cdo. 11 RGPD).

De manera especial, por lo la proliferación de servicios tecnológicos que allí se ofrecen, hay que tener presente la situación de Estados Unidos, máxime después de la anulación del llamado *Puerto Seguro* por el Tribunal de Justicia de la Unión Europa y posterior creación del *Escudo de Privacidad* por *Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016* que posibilita que los datos personales puedan ser transferidos a una empresa de dicho país únicamente si dicha empresa procesa (usa, almacena y transfiere posteriormente) los datos personales con arreglo a unas normas de protección y salvaguardias bien definidas acordes, lógicamente, a los principios de protección de datos de la Unión Europea.

Es decir, no se incluyen por defecto la totalidad de empresas del país sino sólo aquellas que se hayan adscrito a este marco, pudiéndose consultar la lista en el sitio web del Departamento de Comercio de Estados Unidos (https://www.privacyshield.gov/list).

Realizar una Evaluación de Impactos sobre la Protección de Datos (EIPD)

Siguiendo el principio *accountability*, el art. 35 del RGPD señala que "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la

[19] https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

protección de datos personales" e impone, como obligatoriedad que sea llevada a cabo en los casos de que se fuera a realizar una "evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar", el "tratamiento a gran escala de las categorías especiales de datos" o la "observación sistemática a gran escala de una zona de acceso público".

Puesto que, las *apps de salud* tratan datos de una categoría especialmente protegida y además lo hacen en un entorno tal que posibilita que puedan ser utilizadas por un número indeterminado de personas, el tratamiento debe considerarse de gran escala y, por tanto, se tiene que proceder a realizar una *Evaluación de Impacto en la Protección de Datos Personales*.

Conocida por sus siglas EIPD, o por el término anglosajón *Privacy Impact Assessment* (PIA), es "una metodología para evaluar el impacto en la privacidad de un proyecto, política, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales y, tras haber consultado con todas las partes implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos. Una evaluación de impacto en la privacidad es un proceso que debería comenzar en las etapas más iniciales que sea posible, cuando todavía hay oportunidades de influir en el resultado del proyecto" (Wright y de Hert, 2012).

Efectivamente, y como también señala la AEPD, el beneficio derivado de la realización de una EIPD en las etapas iniciales del diseño de un nuevo producto, servicio o sistema de información es que permite identificar los posibles riesgos y corregirlos anticipadamente, evitando tener que descubrirlos cuando el sistema ya se encuentra en funcionamiento o, en el peor de los casos, cuando se haya producido una lesión de los derechos de los interesados.

Pero no solo se debe realizar una EIPD en la fase inicial de diseño sino también cuando se vaya a actualizar la *app* incluyéndose nuevas funcionalidades y recogidas de categorías de datos distintos a los inicialmente previstos (por ejemplo, si se van a tratar datos biométricos, de geolocalización, etc., que inicialmente no estaban contemplados); cuando se fueran a incluir nuevos fines de tratamiento (especialmente, si se van a realizar evaluaciones o predicciones de aspectos de los usuarios como su comportamiento, agrupaciones de perfiles o tratamientos de grandes volúmenes a través de *big data*); o cuando se fueran a efectuar cesiones a terceros o fuesen a utilizarse datos no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.

Para facilitar la realización de una EIPD, la AEPD elaboró en el año 2014 (estando, por tanto, expuesta a una revisión tras la aprobación del RGPD), una completa guía en la que analiza cada una de las fases de la que consta y una lista de los principales riesgos con las medidas para afrontarlos.

De forma resumida, las ocho fases principales de un EIPD, son las siguientes:

1. Análisis de necesidad.

Valoración de la conveniencia de llevar a cabo o no una EIPD en función de si van a recabarse datos de carácter personal de una categoría especial, si se van a comunicar a terceros o si se va a utilizar tecnología invasiva para la privacidad.

2. Descripción del proyecto y de los flujos de información.
   Análisis en profundidad del proyecto, obteniendo el detalle de las categorías de los datos que se tratan, los usuarios de los mismos, los flujos de información y las tecnologías utilizadas.

3. Identificación de los riesgos.
   Análisis de los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad de que sucedan y del daño que causarían si se materializaran. También se deben valorar los posibles riesgos que puede sufrir la organización (como la pérdida de reputación o por la imposición de sanciones)

4. Gestión de los riesgos identificados.
   Determinación de los controles y las medidas que han de adoptarse para eliminar, mitigar, transferir o aceptar los riesgos detectados.

5. Análisis de cumplimiento normativo.
   Verificación de que el producto o servicio que se está desarrollando cumple con los requerimientos legales, generales o sectoriales, en materia de protección de datos.

6. Informe final.
   Relación detallada de los riesgos identificados y de las recomendaciones y propuestas para eliminarlos o mitigarlos siendo el destinatario final del mismo, la dirección de la propia organización.

7. Implantación de las recomendaciones.
   Decisión sobre las recomendaciones del informe final y las acciones que deben llevarse a cabo, incluyendo la asignación de los recursos necesarios para su ejecución y la designación del responsable de implantarlas.

8. Revisión y realimentación.
   Análisis del resultado final para comprobar la efectividad de la EIPD y verificar si se han creado nuevos riesgos o se han detectado otros que habían pasado desapercibidos, utilizando los resultados obtenidos para realimentar la evaluación de impacto y actualizarla cuando sea necesario.

Además, durante todo el proceso y para llevar a cabo una correcta identificación de los riesgos, es imprescindible efectuar las consultas apropiadas con todas aquellas partes que pudiesen verse afectadas por el mismo, tanto las internas de la propia organización responsable del tratamiento como las externas.

Designar un delegado de protección de datos.

Según el art. 37 del RGPD, se debe proceder a la designación de un *Delegado de Protección de Datos* cuando el tratamiento lo lleve a cabo una autoridad y organismo público; cuando las actividades principales del responsable consistan en operaciones de tratamiento que por su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala; o cuando las actividades principales del

responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales.

Esta nueva figura, más conocida por sus siglas DPO (del inglés, *Data Protection Officer*), constituye uno de los elementos claves del RGPD y un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, debiendo ser nombrado atendiendo a sus cualidades profesionales y a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y pudiendo formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

Entre las funciones que debe desempeñar, con independencia y tras haberle facilitado todos los recursos necesarios, destacan las de informar y asesorar a los responsables y encargados del tratamiento de datos personales (y a sus empleados) de las obligaciones que tienen derivadas de la normativa; supervisar el cumplimiento de dicha normativa y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; ofrecer el asesoramiento que se le solicite para hacer la evaluación de impacto de un tratamiento de datos personales, cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas, y supervisar luego su aplicación; y cooperar con las "autoridades de control" actuando como su "punto de contacto" ante cualquier consulta sobre el tratamiento de datos personales (especialmente, la citada consulta previa obligatoria en los casos en los que el tratamiento entrañe un alto riesgo).

Acreditar el cumplimiento de los requerimientos del RGPD

Como se señalaba anteriormente, el principio de responsabilidad proactiva obliga a que el responsable del tratamiento demuestre que ha implementado las medidas adecuadas y eficaces para aplicar los principios de protección de datos.

La LOPD, de alguna manera ya imponía una serie de requisitos (o formalidades, que decían algunas voces) al responsable del tratamiento debiendo, entre otros aspectos, proceder a la inscripción de los ficheros a la AEPD, elaborar un documento de seguridad permanentemente actualizado o realizar auditorías periódicas para verificar la correcta implantación de las medidas de seguridad a adoptar en la organización.

Si bien algunas de estas obligaciones (como la notificación de la creación de ficheros a la AEPD) parece que van a desaparecer quedando otras todavía supeditadas a sufrir adaptaciones para la correcta adecuación al RGPD, parece recomendable mantener (por el momento) algunas de estas prácticas como el *documento de seguridad*, un documento donde se recogen las medidas de índole técnica y organizativa acordes con la normativa estribando su importancia en la obligación que conllevaba "inventariar los equipos, redes, programas, ficheros, etc. y de la reflexión que exige sobre las medidas a aplicar en cada caso plasmando todo ello en un texto que debe estar permanentemente actualizado y a disposición de la Agencia de Protección de Datos" (Ribagorda, 2010).

Su contenido mínimo estipulado incluía la definición del ámbito de aplicación; las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido (recordamos que la LOPD establecía diferentes niveles de seguridad en función de las categorías de datos tratados); las funciones y obligaciones

del personal; la estructura de los ficheros con datos de carácter personal, describiendo el sistema de información; el procedimiento de notificación de incidencias; y el procedimiento de realización de copias de respaldo.

Por otra parte, según prevé el RGPD en su art. 30, los responsables de tratamiento que habitualmente realicen tratamientos de datos de riesgo para la privacidad de los interesados, o traten datos sensibles, deberán contar con un *registro de las actividades de tratamiento efectuadas bajo su responsabilidad.*

Dicho registro, debe contener:

- el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

- los fines del tratamiento;

- una descripción de las categorías de interesados y de las categorías de datos personales;

- las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

- en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional o la documentación de garantías adecuadas en los casos donde no haya consenso sobre la adecuación de los países destinatarios;

- cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

- cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

Como se puede observar, gran parte de esta información coincide con la que hasta ahora se debía proporcionar en la inscripción de los ficheros a la AEPD, por lo que ésta misma institución sugiere que, una buena forma de afrontar este nuevo registro, es partir de los ficheros que actualmente se tengan notificados, "detallando todas las operaciones que se realizan sobre cada conjunto estructurado de datos" y "en torno a operaciones de tratamiento concretas vinculadas a una finalidad común de todas ellas".

En cualquier caso, y pese a que no se imponga una obligación taxativa, parece que es una ocasión propicia para fomentar la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) basado, a su vez, en el modelo PDCA conocido también como *Círculo de Deming* (por el estadista estadounidense William Edwards Deming, padre del concepto de calidad total), donde las citadas siglas hacen referencia a los términos ingleses establecidos como sus cuatro principios fundamentales: *Plan* (planificar), *Do* (hacer), *Check* (controlar, verificar) y *Act* (actuar).

PDCA es un ciclo de vida continuo o de *espiral de mejora continua* (por tanto, de conceptualización similar al anteriormente explicado EIPD) en donde la última fase *Act* lleva de nuevo a la fase primera *Plan*, iniciándose un nuevo ciclo.

En el caso concreto de un SGSI, el PDCA se adaptaría de esta manera:

1. *Plan*: fase de diseño del SGSI en la que se realiza la evaluación de riegos de seguridad de la información y la selección de controles adecuados.

2. *Do*: fase que envuelve la implantación y operación de los controles

3. *Check*: fase que tiene como objetivo revisar y evaluar el desempeño del SGSI en cuanto a eficiencia y eficacia.

4. *Act*: fase en la que se realizan los cambios cuando sea necesario para llevar de vuelta al SGSI a su máximo rendimiento.

Aunque realizar un exhaustivo y detallado estudio de un SGSI requeriría un esfuerzo tal que podría ser objeto de otro trabajo al sobrepasar las expectativas y dimensiones esperadas en el presente, sí que es primordial decir que la adopción de un sistema de gestión de seguridad de la información (siguiendo, por ejemplo, el esquema de estándares internacionales como UNE-ISO/IEC 27001) garantiza que la seguridad de la información es gestionada correctamente al hacer uso de un proceso sistemático, documentado y conocido por toda la organización desde un enfoque de riesgo.

De hecho, la norma UNE-ISO/IEC 27001 se adecúa también al modelo de cuatro pirámides desde el ámbito de la gestión de calidad de tal forma que:

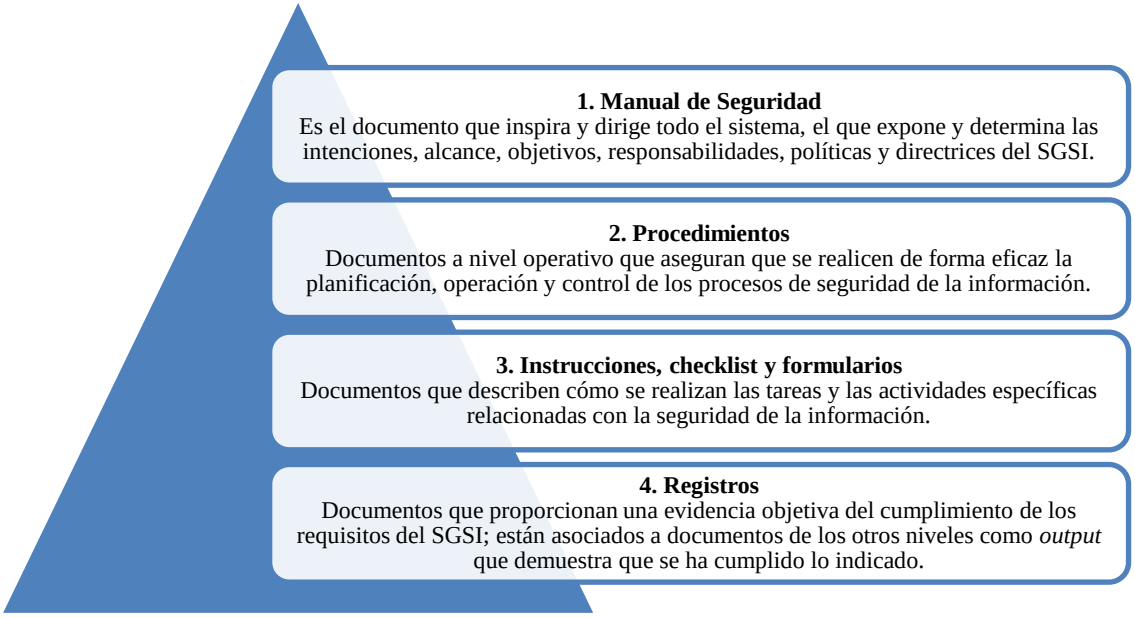

Ilustración 4: Pirámide con los diferentes tipos de documentos necesarios en UNE-ISO/EEC 27001

Por tanto, conseguir la certificación de un SGSI basado en la citada norma o en otras similares, es una buena forma de garantizar la privacidad de los datos personales de los

usuarios y demostrar el cumplimiento del RGPD, además de suponer un ejercicio de transparencia, siendo ésta la base de una relación de confianza.

Transmitir confiabilidad a los usuarios.

La confianza es especialmente crucial para mitigar las percepciones de riesgo, máxime, cuando los usuarios pueden tener dificultades para determinar si un servicio se proporciona correctamente debido a su falta de experiencia o conocimiento (Culnan y Armstrong, 1999), por lo que se debe tratar de transmitir confiabilidad a los usuarios de que sus datos y los tratamientos que se lleven a cabo con ellos cumplen con los principios fundamentales de la normativa en materia de protección de datos.

La simple publicación de la *app* en una de las tiendas oficiales de la plataforma correspondiente ya puede constituirse como un pequeño indicio de que el desarrollo de la *app* se ha realizado con cierto rigor y que procede de una fuente de confianza. Precisamente, en el último estudio *Ciberamenazas y tendencias* correspondiente a 2017 publicado por el Centro Criptológico Nacional se puede constatar que las *apps* más peligrosas para la privacidad de los usuarios, presentando en muchos casos código dañino como troyanos y *ransomware*, son aquellas que se descargan de tiendas no oficiales.

Otra forma de transmitir confiabilidad podría ser mediante la adhesión voluntaria a un determinado *Código Tipo* (como se denominan en la LOPD) o *Código de Conducta* (su equivalente en el RGPD) al constituirse como un instrumento autorregulatorio orientado a la adopción de reglas y estándares específicos y otras normas y códigos deontológicos[20].

Algunos de estos códigos tipo, como el de *Confianza On-Line* promovido en 2002 por la Asociación para la Autorregulación de la Comunicación Comercial y la Asociación Española de la Economía Digital y pertinentemente aprobado por la AEPD, ha ido evolucionando de tal manera que dio lugar a un distintivo público reconocido por el Ministerio de Industria, Turismo y Comercio y el Instituto Nacional del Consumo que abarca cuatro grandes áreas entre las que se incluye la protección de datos personales, debiéndose garantizar el cumplimiento de la normativa y asegurando que se han establecido medidas de seguridad y confidencialidad en las comunicaciones.

Por su parte, los *Códigos de Conducta* previstos por el RGPD están destinados a contribuir a la correcta aplicación del mismo "teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas" (art. 40.1 RGPD) pudiendo adherirse a los mismos para ser utilizados "como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento" (art. 24.3 RGPD).

Precisamente, la Comisión Europea hizo público en junio de 2016 el borrador del *Código de Conducta sobre privacidad para aplicaciones móviles de salud* elaborado por un equipo conformado por representantes de empresas tecnológicas, especialmente, por The App Association (que representa a más 5.000 empresas en todo el mundo de aplicaciones y empresas de tecnología de la información en la economía móvil) y

[20] Estos, además, incluyen ejemplos y modelos de cláusulas y para el ejercicio de los derechos, que permiten armonizar los tratamientos de datos efectuados por aquellos que se adhieren a los mismos.

específicamente dirigido a desarrolladores con el objeto de facilitar el cumplimiento normativo y promover "buenas prácticas" en este campo en relación con las aplicaciones *mHealth*. Sin embargo, este borrador ha sido puesto en entredicho tras la revisión llevada a cabo por el GT29 tal y como se desprende de la carta firmada con fecha 10 de abril de 2017 por la presidenta del GT29, Isabelle Falque-Pierrotin, al redactor principal del borrador, Hans Graux, y en donde se argumenta (entre otras cosas) que el Código no aporta un valor añadido al RGPD ni a las disposiciones de las legislaciones nacionales, no haciendo referencia a todos y cada uno de los principios fundamentales de la protección de datos y no clarificando suficientemente las referencias al nuevo marco jurídico.

Así que, mientras se clarifica el futuro del citado *Código de Conducta* así como los programas de certificación en materia de protección de datos previstos en el art. 42 del RGPD, una buena alternativa para transmitir la tan necesaria confiabilidad, son los programas de certificación específicos de las *apps de salud*. Estos programas, decía ya el *Libro Verde*, pueden ser indicadores fiables para los profesionales sanitarios y los ciudadanos, ya que podrían verificar tanto si la *app* ofrece contenido fiable como garantías al respecto de los datos de los usuarios y si funciona según lo previsto. Afortunadamente, y a diferencia del comentado caso del NHS británico, en España existen dos procesos de acreditación pioneros como son el distintivo *AppSaludable* en Andalucía y *AppSalut* en Cataluña debiéndose superarse en ambos una serie de criterios entre los que se encuentran el garantizar la confidencialidad y la privacidad así como la evaluación de las medidas de seguridad implementadas.

Estos dos proyectos sirvieron, a su vez, de modelo y ejemplo para la Comisión Europea quien en febrero de 2016 trató de organizar un grupo de trabajo (compuesto por representantes de pacientes, profesionales de salud, proveedores, industria tecnológica, universidades y autoridades públicas) encargándosele la elaboración de una serie de directrices que permitieran la evaluación de *mHealth* en toda Europa. Sin embargo, el proyecto fracasaría al determinarse que la elaboración de dichas directrices era un ejercicio mucho más complejo de lo que se esperaba inicialmente, no llegando tampoco a un nivel mínimo de consenso entre los diferentes miembros, lo que hacía imposible lograr y aprobar ninguna guía.

Iniciar el proceso de obtención de la certificación CE de conformidad de la *app* como *producto sanitario* no solo es obligatorio (según la Directiva 2007/47/CE transpuesta en España mediante el Real Decreto 1591/2009, de 16 de octubre, por el que se regulan los productos sanitarios) en el caso de que la *app* encaje dentro de las directrices previstas en la *Guidelines on the Qualification and Classification of stand alone software used in healthcare within the regulatory framework of Medical Devices* sino que, además, denota la calidad del producto y un compromiso para garantizar la protección de datos.

En este caso, y además de documentar los procesos de diseño, desarrollo, verificación, validación y mantenimiento (es decir, las fases del ciclo de vida) también se debe establecer un seguimiento de post-comercialización con el que verificar continuamente la efectividad de la *app* y asegurar las condiciones (incluyendo un análisis de riesgos), debiendo velar en todo momento por mantener taxativamente la confidencialidad de los datos obtenidos en los dispositivos, puesto que así lo dispone en el texto introductorio del Real Decreto 1591/2009, "en lo que concierne al tratamiento de los datos personales, el respeto a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo".

3.2. Cumplir con el deber de informar al usuario

Puesto que, generalmente, en el uso de una *app de salud* los datos personales se obtienen del propio usuario, se ha de cumplir el deber de información al interesado por parte del responsable del tratamiento. Y se ha de cumplir siempre puesto que en el RGPD solamente se contempla una excepción posible a este deber referida a cuando el interesado ya disponga de la información (art. 13.4). Esto significa que, aunque no llegase a precisarse la obtención del consentimiento en el hipotético caso de que quedase amparado el tratamiento de los datos personales bajo uno de los supuestos que excepciona la normativa, es totalmente imperativo proporcionar la información requerida (comentada anteriormente en el art. 13.1 del RGPD).

Proporcionar la información al interesado antes de que proceda a la instalación de la *app* y en el momento de iniciarse por primera vez.

En el caso concreto de las *apps*, tal y como ya advertía el GT29, hay que considerar que la recogida de datos puede tener lugar durante su propia instalación (al recopilar datos para fines de seguimiento o depuración de errores) por lo que "facilitar dicha información únicamente después de que el tratamiento de datos personales se haya iniciado (que suele comenzar durante la instalación) no se considera suficiente ni tiene validez jurídica" (WP202). Y, como además, para el GT29 resulta totalmente inaceptable el que los usuarios se vean en la situación de tener que buscar por sus propios medios las políticas de tratamiento de datos de la *app*, "en lugar de ser informados directamente por el desarrollador de la misma u otro responsable del tratamiento de los datos", la información (llamada habitualmente *Política de Privacidad*) debe ser fácilmente accesible y proporcionarse mediante un medio propio del responsable del tratamiento (o si es del desarrollador y no es él el responsable, que haga obligada referencia al verdadero responsable del tratamiento).

De esta manera, si la *app* se distribuye a través de la propia web del responsable del tratamiento, se debe incrustar la información en la misma página desde la que se procede a la descarga de la *app* para que el interesado pueda leerla sin tener que navegar por páginas distintas. Si la *app* se encuentra disponible en una tienda de aplicaciones, es necesario incluir el enlace a dicha URL en los apartados específicamente reservados para ese fin, tal y como además requiere el cumplimiento de políticas para programadores de algunas de estas tiendas.

En cualquier caso, siempre es recomendable que, al iniciar la *app* y antes de que el usuario otorgue su consentimiento, vuelva a aparecer la información así como que siempre esté fácilmente localizable, resultando conveniente incluir un enlace o *link* permanentemente incrustado entre las opciones principales de los menús.

Como ejemplo de "buena práctica" y puesto que, como ya se ha señalado, ofrecer la información de la forma adecuada es vital para la obtención lícita del consentimiento, podría establecerse un mecanismo por el que resulte imposible la introducción de dato alguno sin que previamente se haya mostrado dicha información (AEPD, Informe Jurídico 93/2008).

De esta manera, podría implementarse en la *app* una opción en la que, tras haber concluido la instalación y se inicie por vez primera, se cargue en la *Política de*

Privacidad de nivel abreviado (de la forma que a continuación se detallará) para no saturar al usuario (pudiendo incrustarse un *link* hacia el texto de máximo nivel) y que, antes del siguiente paso de registro y de otorgación del consentimiento, y puesto que aún con un texto reducido será difícil que se muestre completamente en la pantalla, se controlen los eventos del *scroll* sobre el texto para que únicamente se habilite el botón de "He leído" (o la casilla de marcar o similar) cuando se haya llegado a su tope.

También, por ejemplo, se puede presentar la información de los distintos epígrafes (como recomienda la AEPD) en varias pestañas y controlar que el usuario solamente pueda confirmar la lectura cuando haya pasado por cada una de ellas. O, también, se puede establecer un control de tiempo de manera que el botón o la casilla solo se activen al transcurrir el tiempo prudencial estimado para una lectura comprensiva[21] del texto.

Obviamente, ninguno de estos métodos determinará que realmente el usuario haya procedido a la lectura de toda la política (y ni mucho menos, lo haya hecho de la forma atenta y rigurosa que debiera) pero sí al menos puede evitar que instintivamente se pulse el botón o active la casilla.

El deber de información implica lealtad y transparencia, proporcionando aquella información complementaria que pueda resultar relevante.

Como ya se ha comentado, la información que debe ofrecerse al interesado debe ser transparente por lo que, además de detallar la información requerida en el RGPD**, se** debe facilitar aquella información técnica que pueda resultar relevante: dónde se encuentra ubicado el fichero en el que se registran los datos (si lo hace en modo local en el propio dispositivo o en medios externos como tarjetas de memoria o si utilizan servicios en la nube); cómo se va a llevar a cabo la recogida de datos, puesto que puede ocurrir que no sean directamente introducidos en la *app* a través de la interfaz propia sino mediante la conectividad con sensores y otros dispositivos wearables; si se utilizan *APIs* de terceros, garantizando que se cumplen los términos y condiciones impuestas por las empresas propietarias de las mismas; cuál es el motivo por el que la *app* va a usar ciertos recursos del dispositivo, tanto los referentes al uso de la red móvil como, especialmente, de los citados "riesgosos"; o porqué y con qué fin se está llevando a cabo un seguimiento *mobile tracking* o de *publicidad comportamental*.

Tampoco puede resultar superfluo informar sobre los mecanismos de seguridad utilizados, puesto que en las *apps* es difícil que los usuarios puedan conocer por sus propios medios los funcionamientos internos de las mismas. En pro de transmitir confiabilidad, adicionalmente al contenido obligatorio expresado en la normativa, parece pertinente que el responsable del tratamiento proceda a aclarar algunos aspectos técnicos relacionados con la *app* y con el tratamiento de los datos, de tal manera que sin dar a conocer aspectos internos de la organización, sí que pueda informar sobre si se está aplicando algún estándar, recomendación o política de seguridad o de los métodos de cifrado o encriptación empleados, facilitando así que el interesado pudiera concluir sobre las garantías que se le ofrecen o los posibles riesgos a los que se exponen sus datos personales si procede a la instalación y uso de la *app*.

[21] La velocidad de lectura de comprensión está determinada en unas 200-400 palabras por minuto (Colaboradores de Wikipedia. Lectura. Wikipedia, La enciclopedia libre, 2017 [fecha de consulta: 12 de junio del 2017]. Disponible en https://es.wikipedia.org/w/index.php?title=Lectura&oldid=99768855).

La información debe ser legible, accesible, entendible, adecuada y adaptada.

El principio de transparencia exige que la información proporcionada sea "fácil de entender, y que se utilice un lenguaje sencillo y claro" (cdo. 39 RGPD) presentándose "en forma concisa" y evitando un extenso y engorroso texto legal que pudiera llegar a favorecer que el interesado decidiera no leerlo.

En cuanto al idioma, el RGPD no hace referencia a cuál debe presentarse obligatoriamente[22] y cuáles complementariamente, sobreentendiéndose que debería ser en el oficial/es del responsable del tratamiento. En cualquier caso y como sugería la AEPD, y aunque la normativa sobre protección de datos no recoja esta obligación específica, sí que puede resultar conveniente "acudir al espíritu y finalidad de la ley" constituyendo "una manera más adecuada e inequívoca de llevar a cabo la información" en atención al *target* o público objetivo de usuarios (máxime en un entorno globalizado como éste) el que también se presente en un "idioma ampliamente conocido como es el inglés" (AEPD, Informe 0340/2010).

Lo que sí que puede resultar conveniente a este respecto (como señala el art. 12.7 del RGPD) es la utilización de iconos o infografías que referencien de forma sencilla y rápida el cumplimiento normativo de los principales aspectos. Así, y de modo similar a las etiquetas PEGI empleadas incluso por las propias tiendas de aplicaciones para señalar la idoneidad del contenido de *apps* y videojuegos en términos de protección de menores, resultó de interés la proposición formulada en 2013 por la Comisión LIBE del Parlamento Europeo en sus enmiendas a la propuesta del RGPD.

	No se recogen datos personales más allá del mínimo necesario para cada finalidad específica del tratamiento
	No se conservan datos personales más allá del mínimo necesario para cada finalidad específica del tratamiento
	Ningún dato personal se procesa con finalidades distintas de las que fueron recopilados
	No se divulgan datos personales a terceros para finalidades comerciales
	No se venden ni se alquilan datos personales
	No se conservan datos personales en forma no cifrada

Tabla 1. Iconos propuestos por la LIBE para la estandarización de políticas de información

[22] Sí que hay que presentarse "en un idioma compresible" en caso de las cláusulas para la transferencia internacional de datos personales, tal y como señala el Apéndice 2 de la Decisión 2001/497/CE de la Comisión Europea, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.

Lo conveniente sería proporcionar la información suficiente y útil, sin sobrecargar con demasiados detalles, en los momentos adecuados en los que se requiere un registro de datos. Momentos tales como cuando se van a realizar determinadas comunicaciones, cuando la *app* va a acceder a recursos del dispositivo o a datos almacenados en él e, incluso, cuando se deba notificar cualquier variación que se produzca en la *app* o en cualquier otro aspecto referente al tratamiento de los datos (ampliación de la finalidad de los tratamientos, cambio del responsable, etc.).

Así, la AEPD ya recomendaba para las webs (aunque totalmente aplicables a las *apps*) que, en las recogidas de datos realizadas mediante un formulario, se debía incluir en el mismo y de forma clara la información que hacía referencia el art. 5 de la LOPD (predecesor del art. 13 del nuevo RGPD) considerando más adecuado "propiciar la lectura de dicha información de modo ineludible (y no optativa) dentro del flujo de acciones que deba ejecutar el usuario para expresar la aceptación definitiva de la transmisión de sus datos" (AEPD, 2005).

Por su parte, el GT29 en el ya citado WP100 aprobaba "el principio de que no es necesario que un aviso sobre tratamiento leal esté contenido en un único documento", procediendo a recomendar la utilización de un formato de múltiples niveles para la información destinada a los interesados, contribuyendo así a mejorar la legibilidad y la calidad de la información al centrar en cada nivel la información precisa para comprender su posición y adoptar decisiones. Un sistema que proporcionaría la información esencial requerida por la normativa sin exigir que el usuario tuviera que desplazarse inicialmente por un extenso texto legal (lo que podrá hacer en el nivel último), utilizándose para ello otros niveles de información "jurídicamente aceptables en el marco de una estructura de múltiples niveles que sea conforme en su conjunto", más breves y acordes al reducido espacio de visualización que por sus características intrínsecas ofrecen los *smartphones*.

De esta manera y siguiendo esta pauta, la AEPD en su *Guía para el cumplimiento del deber de informar* recomienda que, a efectos de organización y presentación, la información se pueda agrupar en diversos epígrafes (referentes al responsable, finalidad, legitimación, destinatarios y derechos[23]) y en dos capas o niveles[24]:

- Un primer nivel, de aviso breve y resumido con la información más básica, debiéndose proporcionar en el mismo momento y en el mismo medio en que se vayan a recoger los datos.

- Un segundo nivel, más detallado con todas las especificidades y requisitos previstos en el art. 13 del RGPD y accesible en todo momento.

La información, por tanto, debe presentarse de un modo adecuado al entorno, no resultando coherente proporcionarla por medios distintos a los electrónicos en el contexto de una *app* y siendo deseable que el usuario pudiera conservar una copia del texto de máximo nivel posibilitándose su descarga o impresión. Esta adecuación, también incluiría que la información plasmada en los epígrafes requeridos (como por ejemplo en los datos de contacto del responsable, encargados, representante o delegado

[23] Y un epígrafe más denominado "Procedencia" a presentar únicamente cuando los datos personales no se hayan obtenido del interesado.

[24] El GT29 en su WP100 establecía inicialmente tres niveles.

de protección de datos) sea apropiada, y por tanto no procedería únicamente indicar la dirección del domicilio para correspondencia ordinaria o un número de fax, sino que se requeriría una dirección de correo electrónico, un enlace a su web o cualquier otro medio que resulte pertinente para el entorno tecnológico.

Y para llevar a cabo esta adecuación se han de seguir las guías y recomendaciones de las diferentes plataformas y, fundamentalmente, aplicar los principios de *diseño web adaptativo* para que se adecuen automáticamente al tamaño del dispositivo en el que se visualizan (especialmente las webs a las que se accede desde un enlace en la *app* y que puede que no se encontrasen inicialmente preconcebidas para usarse en *smartphones* y *tablets*), y las normas de *Diseño Universal* para facilitar la navegabilidad y accesibilidad a personas con discapacidades.

A este respecto hay que considerar que, según la legislación española, las páginas web de organismos públicos deben satisfacer los requisitos de prioridad 1 y 2 de la norma UNE 139803:2012 (equivalente a nivel AA en WCAG 2.0 de la W3C), debiéndose aplicar a las *apps* tras la entrada en vigor de la *Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.*

3.3. Obtener la legitimación para el tratamiento de los datos personales

Puesto que los datos objeto de tratamiento por la *app* pertenecen a una de las categorías estipuladas como "especiales" y excepto que el tratamiento de dichos datos esté contemplado en los casos anteriormente enumerados que lo licitan, especialmente en este entorno lo estipulado en el art. 9.2.h RGPD "para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario" (lo que puede ocurrir cuando la *app* tiene como funcionalidad la prestación de atención sanitaria con un servicio autonómico de salud, un centro sanitario del Sistema Nacional de Salud o forme parte de los servicios prestados por una entidad aseguradora con la que el usuario mantiene una relación contractual previa), en términos generales en el ámbito de la *apps de salud*, **el consentimiento del interesado se establece como el único fundamento de legalidad en el tratamiento de los datos personales de los usuarios de las mismas** debiendo ser informado (como se decía) pero también libre, específico, inequívoco, explícito, demostrable, revocable.

El consentimiento debe ser libre e informado y obtenerse específicamente para los fines previstos antes de que el usuario introduzca sus primeros datos personales.

Para que el consentimiento sea dado por el interesado libremente, hay que poner soluciones mucho antes de que la *app* llegue a instalarse en el dispositivo, no pudiendo de ninguna manera condicionar, ni presionar ni amenazar al usuario desestimándose, por tanto, el uso de técnicas y recursos basados en la transmisión de miedo en anuncios e informaciones promocionales sobre la *app*.

Esta cuestión ética, que incluso está tipificada como práctica comercial desleal[25], fue estudiada por Kharrazi et al. (2012) en aplicaciones *PHR*, detectando que alrededor de la mitad de ellas utilizaban estas tácticas para incitar a los usuarios a adquirirla con frases como "esta sencilla aplicación ha salvado vidas", "las emergencias pueden suceder a cualquier persona, en cualquier momento y en cualquier lugar" o "utiliza nuestra *app* para mejorar la seguridad y protección de tu familia" (un eslogan que utiliza una de las *apps* de emergencias desarrollada en España con más descargas).

Tampoco se puede considerar que se cumpla con el requisito de libre cuando la prestación del servicio que se desea proporcionar con la *app* está supeditada a la imposición obligatoria del tratamiento de datos personales que no sean estrictamente necesarios para el cumplimiento de dicho servicio (art. 7.4 RGPD) por lo que, como se verá, no se puede obligar al usuario a aceptar la monitorización de su comportamiento puesto que, como señalaba al respecto el GT29, este instrumento no es "estrictamente necesario para prestar una funcionalidad explícitamente solicitada por el usuario" (WP194).

Como el consentimiento ha de ser informado, éste debe obtenerse una vez se haya ofrecido la información anteriormente citada y previamente a recoger los primeros datos personales del usuario. Y, al igual que dicha información proporcionada en la *Política de Privacidad*, debe ofrecerse bajo una formulación inteligible y de fácil acceso, que emplee un lenguaje claro, sencillo y sin contener cláusulas abusivas (cdo. 42 RGPD) presentándose, además, separadamente de los demás asuntos como los términos y condiciones de uso de la *app* o el contrato de licencia para el usuario final (EULA).

Además, el consentimiento no puede obtenerse sin especificar la finalidad exacta del tratamiento. No es admisible, por tanto, el consentimiento "para todo" referido a un conjunto indefinido e indeterminado de actividades de tratamiento sino que se debe solicitar el consentimiento de forma diferenciada o granular para cada uno de los tratamientos de datos que sean completamente distintos del necesario para la funcionalidad de la *app* y para la prestación del servicio que se quiera dar (que en muchos de los casos en las *apps de salud*, al fin y al cabo y de una manera más evidente que otra, será la prestación de asistencia sanitaria).

Por consiguiente, es exigible el consentimiento diferenciado cuándo terceros recogen datos personales para la monitorización del comportamiento del usuario a través de *DARD* (dispositivos de almacenamiento de recuperación de datos), ya sea mediante *cookies* u otras herramientas o librerías análogas (por ejemplo, algunos *SDK* ofrecidos por redes publicitarias).

Como señala la LSSICE, el GT29 y la AEPD, los *DARD* únicamente se encuentran exentos del consentimiento del usuario cuando el almacenamiento o acceso de índole técnica se produzca "al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas" o cuando sea "estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado" por lo que no requerían la

[25] "Hacer afirmaciones materialmente inexactas en cuanto a la naturaleza y la extensión del peligro que supondría para la seguridad personal del consumidor o de su familia el hecho de que el consumidor no compre el producto". (punto 13 del anexo I de la Directiva 2005/29/CE del Parlamento Europeo y del Consejo de 11 de mayo de 2005 relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior".

obtención de dicho consentimiento *cookies* empleadas para la entrada del usuario, la autenticación, de seguridad, de sesión de reproductor multimedia, para equilibrar la carga, de personalización de la interfaz del usuario o de complemento para intercambiar contenidos sociales (WP194).

Por tanto, los *DARD* de terceros que se utilizan en la publicidad comportamental en línea u otras técnicas *retargeting* no entrarían en estos supuestos excepcionales y no quedan exentos de ninguna manera del requisito de consentimiento[26].

Similar situación ocurre con las *cookies* analíticas, utilizadas por los desarrolladores para monitorizar el comportamiento del usuario en la *app* (cuántas veces la utiliza al día, con qué frecuencia y a qué horas, qué opciones concretas, etc.) pudiéndose distinguir claramente entre los análisis propios y los análisis de terceros.

En las empleadas para análisis propios, es improbable que supongan riesgos para la privacidad siempre y cuando se limiten estrictamente a fines estadísticos agregados propios, que se ofrezca información clara sobre las mismas en su *Política de Privacidad* y que se garantice el uso de mecanismos que permitan una recogida de datos lo más anonimizada posible, optando por no recopilar informaciones identificables (como el ID del dispositivo o las direcciones IP). Por tanto, en este caso y siempre que se cumplan estrictamente las condiciones citadas, se puede entender que queden circunscritas dentro del otorgamiento general del consentimiento.

Por el contrario, las de terceros, que si pueden suponer un "riesgo notablemente más elevado para la privacidad" puesto que pueden utilizar los datos recopilados para fines propios, se debería obtener el consentimiento "diferenciado", informando claramente al usuario en el momento de que se le solicite (aunque se pueda aportar información más detallada y más ajustada a los requerimientos legales en la *Política de Privacidad*) de los datos que serán recopilados, las finalidades y la identidad de dicho tercero.

En cualquier caso, hay que evitar el "todo o nada" al igual que tampoco resulta práctico ni leal el tener que otorgar (aunque sea de modo "granular") todos los consentimientos *ex ante*, es decir, antes de la instalación o al iniciarse por vez primera. Lo recomendable es que los consentimientos para el tratamiento de los datos, para los permisos de acceso a recursos del dispositivo o para compartir ciertas informaciones con otras *apps* o sistemas, se produzca en el momento en que sea necesario (*ex post*), en tiempo de ejecución, facilitando así que el usuario pueda valorar el motivo por el cual se está pidiendo y decida su otorgación tras considerar que está suficientemente justificado.

Incluir un mecanismo de acción positiva para que el usuario manifieste inequívoca y explícitamente su otorgación de consentimiento.

Puesto que en el ámbito de las *apps*, donde se recogen datos de salud, el consentimiento tiene que ser inequívoco y explícito, el procedimiento implementado para su obtención no tiene que dejar duda alguna sobre la intención del interesado en concederlo, por lo que se ha de incluir un mecanismo de acción positiva. Consiguientemente, el silencio,

[26] Esto no quiere decir que la *app* no pueda incluir publicidad para su financiación ni que para poderla mostrar se requiera siempre el consentimiento del usuario puesto que en el caso de que, por ejemplo, la *cookie* se utilice única y exclusivamente para poder cumplir el contrato y poder cobrar las comisiones por cada uno de los *clics* que haga el usuario sobre los *banners* ofrecidos, sí que sería considerada una *cookie* "técnica" y no requeriría el consentimiento del usuario.

las casillas ya marcadas o la inacción no constituyen consentimiento (cdo. 32 RGPD). De este modo, el sistema *opt-out* durante años tan manido en marketing y en donde se redactaba el texto en sentido negativo, teniendo que ser el usuario quien marcase una casilla de verificación para manifestar su denegación al consentimiento, ha de considerarse totalmente inválido ya que en este sistema no existe una manifestación de voluntad entendida en el sentido de conducta activa.

Por tanto, debe implementarse un sistema *opt-in* donde el usuario, como ya señalaba la AEPD en su Informe 0011/2014, otorgue su consentimiento haciendo *clic* en un botón o marcando un *checkbox* no premarcado.

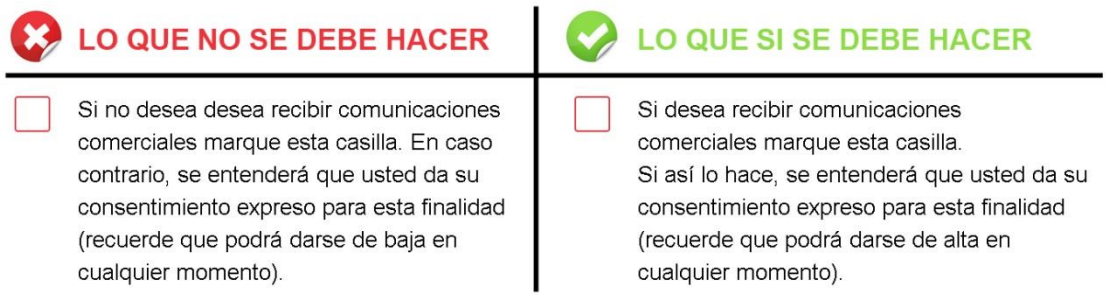

Ilustración 5: A la izquierda, lo que aparece en una conocida *app* de dermatología; y a la derecha modo correcto en el que debería haberse implementado.

Por todos estos motivos, y pese a tratarse de una acción positiva manifestada por el usuario, para considerar lícito el consentimiento no puede ser suficiente el mero hecho de que un usuario haya pulsado el botón "instalar" de una *app* concreta disponible en una tienda de aplicaciones. Y es que, pese a que sorprendentemente la AEPD sí que avala que la "descarga y uso de este tipo de aplicaciones responde a la voluntad del usuario que decida libremente utilizarlo"[27], el propio GT29 en el reiteradamente citado *WP202* señalaba que solamente en algunas circunstancias tal acción cumple el requisito de consentimiento siendo "improbable que aporte suficiente información para servir como consentimiento válido para el tratamiento de datos personales".

Esforzarse para verificar que, en caso de menores de edad, el consentimiento ha sido otorgado por el titular de la patria potestad o de la tutela del mismo.

Adicionalmente, el RGPD estipula que para que pueda considerarse lícito el consentimiento en menores de edad[28], que por sí mismos carezcan de las condiciones de madurez precisas para consentir el tratamiento de sus datos personales, el responsable del tratamiento "hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible" (art. 8.2 RGPD).

[27] Agencia Española de Protección de Datos. Resolución de 16 de marzo de 2017 sobre el archivo de actuaciones del expediente nº E/02661/2016.

[28] El RGPD establece dicha edad en 16 años aunque posibilita que los Estados miembros puedan "establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años", determinándose en España, dicha edad la de 14 años (Informe Jurídico de la AEPD 2000/0000, sobre el consentimiento otorgado por menores de edad).

Para cumplir esta disposición, se deben afrontar dos problemas claves (nada sencillos de resolver en la práctica): cómo comprobar la edad del usuario de la *app*, es decir, cómo conocer que dicho usuario es un menor de la edad establecida; y cómo proceder a verificar el consentimiento de los progenitores.

Ni en el RGPD ni en dictámenes del GT29 establecen un procedimiento de cómo llevar a cabo estas dos acciones, siendo el método habitual para la verificación de la edad el preguntar directamente al propio usuario los años que tiene o su fecha de nacimiento, por lo que de esta manera se "abre la puerta" a que el usuario pueda falsear la información para obtener el deseado acceso.

GSMA en su directriz NA4 para el *diseño y privacidad en el desarrollo de aplicaciones* sugiere que cuando el establecimiento de controles de acceso no sea posible y se tenga que recurrir a la autocertificación de la edad, se procure implantar un control por el que después de que el usuario haya introducido su edad real y no se le haya autorizado el acceso al no cumplir con el mínimo legal, la *app* se bloquee y no permita un segundo intento en el que el usuario dé un dato falso para superar esta salvaguarda.

Este método ya fue propuesto en la 31º Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en 2009 por el director de *The Future of Privacy Forum*, Jules Polonetsky, junto a otros métodos (muy complejos y que pueden resultar, en muchos casos, excesivos) tales como el análisis semántico a la hora de crear el perfil, uso de códigos de identificación (eID), el análisis de huellas digitales, la verificación en entorno móvil (incluida la geolocalización) o el acceso a bases de datos con contenidos públicos (registros de carnés de conducir, censos electores).

Un sistema más factible ya en uso (no sólo para verificar la edad sino también para cualquier otro tipo de identificación, especialmente en el ámbito del *elearning*) es el de capturar a través de la *webcam* el rostro de la persona junto al DNI u otro documento de identificación oficial, ejecutando un proceso de biometría facial.

Aunque posiblemente la solución más eficaz para resolver esta cuestión sería la acreditación de identidad mediante certificado digital. Pero, a día de hoy, esta solución también se topa con algunos problemas ya que ni tan siquiera las *apps* oficiales del Estado posibilitan su uso (redirigiendo habitualmente desde la *app* en diferentes acciones que así lo requieren a la URL de la versión web en donde sí está habilitado). Además, los *certificados digitales FNMT de Personas Física* solamente pueden ser solicitados por mayores de 18 años o menores emancipados[29].

El DNI electrónico, sin embargo, sí que incorpora un certificado digital que en el caso de menores de edad les permite la autenticación (solo esta función y no la de firma electrónica). De hecho, inicialmente no estaba contemplada esta posibilidad pero fue la AEPD la que instó al Consejo de Ministros a que aprobara la modificación del *Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica*, en pro de la protección de la infancia en el uso de internet, posibilitándose de esta forma la acreditación de la identidad de los menores por medios telemáticos.

Sin embargo, el uso del *DNIe* está todavía lejos de ser generalizado (Davara, 2017), esperándose que esto se produzca con la evolución del mismo hacia el *DNI 3.0*, que

[29] https://www.sede.fnmt.gob.es/certificados/persona-fisica

incorpora un chip RFID (*Radio Frequency IDentification*) que posibilita la conectividad de forma inalámbrica a través de la tecnología NFC (*Near Field Comunication*)[30], puesto que hasta ahora son pocos los casos (aún menos en soluciones ofrecidas fuera de las administraciones públicas y más reducido todavía en el ámbito de las *apps*) en los que se ha implementado un sistema de verificación de identidad online basado en el mismo, siendo Tuenti uno de los pioneros en seguir las recomendaciones de la AEPD al proceder a verificar la identidad de sus usuarios obteniendo del DNI-e los datos referentes a nombre completo, nº de DNI y fecha de nacimiento[31].

Por su parte, para la verificación del consentimiento paternal o del tutor legal, parecen muy limitados los procedimientos basados simplemente en preguntar al menor si sus progenitores han dado su autorización (Buttarelli, 2011), no pudiendo tampoco recabar, en ningún caso, datos que permitan obtener informaciones sobre sus padres o tutores legales (tales como actividades profesionales, información económica o sociológica) excepto aquellos datos que sirvieran para poder contactar con los mismos para obtener el pertinente consentimiento.

A falta de unos métodos estandarizados en Europa, se pueden tratar de imitar las pautas de la legislación estadounidense en materia de protección de la privacidad infantil en internet, la Children's Online Privacy Protection Act, más conocida por su acrónimo COPPA. Por la misma, la recolección, uso o revelación de datos personales de los menores de 13 años no se puede llevar a cabo hasta que no se obtiene el consentimiento paternal o del tutor legal, para lo cual se establecen varios medios que van desde un formulario de consentimiento que tras ser firmado debe ser enviado mediante email o fax, la disposición de ciertos teléfonos gratuitos y sistemas de videoconferencia o requerirse una transacción monetaria en la que se use una tarjeta de crédito, tarjeta de débito u otro sistema de pago en línea que proporcione notificación del titular.

En el aire podría quedar la cuestión de si no sería factible que, por ejemplo, en una *app* que sirve para monitorizar los niveles de glucemia o la adhesión a un tratamiento de un menor, no sería suficiente con que fuera el padre/madre/tutor legal quien se registrara aunque los datos recabados por el uso de la *app* fueran los del menor. Sin embargo, esto no solo iría en contra del principio de exactitud de los datos sino que también podría poner en riesgo la seguridad del paciente al ser la edad un dato determinante para el seguimiento de la salud e, incluso, un factor de riesgo en muchas enfermedades. En todo caso, lo que tal vez podría plantearse es que la *app* no fuese individualizada para una única persona sino que posibilitara la creación de perfiles asociados al titular del registro, siempre y cuando fuesen menores de 14 años o personas incapacitadas legalmente que estuvieren a su cargo.

El consentimiento debe ser demostrable.

El responsable del tratamiento debe acreditar quién consintió, cuándo y cómo lo hizo y cuál fue la información que se le proporcionó para que, efectivamente, otorgara su consentimiento para el tratamiento de sus datos personales. Es decir, como en otras diferentes funcionalidades que se irán detallando, es preciso gestionar un registro o *log* de este proceso particular.

[30] https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_038
[31] http://corporate.tuenti.com/es/blog/en-tuenti-somos-pioneros-en-la-verificacion-de-identidad-a-traves-de-certificado-electronico

La autoridad británica de protección de datos, la Information Commissioner's Office, recientemente daba una serie de recomendaciones sobre qué información debe documentarse a este respecto señalando que, en un entorno online como el de las *apps*, se deberían al menos registrar los siguientes datos ofreciéndose, en todo caso, las garantías exigibles en cuanto a la integridad y confidencialidad:

- Quién otorgó el consentimiento: registrando el nombre del individuo u otro identificador (nombre de usuario de la *app*, ID de sesión, correo electrónico, dirección IP). Aquí cabe añadir que, en adecuación a lo señalado en cuanto a los menores, habría que incluir "en nombre de quién" debiendo en su caso identificar al menor en cuestión sobre el que la figura parental o tutor legal ha dado su consentimiento.

- Cuándo lo otorgó: registrando un sello de tiempo o *timestamp* con la fecha y hora exacta en que se otorga el consentimiento.

- Qué información se proporcionó: puesto que pueden producirse modificaciones de la *Política de Privacidad* y las condiciones particulares del consentimiento a lo largo del tiempo, debe poderse constatar de qué exactamente se informaba al usuario debiéndose por ello registrar el número de versión de la política ofrecida, los textos plasmados en el formulario del consentimiento o una copia íntegra del contenido de ambos.

- Cómo se produce: si el consentimiento se obtuvo desde la propia *app*, desde un formulario web alternativo o desde cualquier otro medio así como las casillas o campos concretos que han sido marcados (y los que no) en los casos de otorgarse o denegarse varios consentimientos granulares para distintas categorías de datos, finalidades o terceros.

Un sistema muy utilizado para demostrar que el consentimiento fue otorgado realmente por quién procede al registro, es el método de confirmación doble, por el cual y tras el registro del usuario, se le envía un email de confirmación a la dirección facilitada por el mismo adjuntándose un enlace sobre el que se tiene que pulsar para obtener la activación del acceso a la *app* que, hasta ese momento, queda bloqueada. Esta técnica de *doble opt-in* refuerza la otorgación del consentimiento y, adicionalmente, posibilita la comprobación de que el correo electrónico facilitado es gestionado por su titular y no por un tercero de forma indebida.

El usuario debe tener derecho a retirar su consentimiento en cualquier momento.

El art. 7.3 del RGPD estipula que el consentimiento no puede ser "para siempre" sino para un periodo de tiempo limitado debiéndose obtenerse pasado dicho plazo (por ejemplo, un año) un nuevo consentimiento (WP131).

La validez del consentimiento debe ser por un tiempo determinado porque, como señalaban Anderson y Agarwal (2011), las emociones y el estado de salud pueden cambiar con el tiempo. Y es que, cuando los individuos se sienten tristes, enojados y ansiosos por su estado de salud actual, están más dispuestos a proporcionar sus datos personales y el acceso a sus historiales clínicos electrónicos, quedando así más vulnerables a las solicitudes oportunistas. Y, por contra, las personas en un estado de falta de emoción pueden sentir fuertemente que no quieren ser "una rata de laboratorio"

o un "conejillo de indias", por lo que puede provocarse el efecto contrario y no proporcionar la información hasta llegar a poner en juego su propia vida.

Además, el principio de limitación de la finalidad excluye los cambios súbitos de las condiciones claves del tratamiento, por lo que los cambios que se produzcan en este sentido modificando las *Políticas de Privacidad* o mediante actualizaciones semiautomáticas requieren la renovación del consentimiento. El GT29 recomendaba incluso que, cuando un usuario no haya utilizado activamente el servicio durante un periodo de tiempo, también se proponga la renovación del consentimiento o se proceda al ejercicio automático del derecho de supresión (WP185).

De cualquier modo, los usuarios deben ser capaces de retirar su consentimiento utilizando mecanismos accesibles y fáciles de entender, al menos, de una forma igual de sencilla que la usada para obtener el consentimiento y sin obligarles a motivar su decisión. Además, hay que informar también de forma clara sobre los efectos que provocará la retirada (eliminación o bloqueo de datos, renunciar forzosamente al uso de la *app* al carecer de funcionalidad ante la ausencia de datos) así como informar sobre las acciones que se van realizar para comunicar a terceros que se ha procedido a la retirada.

Como "buena práctica" al respecto, se puede recomendar la implantación de un panel de control (*privacy dashboard*) sobre la privacidad en donde, además de incorporar diferentes aspectos de los que se tratan en el presente trabajo, se facilite la posibilidad de retirar fácilmente el consentimiento, recordando a los usuarios cada vez que accedan al mismo (o redirigiéndolos a esta opción periódicamente cada cierto número de días o semanas) el estado de sus consentimientos (cuando son varios) y el histórico de las otorgaciones y retiradas llevadas al cabo del tiempo.

3.4. Recogida de "datos de calidad": adecuados, pertinentes, no excesivos, exactos y actualizados

Los datos tratados en la *app* se deben obtener por medios que no sean fraudulentos, leales y lícitos y deben ser "datos de calidad", es decir (como emanaba la LOPD): adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido; exactos, con el menor número posible de términos en evitación de ambigüedades e imprecisiones, y puestos al día de forma que respondan con veracidad a la situación actual del afectado, debiéndose registrarse lo más cercanamente en el tiempo al momento de producirse.

Requerir únicamente los datos personales que sean adecuados y pertinentes para la finalidad del tratamiento y minimizar la recopilación de los datos especialmente en los sistemas de recogida automática de la información.

El principio de minimización de los datos consagra el que no quepa cualquier tratamiento de cualquier dato, ni siquiera cuando el interesado haya prestado su consentimiento, sino que establece la necesidad de utilizar sólo los datos "no excesivos" en relación con "finalidades determinadas, explícitas y legítimas", lo que implica "la aplicación del principio de proporcionalidad, asegurando que sólo se utilizan los datos necesarios para las finalidades determinadas" (AEPD, Informe 0012/2013).

Por tanto, en una *app* para seguir la adherencia de un tratamiento no tiene cabida el que se soliciten datos como la ideología política, debiéndose valorar el contexto concreto y la funcionalidad de la *app* para determinar si son pertinentes y no excesivos otros datos de salud (siguiendo el ejemplo, podría ser pertinente solicitar las alergias pero no los antecedentes familiares).

Esto es especialmente relevante en la recopilación automática de la información puesto que los *wearables* suelen captar infinidad de datos primarios (como los movimientos de la persona que los lleva) utilizando complejos algoritmos para extraer la información sensible (como el número de pasos). Sin embargo, estos dispositivos no suelen permitir interactuar directamente con el titular del mismo sino que lo que hace es enviar los datos al sistema de información del fabricante quien, seguidamente, mediante el acceso a una *app* o un portal web pone a disposición del usuario una versión degradada de la información (por ejemplo, la condición física) deducida de la información primaria. Por ello, el GT29 recomienda que "cuando los fines se puedan alcanzar mediante datos agregados" no se requiere almacenar la totalidad de los datos en bruto y, por tanto, se debería seguir "un enfoque de intimidad desde el diseño y reducir la cantidad de datos recogidos al mínimo necesario para la prestación del servicio" (WP223).

Además también se debería posibilitar al usuario la elección de qué datos concretos, ámbitos o tipos de datos de entre todos los posibles son los que realmente desea que sean tratados ya que, por ejemplo, si el usuario no le interesa el registro continuo de la frecuencia cardiaca porque "sólo" estuviera interesado en usar el dispositivo como podómetro, aunque la *smartband* tuviera la posibilidad de recoger esos datos, no se deberían tratar al considerarse excesivos para el consentimiento específico otorgado.

Otro caso similar sería el de los datos de geolocalización, debiéndose ofrecer al usuario el nivel de precisión de la misma (por ejemplo, a escala de un país, ciudad, código postal o con la mayor posible) y avisando permanentemente (mediante un icono, por ejemplo) de que se encuentra activada esta opción. Y puesto que, como se ha señalado, el consentimiento es específico para unas finalidades concretas, los datos recolectados automáticamente también deben ser pertinentes para las finalidades informadas, de tal modo que si (por ejemplo) una *app* tiene como finalidad que el usuario pueda localizar los centros sanitarios, consultas de profesionales sanitarios o las farmacias que se encuentren más cercanas al lugar donde se halla en ese momento, los datos a recoger deberían ser única y exclusivamente los que se generen en el momento de producirse el acceso a esta función determinada de la *app*, no habilitándose la recogida permanente y continuada de datos cuando el usuario esté en opciones distintas de la *app* y, ni mucho menos, cuando no la esté utilizando.

Por tanto, hay que minimizar los datos recogidos evitando (como se señalaba anteriormente) la solicitud indiscriminada de "por si acaso" tuvieran transcendencia en un futuro sin ajustarse en el momento presente a la finalidad de la *app* (o a sus fines secundarios y compatibles).

Establecer controles y sistemas de ayuda en los formularios de entrada de datos para evitar que se introduzcan datos erróneos o equivocados.

El RGPD establece que los datos deben ser exactos, motivo por el cual (y más en un contexto como el de las *apps de salud* donde los datos suelen ser proporcionados por los propios usuarios), se deben implantar los mecanismos oportunos para que los datos personales introducidos no sean erróneos.

Un problema que transciende lo estrictamente requerido por la normativa de protección datos, llegando en un extremo a ser particularmente grave al poner incluso en peligro la seguridad del paciente puesto que algunos datos, como serían los resultados de los controles de nivel de glucemia, pueden servir de base para cálculos adicionales sugiriendo la dosis requerida de insulina (Monkman y Kushniruk, 2013). Incluso, las dificultades de interactuar con una *app* puede entorpecer la obtención de los resultados de eficacia previstos por el uso de la misma (Sarkar et. al, 2016), máxime cuando entre el *target* de usuarios se encuentra un amplio espectro de población con diversidad de condiciones y barreras tales como la edad o ciertas discapacidades que pueden impedir el llegar a completar tareas básicas y críticas o que lo hagan sin controlar posibles errores y fallos.

Aplicar a las *apps* los principios de usabilidad en el diseño de la interacción contribuye sobremanera a cumplir con los principios de calidad de los datos, pudiéndose considerar los principios heurísticos propuestos por Jakob Nielsen que, aunque originalmente fueron pensados para el contexto de ordenadores de sobremesa y aplicaciones de escritorio con teclado y ratón, siguen siendo válidos en otros contextos como las *apps* para dispositivos móviles:

1) Visibilidad del estado del sistema.
   El sistema siempre debe mantener a los usuarios informados sobre lo que está pasando, a través de una retroalimentación adecuada dentro de un tiempo razonable.

   Ejemplos de este principio serían el uso de barras de progreso en el almacenamiento de datos, los *breadcrumbs* ("migas de pan") que indican en que apartado de la *app* se encuentra el usuario, los indicadores en los procesos de registro que indican en qué fase se encuentra al usuario y cuántas le quedan para concluir o los avisos de que se ha completado satisfactoriamente una operación.

2) Correspondencia entre el sistema y el mundo real.
   El sistema debe "hablar" el lenguaje de los usuarios, con palabras, frases y conceptos que le sean familiares, siguiendo las convenciones del mundo real como metáforas y haciendo que la información aparezca en un orden natural y lógico.

   Refiere, por ejemplo, al uso de imágenes suficientemente identificativas de la acción que va a ejecutarse, de tal manera, que el usuario no se equivoque puesto que ya intuye para que puede servir. Sería el caso de utilizar el icono de una papelera para el botón de eliminar, del signo + para el de agregar un registro o el de un lápiz para modificar o editar un registro existente.

3) Libertad y control por parte del usuario.

Cuando los usuarios elijan alguna opción o función del sistema por error se debe disponer de una "salida de emergencia" claramente marcada para abandonar el estado no deseado sin tener que pasar por extensos diálogos.

Y además se debe facilitar el poder deshacer una acción realizada, por lo que hay que ofrecer al usuario la posibilidad de subsanar los errores que haya podido cometer antes de llegar a almacenar la información.

4) Consistencia y estándares.
Los usuarios no deben preguntarse si diferentes palabras, situaciones o acciones significan lo mismo por lo que conviene utilizar estándares.

Si bien este principio refiere más a casos como que los menús y demás elementos de la *app* funcionen de la misma manera en todas las opciones de la misma y que una opción (por ejemplo, un botón para borrar un dato) se denomine siempre igual (no en una opción "borrar" y en otras "eliminar"), también podría aplicarse a facilitar a los usuarios el que todos introduzcan los datos de un mismo modo y bajo un mismo significado.

Esto se consigue evitando que, en las partes que sea posible y que no requieran un gran sobreesfuerzo para el usuario (o en las que el beneficio obtenido sea superior a la incomodidad ocasionada), los datos no se introduzcan en lenguaje natural en campos de texto libre sino que se implemente una estructura en la que se unifiquen las posibles respuestas utilizando para ello cuadros combinados desplegables, casillas de verificación, grupos de opciones, campos autocompletables.

De esta manera, también se habilita la introducción de sistemas de clasificación y codificación estandarizados con los que, además de favorecer la interoperabilidad entre sistemas (y con ello, la portabilidad impuesta como nuevo derecho de los interesados en el RGPD) se garantiza una mejor interpretación de los datos y hasta una automatización de procesos, puesto que los valores introducidos (por muy complejos que sean) se basan en un idéntico modelo semántico en la definición de conceptos y se registran con una representación fija.

Siendo totalmente imprescindible en *apps* destinadas a ser empleadas por profesionales sanitarios, también puede ser de gran utilidad (en grados de menor complejidad) en las utilizadas por los pacientes ya que evitaría que, por ejemplo, un usuario registrase erróneamente una alergia que tuviera, pudiéndose incluir en la estructura reservada para esta información las descripciones de SNOMED CT correspondientes a las alergias para que se seleccione la oportuna (por ejemplo: al látex) aunque internamente en el campo se guarde el código correspondiente (1367842017); o similar con las opciones de seguimiento de un tratamiento (donde existen claras dificultades en los nombres, presentaciones, etc. que podrían dar lugar a fáciles equivocaciones) cuando se puede utilizar una clasificación de fármacos oficial donde, por ejemplo, un cuadro de texto se vaya autocompletando a medida que se introducen caracteres, pudiéndose guardar internamente el código nacional otorgado por la AEMPS.

5) Prevención de errores.
Incluso mejor que los buenos mensajes de error es un diseño cuidadoso que impida que un problema se produzca. Hay que eliminar las condiciones propensas a errores,

comprobar las mismas y presentar a los usuarios una opción de confirmación antes de comprometerse con la acción.

La prevención se puede facilitar introduciendo en cada campo de un formulario ejemplos de valores correctos (por ejemplo, máximos y mínimos admitidos) controlando que se ajustan a dicha horquilla e, incluso, proponiendo valores similares a los introducidos pero que fuesen correctos. También mediante la utilización de los teclados adecuados para cada tipo de dato (por ejemplo, teclado numérico para introducir un valor de nivel de glucemia) o componentes y otros *widget* que ayuden a introducir los datos en los formatos correctos de una manera sencilla, como ocurre con los selectores de fecha (*datapicker*) por el que en los campos de tipo fecha se posibilita introducirla a través de un calendario gráfico que emerge en pantalla. Adicionalmente, la validación de datos también contribuye a mejorar la seguridad del sistema pues evita desbordamientos de *buffer* originados al introducir valores que rebosan el tamaño máximo estipulado para un campo.

6) Reconocer antes que recordar.
Se deben hacer visibles objetos, acciones y opciones para evitar que el usuario tenga que memorizarlas o recordarlas, por lo que las instrucciones de uso del sistema deben ser visibles o fácilmente recuperables cuando sea apropiado.

Un ejemplo sería la utilización de asistentes (*wizards*) que guían al usuario a una adecuada introducción de datos sin tener que acceder por diferentes opciones; las máscaras de entrada en los campos para conocer en qué formato se ha de introducir el dato (por ejemplo: dd/mm/aaaa); o el uso de vista preliminar en una *app*, por ejemplo, que requiera el uso imágenes (*apps* de dermatología, úlceras por presión) y que permitan al usuario visualizar una miniatura de la misma para proceder a seleccionar la que desee (sin tener que recordar el nombre del fichero) o, en el caso de tratar una imagen (tras recortarla, rotarla, etc.) ver como ha quedado antes de guardarla o enviarla.

7) Flexibilidad y eficiencia en el uso.
Los accesos rápidos y atajos pueden hacer más rápida la interacción para los usuarios expertos, de tal forma que la *app* sea útil tanto para usuarios básicos como avanzados. Ejemplos de este principio podrían ser la automatización de tareas frecuentes y repetitivas o la inclusión de valores predeterminados en algunos campos, tales como la fecha y hora del sistema, que evitan en la gran mayoría de situaciones que el usuario tenga que introducirlas.

8) Diseño estético y minimalista.
La *app* no debe contener información que sea irrelevante o raramente necesaria. Cada unidad extra de información rivaliza con aquello que es relevante, además de que distrae al usuario y puede llegar incluso a molestarle.

Contra más "limpia" permanezca la pantalla, mucho mejor. Y es que, por ejemplo, para avisar de que se ha cometido un error no se puede lanzar un *pop-up* que ocupe toda la pantalla tapando el campo sobre el que se ha introducido un dato erróneo, máxime cuando en el aviso tampoco se alerta de lo que provoca el error. En tal caso, es preferible colocar un icono persistente al lado del campo. Y tampoco tiene utilidad sobrecargar al usuario con sucesivos cuadros de diálogo cuando se puede incluir en uno solo todo lo que se le quiera comunicar.

9) Ayuda a los usuarios a reconocer, diagnosticar y recuperarse de los errores.
   Los mensajes de error deben expresarse en lenguaje sencillo, indicando con precisión el problema, sugiriendo una solución de forma constructiva y, a poder ser, en el momento en que se producen, es decir, validando cada campo (por ejemplo, al perder el enfoque y saltar al siguiente) en vez de hacerlo al pulsar sobre un botón de "guardar" o "enviar" revisándose entonces todos los campos de un formulario.

   De esta manera, se recomienda evitar presentar solamente códigos complejos como "se ha producido el error (x)" que, aunque pueden contribuir a identificarlos en las comunicaciones con el soporte técnico, no sirven en ese momento al usuario al no conocer su significado ni lo que tienen que hacer. Los avisos hay que acompañarlos con descripciones precisas de los problemas exactos que se han producido. Además, los textos deben ser educados y en un tono cortés que no culpe al usuario de ser incompetente ni dando la impresión de que se les acusa de hacer las cosas mal. Y siempre tratando que aprenda del error y esté preparado, en sucesivas ocasiones, para evitarlo o solucionarlo.

10) Ayuda y documentación.
   Aunque siempre es preferible que la *app* sea usada sin ayuda, puede ser necesario proveer cierto tipo de información que permita al usuario disipar sus dudas.

   En este caso, la ayuda debe ser fácil de localizar, especificar los pasos necesarios y, sobretodo, ofrecerla de forma concisa y oportuna colocando, por ejemplo, iconos con el signo de interrogación cerca de algunos campos u opciones. También, puede ser pertinente la implantación de un mini-tutorial (en vez de un extenso manual descargable con cientos de páginas), incorporar un *tour* por la *app* explicando su funcionamiento esencial y tener un apartado de *Preguntas Frecuentes* (más conocido por su acrónimo inglés, F.A.Q.).

Establecer mecanismos para que los datos sean introducidos una única vez en la *app* evitando duplicidades o que se pierdan accidentalmente y que puedan ser modificados en caso de detectarse que son inexactos o incompletos.

Un dato debe ser introducido una única vez cuándo, dónde y por quién lo genera evitando pasos intermedios que no añaden valor pero incrementan las posibilidades de error (Escobar, Iraburu y Manso, 2003).

En las *apps de salud* es especialmente relevante que los datos se puedan registrar en todo momento, de una u otra manera, porque un dato es irrepetible y de la existencia del mismo puede depender un control adecuado sobre la salud. Y si no se quiere perder al usuario, éste no puede estar utilizando otros medios para anotar una cifra de nivel de glucemia o una administración de un medicamento para registrarlo en otro momento porque la *app* no está disponible porque, al final, acabará optando por desinstalarla y buscar otra solución probablemente en la competencia.

Por tanto, a una *app* se le debe haber provisto de los controles suficientes como para evitar que un dato que ya se ha introducido no llegue nunca a almacenarse en el correspondiente *back-end* y acabe perdiéndose a causa de que la *app* haya dejado de funcionar o se haya cerrado inesperadamente por un mal desarrollo que no ha contemplado un problema que, en cierto modo, es relativamente probable que suceda en los casos donde residen en un servidor y no en el propio dispositivo (como puede ser

una caída puntual del servidor, un fallo en la red o la pérdida de conectividad a internet del dispositivo). Por eso es importante que, como en cualquier otro tipo desarrollo de software en el que su arquitectura requiera un servidor, se compruebe el estado de la conexión en cada acción que fuese a requerir comunicación con el mismo.

Obviamente, hay situaciones que serán complejísimas o imposibles de solucionar pero habrá que tratar de poner remedio a aquellas que si puedan preverse, siendo este un buen momento para adoptar los principios de usabilidad antes comentados sobre la visibilidad del estado del sistema y, principalmente, realizar un adecuado tratamiento de excepciones implementando soluciones en las que ocasionalmente el conjunto de datos queden guardados en caché o en una base de datos temporal en local (con las medidas de seguridad adecuadas) hasta que se recupere la conexión con el servidor y se transfieran definitivamente. De ahí que al principio, cuando se realiza el análisis de los requerimientos de la *app*, sea tan relevante escoger el *back-end* más adecuado, no pudiéndose descartar con ligereza los sistemas de sincronización remota de datos sin analizar los pros y contras del mismo en relación con funcionalidad principal de la *app*.

Otro "problema" que hay que tratar de evitar son las redundancias, lo que implica que si por ejemplo, en el perfil de la *app* ya se ha informado sobre el sexo del usuario, en todas las demás opciones que se pudiera requerir esa información (porque se va a ejecutar un algoritmo, por ejemplo) se debe tomar el dato ya registrado al inicio y no volver a solicitarlo (o, al menos, tomarlo como valor predeterminado).

Otra situación parecida podría producirse con un determinado registro introducido "manualmente" por el usuario, por ejemplo, los valores de una medición de tensión arterial tomada con un esfigmomanómetro que no permite la interconectividad directa con el dispositivo. El usuario puede no recordar si efectivamente lo ha registrado o tiene dudas de si ha quedado guardado, por lo que directamente pulsa sobre el botón de agregar un nuevo registro para introducir (nuevamente) los valores de la toma. Pues bien, la *app* debería tener implementados unos controles que evitasen, o al menos, dieran aviso de que ya se encuentran registrados datos de una toma en esa misma fecha y hora, posibilitando al usuario si desea cancelar la nueva operación, si desea reemplazar los datos primigenios por los nuevos datos o si realmente desea continuar con el registro nuevo porque efectivamente se corresponde con otra medida.

Además, hay que procurar evitar las inconsistencias lógicas, dejando constancia de cualquier modificación o actualización llevada a cabo, para lo cual es relevante que en cada registro agregado se identifique, al menos: el origen del mismo (tanto si se ha proporcionado de forma activa al introducirlos "manualmente" en la *app* por el propio usuario como aquellos otros automatizados derivados de la conectividad con *wearables* o sensores, en cuyo caso, se podría identificar adicionalmente la marca, nº de serie o Id de dicho dispositivo); y la localización en el tiempo (fecha y hora) referente al momento exacto en el que el dato queda registrado en la *app* (y que puede diferir del momento de originarse el dato, como por ejemplo, una administración de medicación prevista a las 21:00 horas, que efectivamente se toma a dicha hora pero que se registra en la *app* media hora más tarde porque el usuario no ha tenido tiempo de hacerlo antes).

Con esa base, cada modificación que se produzca sobre el dato original, también se debe controlar e identificar, de tal manera que quede constancia de que se ha producido una variación del dato/s original/es informándose nuevamente de quién y cuándo se ha producido dicha modificación y de cuáles eran los valores originales.

En todo caso, se deben evitar las eliminaciones y modificaciones "accidentales", y volviendo a los principios de usabilidad, no posibilitar la ejecución directa tras pulsar los botones para estas acciones sino solicitar al usuario la confirmación mediante concisos cuadros de diálogos o, incluso (en según qué datos) imposibilitando la eliminación o modificación directa al transcurrir un tiempo prudencial prefijado.

3.5. Implementar adecuadas medidas de seguridad en la *app*, en toda la infraestructura del sistema de información y en el tratamiento de los datos personales

El RGPD estipula que tanto el responsable como el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (art. 31).

Si bien el RGPD, a diferencia del RDLOPD, apenas describe medidas específicas ni diferencia entre diferentes niveles concretos a aplicar según la categoría de los datos (básico, medio o alto —que es el que correspondía a los datos de salud—), sí que señala que se deberá evaluar la adecuación del nivel de seguridad "teniendo en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

Precisamente por tratar datos sensibles especialmente protegidos, las *apps de salud* y toda su infraestructura técnica, requiere un nivel de seguridad lo más elevado posible tratando de implementar las medidas más adecuadas. Para ello, y debido a la complejidad de llevar a cabo todas las acciones necesarias, los desarrolladores deben seguir guías y metodologías expresamente dedicadas al desarrollo seguro de aplicaciones para *smartphones*, que permiten identificar los riesgos predominantes en este entorno sugiriendo los controles que se han de implementar para prever y reducir, en su caso, el impacto que puedan llegar a ocasionar.

Seguridad durante todo el ciclo de vida e identificación de las vulnerabilidades y análisis de los riesgos de seguridad que puede presentar la *app*.

El primero, y seguramente el más relevante, de los principios de *Privacy by Design* es que se ha de ser proactivo y preventivo, es decir, se han de anticipar y prevenir los riesgos. Por eso se han de identificar, evaluar y, finalmente, mitigar desde el mismo diseño los posibles riesgos de seguridad.

Pese a que los peligros son innumerables, el proyecto OWASP (de similar modo a cómo hiciera desde 2003 con las aplicaciones web) identifica en su *Top 10 Mobile Risk* los principales riesgos a los que está sometida la seguridad en los dispositivos móviles enfocándolos, principalmente, en la capa de aplicación aunque tratando también la infraestructura de servidores con los que se comunican las *apps*, así como en la integración entre ellas, los servicios de autenticación remota y las características específicas de la plataforma en la nube.

A continuación, se desglosan brevemente cada uno de estos riesgos:

Ilustración 6: El *Top 10 Mobile Risk* del *OWASP Mobile Security Project* en el año 2014[32].

1. Debilidad en los controles del servidor de la *app*.
   Cuando el servidor al que se conecta remotamente la *app* (mediante *APIs* de tipo *REST*, *SOAP* o *HTTP*) no posee controles suficientes de seguridad, puede quedar expuesto a una vulnerabilidad *XSS* (*Cross-site scripting*) explotable mediante ataques de inyección *SQL* o *LDAP* con los que se accede a datos no autorizados o a realizar acciones arbitrarias que afecten a los mismos.

2. Almacenamiento de datos inseguro.
   Cuando la *app* conserva los datos en el almacenamiento interno del dispositivo, principalmente cuando no lo hace de forma segura, está expuesto a fugas y alteraciones de la información por la posibilidad de que éste se extravíe, sea robado o, incluso se produzca un acceso al mismo sin requerir tenerlo físicamente (por ejemplo, a través de *exploits in the wild* u otro *malware* que incluso puede eludir ciertos cifrados).

3. Protección insuficiente de la capa de transporte.
   Cuando la *app* se conecta al servidor para enviar información y no lo hace de modo seguro (sin cifrar), esta transmisión se encuentra en riesgo de ser interceptada mediante ataques MITM (*Man-in-the-middle*) y *phising* quedando, por tanto, los datos expuestos a fugas o modificaciones no autorizadas.

4. Fuga de datos involuntaria.
   Cuando la *app* guarda datos temporalmente en ubicaciones poco seguras (como el *buffer* de copiar/pegar, *content providers*, en la cache, en cookies del navegador o en el *log* del sistema) al que suelen acceder otros agentes sobre los que la *app* no puede ejercer ningún control (como el propio sistema operativo, *hardware* o *frameworks* de otras *apps*) se pueden producir fugas de información, ya que existe malware que precisamente busca en estas ubicaciones.

[32] En 2016, se volvió a reelaborar el listado y las diez categorías principales quedaron más centradas en la propia app más que en el servidor https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

5. Autenticación y autorización pobres.
   Si la *app* no provee los niveles adecuados y necesarios de autorización y autenticación podrían producirse accesos no autorizados mediante ataques de fuerza bruta, suplantaciones de identidad o, incluso, modificaciones de los niveles de autorización.

6. Criptografía rota.
   La *app*, pese a utilizar cifrado para almacenar o transmitir la información, usa métodos débiles o que han quedado obsoletos, por lo que los datos resultan igual de desprotegidos que si no estuviesen cifrados.

7. Inyección del lado del cliente.
   Si la *app* no posee controles suficientes de seguridad en la entrada de datos (campos de formularios, barras de direcciones), se estaría expuesto a posibles ataques en los que se inyectaran sencillos *exploits* enviándole valores que no pudieran ser procesados adecuadamente y desbordar así el sistema.

8. Decisiones de seguridad vía entradas no confiables.
   Debido a que los procesos entre *apps* y sistemas operativos comparten espacios de memoria para permitir la comunicación y sincronización entre los mismos, podría suceder que la *app* en cuestión recibiera comunicaciones de diferentes fuentes no confiables (como otras *apps* maliciosas que estuvieran instaladas), que al no ser debidamente validadas, podrían provocar también ataques a la seguridad.

9. Manejo de sesiones inapropiado.
   Vulnerabilidad que, aprovechando la autenticación débil, podría provocar que un atacante interceptase una sesión abierta o que llegase a clonar una sesión válida por capturar o prever los identificadores de sesión persistentes.

10. Falta de protección de los binarios.
    La falta de protección de la *app* a nivel binario posibilita el ataque mediante ingeniería inversa por el que, a través de la descompilación, se pueda conocer el código incrustado (por ejemplo, obteniendo la cadena de conexión al servidor) o, incluso, modificar el código de tal forma que se varíe el comportamiento de la *app* provocando, por ejemplo, que los datos se envíen a otro servidor distinto del autorizado.

Una vez identificados los principales riesgos, se debe proceder a implementar las medidas adecuadas siguiendo, por ejemplo las directrices plasmadas en la *Smartphone Secure Development Guidelines*, una guía elaborada por Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) nacida conjuntamente con el proyecto de seguridad móvil OWASP en 2011 y que recientemente, en el pasado mes de febrero, ha sido actualizada desglosando medidas para hasta trece tipos de riesgos distintos.

A lo largo del presente trabajo, ya se están indicando algunas de las recomendaciones señaladas en esta guía por lo que no refiere volverlas a indicar u otras se señalarán en su correspondiente apartado. En cualquier caso, sí que es importante señalar algunos aspectos que en ella se indican y que afectan al ciclo de vida de desarrollo, empezando por la propia adopción del tipo de *app* que se desea desarrollar (nativa, web o híbrida) y por la plataforma (o incluso, multiplataforma), debiendo en todo caso analizar las

características de cada una de ellas y comprender las diferencias existentes para que, independientemente de la elección final, se aseguren las configuraciones de seguridad particulares más adecuadas para lo cual es transcendental seguir las guías oficiales para desarrolladores.

En todo caso, se debe minimizar las líneas de código y su complejidad, evitando los desarrollos llevados a cabo con herramientas de creación poco comunes que pudieran provocar la publicación de *apps* inseguras o, incluso, infectadas "de fábrica" (ya que algunas de estas herramientas, sencillas de obtener en internet y en muchos casos gratuitas, suelen contener virus).

De similar manera, se deben identificar los estándares, *SDK*, *API* y bibliotecas comunes que se adapten mejor no sólo a los requisitos funcionales sino los que también ofrezcan garantías suficientes para proteger los datos personales que en la *app* se gestionen. De esta manera, las *APIs* y códigos de terceros que se fuesen a implementar deben ser analizados determinando cuál va ser el tráfico de datos, qué tipo de datos, si va a ser unidireccional (de "nuestra" *app* al sistema de información del tercero, o al revés) o bidireccional (intercambiando datos entre ambos sistemas). Además, es preferible escoger código y librerías de fuentes confiables y de desarrolladores con reputación y fiabilidad contrastada que, además, ofrezcan un mantenimiento continuo proporcionándose los pertinentes parches y actualizaciones.

Otro aspecto que se debe prever es el control sobre el acceso ilícito a recursos de pago o el abuso en el mismo, evitando que la *app* (o cualquiera de las librerías de terceros incrustadas) accedan, automáticamente y sin el consentimiento del usuario, a servicios *premium*, itinerancia de datos, etc.

En apartados anteriores, se hablaba de la importancia de establecer mecanismos de control en la recogida de datos para evitar la introducción de datos erróneos o inexactos. Pues bien, algunos de estos controles (como se ha visto en el *OWASP Top 10 Mobile Risk*) también posibilitan garantizar la seguridad de los datos al evitar que se produzcan desbordamientos y otros ataques para colapsar el servicio. Adicionalmente también se pueden implementar otras salvaguardias al respecto como la no utilización de teclados de terceros, siendo preferible desarrollar teclados personalizados para los diferentes tipos de datos requeridos; o la deshabilitación de las funcionalidades de "cortar, copiar y pegar" (restringiendo también el uso del portapapeles) y de las capturas de pantalla (si bien algunas plataformas como iOS no admiten esta posibilidad).

La recomendación generalizada es que los datos personales sensibles recabados por una *app* se almacenen directamente en el servidor en vez de en el propio dispositivo, puesto que los dispositivos móviles son muy susceptibles de ser sustraídos o extraviados[33] procediendo siempre a su cifrado.

Otra fase relevante que se debe cumplir es la de "testeo", no debiéndose saltar de ninguna manera por las prisas de publicar. Toda *app* necesita ser depurada, realizándose las pruebas pertinentes garantizando, en caso de que se fuera a recabar datos reales, las mismas medidas de seguridad que si estuviera ya puesta en real. Para esta fase se puede seguir la *Mobile Security Testing Guide* (MSTG), una guía que está elaborando el grupo

[33] Como ya se ha indicado con anterioridad, si únicamente los datos se almacenan en el propio dispositivo y no se procede a tratar ningún dato, no se requiere el cumplimiento normativo de protección de datos y, por tanto, quedaría también fuera del objeto del presente trabajo.

de trabajo de OWASP dirigido por Bernhard Mueller y Sven Schleier para realizar todo tipo de pruebas exhaustivas que cubran los procesos, técnicas y herramientas utilizados durante una prueba de seguridad de aplicaciones para móviles.

Y como también se decía anteriormente, la publicación de la *app* en determinadas tiendas transmite confiabilidad a los usuarios porque controlan la calidad y el contenido de la misma estableciendo (en algunos casos) rigurosos controles por los que se eliminan aquellas *apps* defectuosas, que se encuentren infectadas o, directamente, que sean maliciosas. Es decir, que someterse al proceso de aprobación de la publicación en un *market* concreto, también puede proporcionar una vía para conocer vulnerabilidades graves en la *app*.

Finalmente, también la *app* debe ser diseñada de tal forma que permita las actualizaciones y parches de seguridad, debiendo verificar las descargas de código dinámico y las actualizaciones en el lado del cliente y sometiendo también a un proceso de validación de integridad a aquellos recursos que se estén recuperando de un servicio externo (por ejemplo, los archivos APK).

El cifrado, método idóneo para la protección permanente de los datos personales.

Los datos personales deben estar protegidos permanentemente, es decir, tanto en el almacenamiento como en el transporte e, incluso, cuando son exportados en cualquier soporte para tratamientos ulteriores realizados por el responsable del tratamiento, por el encargado o por cualquier otro tercero. Y, para ello, el cifrado se constituye en el medio técnico idóneo por el que se garantiza esta protección, debiéndose invertir los recursos que sean necesarios para su correcta implementación.

Pero no sólo es necesario cifrar sino hacerlo de "forma que la información no sea inteligible ni manipulada por terceros", resultando imprescindible que "el sistema cifrado a emplear no esté comprometido, es decir, que no se conozca forma de romperlo" y considerando también que la garantía necesaria para preservar la confidencialidad de las comunicaciones no "solo descansa en el sistema de cifrado, sino también en el sistema de gestión de claves, en particular, y en el procedimiento de administración de material criptográfico, en general" (AEPD, Informe 0494/2009).

El RGPD no determina el tipo de cifrado y ni siquiera hace referencia a si debe ser mediante un algoritmo estándar o mediante cualquier otro mecanismo alternativo que garantice que la información no sea legible ni manipulada por terceros

Desde luego, parece más recomendable implementar un sistema convencional cuya eficacia y robustez esté ya demostrada. Posiblemente, el más adecuado para el almacenamiento seguro es *AES* (*Advanced Encryption Standard*), establecido como estándar de cifrado simétrico para el National Institute of Standards and Technology (NIST) en sustitución de *DES* y que fue desarrollado por los criptógrafos belgas Joan Daemen y Vincent Rijmen en 1997 bajo el nombre original de *Rijndael*, tratándose de un algoritmo que soporta bloques de 128 bits y claves de cifrado de longitud 128, 192 o 256 bits. (NBS, 2001)

Para la transmisión de los datos, hay que tener presente que los ataques basados en la red son una de las principales amenazas para las *apps*, fundamentalmente porque los *smartphones* suelen contener múltiples tecnologías de redes diferentes de las cuales hay

que considerar *a priori* a algunas de ellas como no confiables (como las redes *WiFi*, especialmente, aquellas abiertas).

Por ello, las *apps* deben utilizar un canal seguro de extremo a extremo al enviar información a través de cualquier red. Es decir, se debe ofrecer confidencialidad, en cuanto a que la información se envía cifrada; integridad, en cuanto a que la información cifrada no puede sufrir modificaciones malintencionadas; y autenticidad, pues el servidor certifica que es quien realmente dice ser.

De entre todos los protocolos criptográficos que proporcionan comunicaciones seguras por una red, actualmente destaca sobremanera *Transport Layer Security* (TLS), un protocolo estandarizado por la IETF (Grupo de Trabajo de Ingeniería de Internet) que fue definido en 1999 y redefinido en diversas ocasiones (la última en 2011 con la RFC 6176). Basado en las especificaciones de su antecesor Secure Sockets Layer (SSL) creado por Nestcape Communications Corporation, utiliza criptografía simétrica (cifrado del mensaje), criptografía asimétrica (cifrado) y función hash, combinado con certificados y firmas digitales.

El uso de TLS, como informa el Centro Criptológico Nacional, sigue creciendo siendo la tendencia predominante para el tráfico intercambiado entre las *apps* móviles y los servicios remotos, empezando a frecuentarse su uso (o el de otros protocolos derivados) al quedar implementados en los propios sistemas operativos. Esto ocurre, por ejemplo con *App Transport Security* (ATS), introducido en *iOS 9* en 2015 y que hace uso de *HTTPS* con requisitos de seguridad elevados con *TLS 1.2* y claves *RSA* de 2.048 bits y algoritmos *hashing* mediante SHA-256, habiendo anunciado Apple en su conferencia de desarrolladores WWDC de junio de 2016 que su uso sería obligatorio para todas las *apps* que se publiquen en la App Store, si bien todavía no se ha cerrado ese plazo y ha quedado indefinida la fecha límite (Rozalén, 2016).

Si por cualquier motivo los datos debieran permanecer en el propio dispositivo, bien porque se utilizan sistemas en los que se sincronizan los datos o en casos puntuales como los que se comentaban para evitar que los datos introducidos se perdiesen ante una hipotética desconexión con el servidor (incluyendo en este método, la escritura en caché) también durante este tránsito deben permanecer cifrados además de establecerse mecanismos que periódicamente (si no se ha procedido ya a su transferencia al servidor) proceda a la eliminación de esta información para que no quede almacenada indefinidamente.

Implementar en la *app* un sistema robusto de autenticación.

El uso de un elemento o factor basado en una contraseña ha sido el mecanismo más común a la hora de proceder a la autenticación de un usuario en un sistema informático y, por ende, así se ha seguido haciendo en las *apps*, un ámbito en el que (como ya se ha indicado cuando se hacía referencia a la verificación de la edad para el acceso de menores) todavía no se encuentra extendida mayoritariamente la implementación de otros factores añadidos a este citado de "algo que el usuario sabe o conoce", tales como los factores de "algo que tenga o posea" (como un código de seguridad recibido en un teléfono móvil o *token*) o los de "algo que el usuario sea" (es decir, una característica intrínseca de su ser como las huellas dactilares o el iris).

Pese a todo, el doble factor se ha convertido ya en un método no tan infrecuente para reforzar el sistema de autenticación, requiriéndose para proceder a la autenticación en la *app* la utilización de dos de esos factores citados, siendo los más habituales aquellos en los que se combinan los factores de conocimiento y posesión, como por ejemplo, la generación automatizada de una clave de validación que el usuario debe introducir adicionalmente a su *password* y que le habrá sido proporciona a través de un SMS. Un método que ha evolucionado en sofisticación y seguridad hasta el llamado TOTP (*Time-based One Time Password*) en el que, como su propio nombre indica, se utiliza un código que se remite al dispositivo concreto donde se desea utilizar y que sólo se puede usar una vez, caducando al transcurrir unos segundos.

Quizás, la implementación de un sistema de este tipo pudiera resultar exagerado en la mayoría de casos para una "simple" *app* pero, si nadie pone en duda que cuando se va a realizar un pago online el sistema del banco correspondiente emplee un método 2FA, no debería resultar excesivamente traumático hacer lo propio en el manejo de *apps* en donde residen (nada menos) que datos de salud.

En cualquier caso, siempre que se vaya a utilizar un sistema basado en contraseñas, se debe establecer una política que garantice su seguridad, implementando restricciones sobre la longitud y formación de la misma, su reutilización y duración por lo que, al menos, se deben establecer controles automatizados para que a la hora de conformar una nueva contraseña, ésta se rija por unos criterios como:

- que la longitud de la contraseña tenga, como mínimo, ocho caracteres.

- que sea lo menos "regular" posible, es decir, que no se cree con series de caracteres dispuestos adyacentemente en el teclado ("qwerty") o siguiendo un orden alfabético o numérico ("123456", "abcde"), ni incluyendo el ID del usuario utilizado para *loguearse*, ni (a poder ser) palabras del diccionario.

- que se alternen mayúsculas y minúsculas, números y caracteres especiales

Además, es recomendable que los campos en donde se vayan a introducir contraseñas (tanto para registrarla la primera vez como en los controles de autenticación y opciones de renovaciones posteriores) por defecto tengan máscara de entrada (para que no se visualicen directamente los caracteres introducidos siendo sustituidos por asteriscos) aunque posibilitando al usuario la opción de *desenmascarar*. En el caso de proceder al registro o a modificaciones posteriores, antes de confirmar el guardado de la misma y en evitación de posibles errores que haya podido cometer el usuario, se debe incorporar otro campo para que el usuario repita la contraseña que ha establecido en el primero con el fin de validar que, efectivamente, es la misma.

Adicionalmente a los métodos de control establecidos y cuando éstos no lleguen, también parece pertinente ofrecer recomendaciones a los usuarios para que tengan en cuenta una serie de pautas que contribuyan a la generación de contraseñas seguras, indicándoles que para conformar la contraseña no se debe utilizar información personal tal como (fecha de nacimiento, nombre propio o de familiares, aficiones). Tampoco se recomienda utilizar la misma contraseña para todas las cuentas de servicios en línea ni conservar anotada la contraseña en un lugar público y accesible al público ni compartirlas mediante correo electrónico o teléfono.

Por otra parte, las contraseñas no deben almacenarse en texto claro ni en binario, es decir, que deben estar permanentemente cifradas y, siempre que sea posible (al igual que el resto de datos) en un servidor. En el caso de que fuese preciso su almacenamiento en el dispositivo, se pueden aprovechar los mecanismos de encriptación y almacenamiento de claves proporcionados por el correspondiente sistema operativo.

También resulta conveniente, teniendo en cuenta la categoría de datos personales tratados en la *app*, el que las sesiones de la misma se cierren automáticamente tras cierto tiempo de inactividad. Esto lleva también a plantear dudas sobre la idoneidad de utilizar los llamados *login persistentes*, es decir, aquellos en los que la autenticación permanece pese a cerrarse una sesión o apagarse el dispositivo. Sea cual fuere la decisión del desarrollador sobre la cuestión, lo que sí se deben proteger son los identificadores de sesión, no utilizando los específicos del dispositivo sino otros identificadores que sean aleatorios, específicos (a poder ser) de la propia *app* e impredecibles. Para ello, tal y como recuerda OWASP, hay que considerar que a los generadores de números aleatorios hay que proporcionarles una semilla impredecible (por lo que el solo uso de fecha y hora no es seguro) siendo mucho más recomendable utilizarlos en combinación con otros valores tales como los obtenidos mediante el sensor de temperatura del dispositivo o los del sensor del giroscopio.

Además, se deben prever y hacer frente a los ataques de adivinación o fuerza bruta, estableciendo mecanismos tales como el bloqueo de acceso a la *app* tras un número de intentos de acceso fallidos incorporando, incluso, un sistema CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) que compruebe que los intentos están siendo efectuados por personas y no por computadoras mediante sistemas automatizados.

Un apunte a tener en cuenta, aunque suelen estar basados en *OAuth* y pese a todas las comodidades y facilidades que ofrecen para el usuario, para este tipo concreto de *apps* no parece muy recomendable la implementación de *social login*, el sistema por el que se utilizan las credenciales de acceso que el usuario tuviera en alguna red social (como Facebook, Google+ o Twitter). Y es que, pese a ser actualmente uno de los sistemas de registro más prolíficos y preferidos por los usuarios, ya que además de su simplificación evita lo que se ha denominado *password fatigue* (es decir, el cansancio y agobio del usuario al tener que recordar un número excesivo de contraseñas) sin embargo, teniendo en cuenta que no deja de ser un uso de la *API* correspondiente que tiene sus propios términos y condiciones y que desde un punto de vista de la seguridad requerida para datos especialmente sensibles (como son los que maneja una *app de salud*), no resulta aconsejable que el control absoluto de uno de los aspectos clave en la seguridad recaiga sobre un tercero sin que el responsable del tratamiento pueda hacer nada al respecto en cuanto a política de contraseñas, caducidad, métodos de recuperación, etc.

Mantener la seguridad *back-end* y controlar los sistemas de información donde se realizan los tratamientos de los datos personales recopilados en la *app*.

Las medidas requeridas por el RGPD refieren a todos los sistemas y servicios de tratamiento y, por lo tanto, no se limitaría (en nuestro caso) a la *app de salud* sino a toda la infraestructura que utilice, principalmente, el *back-end* y los sistemas de información que tratan los datos personales recabados por la misma.

Por tanto, hay que evitar lo que algunas empresas de seguridad han bautizado ya como *HospitalGown*[34] porque, al igual que las batas de hospital que cubren por delante pero dejan al descubierto la espalda del paciente, la seguridad en el ecosistema móvil está enfocada principalmente en el propio dispositivo, en las *apps* que ejecuta y en las redes que se conecta dejando a un lado al *back-end* concurriendo, de este modo, en grave riesgo la seguridad de los datos que allí se almacenan y que afectan ya no solo a un determinado usuario sino a la totalidad de quienes utilizan la *app*.

Generalmente, el personal perteneciente a la organización del responsable del tratamiento o a cualquiera de los encargados del tratamiento (por ejemplo, los ya varias veces citados profesionales sanitarios que atienden las consultas de los usuarios o realizan el seguimiento de una monitorización), llevan a cabo el acceso a los datos personales de los usuarios recabados en la *app* a través de aplicaciones web.

Actualmente, estas aplicaciones tienen una arquitectura de tres capas (con un servidor web, servidor de aplicación y servidor de base de datos) sobre la que se debe disponer de mecanismos de seguridad adecuados que garanticen la confidencialidad y la integridad de los datos. Para ello, y además de emplear el puerto TCP/443 (HTTPS) tras el cifrado SSL/TLS o utilizar una red privada virtual (VPN), también se deben implementar mecanismos que permitan la detección y protección a nivel de red, incluyendo elementos de seguridad tradicionales como cortafuegos o sistemas de detección de intrusos. E igualmente, se debe implementar un sistema de gestión de vulnerabilidades y de protección pertinente para hacer frente a ataques directos (tales como accesos no autorizados sobre cualquier elemento que conforma el entorno de la aplicación web), ataques indirectos (donde se atacan otros elementos para que, a su vez, sirvan como herramienta de ataque, como por ejemplos los DNS) o los ataques de denegación de servicio que hacen peligrar la disponibilidad y la resiliencia del servicio al sobrecargarlo hasta llegar, incluso, a provocar su caída.

También se deben aplicar los últimos parches de seguridad en cada uno de los elementos software que forman parte de la plataforma como el software de dispositivos de red y *firewalls*, el propio sistema operativo de los servidores e, incluso el software de la plataforma de desarrollo (Java, PHP, .NET, etc.) así como determinar una planificación o estrategia de copias de seguridad (completas, incrementales, diferenciales) con las que restaurar los datos personales que pudiera haber quedado afectados en un momento dado.

Todas estas medidas, y debido a que en muchas ocasiones el desarrollador no dispondrá de recursos propios para preparar toda esta infraestructura debiendo (como se decía anteriormente) contratar los servicios de proveedores de *hosting* y *cloud computing*, son la que se deben asegurar que figuren en el contrato que hay que regularizar al considerar a estos proveedores como encargados de tratamiento.

Particularmente importante resulta la implementación de medidas de seguridad en la aplicación web sobre la que frecuentemente se realizan tratamientos de datos personales puesto que, en muchas ocasiones, también estos sistemas son desarrollados por los mismos desarrolladores y se incluyen dentro de un mismo paquete de servicios.

[34] https://www.appthority.com/mobile-threat-center/blog/hospitalgown-appthority-discovers-backend-exposure-of-43tb-of-enterprise-data/

En este punto, siguiendo lo indicado hasta el momento por el RDLOPD, es importante hacer hincapié en los siguientes aspectos:

Control de accesos:
Una de las principales medidas para la protección de la información es un riguroso control de accesos, de manera que los datos solo sean consultados y registrados por las personas autorizadas, en el momento pertinente y de acuerdo con el método preestablecido (Martínez Santiago & Rojas de la Escalera, 2014).

Habitualmente, los derechos de acceso (lectura, escritura, ejecución, edición y eliminación) se limitan atendiendo al principio de "mínimo privilegio", por el cual los privilegios de cada usuario se reducen al mínimo estrictamente necesario para cumplir sus obligaciones (acotando así los daños ocasionados de forma accidental o intencionada); de "necesidad de conocer", limitando los privilegios de modo que los usuarios solamente accederán al conocimiento de aquella información requerida para cumplir sus funciones; y de "capacidad de autorizar", por el que exclusivamente el personal con competencia para ello puede conceder, alterar o anular la autorización de acceso a los recursos (ENS 4.2.2)

Para facilitar la asignación de los permisos, suele utilizarse un sistema RBAC (*Role-Based Access Control*) en el que se definen roles para diferentes usuarios con un perfil similar en la organización, asignándose cada usuario a un (o varios) de esos roles.

Identificación y autenticación:
En este entorno donde acceden diferentes personas pueden acceder a diversidad de datos personales, es especialmente relevante verificar que dichas personas a las que se les ha otorgado la autorización pertinente, sean efectivamente quienes afirman ser para que, de este modo, puedan ejercer dichas competencias asignadas y que su identidad le confiere posibilitando, además, garantizar el no repudio de las acciones llevadas a cabo.

Para este caso, sí que resulta totalmente pertinente y necesario la utilización de mecanismos de autenticación robustos (como los ya citados de 2FA) y, fundamentalmente, sistemas de identificación seguros como el DNI-e o los certificados electrónicos, y a poder ser, en un sistema de autenticación *Single Sign-On* (SSO) por el que se habilita la autenticación en diferentes sistemas con una sola instancia.

Registro de accesos:
Constituido como un adecuado sistema de rastreo de las acciones llevadas a cabo sobre los datos personales en un sistema de información siendo totalmente auditable. El RDLOPD preveía su implantación entre las medidas de seguridad de nivel alto (art. 103) instando a que "de cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado" y a que "en el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido". También se señalaba que estos mecanismos que permiten el registro de accesos "estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos" siendo este responsable de seguridad quien "se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados" y quedando estipulado "el período mínimo de conservación de los datos registrados será de dos años".

La anonimización y seudonimización como medidas de seguridad en los tratamientos de datos personales ulteriores y no como técnicas a emplear para evitar el cumplimiento normativo en materia de protección de datos.

Los datos anónimos son aquellos sobre los que no es posible identificar al interesado de ninguna manera mientras que los datos seudonimizados son aquellos en los que se ha sustituido alguno de sus atributos (normalmente uno que sea único) por otro en un registro de tal manera, que no puedan atribuirse a un interesado sin utilizar información adicional.

En base a estas definiciones, se puede determinar *a priori* que los datos anónimos, al no tratar datos de personas identificadas o identificables, quedan excluidos de los principios de protección de datos y, por tanto, del ámbito de aplicación del RGPD mientras que la seudonimización, que si permite singularizar a los interesados y vincularlos entre conjuntos de datos diferentes pudiéndose producir la identificabiliad, sí que entra dentro del ámbito de aplicación del RGPD.

En un entorno idílico y bajo una interpretación de los principios PbD, se debería facultar al usuario a utilizar la *app* de forma anónima, es decir, sin que tenga que registrarse o proporcionar algún tipo de información que lo pudiera identificar en un momento dado; o, en su defecto, seudónima, mediante el registro de un identificador construido voluntariamente por el usuario o por un sistema de valores únicos automatizado y aleatorio (no admitiéndose otros datos como un número de teléfono o el email, sobre todo si está conformado con nombres, apellidos o fechas de nacimiento, ya que, como se ha indicado anteriormente son datos personales en sí mismos).

Sin embargo, y más en un ámbito como el de las *apps de salud*, el llevar a la práctica estas opciones entraña ciertas dificultades puesto que la prestación de atención sanitaria requiere que de forma univoca e inequívoca se pueda identificar al individuo al que se le presta asistencia. Igualmente se requiere esta identificación para las *apps* que ofrecen la gestión de trámites, el acceso a una HCE, o para la monitorización y seguimiento de tratamientos que incluyen la asistencia de profesionales sanitarios. O, simplemente, porque el responsable del tratamiento por las razones legítimas que fuesen tenga interés por recabar los datos personales de quiénes utilizan la *app*. O, incluso, porque sean los propios usuarios los que estén interesados en proporcionarlos pensando así que existe una mayor personalización en el servicio.

Por cualquiera de estos supuestos, el uso cotidiano de la *app* (incluyendo todas las circunstancias que pudieran requerir cualquier tipo de tratamiento en "tiempo real") con datos anonimizados es complejo y está circunscrito a limitadas funcionalidades y, puesto que el uso de datos seudonimizados requiere la implementación de las salvaguardas requeridas, donde parece que es más factible y pueden resultar más eficaces estas técnicas, es en los tratamientos ulteriores y en la conservación requerida de los datos, tratando de que sean ejecutadas con la mayor celeridad.

A este respecto, hay que tener en cuenta varias consideraciones y es que estas técnicas ya implican intrínsecamente un tratamiento posterior de los datos personales y, por tanto, "deben satisfacer el requisito de compatibilidad teniendo en cuenta las circunstancias y los fundamentos jurídicos de dicho tratamiento" (WP216).

Por otra parte, la AEPD en sus *Orientaciones y garantías en los procedimientos de anonimización de datos personales* recuerda que, aunque la finalidad de los procesos de anonimización no es otra que la de "eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados", se debe mantener "la veracidad de los resultados del tratamiento de los mismos". Es decir, que se "debe garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleve una distorsión de los datos reales".

Como señalaba el GT29 en su extenso *Dictamen 05/2014 sobre técnicas de anonimización*, la anonimización efectiva es francamente difícil de lograr, máxime en un entorno como la *mHealth* donde se produce una continua, diversa, masiva y ubicua recogida de datos que combinándolos (incluso con otras fuentes) pueden llevar a que una persona pueda ser identificada, por lo que antes de aplicar una técnica concreta se ha de determinar el grado de solidez que ofrece la misma así como el estado actual de la tecnología y los siguientes tres riesgos claves:

- *Singling out* (singularización), o la capacidad de poder aislar algunos o todos los datos de un mismo individuo dentro del fichero.

- *Linkability* (vinculabilidad), o la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas. Si el atacante puede determinar (por ejemplo, mediante un análisis de correlación) que dos registros están asignados al mismo grupo de personas pero no puede singularizar a las personas en este grupo, entonces la técnica es resistente a la singularización, pero no a la vinculabilidad.

- *Inference* (inferencia), o la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros atributos.

El GT29 en el citado documento analizaba las principales técnicas de anonimización existentes, dividiéndolas en dos grandes grupos:

- Las técnicas de "asignación al azar" o de *randomización*: utilizadas con el fin de eliminar el vínculo entre los datos y los individuos de tal manera que, si los datos son suficientemente inciertos o ambiguos, ya no se pueda hacer referencia a un individuo concreto. A esta familia, pertenecerían técnicas como la "adición del ruido", por la que se modifican los atributos en el conjunto de datos haciéndolos menos exactos; la de "permutación", por la que se mezclan los valores de los atributos en una tabla para que algunos de ellos queden artificialmente vinculados a diferentes titulares de los datos; o la de "privacidad diferencial", que a su vez utiliza el añadido de ruido en la generación de vistas de un conjunto de datos, en la cantidad y forma que se determine sin llegar a modificar los datos originales, por lo que únicamente se enmascara la identidad de cada uno de los individuos en los resultados de las consultas.

- La otra familia, aglutinaría las técnicas de "generalización" consistentes en generalizar o diluir los atributos de los interesados modificando las respectivas escalas u órdenes de magnitud (por ejemplo, sustituyendo una ciudad por una región, o una semana por un mes). Así aparecen las técnicas de "agregación" y

de “anonimato k” que tienen el objetivo de impedir que un interesado sea singularizado cuando se le agrupa junto con, al menos, un número k de personas, haciéndose efectiva cuando los atributos se generalizan hasta tal punto que todas las personas acaban compartiendo el mismo valor; o las técnicas de “diversidad L” y “proximidad T” que extienden y dan complejidad a las técnicas anteriores.

Pues bien, el GT29 acabaría concluyendo (como se puede observar en la Tabla 3) que ninguna de estas técnicas cumplían al 100% los criterios de anonimización efectiva porque “no es posible singularizar a una persona; no existe vinculabilidad entre los registros de una misma persona, y no se puede inferir información sobre una persona”.

Técnica	**¿Existe riesgo de singularización?**	**¿Existe riesgo de vinculabilidad?**	**¿Existe riesgo de inferencia?**
Adicción de ruido	Si	Puede que no	Puede que no
Sustitución	Sí	Sí	Puede que no
Agregación y anonimato k	No	Sí	Sí
Diversidad l	No	Sí	Puede que no
Privacidad diferencial	Puede que no	Puede que no	Puede que no
Hash / Token	Sí	Sí	Puede que no
Seudonimización	Sí	Sí	Sí

Tabla 2: Fortalezas y debilidades de las técnicas según el *Dictamen 05/2014 sobre técnicas de anonimización* del GT29

Al no garantizar completamente la no reidentificación de las personas, como recomienda la AEPD, siempre que se vaya a utilizar esta técnica es “necesario sustentar la fortaleza de la anonimización en medidas de evaluación de impacto (EIPD), organizativas, de seguridad de la información, tecnológicas y, en definitiva, cualquier medida que sirva tanto para atenuar los riesgos de reidentificación de las personas como para paliar las consecuencias de que éstos se materialicen”.

Por su parte, y tal y como ya se ha comentado, la seudonimización no es anonimización así que, con la aplicación de técnicas como el cifrado con clave secreta o almacenada o mediante función *hash* o, incluso mediante la descomposición en *tokens* en ningún caso se consigue la anonimización de los datos y, consiguientemente, se debe cumplir con lo estipulado en el RGPD para proteger los datos personales.

Conclusivamente, la anonimización como la seudonimización son excelentes métodos para reducir los riesgos derivados del tratamiento de datos de carácter personal de los interesados afectados y para ayudar a los responsables y a los encargados del tratamiento a cumplir con sus obligaciones de protección de los datos no debiéndose ser vistas como vías para lograr la exención del cumplimiento de la legislación sino, más bien, como medidas de seguridad útiles, efectivas pero no definitivas al encontrarse limitadas inherentemente al avance de la tecnología.

Obligatoriedad de notificar las violaciones de seguridad de los datos personales a la autoridad de control competente.

Finalmente, y aun habiendo implantado la mejor infraestructura no se puede garantizar que se produzcan violaciones en la seguridad de los datos personales, entendiendo estas como “toda violación de la seguridad que ocasione la destrucción, pérdida o alteración

accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos" (art 4.12 RGPD).

Así que el principio de responsabilidad proactiva implica que, en caso de producirse una violación de la seguridad de los datos personales, se debe proceder a notificarla ante la autoridad de control competente y ante los interesados (excepto en los casos contemplados que se detallarán).

Esta obligación no es ni mucho menos una novedad ya que estaba prevista en el Reglamento (UE) nº 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la *Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas* y en la *Ley 9/2014, de 9 de mayo, General de Telecomunicaciones*, habiendo habilitado la propia AEPD un sistema online para comunicarle dichas violaciones.

Para afrontar estas situaciones, y siguiendo lo estipulado por el RGPD, las directrices del GT29 emanadas en su *Dictamen 03/2014 sobre la notificación de violación de datos personales* (WP213) y las recomendaciones de la AEPD, se puede seguir un protocolo de actuación parecido a este que a continuación se presenta:

1) Constatar certeramente que se ha sufrido una violación de seguridad sobre datos personales y no sobre otro tipo de datos (en cuyo caso podría implicar otro tipo de notificaciones de incidentes de seguridad pero no relacionadas con la protección de datos personales) debiendo tener suficiente conocimiento de su naturaleza y alcance pues como señala la AEPD, "la mera sospecha de que ha existido una quiebra o la constatación de que ha sucedido algún tipo de incidente sin que se conozcan mínimamente sus circunstancias no deberían dar lugar, todavía, a la notificación, dado que en esas condiciones no sería posible, en la mayoría de los casos, determinar hasta qué punto puede existir un riesgo para los derechos y libertades de los interesados".

2) Investigar las características de la violación, el volumen y categoría de datos afectados y analizar las consecuencias que podría tener para los interesados.

   Las violaciones se examinan con arreglo a los tres criterios de seguridad clásicos, es decir, si se ha producido una violación de la disponibilidad, correspondiendo a la destrucción accidental o ilegal o a la pérdida de datos personales; de la integridad, a la alteración de datos personales; y/o de la confidencialidad, a la revelación no autorizada de datos personales o al acceso no autorizado a los mismos.

   Hay que tener en cuenta que la brecha puede haberse producido sobre los recursos propios de un encargado del tratamiento, por lo que una vez constatada la violación de datos personales, éste debe alertar e informar al responsable del tratamiento, según lo estipulado en el contrato, para que "tome las riendas" de la situación y, en su caso, adoptar conjuntamente las medidas correctoras oportunas.

   La AEPD recomienda ponerse en contacto con ella "tan pronto como existan evidencias de que se ha producido alguna situación irregular respecto a la seguridad de los datos" en caso de quiebras que por sus características tuvieran un gran impacto o un alto riesgo, entendiéndose éste en el sentido que ocasione daños a los

interesados (desvelarse información confidencial, difusión masiva de datos sensibles como los de salud o perjuicios económicos para los afectados).

3) Aplicar las medidas técnicas u organizativas apropiadas, siguiendo el SGSI predefinido, para atajar la brecha de seguridad que se haya producido.

   En según qué circunstancias, las medidas correctoras pueden pasar por lanzar una actualización de la *app* con las modificaciones pertinentes o, incluso, requerir que los usuarios deban realizar determinadas acciones como, por ejemplo, autentificarse nuevamente estableciendo obligatoriamente una nueva contraseña por haberse comprometido o manipulado las existentes. En otras, quizás no se pueda resolver con los medios propios del responsable del fichero debiendo recurrir a expertos en ciberseguridad o, sobre todo si el responsable del tratamiento es una administración pública (al ser de obligado cumplimiento por el ENS), al *Computer Emergency Response Team* (CERT) del CCN.

4) Proceder, sin dilación y un plazo menor a 72 horas después de tener constancia de la brecha, a la notificación preceptiva de la violación de seguridad a la AEPD, mediante el sistema que tenga implementado en su sede electrónica (actualmente ya posee uno[35] pero seguramente deberá adecuarse a lo que disponga el GT29 quien está preparando un formulario estandarizado a nivel europeo).

   Dicha notificación, y como dispone el RGPD en su art. 33.3, debe incluir un contenido mínimo que incluya la naturaleza de la violación de seguridad de los datos personales, las categorías de los datos, el número de registros afectados y a cuántas personas aproximadamente les corresponden. Además, se debe comunicar el nombre y datos de contacto del Delegado de Protección de Datos, las posibles consecuencias de la violación y describir las medidas adoptadas o propuestas para solventar la quiebra incluyendo, si proceden las medidas adoptadas para mitigar los posibles efectos adversos. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

5) Proceder a comunicar la violación de la seguridad de los datos a los interesados cuando entrañe un alto riesgo para los derechos y libertades de las personas físicas, para lo cual se debe determinar previamente si ésta comunicación se requiere obligatoriamente puesto que el RGPD exceptúa diferentes casos:

   a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

   b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo.

   Pese a que no se requiriese legalmente esta notificación, como recomendaba el GT29, constituye una "buena práctica" en pro de la deseable confiabilidad, la comunicación a los interesados de todas las violaciones (o, por lo menos, las más

[35] http://sedeagpd.gob.es/sede-electronica-web/vistas/formQuiebraSeguridad/procedimientoQuiebraSeguridad.jsf

relevantes). Para ello, se pueden utilizar como medios los correos electrónicos registrados y, aún mejor, a través de *notificaciones push* en la propia *app* sirviendo así también de justificación para las medidas correctoras en las que deba intervenir el propio usuario (como las citadas anteriormente).

Si la comunicación supone un esfuerzo desproporcionado (cosa improbable en este ámbito eminentemente interactivo), el RGPD prevé sustituir la notificación individual por una comunicación pública (por ejemplo a través de la página web o redes sociales corporativas) en la que se informe de manera igualmente efectiva a los interesados.

3.6. Facilitar el ejercicio de los derechos de los usuarios

Cuando los datos personales son tratados mediante medios electrónicos (lo que sucede con las *apps*) el RGPD obliga al responsable del tratamiento a proporcionar las vías pertinentes por este mismo medio para que los interesados puedan presentar sus solicitudes referentes al ejercicio de los derechos de acceso, rectificación, supresión, limitación al tratamiento, portabilidad de los datos, oposición y a las decisiones individuales automatizadas.

El GT29 ya recomendaba "el diseño y la aplicación de herramientas de acceso en línea simples pero seguras" que fuesen "accesibles preferiblemente dentro de cada aplicación o a través de un enlace a un mecanismo en línea mediante el que los usuarios puedan acceder inmediatamente a todos los datos objeto de tratamiento y a las explicaciones correspondientes" (WP202).

Implementar opciones en la propia *app* desde las que se faciliten el ejercicio de los distintos derechos.

En el caso de las *apps*, el entorno tecnológico invita claramente a que el ejercicio de los derechos sea lo más fácil y accesible posible, pudiendo implementarse en la interfaz opciones que posibiliten el ejercicio de los derechos, y además, hacerlo tras verificarse la identidad del interesado garante del "personalísimo" derecho (que dice la LOPD) puesto que, como recuerda el GT29, "podría bastar con la autentificación en lugar de la identificación completa", lo que ya se requiere para utilizar y acceder a la *app*.

Para ello en la *app* se podría integrar un *Panel de Privacidad*, fácilmente accesible desde cualquier *pantalla* de la misma mediante un *acceso rápido*, posibilitando al usuario el cumplimentar una serie de formularios ya estructurados (de similar manera a como se han tenido previstos habitualmente en formato papel o en otros formatos electrónicos editables) referentes a cada uno de los derechos contemplados en el RGPD.

Complementariamente, para facilitar a los usuarios la resolución de posibles dudas sobre sus derechos e inicios de trámites que finalmente den como resultado la denegación del ejercicio, puede ser de cierto interés que dentro de la referida sección de *Preguntas Frecuentes* y además de explicar qué es cada derecho e informar sobre aspectos preceptivos como "la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento" y "el derecho a presentar una reclamación ante una autoridad de control" (redundando en el también

objetivo de empoderamiento del usuario que requiere PbD), se detallasen las distintas restricciones que sobre el ejercicio de los derechos puedan derivarse por encontrarse los datos tratados sujetos a diferentes leyes del ordenamiento jurídico español.

Sin embargo, implementar únicamente medidas meramente informativas a través de la *app* (aun suponiendo una mejora considerable al habitual recurso de brindar, a lo sumo, una dirección de email a la que el interesado se debe dirigir), parece desaprovechar las posibilidades que ofrece este entorno tecnológico para, en muchas ocasiones, disipar verazmente y en "tiempo real" las preocupaciones de los usuarios sin que tengan que llegar a iniciar un trámite burocrático sobre algunos de los derechos que le amparan.

Implementar opciones automatizadas que permitan al usuario tener conocimiento sobre el tratamiento llevado a cabo sobre sus datos personales sin que llegue a iniciarse el proceso administrativo de ejercicio de los derechos.

Así por ejemplo, en el ejercicio del derecho de acceso y según dispone el art. 15.1 del RGPD, el responsable del tratamiento deberá confirmar al interesado si se están tratando o no datos personales que le conciernen así como ofrecerle la siguiente información: los fines del tratamiento; las categorías de datos personales de que se trate; los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales (en particular destinatarios en terceros u organizaciones internacionales); de ser posible, el plazo previsto de conservación de los datos personales (o, de no ser posible, los criterios utilizados para determinar este plazo); y la existencia de decisiones automatizadas, incluida la elaboración de perfiles.

A este respecto, y teniendo en cuenta que se debe llevar el registro de las actividades de tratamientos y que, como indicaba el RDLOPD (e incluido como "buena práctica" en este trabajo) se debería adoptar un log de accesos, parece factible implementar una opción en la *app* (complementaria al ejercicio del derecho de acceso) que ofrezca regularmente los accesos realizados a sus datos y los tratamientos llevados a cabo con los mismos.

Este procedimiento, que ya fue sugerido por el GT29 en su *Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME)* a fin de suscitar la confianza del usuario, puesto que "una lista de las personas o instituciones que han accedido a su expediente tranquilizaría a los pacientes por lo que respecta a su capacidad de saber lo que sucede con sus datos en el sistema de HME" (WP131), permite ofrecer a los usuarios la trazabilidad sobre el acceso y el tratamiento de sus datos, posibilitando la verificación de la legitimidad de los mismos al ejercer el propietario de los datos como una especie de *auditor del sistema*.

Pareciendo evidente que esta medida reforzaría las garantías dirigidas a la protección de datos así como aumentaría el nivel de transparencia y lealtad del responsable del tratamiento al poner en evidencia que no tiene nada que esconder. Adicionalmente hay que considerar que, cuando se presta cualquier tipo de asistencia sanitaria con independencia del medio empleado (como sucede en algunas *apps* cuya funcionalidad principal sea la realización de consultas a profesionales sanitarios debiendo, en muchos casos, proporcionar diversas informaciones que en su conjunto conforman una historia clínica a todos los efectos al encontrarse estructuradas), el paciente tiene derecho "a conocer el nombre, la titulación y la especialidad de los profesionales sanitarios que les

atienden" (art. 5.e de la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias).

Sin embargo, a lo largo de los años han existido no pocas controversias al respecto siendo la propia AEPD la que en su *Informe Jurídico 167/2005, sobre Naturaleza y alcance del Derecho de Acceso* al que alude en su jurisprudencia en reiteradas ocasiones (las últimas en este mismo 2017[36]), la que ha dictaminado que "el derecho concedido al interesado por la Ley únicamente abarcaría el contenido de la información sometida o tratamiento, pero no qué personas, dentro del ámbito de organización del responsable del fichero han podido tener acceso a dicha información".

Otras voces, por el contrario, se posicionan favorablemente a la implantación de este procedimiento de trazabilidad argumentando, entre otros aspectos ya comentados, que si está tipificado como delito el "que sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos" agravándose cuando "afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual" (art. 197 del Código Penal), parece congruente que el paciente pueda tener conocimiento de la identidad de los autores que hayan procedido a realizar accesos indebidos (máxime cuando, como ya se ha explicado, se deben implantar medidas de seguridad físicas y lógicas para que esto no ocurra y se debe identificar cada acceso) con el fin de evitar que estos actos quedasen impunes (Gallego Riestra, 2012; González García, 2014).

Actualmente en el sistema de Historia Clínica Digital del Servicio Nacional de Salud (HCDSNS) ya se encuentra disponible una funcionalidad acorde a la propuesta del GT29 sobre la que se le han adoptado las directrices de la AEPD, de tal manera que se ofrece "información relativa al momento en que se realizó el acceso, servicio de salud, centro sanitario y servicio desde el que se realizó cada acceso, así como las características del documento electrónico accedido".

Siguiendo este modelo, se podría implementar una opción en el propio sistema (en este caso, la *app*) por la que el responsable del tratamiento voluntariamente pone a disposición de sus usuarios una serie de informaciones sobre los tratamientos llevados a cabo en sus datos personales, pudiendo ser los siguientes campos:

- Fecha y Hora, en la que se haya llevado a cabo el tratamiento.

- Tipos de datos tratados o apartados estructurados que hubiese en la *app*, como por ejemplo la ficha de datos personales, ficha de historial médico, ficha de tratamientos actuales, registro de niveles de glucemia.

- Tipo de tratamiento, es decir, si se ha accedido para consultar (en el caso, por ejemplo, de requerirlos para una prestación sanitaria o el seguimiento de una determinada monitorización siendo éste el motivo que habría que informar en el siguiente ítem), si se han empleado para fines secundarios, si se han comunicado a un tercero, o si se han llevado a cabo decisiones automatizadas.

- Finalidad o motivo por el cual se han tratado.

[36] Resolución nº: R/01364/2017

- Identificación de quién realiza el tratamiento, que sin entrar en la polémica de señalar la persona concreta de la organización del responsable o encargado del tratamiento, si al menos especificase la persona jurídica que lo haya llevado a cabo tanto si ha sido el propio responsable del tratamiento, alguno de los encargados del mismo o, aún más si cabe, si ha sido un tercero.

Asimismo, el derecho de acceso incluye que el responsable del tratamiento facilite una copia de los datos personales objeto de tratamiento. Puesto que el art. 15.3 del RGPD ampara que cuando la solicitud se realice por medios electrónicos esta información se pueda facilitar en un formato electrónico de uso común, y puesto que los datos sobre los que se pueden llevar a cabo tratamientos son, principalmente, los que se encuentran registrados en la propia *app*, una forma de cumplir con este requisito sería la de implementar un sistema de exportación de datos en formato abierto (TXT, RTF, HTML, PDF) que se pueda descargar e incluso imprimir, siendo en todo caso está opción, diferente al nuevo derecho de portabilidad previsto por el RGPD de los datos que, seguidamente, se detallará.

Por su parte, el derecho por el que los interesados puedan obtener "sin dilación" la rectificación de los datos personales que sean incorrectos, inexactos o incompletos, parece estar asegurado en un entorno como el de las *apps* a través de las propias opciones básicas que permitan la edición o modificación de los datos registrados.

Para el ejercicio de los derechos de oposición o limitación del tratamiento, se podrían habilitar opciones de marcas lógicas por categorías de datos, finalidades de tratamiento, periodos de fechas u otras opciones en el recomendado *Panel de Privacidad*. Aunque, al igual que en el derecho de supresión, pueden surgir múltiples y diferentes aspectos a tener en cuenta que derivan en que no todo sea tan sencillo como lo que teóricamente pudiera parecer.

Lo lógico sería que, así como los usuarios encuentran facilidades para instalar y empezar a usar la *app* (iniciándose la recogida y almacenado de datos personales) también se debieran proporcionar mecanismos sencillos y ágiles para ejercer el derecho de supresión. De hecho, el GT29 instaba a que el derecho de supresión pueda ejercerse con el mero hecho de desinstalar la *app*, procediendo entonces a eliminar todos los datos personales "incluidos aquellos almacenados en los servidores de los responsables del tratamiento de datos" (WP202) sugiriendo que los fabricantes de sistemas operativos enviasen a los desarrolladores "una señal cuando el usuario desinstala una aplicación mediante una API".

Sin embargo, generalmente esto no se lleva a la práctica, principalmente porque los datos personales que se almacenan en servidores habitualmente quedan asociados a las cuentas creadas por los usuarios al proceder a su registro en la *app* no quedando asociados al dispositivo sino a dicho perfil del usuario garantizando de, esta manera, que ante cualquier problema surgido en el dispositivo (rotura, desinstalación accidental de la *app*, etc.) los datos no se pierdan y que al reinstalar la *app* en el mismo dispositivo o, incluso, en otro, sigan apareciendo todos los datos registrados. Es decir, esta funcionalidad (inicialmente buena, pues garantiza la conservación de los datos) debe controlarse de forma que el usuario pueda dar de baja su perfil en cualquier momento y de una forma sencilla y accesible desde la propia *app*, sin tener que acceder a otro sistema de información (como una web, aunque también pueda hacerse a través de la misma).

Más complejo es afrontar lo que se deriva del análisis de este "derecho al olvido" previsto en el RGPD y que sustituye al llamado "derecho de cancelación" de la anterior Directiva (y, por tanto, de la LOPD).

Inicialmente, entre ambos derechos existe una importante diferencia ya que el RGPD habla directamente de supresión mientras que en la LOPD la cancelación daba "lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas" (art. 16.3 LOPD), procediéndose a la supresión únicamente cuando se cumpliera dicho plazo.

El RGPD estipula en su art. 17 que "el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan" estableciéndose la obligación de suprimir los datos personales cuando ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo, el interesado retire el consentimiento en que se basa el tratamiento, el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento, los datos personales hayan sido tratados ilícitamente o sin la obtención, en caso de menores, del consentimiento del titular de la patria potestad o tutela.

Sin embargo y pese a lo que pudiera parecer, el apartado 3 del mismo art. 17 del RGPD restringe la aplicación de este derecho cuando el tratamiento sea necesario para:

- ejercer el derecho a la libertad de expresión e información;

- para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

- por razones de interés público en el ámbito de la salud pública cuando "el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario" o "el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios".

- con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad;

- para la formulación, el ejercicio o la defensa de reclamaciones.

Aún sin considerar la última excepción (más comprometida de dilucidar), rápidamente se puede deducir que muchas de las *apps de salud* se les pueden aplicar estas excepciones y, por tanto, los usuarios no pudieran proceder a la eliminación directa de

sus datos personales en el momento que ellos estimasen oportuno (normalmente, cuando ya no deseasen seguir utilizando la *app*).

En las *apps de salud* más complejas donde los datos recopilados van a formar parte de una historia clínica (por ejemplo, la monitorización de ciertos parámetros como el nivel de glucemia o el INR o el seguimiento de ciertos tratamientos) o si se utiliza la *app* en un contexto de asistencia sanitaria prestada por centros, servicios y profesionales sanitarios, le es aplicable tanto la *Ley General de Sanidad 14/1986, de 25 de abril como la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de sus derechos y obligaciones en materia de información y documentación clínica* así como las diversas normas en relación con la sanidad dictaminadas por las comunidades autónomas y, por tanto, el periodo de conservación de los datos quedaría regulado por las mismas, requiriéndose un plazo "como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial" (art. 17 LBAP, siendo incluso superior el tiempo marcado en otras normativas autonómicas como en la en la *Ley 16/2010 de Cataluña* donde se estipulan veinte años desde su muerte estipulado).

La conclusión es que hay que contemplar (y hacer que los usuarios lo comprendan) que en, no pocas ocasiones, el ejercicio de supresión no va a implicar la eliminación directa y en el acto de los datos sino que, en realidad, lo que se estará haciendo es ejercer un derecho de "supresión cautelar" (con similares resultados a los obtenidos tras el ejercicio de los derechos de oposición o limitación de tratamiento) ofreciéndose, en el mejor de los casos, un bloqueo en el acceso a los datos o un traslado a otro sistema de almacenamiento apartado del habitual en el que se realizan los tratamientos.

Uso de estándares para garantizar el derecho a la portabilidad de datos.

El RGPD habilita a que el usuario de la *app* tenga derecho a recibir los datos personales que le incumban y que haya facilitado (o se hayan recolectado automáticamente) a través de la misma en "un formato estructurado, de uso común y lectura mecánica", y a transmitirlos a otro responsable del tratamiento (incluyendo la remisión directa de responsable a responsable cuando sea técnicamente posible).

El considerando 21 de la Directiva 2013/37/UE17 define "legible por máquina" como "un formato de archivos estructurado de forma que las aplicaciones informáticas puedan fácilmente identificar, reconocer y extraer datos específicos, inclusive exposiciones personales de hechos, y su estructura interna. Los datos codificados en archivos que están estructurados en un formato legible por máquina son datos legibles por máquina. Los formatos legibles por máquina pueden ser de uso libre o patentados; pueden ser estándares formales o no".

Por tanto, la provisión de los datos en formatos como los antes citados (PDF y similares) para facilitar el derecho de acceso, no son adecuados para el ejercicio de la portabilidad puesto que carecen de suficiente estructuración y los datos no pueden extraerse fácilmente de manera automatizada, recomendando el propio GT29 la utilización de formatos abiertos tales como XML, JSON o CSV (WP242)

Puesto que desde el propio RGPD se alienta a los responsables a usar formatos interoperables que posibiliten la portabilidad de los datos, parece buen momento para afrontar el reto de la ausencia de normas "que obliguen a la interoperabilidad entre las

soluciones y los dispositivos de sanidad móvil y que impiden la innovación y las economías de escala" y que ya ponía de manifiesto el *Libro Verde*.

De esta manera, y dependiendo de la funcionalidad y de los tipos de datos tratados en la *app* y, como se decía anteriormente (cuando se hablaba de la usabilidad) previa dotación de una estructura suficientemente preparada para este fin (debiéndose analizar con anterioridad y no como un añadido final pues puede resultar incompatible *a posteriori*), se pueden utilizar estándares para el intercambio de datos de la historia clínica electrónica (*HL7 CDA, OpenEHR, CEN/ISO 13606*), de interoperabilidad de dispositivos médicos (*IEE11073*) o de imagen médica (*DICOM*) con los que, adicionalmente, se contribuya (como ya ha planteado Apple en su *HealthKit* para *iOS 10*, al anunciar la implementación de *HL7 CDA*[37]) a que los usuarios faciliten sus datos a otros proveedores de servicios fuera incluso del ámbito móvil, tal como médicos de atención primaria y atención especializada que podrían incorporar los datos gestionados en *app* a la Historia Clínica Electrónica "oficial" (la del Sistema Nacional de Salud o la que tuviera abierta en cualquier otra entidad privada) o, al revés, pudiendo recibir en su propio dispositivo datos médicos que le atañen procedentes de resultados de pruebas analíticas, diagnósticas, etc.

Y, finalmente, concienciar al usuario sobre el valor que tienen sus datos personales y la importancia de protegerlos adecuadamente.

El séptimo y último principio del PbD hace referencia precisamente a colocar en el centro al usuario. Pues bien, que mejor manera de hacerlo que concienciándole sobre el valor que tienen sus datos personales instándoles a que, la mejor protección de los mismos, es la que ellos mismos pueden hacer.

Se debería, por tanto, proporcionarles información sobre las opciones de privacidad y seguridad y las funciones y servicios que incorpora la *app*, cómo activarlas y administrarlas. Y, aunque pudiera parecer presuntuoso, tampoco estaría de más poner a disposición de los usuarios informaciones sobre cómo proteger su privacidad en general, recomendándoles la instalación de antivirus y cortafuegos en sus dispositivos, a mantener todo el software actualizado, a realizar copias de seguridad, a cifrar la información sensible, a monitorizar el uso de recursos, a deshabilitar los sistemas de comunicación cuando no se utilicen o a revisar, y en su caso, eliminar la información confidencial antes de desechar o reutilizar el dispositivo.

En definitiva, poco esfuerzo puede suponer el colocar en las opciones de ayuda, en las citadas F.A.Q., en el propuesto *Panel de Privacidad* o en cualquier otro lugar de la *app* o, incluso, de la web corporativa, enlaces a las webs de la AEPD o de la Oficina de Seguridad del Internauta de INCIBE donde, entre otros muchos aspectos, se pueden descargar documentos como la *Guía de Privacidad e Internet* además de videos e interesantes infografías que proporcionan las pautas necesarias para utilizar los distintos servicios sin comprometer la seguridad y privacidad.

[37] https://9to5mac.com/2016/06/15/hands-on-hl7-ccd-health-records-ios-10-health-kit/

Conclusiones

El desarrollo de *apps* en el ámbito de la *mHealth* se encuentra en plena eclosión, habiendo cada vez más aplicaciones disponibles que abren un simpar abanico de posibilidades de transformación de la prestación de asistencia sanitaria.

Sin embargo, pese a todos potenciales beneficios que puede llegar a ofrecer, la *mHealth* y, consiguientemente, las *apps de salud* todavía presentan una serie de graves problemas y preocupaciones. La revisión de la literatura científica permite identificar que, en el variopinto ecosistema y en la compleja arquitectura de las *apps de salud*, aparecen importantes riesgos para la privacidad y la seguridad de los datos personales de los usuarios causados, principalmente, por la ausencia de información transparente a los usuarios, la maximización de los datos y multiplicidad de finalidades y por las insuficientes y, en muchos casos, deficientes medidas de seguridad.

Puesto que a través de las *apps de salud* se procede al registro y almacenamiento de datos de una persona física identificada o identificable, la normativa en materia de protección de datos es aplicable desde el momento en que la *app* genera tráfico de datos personales y los datos son accedidos o tratados por cualquier entidad jurídica distinta al titular de los mismo. De esta manera, se debe aplicar el nuevo Reglamento General de Protección de Datos (RGPD) incluso aunque el responsable del tratamiento no estuviera establecido en el territorio de la Unión Europea, puesto que utiliza para el tratamiento de datos medios situados en el territorio de cualquiera de los Estados miembros como son los propios dispositivos pertenecientes a usuarios que si residen en dichos lugares.

El RGPD determina que los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado; recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; serán exactos y, si fuera necesario, actualizados; serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; y tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Además, introduce los conceptos de responsabilidad y privacidad desde el diseño, principios que deben conformarse como la base sobre la que se desarrollen las *apps de salud*. Así, los desarrolladores han de tener presente la privacidad y el cumplimiento de los requerimientos de la normativa de protección de datos desde la propia conceptualización de la *app* y realizando una *Evaluación de Impactos sobre la Protección de Datos* antes de llevar a cabo ningún tratamiento. Además, se deben observar para con la autoridad competente una serie de obligaciones como designar un delegado de protección de datos o proceder a la exhaustiva selección de los encargados de tratamiento, estableciendo una relación contractual con los que se consideren más adecuados.

Con la adopción de la responsabilidad proactiva ya no es suficiente con no incumplir la normativa sino que se debe acreditar el cumplimiento del RGPD. Para ello, es

recomendable la adopción de un *Sistema de Gestión de Seguridad de la Información* así como someterse a procesos que posibiliten la transmisión de confiabilidad a los usuarios tales como la publicación de la *app* en tiendas oficiales, la adhesión a códigos de conducta autorregulatorios y, principalmente, a través de someter a la *app* a procesos de acreditación de calidad como *AppSaludable* o *AppSalut* o a la *certificación CE* de conformidad de la *app* como producto sanitario.

También han de cumplir con el deber de informar al usuario, proporcionándole la información antes de que proceda a la instalación de la *app* y en el momento de iniciarse por primera vez. Se ha de tener presente que el deber de información implica lealtad y transparencia, proporcionando aquella información complementaria que pueda resultar relevante (inclusive la técnica) pero siempre presentándola en los momentos adecuados en los que se requiere un registro de datos de una forma legible, accesible, entendible, adecuada y adaptada, sin sobrecargar al usuario con engorrosos y largos textos, utilizando iconos y estructurando la información en niveles.

Los tratamientos de los datos personales deben estar legitimados lo que, principalmente, se conseguirá mediante la obtención del consentimiento del interesado. Dicho consentimiento debe ser libre e informado y obtenerse específicamente para los fines previstos antes de que el usuario introduzca sus primeros datos personales, debiéndose incluir en la *app* un mecanismo de acción positiva para que el usuario manifieste inequívoca y explícitamente su otorgación y debiendo también que esforzarse para verificar que, en caso de menores de edad, el consentimiento ha sido otorgado por el titular de la patria potestad o de la tutela del mismo. Además, se deben implementar sistemas que permitan demostrar que el usuario, efectivamente, ha dado su consentimiento ofreciendo a éste la posibilidad de retirarlo en cualquier momento.

A través de la *app* se deben recoger datos de calidad, solicitando únicamente aquellos datos personales que sean adecuados y pertinentes para la finalidad del tratamiento y minimizando la recopilación de los datos, especialmente en los sistemas de recogida automática de la información. Además, y basándose en los *principios de usabilidad*, se deben establecer controles y sistemas de ayuda en los formularios de entrada de datos para evitar que se introduzcan datos erróneos o equivocados, procurando implementar mecanismos que garanticen que los datos sean introducidos una única vez, evitando duplicidades y pérdidas accidentales, y posibilitando que los usuarios puedan modificarlos en caso de detectar que fuesen inexactos o incompletos.

Se deben implementar adecuadas medidas de seguridad en la *app*, en toda la infraestructura del sistema de información y en el tratamiento de los datos personales ofreciendo seguridad durante todo el ciclo de vida, identificando previamente las vulnerabilidades y analizando los riesgos de seguridad que puede presentar la *app* para poderlos mitigar desde la propia fase de diseño y desarrollo. Entre las principales medidas a implementar se encuentra el cifrado en los datos tanto en el almacenamiento como en la transmisión, el instaurar un sistema robusto de autenticación (a poder ser basado en el doble factor y con políticas de contraseñas seguras) y emplear técnicas para anonimización y seudonimización, viéndolas como medidas de seguridad válidas y efectivas para los tratamientos ulteriores y conservaciones de datos requeridas y no como técnicas a emplear para evitar el cumplimiento normativo en materia de protección de datos.

Y sí, pese a haber puesto todas las medidas de seguridad posibles, se produjeran violaciones en la seguridad de los datos personales, se ha de seguir un protocolo de actuación que requiere la notificación a la autoridad de control pertinente comunicando también, como ejercicio de confiabilidad, las incidencias a los usuarios de la *app* que pudieran haber resultado afectados.

También se debe facilitar el ejercicio de los derechos de los usuarios previstos en el RGPD a través de opciones directas dispuestas en la propia *app* puesto que el entorno tecnológico invita claramente a ello pudiendo, adicionalmente, implementar opciones automatizadas que permitan a los usuarios conocer con veracidad y en tiempo real los supuestos tratamientos llevados a cabo sobre sus datos personales sin tener que iniciarse el proceso administrativo de ejercicio de los derechos, especialmente, en el de acceso, portabilidad (tratando de utilizar estándares interoperables del sector sanitario) y en el de supresión, si bien este puede encontrarse supeditado a periodos de conservación previstos tanto por el propio RGPD como por la legislación sanitaria española.

Finalmente, los desarrolladores deben tomar conciencia de la transcendencia que tiene el garantizar el cumplimiento de la normativa sobre privacidad y protección de datos y de la relevancia (incluso para su propio negocio) de transmitir confiabilidad en todo momento y a todo el mundo, viendo esta obligación no sólo como una imposición legal sino como una oportunidad de mejorar sus soluciones centrándose en el usuario en todos los aspectos, incluso, también enseñándoles a conocer el valor que tienen sus datos y la importancia de que ellos mismos los protejan adecuadamente.

Referencias

31th International Conference on Data Protection and Privacy Commissioners (ICDPPC), 2009, Resolution on Privacy by Design. Madrid. [online]. [Accessed 26 May 2017]. Available from: http://www.privacyconference2009.org/home/index-ides-idweb.html

32th International Conference on Data Protection and Privacy Commissioners (ICDPPC), 2010, Resolution on Privacy by Design. Jerusalem. [online]. [Accessed 16 May 2017]. Available from: https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

35th International Conference on Data Protection and Privacy Commissioners (ICDPPC), 2013, Warsaw declaration on the "appification" of society. [online]. [Accessed 16 April 2017]. Available from: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/13-09-24_Declaration_Appification_Society_EN.pdf

36th International Conference on Data Protection and Privacy Commissioners (ICDPPC), 2014, Resolution on Big Data. Fort Balaclava. [online]. [Accessed 16 May 2017]. Available from: https://icdppc.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf

Ackerman, Linda, 2013, Mobile Health and Fitness Applications and Information Privacy. Privacy Rights Clearinghouse, San Diego [online]. 2013. [Accessed 4 May 2017]. Available from: https://www.ft.com/content/b709cf4a-12dd-11e3-a05e-00144feabdc0

Agencia Española de Protección de Datos (AEPD) (2005). Selección de personal a través de internet. Plan de Inspección de oficio: informe de conclusiones y recomendaciones.

Agencia Española de Protección de Datos (AEPD) y Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain), 2017, Código de buenas prácticas en protección de datos para proyectos de Big Data [online]. [Accessed 16 May 2017]. Available from: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf

Agencia Española de Protección de Datos (AEPD). Informe 0012/2013

Agencia Española de Protección de Datos (AEPD). Informe 0060/2004

Agencia Española de Protección de Datos (AEPD). Informe 0093/2008

Agencia Española de Protección de Datos (AEPD). Informe 0167/2005

Agencia Española de Protección de Datos (AEPD). Informe 0340/2010

Agencia Española de Protección de Datos (AEPD). Informe 0494/2009

Agencia Española de Protección de Datos (AEPD). Informe 0574/2009

Agencia Española de Protección de Datos, 2014, Guía para una Evaluación de Impacto en la Protección de Datos Personales [online]. [Accessed 25 May 2017]. Available from: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

Agencia Española de Protección de Datos, 2017, Directrices para la elaboración de contratos entre responsables y encargados del tratamiento [online]. [Accessed 1 June 2017]. Available from: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf

Agencia Española de Protección de Datos, 2017, Guía para el cumplimiento del deber de informar [online]. [Accessed 7 June 2017]. Available from: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

Agencia Española de Protección de Datos, 2017, Orientaciones y garantías en los procedimientos de anonimización de datos personales [online]. [Accessed 10 June 2017]. Available from: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf

Akter, Shahriar, D'Ambra, John and Ray, Pradeep, 2013, Development and validation of an instrument to measure user perceived service quality of mHealth. Information & Management. 2013. Vol. 50, no. 4, p. 181-195. DOI 10.1016/j.im.2013.03.001. Elsevier BV

Anderson, Catherine L. and Agarwal, Ritu, 2011, The Digitization of Healthcare: Boundary Risks, Emotion, and Consumer Willingness to Disclose Personal Health Information. Information Systems Research. Vol. 22, no. 3, pp. 469-490. DOI 10.1287/isre.1100.0335. Institute for Operations Research and the Management Sciences (INFORMS)

Armstrong, Stephen, 2016, What happens to data gathered by health and wellness apps?. BMJ. 2016. P. i3406. DOI 10.1136/bmj.i3406. BMJ

Arxan Technologies, Inc, 2016, 5th Annual State of Application Security Report Perception vs. Reality [online]. [Accessed 15 May 2017]. Healthcare Edition. Available from: https://www.arxan.com/wp-content/uploads/2016/01/State_of_Application_Security_2016_Healthcare_Report.pdf

Asociación Médica Mundial (AMM), 2015, Declaración sobre la Salud Móvil. Moscú : Adoptada por la 66a Asamblea General de la AMM. [online]. [Accessed 5 May 2017]. Available from: https://www.wma.net/es/policies-post/declaracion-sobre-la-salud-movil/

Asociación Médica Mundial (AMM), 2016, Declaración sobre los ciberataques a la salud y otra infraestructura vital. Taipei : Adoptada por la 67a Asamblea General de la AMM. [online]. [Accessed 5 May 2017]. Available from: https://www.wma.net/es/policies-post/declaracion-de-la-amm-sobre-los-ciberataques-a-la-salud-y-otra-infraestructura-vital/

Association of the Internet Industry (ECO), 2016, eco Directiva relativa al marketing por correo electrónico admisible Directrices para la práctica [online]. [Accessed 7 June 2017]. Available from: https://certified-senders.eu/wp-content/uploads/2017/05/Directive_for_e-mail_Marketing_ESP.pdf

Audiencia Nacional. Sala de lo Contencioso. Sentencia 3888/2001, de 15 de junio de 2001.

Barbará i Fondevila, María Ángels, 2014, El principio de limitación de la finalidad a debate: los usos secundarios. I+S: informática y salud, ISSN 1579-8070, Nº. 104, 2014, págs. 9-10.

Barton, Amy J, 2012, The regulation of mobile health applications. BMC Medicine. 2012. Vol. 10, no. 1. DOI 10.1186/1741-7015-10-46. Springer Nature

Bilton, Nick, 2010, The Price of Facebook Privacy? Start Clicking. Nytimes.com [online]. [Accessed 1 June 2017]. Available from: http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=0

Bitglass, 2014, The 2014 Bitglass Healthcare Breach Report. Is Your Data Security Due For a Physical?. Healthcare Breach Report [online]. [Accessed 10 May 2017]. Available from: https://media.scmagazine.com/documents/95/bitglass_healthcare_report_23621.pdf

Blenner, Sarah R., Köllmer, Melanie, Rouse, Adam J., Daneshvar, Nadia, Williams, Curry and Andrews, Lori B., 2016, Privacy Policies of Android Diabetes Apps and Sharing of Health Information. JAMA. 2016. Vol. 315, no. 10, p. 1051. DOI 10.1001/jama.2015.19426. American Medical Association (AMA)

Buttarelli, Giovanni, 2011, Los menores y las nuevas tecnologías. In: Redes sociales y privacidad del menor. Social networks and children's privacy. Madrid : Editorial Reus. p. 150.

Carnicero J. y Rojas D. (Coordinadores), 2016, La explotación de datos de salud: Retos, oportunidades y límites. Pamplona: Sociedad Española de Informática de la Salud.

Cavoukian, Ann, 2009, Privacy by Design. The 7 Foundational Principles. [online]. [Accessed 1 June 2017]. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Centro Criptológico Nacional, 2017, Ciberamenazas y Tendencias, Edición 2017. CCN-CERT IA-16/17. [online]. [Accessed 5 June 2017]. Available from: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2224-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017/file.html

Comisión Europea (COM), 2012, Guidance document Medical Devices - Scope, field of application, definition - Qualification and Classification of stand alone software - MEDDEV 2.1/6.

Comisión Europea (COM), 2014, Libro Verde sobre Salud Móvil en la UE. 219 final Bruselas.

Comisión Europea, 2016, Code of Conduct on privacy for mHealth apps has been finalised. [online]. [Accessed 1 May 2017]. https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised

Comisión Europea. Annex: health data in apps and devices. Available from: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

Comisión Europea: Guía acerca del Escudo de Privacidad UE - EE. UU. [online]. [Accessed 20 June 2017]. Available from: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Guia_acerca_del_Escudo_de_Privacidad.pdf

Culnan, Mary J. and Armstrong, Pamela K., 1999, Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organization Science. 1999. Vol. 10, no. 1, p. 104-115. DOI 10.1287/orsc.10.1.104. Institute for Operations Research and the Management Sciences

Gartner IT, 2017. Gartner IT Glossary - Dark Data [online], [Accessed 2 May 2017]. Available from: http://www.gartner.com/it-glossary/dark-data/

Davara Fernández de Marcos, L., 2017, Menores en internet y redes sociales. Derecho aplicable y deberes de los padres y centros educativos. Breve referencia al fenómeno Pokémon Go. Boletín Oficial del Estado, Madrid.

Dehling, Tobias, Gao, Fangjian, Schneider, Stephan and Sunyaev, Ali, 2015, Exploring the Far Side of Mobile Health: Information Security and Privacy of Mobile Health Apps on iOS and Android. JMIR mHealth and uHealth. 2015. Vol. 3, no. 1, p. e8. DOI 10.2196/mhealth.3672. JMIR Publications Inc.

Ditrendia, 2016. Informe Mobile en España y en el Mundo [online]. [Accessed 2 May 2017]. Available from: http://www.amic.media/media/files/file_352_1050.pdf

Escobar, F., Iraburu, M. y Manso, E., 2003, Modelos de Historia de Salud Electrónica. V Informe Seis.

European Commission, 2017, Report of the Working Group on mHealth Assessment Guidelines February 2016 – March 2017 [online]. [Accessed 5 June 2017]. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=45251

European Network and Information Security Agency (ENISA), 2011, Smartphone Secure Development Guidelinesl [online]. [Accessed 15 June 2017]. Available from: https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines

Eysenbach, Gunther, 2001, What is e-health?. Journal of medical Internet research. 2001. Vol. 3, no. 2. DOI 10.2196/jmir.3.2.e20.

Federal Trade Commission, 2015. Complying with COPPA: Frequently Asked Questions [online]. [Accessed 8 June 2017]. Available from: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Fundación Telefónica y Editorial Ariel, S.A., 2013, TIC y salud personal [online]. [Accessed 10 May 2017]. Available from: https://publiadmin.fundaciontelefonica.com/index.php/publicaciones/add_descargas?tipo_fichero=pdf&idioma_fichero=_&title=TIC+y+salud+personal&code=231&lang=es&file=ticysaludpersonal.pdf&_ga=2.57712873.210181178.1495619723-1649832.1493720872

Future of Privacy Forum (FPF), 2016, Mobile Apps Study [online]. [Accessed 5 May 2017]. Available from: https://fpf.org/wp-content/uploads/2016/08/2016-FPF-Mobile-Apps-Study_final.pdf

Gallego Riestra, S., 2012, ¿Tiene el paciente derecho a saber quiénes y porqué han accedido a su historia clínica?, Derecho y Salud, Vol. 22, nº1 Enero-junio 2012

García Mexía, Pablo, 2014, Dark Data: la privacidad ante el Big Data "abisal". La Ley en la Red (Blogs ABC) [online]. [Accessed 20 May 2017]. Available from: http://abcblogs.abc.es/ley-red/public/post/dark-data-la-privacidad-ante-el-big-data-abisal-15882.asp/

Gelbstein, E. 2011. La integridad de los datos: el aspecto más relegado de la seguridad de la información. Isaca.org [en línea]. [Consulta: 23 mayo 2017]. Disponible en: https://www.isaca.org/Journal/archives/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx.

GfK, 2016, Seguimiento de la salud y la forma física [online]. [Accessed 5 May 2017]. Available from: https://www.gfk.com/fileadmin/user_upload/dyna_content/ES/documents/Estudio_Global_GfK__Seguimiento_de_la_salud_y_la_forma_fisica__pdf.pdf

González García, L, 2014, Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos. Derecho y Salud, Vol. 24 Extraordinario XXIII Congreso 2014

Goodman KW., Ethics, medicine, and information technology: intelligent machines and the transformation of health care. Cambridge: Cambridge University Press, 2015.

Grau, I., Kostov, B., Gallego, J.A., Grajales III, F., Fernández-Luque, L. and Sisó-Almirall, A., 2016, Método de valoración de aplicaciones móviles de salud en español: el índice iSYScore. SEMERGEN - Medicina de Familia. 2016. Vol. 42, no. 8, p. 575-583. DOI 10.1016/j.semerg.2015.12.001. Elsevier BV

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 100). Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 131). Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME).

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 136). Dictamen 4/2007 sobre el concepto de datos personales

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 169). Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento».

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 173). Dictamen 3/2010 sobre el principio de responsabilidad

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 185). Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 194). Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 202). Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes.

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 203). Opinion 03/2013 on purpose limitation

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 208). Documento de trabajo 02/2013 que proporciona orientación sobre la obtención del consentimiento para las cookies

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 213). Dictamen 03/2014 sobre la notificación de violación de datos personales

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 216). Dictamen 05/2014 sobre técnicas de anonimización

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 221). Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 223). Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos

Grupo de Trabajo sobre protección de datos del artículo 29 (WP 238). Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision

GSM Association, 2012, Móviles y Privacidad. Directrices para el diseño de privacidad en el desarrollo de aplicaciones [online]. [Accessed 15 June 2017]. Available from: https://www.gsma.com/publicpolicy/wpcontent/uploads/2016/09/GSMA2012_Guidelines_PrivacyDesignGuidelinesForMobileApplicationDevelopment_Spanish.pdf

Guía del Reglamento General de Protección de Datos para Responsables de Tratamientos

He D, Naveed M, Gunter CA, Nahrstedt K., 2014, Security Concerns in Android mHealth Apps. AMIA Annual Symposium Proceedings. 2014;2014:645-654.

Huckvale, Kit, Prieto, José Tomás, Tilney, Myra, Benghozi, Pierre-Jean and Car, Josip, 2015, Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Medicine. 2015. Vol. 13, no. 1. DOI 10.1186/s12916-015-0444-y. Springer Nature

IDC Analyze the Future, 2015, Iluminar el dato oscuro: Cómo gestionar el dato para convertirlo en un activo del negocio [online]. [Accessed 17 May 2017]. Available from: http://www.proyectosidc.com/Commvault_2015/IDC_Commvault_Client_Connect_Iluminar_Dato_Oscuro.pdf

Identify Theft Resource Center (ITRC), 2015, Data Break Reports [online]. [Accessed 12 May 2017]. Available from: http://techorchard.com/wp-content/uploads/2016/04/DataBreachReports_2015.pdf

IMS Institute for Healthcare Informatics, 2015, Patient Adoption of mHealth. Use, Evidence and Remaining Barriers to Mainstream Acceptance [online]. [Accessed 12 May 2017]. Available from: http://www.imshealth.com/files/web/IMSH%20Institute/Reports/Patient%20Adoption%20of%20mHealth/IIHI_Patient_Adoption_of_mHealth.pdf

Ince, Darrel, 2013, A dictionary of the Internet (3rd ed.). Oxford: Oxford University Press.

Information Commissioner's Office (ICO), 2017, Consultation: GDPR consent guidance [online]. [Accessed 8 June 2017]. Available from: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Instituto Nacional de Estadística (INE), 2016, Equipamiento y uso de TIC en los hogares - Año 2016 [online]. [Accessed 2 May 2017]. Available from:

http://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608

Kharrazi H, Chisholm R, VanNasdale D, Thompson B. Mobile personal health records: an evaluation of features and functionality. Int J Med Inform. 2012 Sep;81(9):579–93. doi: 10.1016/j.ijmedinf.2012.04.007.

Knorr K., Aspinall D., Wolters M., 2015, On the Privacy, Security and Safety of Blood Pressure and Diabetes Apps. In: Federrath H., Gollmann D. (eds) ICT Systems Security and Privacy Protection. SEC 2015. IFIP Advances in Information and Communication Technology, vol 455. Springer, Cham

La Carta de los Derechos Fundamentales para la Unión Europea, 2000 [online]. [Accessed 20 May 2017]. Available from: http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Martínez Santiago, R. y Rojas de la Escalera, D., 2014, Gestión de la seguridad de la información en atención primaria y uso responsable de Internet y de las redes sociales. In: Manual de Salud Electrónica para directivos de servicios y sistemas de salud. Vol. II. Aplicaciones de las TIC a la atención Primaria de Salud. Naciones Unidas y Sociedad Española de Informática de la Salud

Martínez-Pérez, Borja, de la Torre-Díez, Isabel and López-Coronado, Miguel, 2013, Mobile Health Applications for the Most Prevalent Conditions by the World Health Organization: Review and Analysis. Journal of Medical Internet Research. 2013. Vol. 15, no. 6, p. e120. DOI 10.2196/jmir.2600. JMIR Publications Inc.

McAfee. Part of Intel Security., 2016, Alerta sanitaria: El sector de la asistencia sanitaria en el punto de mira de la ciberdelincuencia [online]. [Accessed 12 May 2017]. Available from: http://www.mcafee.com/es/resources/reports/rp-health-warning.pdf

Ministerio de Sanidad y Consumo, 2007-2010, Historia Clínica Digital del Sistema Nacional de Salud. Análisis de Requerimientos del Sistema. . [online]. [Accessed 16 June 2017]. Available from: https://www.msssi.gob.es/organizacion/sns/planCalidadSNS/docs/ARS.pdf

Mirza, F., Norris, T. and Stockdale, R., 2008, Mobile technologies and the holistic management of chronic diseases. Health Informatics Journal. 2008. Vol. 14, no. 4, p. 309-321. DOI 10.1177/1460458208096559. SAGE Publications

Monkman, Helen and Kushniruk, Andre, 2013, A health literacy and usability heuristic evaluation of a mobile consumer health application. Stud Health Technol Inform 2013;192:724-8.

National Bureau of Standards, Data Encryption Standard, FIPS-Pub.197. National Bureau of Standards, U.S. Department of Commerce,Washington D.C., Nov. 2001.

Nielsen, Jakob, 1995, 10 Heuristics for User Interface Design [online]. [Accessed 10 June 2017]. Available from: https://www.nngroup.com/articles/ten-usability-heuristics/

Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), 2016, Los ciudadanos ante la e-Sanidad. Opiniones y expectativas de los ciudadanos sobre el uso y aplicación de las TIC en el ámbito sanitario [online]. [Accessed 2 May 2017]. Available from: https://www.ontsi.red.es/ontsi/sites/ontsi/files/los_ciudadanos_ante_la_e-sanidad..pdf

Organización de Cooperación y Desarrollo Económico (OCDE), 1980, Directrices relativas a la protección de la Intimidad y de la Circulación Transfronteriza de datos personales [online]. [Accessed 26 May 2017]. Available from: http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad..pdf

Organización Mundial de la Salud (OMS), 2011, mHealth: New horizons for health through mobile technologies. Global Observatory for eHealth series 3, 6. [online]. [Accessed 2 May 2017]. Available from: http://www.who.int/goe/publications/goe_mhealth_web.pdf

Organización Mundial de la Salud (OMS), 2016, mSalud: uso de las tecnologías móviles inalámbricas en la salud pública. 139.ª reunión del Consejo Ejecutivo (27 de mayo de 2016) [online]. [Accessed 2 May 2017]. Available from: http://apps.who.int/gb/ebwha/pdf_files/EB139/B139_8-sp.pdf

OWASP Mobile Security Project. [online]. [Accessed 10 June 2017]. Available from: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

Panda Security Mediacenter, 2017, ¿Aceptas los permisos de las aplicaciones sin leer? ¡Deberías tener más cuidado! [online]. [Accessed 2 May 2017]. Available from: http://www.pandasecurity.com/spain/mediacenter/dispositivos-moviles/aceptas-los-permisos-de-las-aplicaciones-sin-leer-deberias-tener-mas-cuidado/

PatientView Ltd, 2015, The myhealthapps directory 2015-2016 [online]. [Accessed 10 May 2017]. Available from: http://www.patient-view.com/uploads/6/5/7/9/6579846/the_myhealthapps_directory_2015-2016.pdf

Patrick, Kevin et al., 2008, Health and the Mobile Phone. American journal of preventive medicine 35.2 (2008): 177–181. PMC.

Pinedo González, E., 2007, La PYME ante la LOPD. 1st ed. [A Coruña]: Netbiblo. p.36

PriceWaterhouseCoopers (PwC), 2013, Socio-economic impact of mHealth [online]. [Accessed 10 May 2017]. Available from: http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/Socio-economic_impact-of-mHealth_EU_14062013V2.pdf

Proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)).

R. S. H. Istepanian and J. C. Lacal, 2003, Emerging mobile communication technologies for health: some imperative notes on m-health. Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (IEEE Cat. No.03CH37439), 2003, pp. 1414-1416 Vol.2. doi: 10.1109/IEMBS.2003.1279581

Rebollo Delgado, L. and Serrano Pérez, M. 2008. Introducción a la protección de datos. Madrid: Dykinson. Pág. 125-158

Red Global de Control de la Privacidad (GPEN), 2014, Resultados del análisis coordinado sobre las condiciones de privacidad de las aplicaciones móviles [online]. [Accessed 2 May 2017]. Available from: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/sep_14/140910_NP_Resultados_analisis_GPEN.pdf

Research2guidance (R2G), 2016, mHealth App Developer Economics 2016. The current status and trends of the mHealth app market. 6th annual study on mHealth app publishing based on 2,600 plus respondents.

Ribagorda Garnacho, A., 2010, Seguridad de los datos, en Troncoso Reigada, A. (Dir.) Comentarios a la Ley Orgánica de Protección de datos de carácter personal. Dir. Ed. Aranzadi, S.A., Navarra, pág. 742

Rozalén, R., 2016. Apple amplía el plazo a los desarrolladores de apps para adoptar la App Transport Security | Silicon. Silicon [en línea]. [Accessed: 22 June 2017]. Available from: http://www.silicon.es/apple-amplia-plazo-los-desarrolladores-apps-adoptar-la-app-transport-security-2325866

Sarkar, Urmimala, Gourley, Gato I., Lyles, Courtney R., Tieu, Lina, Clarity, Cassidy, Newmark, Lisa, Singh, Karandeep and Bates, David W., 2016, Usability of Commercially Available Mobile Applications for Diverse Patients. Journal of General Internal Medicine. 2016. Vol. 31, no. 12, p. 1417-1426. DOI 10.1007/s11606-016-3771-6. Springer Nature

Satish Misra, MD, 2015, NHS Health Apps Library closing amid questions about app security & quality - iMedicalApps. iMedicalApps [online]. 2015. [Accessed 2 May 2017]. Available from: http://www.imedicalapps.com/2015/10/nhs-health-apps-library-closing-commentary

Singh, Karandeep, Drouin, Kaitlin, Newmark, Lisa P, Filkins, Malina, Silvers, Elizabeth, Bain, Paul A, Zulman, Donna M, Lee, Jae-Ho, Rozenblum, Ronen, Pabo, Erika, Landman, Adam, Klinger, Elissa V and Bates, David W, 2016, Patient-Facing Mobile Apps to Treat High-Need, High-Cost Populations: A Scoping Review. JMIR mHealth and uHealth. 2016. Vol. 4, no. 4, p. e136. DOI 10.2196/mhealth.6445. JMIR Publications Inc.

Steel, Emily and Dembosky, April, 2013, Health apps run into privacy snags. Financial Times [online]. 2013. [Accessed 4 May 2017]. Available from: https://www.ft.com/content/b709cf4a-12dd-11e3-a05e-00144feabdc0

Subhi, Yousif, Bube, Sarah Hjartbro, Rolskov Bojsen, Signe, Skou Thomsen, Ann Sofia and Konge, Lars, 2015, Expert Involvement and Adherence to Medical Evidence in Medical Mobile Phone Apps: A Systematic Review. JMIR mHealth and uHealth. 2015. Vol. 3, no. 3, p. e79. DOI 10.2196/mhealth.4169. JMIR Publications Inc.

Sunyaev, A., Dehling, T., Taylor, P. L. and Mandl, K. D., 2014, Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association. 2014. DOI 10.1136/amiajnl-2013-002605. Oxford University Press (OUP)

The App Date, 2014, Informe Apps de salud en español [online]. [Accessed 13 June 2017]. Available from: http://www.ucci.urjc.es/wp-content/uploads/Informe-Apps-Salud.pdf

Tribunal Constitucional. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Tribunal Supremo. Sentencia nº 13/2013 de TS, Sala 1ª, de lo Civil, 29 de Enero de 2013

U.S. Department of Health and Human Services Food and Drug Administration (FDA), 2015, Mobile Medical Applications. Guidance for Industry and Food and Drug Administration Staff [online]. [Accessed 2 May 2017]. Available from: https://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf

United Nations foundation (UNF) & Vodafone foundation, 2009, mHealth for Development: The opportunity of mobile technology for healthcare in developing world [online]. [Accessed 10 May 2017]. Available from: http://www.unfoundation.org/what-we-do/issues/global-health/mhealth-report.html

Wright, D., De Hert, P. Privacy Impact Assessment. Springer (2012).