UNIVERSIDAD POLITÉCNICA DE MADRID

ETS DE INGENIERÍA DE SISTEMAS INFORMÁTICOS

INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

TRABAJO FIN DE CARRERA

LA PROTECCIÓN DE DATOS ANTE EL INTERNET DE LAS COSAS

Autora: Mª Teresa Romero García

Tutora: Celia Fernández Aller

Curso Académico: 2016/2017

A mi familia por estar siempre ahí.

A Alberto por su compañía todo este tiempo.

Y a Manuel por estar a mi lado, darme calma en los malos ratos y confiar en que podría terminar este trabajo.

Gracias.

RESUMEN

La irrupción del Internet de las Cosas (IoT) está cambiando la forma de entender el mundo. Objetos inteligentes conectados a la red interactuando entre sí pueden recoger información y realizar acciones sin necesidad de la intervención humana, nuevas tecnologías pueden analizar los datos y proporcionar nueva información con la que actuar. La independencia de los objetos y la transformación de nuestra relación con ellos, supone un cambio en modelos de negocio y gestión así como un impacto y un cambio en la sociedad. La descentralización, la ubicuidad o la gran cantidad de información que se moverá por la red y puede ser tratada, acomplejan mantener un control sobre los datos de los usuarios que recogerán los dispositivos. La privacidad y protección de nuestra intimidad se encuentra entre las principales amenazas que traen consigo el IoT y que debemos afrontar con la mayor celeridad posible.

Garantizar que no haya un uso malintencionado de los datos, respetar la vida privada de los usuarios y anteponer su privacidad e intimidad por encima de los beneficios económicos o "cotidianos" que el uso de dispositivos inteligentes nos pueden aportar, pasa por la responsabilidad de todos los actores que forman parte de su ecosistema. La Unión Europea ya está trabajando en mejorar y ajustar el marco de protección de ley para minimizar las amenazas y afrontar los riesgos que la llegada del IoT plantea para la seguridad de nuestros datos. Los fabricantes ya saben de estos desafíos y de la necesidad de incluir medidas de seguridad desde el diseño y la planificación de una forma práctica en cada parte del ciclo de vida de los objetos. La sociedad debemos ser conscientes de la importancia del derecho a decidir, controlar y saber sobre nuestros datos así como de la responsabilidad de cuidar de ellos.

En este Trabajo Final de Carrera nos introduciremos en el Internet de las Cosas: pasado, presente y futuro. Características técnicas y campos de aplicación como acercamiento para poder a partir de ahí, hacer un análisis de las amenazas y riesgos que supone para la privacidad de la información vivir en un mundo conectado, así como evaluar las herramientas, tanto actuales como las que se implantarán en un futuro cercano fruto de los estudios por parte de diversos organismos; para enfrentarnos a ellos.

ABSTRACT

The irruption of the Internet of Things (IoT) is changing the way to understand the world. Intelligent objects connected to the Internet and interacting with each other can collect information and plan actions without the human intervention. New technologies can analyze the data and provide new information to act. The independence of the objects and the transformation of our relationship with them implies a change in business and management models as well as an impact and change in society. Decentralization, ubiquity, or the vast amount of information that will be moved and can be managed on the Internet, make it difficult tracking the user data collected by the devices. The privacy and protection of our privacy is among the main threats that the IoT brings with it and that we must face as quickly as possible.

Ensuring no malicious use of data, respecting the users privacy and prioritizing their privacy beyond the economic benefits that the use of smart devices can bring us, is the responsibility of everybody part of this ecosystem. The European Union is already working on improving and adjusting the legal protection framework to minimize threats and face the risks that the IoT presents for the security of our data. Manufacturers already know about these challenges and the need to include safety measures from design and planning in a practical way in each part of the lifecycle of objects. Society must be aware of the importance of the right to decide, control and know about our data as well as the responsibility to care for them.

In this final project we will be introduced in the Internet of Things: past, present and future. Technical characteristics and fields of application as an approach to be able from there, analyze the threats and risk from the information privacy in a connected world, as well as evaluate the tools, the current and the ones to be implemented in near future, result of studies by diverse agencies; to confront them.

ÍNDICE

ÍNDICE ILUSTRACIONES

1 INTRODUCCIÓN

Internet de las cosas (Internet of Things, en adelante IoT) no es una tecnología, no es un producto ni algo en sí material, es un concepto que hace referencia a objetos comunes interconectados a Internet empleando los avances tecnológicos. IoT se empezó a dar a conocer cuando el número de dispositivos fue mayor que el número de personas conectadas a Internet (2008 – 2009). Desde entonces la investigación, el diseño y la fabricación de dispositivos IoT (También llamados objetos inteligentes), han ido en aumento en diversidad de áreas como la industria, medicina, medio ambiente, etc. Desde la transformación de la industria con la realización por parte de la tecnología de tareas mecánicas, hasta el seguimiento de pacientes en urgencias pasando por bombillas inteligentes, lavadoras, botiquines que nos informen de medicamentos caducados o neveras que nos avisen si se ha terminado algún alimento; los objetos conectados a Internet en nuestro día a día suponen un cambio en la forma de entender nuestro entorno, el modelo empresarial o el industrial, la publicidad o las relaciones. La sociedad en general se irá adaptando en mayor o menor medida pero de forma inevitable, a este gran cambio como ya pasó con la llegada de Internet.

Actualmente el uso de smartphone, tablets o portátiles podría decirse que es generalizado en los países del primer mundo y la mayor parte de los hogares disponen de Internet como una herramienta de trabajo, comunicación y gestión de la información. Con la inmersión del IoT, la dependencia de Internet aumentará para poder gestionar dispositivos que utilizamos en el día a día que ofrecerán, además de sus funcionalidades básicas, otras funcionalidades como puede ser el acceso a una mayor cantidad de información. Por ejemplo, los relojes inteligentes pueden, además de cumplir su función, dar información sobre la frecuencia cardiaca o la distancia recorrida y sincronizar después esta información con otros dispositivos.

Considerando las predicciones futuras en las que en 2020 se esperan alrededor de 26.000 dispositivos conectados[1], el aumento de datos sobre nosotros recogidos por los diversos dispositivos y que viajarán por la red aumentará considerablemente. La privacidad y protección de los datos por tanto, supone una de las principales amenazas para las usuarias del IoT a la que fabricantes, organismos y usuarios debemos estar atentos.

Qué derechos debemos proteger y qué responsabilidades podemos exigir o cumplir respecto a la protección de datos, cuáles serán las amenazas y cuáles los requisitos y medidas de protección y las herramientas con las que cuenta nuestra legislación para una regulación que garantice nuestra intimidad, son aspectos que deberán analizarse para minimizar esta

[1] Según informe de la empresa Gartner en línea en http://www.gartner.com/newsroom/id/2905717 [Consulta 05/02/2017]

amenaza y estar preparados para cuando el IoT sea una realidad integrada en todos los aspectos de nuestras vidas. Todos estos puntos se analizarán a lo largo de este trabajo refiriéndonos a todas las áreas de aplicación en general y profundizando en particular en la repercusión que el IoT puede tener en el ámbito sanitario al tratarse de la protección de datos sensibles que afectan a nuestra salud.

El cambio en la relación entre médico – paciente, una mayor autonomía y decisión por parte de este último o los avances en prótesis e imágenes 3D son algunos de los avances que el Internet de las Cosas ha traído. El tratamiento y protección de datos así como la seguridad en estos dispositivos, adquieren mayor relevancia debido a las implicaciones y repercusiones que cualquier uso malintencionado o error puedan conllevar.

2 OBJETIVOS

2.1 OBJETIVOS ESPECÍFICOS

El objetivo principal de este Trabajo Fin de Carrera es analizar desde el punto de vista de la protección de datos y la privacidad, los riesgos que supone el Internet de las cosas en general y el Internet de las Cosas Médicas en particular; para los usuarios. Así como revisar la legislación vigente con la que podemos hacer frente a estos desafíos y las modificaciones que deberán realizarse para adaptar el marco legal a las amenazas del IoT.

Para llegar a este objetivo, realizaremos en primer lugar un acercamiento a lo que significa la inmersión del Internet de las Cosas en la sociedad. Los actores que forman parte y su arquitectura.

Revisaremos las herramientas legales y las líneas en la que se están trabajando en el marco legal para hacer frente a los riesgos que el IoT plantea respecto a la protección de datos para finalmente y en base a ellas, analizar estos riesgos y aportar recomendaciones para minimizarlos.

2.2 ESTRUCTURA DEL DOCUMENTO

El presente trabajo se estructura en dos bloques. El primer bloque tratará el Internet de las Cosas en general. Constará de cinco capítulos (Capítulo 3 – 5):

- Internet de las cosas. En el primer bloque: “Internet de las cosas”, se hace un repaso a la vida de Internet de las Cosas: Pasado, presente y predicciones futuras. Sus características y los campos de aplicación.
- Ecosistema y arquitectura del IoT. En este capítulo se identificarán los principales actores que intervienen en el ecosistema del IoT y realizaremos un acercamiento a la parte más técnica, las características y cómo es una arquitectura IoT.
- Implicaciones en el uso de Internet de las Cosas en el derecho a la protección de datos. Antes de adentrarnos en los retos de privacidad que pueden aparecer, haremos un estudio de la regulación vigente tanto a nivel nacional como comunitario. Debido a los cambios que se están produciendo y la necesidad de adaptar la ley a los avances tecnológicos, repasaremos también las modificaciones regulatorias que entrarán en vigor en 2018 y, analizaremos la opinión del GT29 respecto al Internet de las Cosas.

El segundo bloque que constará sólo de un capítulo (Capítulo 6: Internet de las Cosas en el campo de la salud), profundizaremos en lo que implica el IoT en este campo, líneas de aplicación, características y barreras y regulación específica relacionada con la protección de datos.

Por último, analizaremos todos los retos que el IoT presente respecto a la protección de datos a nivel general y en el sector de la salud en particular así como las recomendaciones a los diferentes actores del ecosistema IoT.

3 INTERNET DE LAS COSAS

Hay múltiples definiciones que explican que es Internet de las cosas o IoT (Internet of Things), como también nos referiremos a lo largo de este trabajo. Como referencia, cogeremos la que el grupo de trabajo CASAGRAS[2] lanzó en 2014: "*Internet de las cosas es una infraestructura global interconectada enlazando objetos físicos y virtuales a través de la explotación de la captura de datos y las capacidades de comunicación. Ofrecerá identificación específica de objetos y capacidades sensoriales y su conectividad como base para el desarrollo de servicios cooperativos y aplicaciones independientes. Se caracterizarán por un alto grado de captura de datos autónoma, transferencias de eventos, conectividad de red e interoperabilidad*".

Se trata entonces, de objetos cotidianos identificados individualmente, conectados entre sí y gestionados por otros equipos con gran cantidad de información y capacidad de actuación, de la misma manera que si fueran gestionados por seres humanos. De esta forma, si termostatos, lámparas, botiquines, neveras… estuvieran conectadas a internet, en nuestra casa la temperatura y la luz se irían regulando dependiendo de nuestras necesidades, no tendríamos medicamentos caducados y podrían actualizar nuestra lista de la compra de forma automática.

3.1 RETROSPECTIVA INTERNET DE LAS COSAS

En 2009, Kevin Ashton dijo: "*Si tuviésemos ordenadores que fuesen capaces de saber todo lo que pudiese saberse de cualquier cosa –usando datos recolectados sin intervención humana- seríamos capaces de hacer seguimiento detallado de todo, y poder reducir de forma importante los costes y malos usos. Sabríamos cuando las cosas necesitan ser reparadas, cambiadas o recuperadas, incluso si están frescas o pasadas de fecha. El Internet de las Cosas tiene el potencial de cambiar el mundo como ya lo hizo Internet. O incluso más*." No era la primera vez que utilizaba el término Internet de las Cosas, en los grupos de investigación en el centro Auto-CID ya lo usaban desde 1999, tampoco era la primera persona que hablaba de interconectar elementos que no fueran computadores, Mark Weiser [3] (1990) defendía la idea de que los ordenadores personales serían reemplazados por "*ordenadores invisibles*" dentro

[2] CASAGRAS: Coordination And Support Action for Global RFID-realted Activities and Standardization. Proyecto marco europeo 7. Creado para considerar las dimensiones internacionales relativas a la normativa, la normalización y otros requisitos respecto al Internet de las Cosas.

[3] Mark Weiser. Defensor de la "Computación ubicua" y autor del libro The Computer for the Twenty-First Century donde habla de elementos conectados. Wikipedia. Mark Weiser (2012). Disponible en línea en: https://es.wikipedia.org/wiki/Mark_Weiser [Consulta: 21/01/2017]

de objetos de uso cotidiano. Fuera como fuese, fue Ashton quien usó el término de forma pública y en el momento idóneo, de hecho, para Cisco Internet Business Solutions Group (IBSG), el IoT surgió entre 2008 y 2009 como el momento en el que había más cosas que personas conectadas a Internet (Abril 2011).

Podemos limitarnos a Ashton al hablar de los orígenes del Internet de las cosas o a un simple momento en el tiempo, pero no sería justo obviar todos los desarrollos y evoluciones tecnológicas que permitieron llegar hasta lo que conocemos hoy como IoT. A continuación haremos un repaso a los acontecimientos que dieron lugar al nacimiento del Internet de las Cosas:

Los objetos conectados se remontan al siglo XIX, cuando se dan los primeros experimentos de telemetría. En 1874 científicos franceses instalaron dispositivos de información meteorológica y de profundidad de nieve en la cima del Mont Blanc que, por medio de un enlace de radio de onda corta, eran transmitidos a París.

1926. Nikola Tesla[4] hizo una entrevista para la revista Colliers. *"Cuando lo inalámbrico esté perfectamente desarrollado, el planeta entero se convertirá en un gran cerebro…", "los instrumentos que usaremos para ello serán increíblemente sencillos comparados con nuestros teléfonos actuales. Un hombre podrá llevar uno en su bolsillo".* Decía Tesla. Más adelante, en 1950 Alan Turing en su artículo Computing Machinery and Intelligence en el Oxford Mind Journal dijo: "*… También se puede sostener que es mejor proveer a la máquina con los mejores órganos de los sentidos que el dinero puede comprar, y luego enseñar a entender y hablar inglés. Este proceso podría seguir la enseñanza normal de un niño*". Nikola, Turing, Marshall McLuhan[5] o Karl Steinbuch[6], fueron personas adelantadas a su tiempo que expresaron la importancia de poder conectar los objetos y dotarlos de inteligencia. Dada la inmadurez tecnológica de la época aquellas ideas quedaron tan solo en premoniciones.

1969. Se envía el primer mensaje a través de ARPANET. La red ARPANET fue una red de ordenadores creada por encargo del Departamento de Defensa de EEUU para comunicarse entre instituciones y con fines de uso militar y académico. En un principio se unieron 4 nodos dentro de la red (Ilustración 1) y poco a poco fueron ampliándose hasta convertirse en una red internacional (Ilustración 2).

[4] Nikola Tesla: inventor, ingeniero mecánico, ingeniero eléctrico y físico. Se le conoce por sus invenciones en el campo del electromagnetismo. Su trabajó ayudó a crear las bases de los sistemas modernos para el uso de la energía eléctrica por corriente alterna.
Wikipedia. Nikola Tesla. 2017 Disponible en línea en: https://es.wikipedia.org/wiki/Nikola_Tesla [Consulta: 21/01/2017]

[5] McLuhan (1911 – 1980): filósofo reconocido como un visionario de la futura sociedad de la información. Wikipedia. Marshall McLuhan. 2015. Disponible en línea en: https://es.wikipedia.org/wiki/Discusi%C3%B3n:Marshall_McLuhan. [Consulta: 21/01/2017

[6] Karl Steinbuch (1917 – 2005). Científico informático alemán pioner de las redes neuronales artificiales. Wikipedia. Karl Steinbuch. 2011 . Disponible en línea en: https://es.wikipedia.org/wiki/Karl_Steinbuch. [Consulta: 21/01/2017]

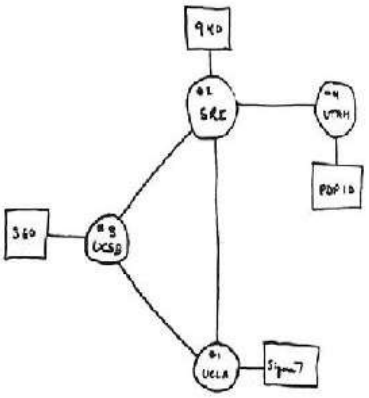

Ilustración 1: ARPANET 1969[7]

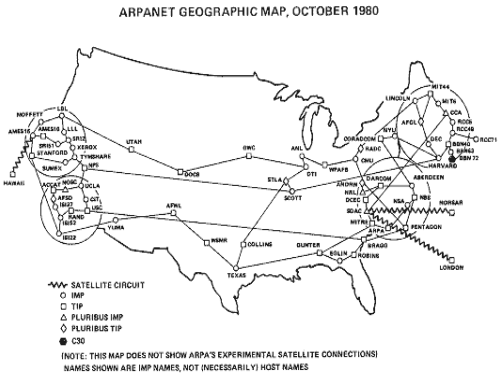

Ilustración 2: ARPANET 1680

1974. Se implantó en la red ARPANET el protocolo TCP/IP, uno de los primeros protocolos de comunicaciones, base de Internet. La red militar y académica se convertía entonces en INTERNET.

1989. Romkey y Simpon Hacket, dos muchachos sin trayectoria, crearon una tostadora que podía conectarse a internet. La tostadora podía encenderse, apagarse y controlar el tostado de la rebanada. La conectividad fue a través del ya mencionado protocolo TCP/IP y el control se realizó mediante SNMP (Simple Network Management Protocol). El problema era, que entonces las comunicaciones que internet ofrecía eran cableadas y que el hardware tenía un coste elevado. La tostadora fue el primer objeto conectado a internet que pasó totalmente inadvertido durante años.

1990. Berners-Lee, conocido por ser el padre de la Web, establece la primera comunicación entre un cliente y un servidor a través de Internet usando HTTP (Hypertext Transfer Protocol). Había inventado la World Wide Web. Un año después, Berners crea una página web. Se acelera el desarrollo tecnológico de forma rápida e imparable.

1999. Como hemos mencionado al principio del punto, Kevin Ashton habla por primera vez de Internet de las Cosas. El término aparece en publicaciones de importantes medios de

[7] Ilustración 1 y 2. ARPANET Maps. 1978. Fuente: http://som.csudh.edu/fac/lpress/history/arpamaps/ [Consulta 27/01/2017]

comunicación. De forma paralela, se despliega la tecnología RFID[8] de manos del Departamento de Defensa de EEUU.

2005. Llega Arduino, el exponente principal para desarrollar y prototipar la interconexión entre objetos. El hardware Arduino programa entradas y salidas y cuenta con un chip de comunicación para traspasar los datos.

2006. Rafi Haladjian y Olivier Mével crearon el Nabaztag (Liebre en armenio). Fabricado por la empresa francesa Violet, Nabaztag es un "objeto inteligente", un conejo que se conecta a Internet por ondas si-fi y con su usuario por mensajes luminosos o vocales o moviendo sus orejas. La primera versión de Nabaztag hablaba solamente en inglés y francés y podía descargar información sobre la meteorología, la Bolsa, calidad del aire, correos electrónicos… para mostrarlos a su usuario.

2008. Un grupo de empresas como Google o Cisco, se unen para crear la IPSO Alliance en 2008 con la finalidad de promover el uso de Internet en redes de objetos inteligentes. Paralelamente aparecen nuevos conceptos como el WSN (Wireless Sensor Networks) o M2M (Machine to Machine) que dan paso a lo que conocemos por el IoT

A partir de ese año comienza a conocerse el IoT. Numerosos medios se hacen eco. El Consejo de Inteligencia Nacional de EEUU cataloga el IoT como una tecnología con impactos potenciales y el primer ministro Chino planea grandes inversiones para lo que considera una industria clave. Las empresas privadas comienzan a interesarse por la nueva tecnología y comienzan a hacerse estudios de marketing que prevén un futuro prometedor.

A continuación mostramos la hoja de ruta de los avances tecnológicos a partir del año 2000.

[8] RFID o identificación por radiofrecuencia es un sistema de almacenamiento y recuperación de datos remotos. Su objetivo es transmitir la identidad de un objeto. Wikipedia. RFID. 2015. https://es.wikipedia.org/wiki/Discusi%C3%B3n:RFID [Consulta: 21/01/2017]

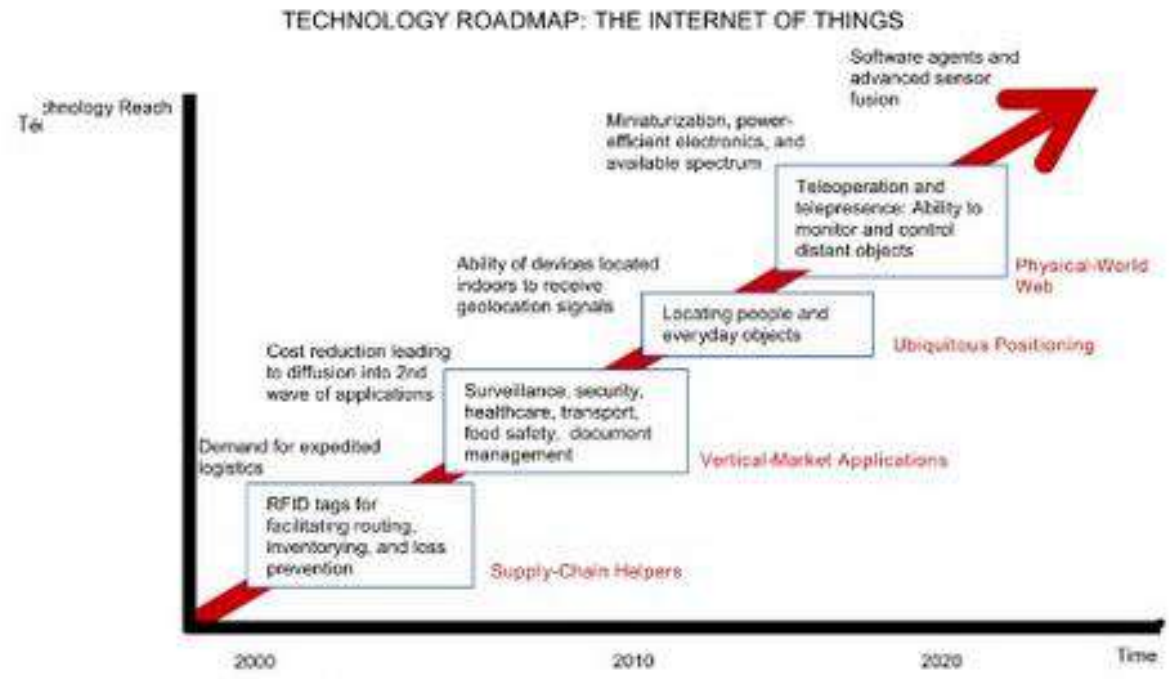

Ilustración 3: Avance de la tecnología[9].

3.2 PRESENTE

Cuando se hablaba de teléfonos inteligentes desde los que consultar tu correo electrónico, conectarte a las redes sociales o instalar aplicaciones como el Whatsapp entre otras funcionalidades, nos mostrábamos cuanto menos escépticos. Los teléfonos inteligentes llegaron, se hicieron hueco en nuestra vida cotidiana y se quedaron. Ahora, resulta extraño encontrar a alguien que no los utilice. Esto mismo, para algunos expertos, es lo que va a pasar con los objetos del Internet de las Cosas. Cada vez es más común encontrar quien tiene un reloj inteligente para contar los pasos que da o las pulsaciones que tiene por minuto, una encuesta en 2016 que PWC [10] hizo a mil consumidores de Estados Unidos, mostraba que el

[9]Fuente: Consulting Business Inteligence / National Intelligence Council – Apéndice F dentro de documento_ Disruptivas 2025 página 1 Figura 15 (Antecedentes: Internet de las Cosas). Disponible en línea https://commons.wikimedia.org/wiki/File:Internet_of_Things.svg#/media/File:Internet_of_Things.svg [Consulta 22/01/2017]

10 La encuesta realizada por PWC (Dedicada a la consultoría de las Big Four). Disponible en línea en http://www.pwc.com/us/en/industry/entertainment-media/assets/pwc-cis-wearables.pdf [Consulta 23/01/2017]

45% tenía una banda de fitness, un 27% un reloj inteligente, y el 12% ropa inteligente. El IoT está cada vez más presente y si tenemos en cuenta el continuo crecimiento de la tecnología, las posibilidades que el IoT ofrece a corto y medio plazo son tales que se habla de una nueva revolución por las implicaciones que va a tener.

En este escenario, IoT fomentará integraciones y descubrirá aplicaciones nuevas en el mundo de la empresa y los negocios. El conocimiento necesario hará que las marcas cambien sus procesos, que aparezcan nuevos puestos de trabajo y, se destruyan otros. Que la forma de relacionarnos, consumir y trabajar se modifique. Hablamos de un futuro no demasiado lejano. La apuesta por el IoT es fuerte, en el 2017 la inversión global para ella crecerá un 15% respecto al año anterior según Everis[11] y se espera que para este año comiencen a notarse algunos cambios como:

- ✓ Mayor número de objetos conectados entre sí. Aunque las cifras varían dependiendo de su fuente, es obvio que la inversión y el uso de dispositivos inteligentes ha aumentado y continuará aumentando en los próximos años. Debido a las cifras positivas, las empresas se están interesando por desarrollar productos IoT.
- ✓ Influencia en modelos de negocio. Especialmente para el marketing, movidos por la eficiencia y el ahorro en costes que el IoT supondrá. El acceso a los datos y la posibilidad de convertirlos en acciones ofrece una innovación en el servicio al cliente y la posibilidad de nuevas oportunidades para mejorar la satisfacción de sus marcas.
- ✓ Recolección de datos de la nube. Es cada vez más una realidad que la información entre objetos – personas y viceversa se almacena, edita, controla directamente desde la nube a través de herramientas como Google Drive o Dropbox. Se trabaja, paralelamente en su seguridad por ahora, sobretodo, con el control de accesos.
- ✓ Pymes con mejores herramientas tecnológicas. Actualmente los sistemas tecnológicos IoT son utilizados mayormente por grandes multinacionales debido al todavía, alto coste que implican. Conforme vaya evolucionando la tecnología, las pequeñas y medianas empresas utilizarán los mismos sistemas sin necesidad de destinar tan elevadas cantidades de dinero. Las Pymes se verán beneficiadas al poder compaginar el IoT y el conocimiento de las necesidades de los consumidores, donde son las mejores posicionadas.
- ✓ Ciudades más conectadas mejorarán su eficiencia conectando su infraestructura a centros de control, generando mejoras para sus habitantes en movilidad principalmente, seguridad, salud y trabajo. De forma indirecta esto implica por un lado, el aumento de oportunidades para las empresas que se dediquen a la tecnología y por otro, a sectores que puedan utilizar esta tecnología sin restricciones.

[11] Informe empresa Everis. Resultados publicados por Expansión. Europa Press. La inversión global en Internet de las Cosas crecerá un 15% en 2017 según Everis. 2016. Disponible en línea en: http://www.expansion.com/agencia/europa_press/2016/11/30/20161130123459.html [Consulta: 23/01/2017]

3.3 FUTURO DEL IOT

Según Cisco (2011), ya hay cuatro mil millones de dispositivos conectados y en 2020 se alcanzarán **26.300** millones, llegando a tener 26 dispositivos conectados por individuo. IHS prevé que en 2020 habrá más de 16.300 millones de dispositivos y 75 en 2025. Las cifras varían igual que las predicciones de impacto del IoT en el futuro y aun así, informes de diferentes fuentes como Analysys Mason indican que pese a todo, el mercado del IoT sigue siendo relativamente pequeño y convencional. La firma de análisis Gartner[12] ha ajustado la cifra de objetos inteligentes en funcionamiento a 20.400 millones para finales de la década, cifra que parece ser la más cercana a la correcta basándonos en el estudio de cifras de años anteriores. Gartner estima que actualmente el número de cosas conectadas ha aumentado un 31% desde 2016, 8.400 millones de dispositivos inteligentes en el mundo, el 67% en el ámbito doméstico, que puede alcanzar los veinticinco mil en tres años.

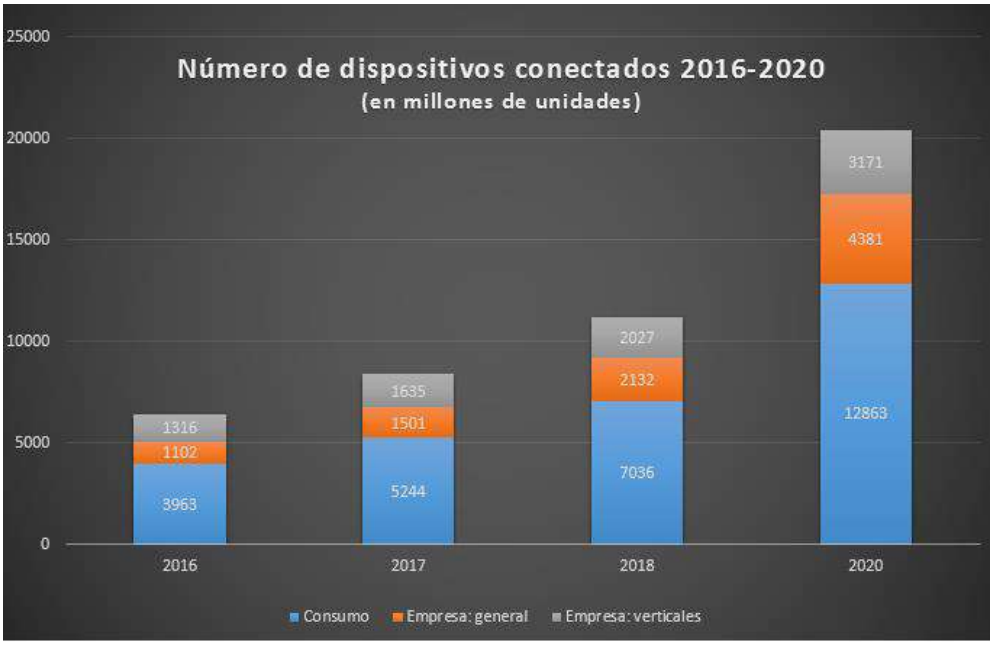

Ilustración 4: Pronóstico del crecimiento de dispositivos conectados[13].

[12] Gartner, empresa consultora de investigación de las tecnologías de la información.

[13] TICbeat: Alberto Iglesias Fraga. 2017 Internet de las Cosas: 8400 millones de dispositivos conectados cuando acabe 2017. Disponible en línea en: http://www.ticbeat.com/innovacion/internet-de-las-cosas-8400-millones-dispositivos-conectados-2017/ [Consulta: 23/01/2017]

Estas cifras supondrán un gasto de más de 1.6 billones en 2017 y más de 2 billones en inversiones en 2018. Por sectores, actualmente el ámbito industrial seguido del transporte y servicios públicos son los sectores de mayor inversión en IoT aunque se espera que el área de consumo adquiera protagonismo. Si hablamos de las regiones que más invierten, Asia/Pacífico está a la cabeza en inversión de soluciones de IoT seguida por Estados Unidos, Europa Occidental y Japón.

Gasto total en Internet de las Cosas

(en billones de dólares, escala anglosajona)

Categoría	2016	2017	2018	2020
Consumo	532.515	725.696	985.348	1.494.466
Empresa: general	212.069	280.059	372.989	567.659
Empresa: verticales	634.921	683.817	736.543	863.662
TOTAL	1.379.505	1.689.572	2.094.881	2.925.787

Ilustración 5: Gasto Total en IoT. Fuente Gartner[14].

En España, los gastos en IoT suponen este año 13.500 millones de euros, un crecimiento que llegará a casi 23.000 millones en 2020. Por sectores, mientras que en 2016 la industria manufacturera estaba a la cabeza en inversión en IoT con un 18% de participación, en 2020 se espera que su participación disminuya hasta el 13% mientras que el sector Retail acumule un 14% de gasto total de España, dos puntos más que en 2016.

Según IDC España (2017), las compañías españolas ven como principales puntos a favor a la hora de adoptar tecnologías de IoT la automatización de procesos, la reducción de costes operacionales y la mejora en la experiencia del cliente. Aún con ello, para estas empresas es complicado abordar iniciativas relacionadas con el IoT debido a sus costes iniciales y las preocupaciones relacionadas con la seguridad y la privacidad, de hecho; el 69% de las organizaciones que adoptan este tipo de tecnologías han creado o planean crear nuevas políticas de seguridad.

En el estudio realizado por Oasys Outsoucing Automation System en 2016 basado en el congreso IoT World Congress en Barcelona, quedan reflejadas las diferencias que todavía existen entre el mercado español y el europeo en la actualidad. Y resaltan una serie de puntos que repercutirán en el futuro del IoT, principalmente en el mercado español. Entre ellos:

[14] Gartner. 2017. Disponible en línea en http://www.gartner.com/newsroom/id/3598917 [Consulta: 28/01/2017]

- ✓ Falta de inversión pública. Mientras que las empresas europeas confían más en la iniciativa privada para desarrollar sus proyectos, las empresas españolas reclaman más inversión pública para tecnología IoT.
- ✓ Preocupación por la modernización de la cultura empresarial. En España tan solo el 25% de las empresas está concienciada de la importancia de establecer un cambio en las bases estructurales de la compañía integrando el IoT frente al 34% que existe en Europa.
- ✓ Resistencia al cambio de los trabajadores. En relación con el punto anterior, Oasys opina que las empresas españolas todavía están estudiando los beneficios de la Transformación Digital sin preocuparse de sus consecuencias como quizá ya esté pasando en el resto de Europa.
- ✓ La ciberseguridad es un tema de gran preocupación a nivel Europeo y menos a nivel nacional donde son los sectores relacionados directamente con la confidencialidad de sus datos, los que han manifestado su preocupación.

3.3.1 DESAFIOS EN EL FUTURO DEL IoT

La fragmentación de las cadenas de suministro y ecosistemas hacen que sea difícil determinar herramientas, componentes, servicios, etc., óptimos. El despliegue de un producto puede suponer relaciones con numerosos proveedores y operadores móviles de distintos países. La diversidad de tecnologías y normas para evaluar con todas las variantes hace que la toma de decisiones sea compleja y larga. Implantar modelos de IoT suele traer consigo la necesidad de cambiar procesos de negocio y de organización fundamentales. La incertidumbre que produce y el riesgo de las organizaciones son altos si, además, existe la dificultad para determinar el retorno de la inversión realizada. Estos, entre otros son, a nivel general, algunos de los factores que suman una complejidad que acaba suponiendo obstáculos a los que hacer frente para que el crecimiento del IoT sea el esperado.

Según el estudio de The Economist Intelligence Unit [15] realizado en 2016, mientras que en 2013 los principales obstáculos era la carencia de conocimientos de esta tecnología en empleados y directivos, actualmente las principales preocupaciones de las empresas son prácticas situándose en primer lugar el alto costo de la inversión necesaria en infraestructura

[15] The Economist Intelligence Unit: unidad de negocios independiente dentro del grupo The Economist. Encargado de hacer pronósticos y asesoramientos. Realizó un informe evaluando el uso de Internet de las cosas en la comunidad empresarial.
Wikipedia. Colaboradores de Wikipedia. 2016. Economist Intelligence Unit. Disponible en línea en: https://es.wikipedia.org/wiki/Economist_Intelligence_Unit [Consulta: 28/01/2017]

(29%), seguido de la seguridad y privacidad (26%), probablemente agravada por los ciberataques sufridos a finales de 2016[16].

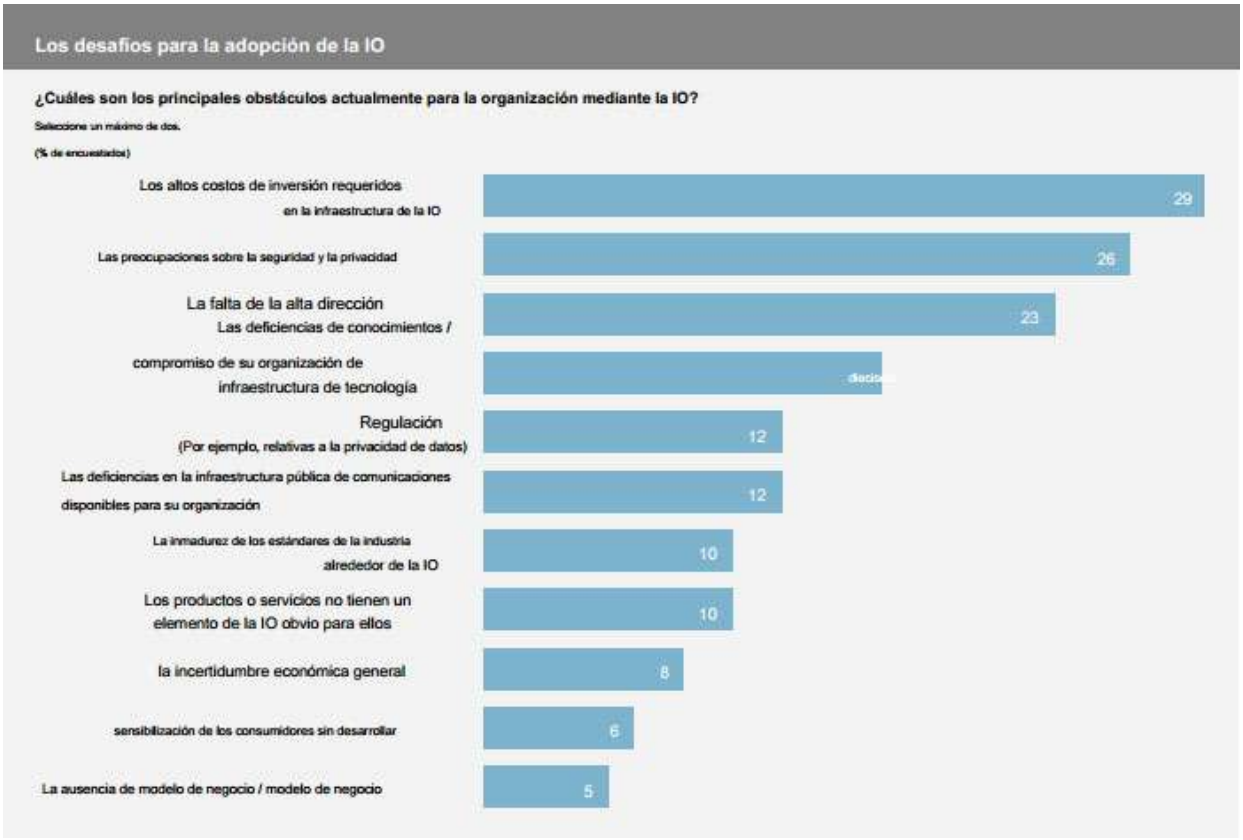

Ilustración 6: Obstáculos en el futuro del IOT. Fuente: Economist Intelligence Unit, 2016

Para algunos expertos, estos obstáculos no son más que los típicos en los inicios de una nueva tecnología. Salir de la zona de confort y enfrentarse a la inexperiencia propia de la novedad. La falta de números y estadísticas en las que basar una inversión segura, etc. Para otros el IoT es algo mucho más complejo que presenta desafíos en todo el ciclo de vida de los objetos conectados, desde su arquitectura hasta la seguridad durante el uso de los objetos. Estos desafíos se analizarán en diferentes apartados con mayor profundidad.

[16] Estudio realizado por The Economist. 2017. Disponible en línea en: https://www.eiuperspectives.economist.com/sites/default/files/EIU-ARM-IBM%20IoT%20Business%20Index%202017%20copy.pdf [Consulta 28/01/2017]

3.4 CARACTERÍSTICAS

A continuación citaremos las características más importantes que hacen que el IoT suponga un avance en la tecnología de Internet.

- INTELIGENCIA

El Internet de las cosas será "no determinista" donde las entidades u objetos virtuales actuaran de forma independiente con objetivos que no siempre serán compartidos. Así mismo, estos agentes trabajarán en diferentes contextos dependiendo de las circunstancias o el ambiente lo que dará lugar a una inteligencia ambiental.

- ARQUITECTURA

En IoT el sistema será una arquitectura orientada a eventos que tendrá en consideración cualquier nivel adicional. Esta arquitectura y el enfoque funcional coexistirán con nuevos modelos capaces de tratar excepciones y la evolución de procesos.

La arquitectura orientada a eventos es un patrón de arquitectura que promueve la producción, detección, consumo de, y reacción de eventos dentro de su contexto. Dado que no es posible crear normas para manejar todos los contextos o usos, éstas no serían estrictamente necesarias. Los actores (servicios, componentes y avatares) estarán referenciados de forma coordinada y si fuera necesario se adaptarían a normal comunes.

- SISTEMA CAÓTICO / COMPLEJO

Debido a la gran cantidad de enlaces diferentes e interacciones entre objetos autónomos y a la necesaria capacidad para integrar nuevos actores, el sistema de IoT será un Sistema Complejo. Esto puede verse como algo caótico en la que multitud de diferentes objetos con diferentes proveedores, protocolos y normas formarán parte del ecosistema IoT.

- CONSIDERACIONES TEMPORALES

En el Internet de las cosas, creado por miles de millones de objetos que pueden dar lugar a eventos que se suceden de forma paralela y simultánea, el tiempo deja de ser común y lineal y pasa a depender de los objetos, procesos, sistemas de información... El IoT deberá basarse en sistemas TI que trabajen con datos masivos y de forma paralela.

3.5 CAMPOS DE APLICACIÓN DE IOT

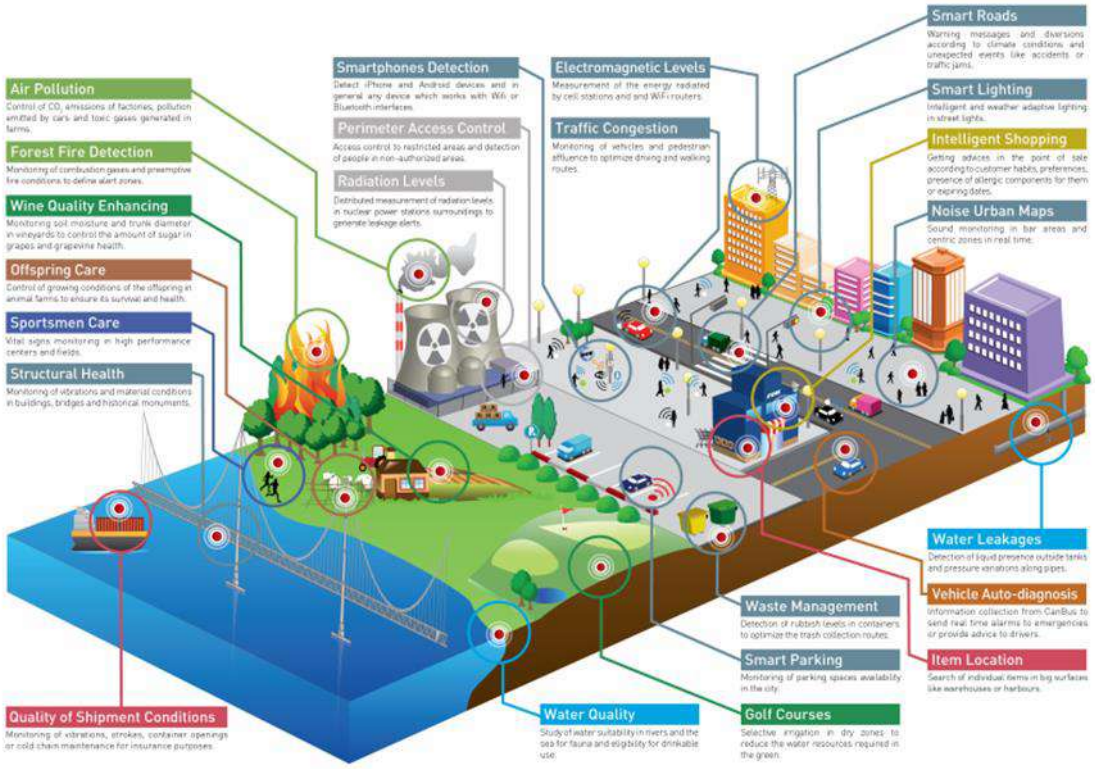

Ilustración 7: Smart World. Fuente: Libelium[17]

Internet de las cosas evoluciona a tal ritmo en los últimos años que es difícil encontrar un campo que no pueda abarcar con mayor o menor facilidad. Desde la industria hasta la educación (Smart Education), todo lo que permita tener sensores interconectados, dará capacidad de comunicarse con otros objetos, interactuar y realizar procesos de análisis con la obtención de datos cruzados. La inmersión del IoT en diferentes áreas, procurará un cambio en éstas pero también en las que directamente están relacionadas con ellas, por poner un ejemplo, parece obvio que la aparición de nuevos objetos en campos como el de la salud con relojes inteligentes o en el de la energía con contadores inteligentes influirá en un cambio en los hábitos de consumo.

En este punto citaremos algunos ámbitos en los que el IoT ha tenido o prevé tener mayor repercusión.

[17] Smart World: Ilustración de Libelium. 2013 Disponible en línea en: http://www.libelium.com/libelium-smart-world-infographic-smart-cities-internet-of-things/ [Consulta 16/04/2017]

- TRANSPORTE

Se incluyen en este punto todos los medios de transporte: vehículos, embarcaciones, aviones, trenes sobre los que se estudia la integración de dispositivos IoT

Transporte de personas y mercancías. IoT permite ampliar la información a los usuarios por medio de dispositivos insertados en los medios de transporte para que se pueda saber por ejemplo, tiempos de espera, dónde se encuentran, etc. Se podrá monitorear el tráfico al instante ofreciendo rutas alternativas que puedan ahorrar tiempo y costes.

Las empresas de transporte de mercancías podrán optimizar su flujo con contenedores de embalaje que puedan pesarse y escanearse. Ofrecer alternativas de sistemas de peaje y tarificación, control de cargas y mercancías por ejemplo, aumentando la temperatura del contenedor para garantizar que la mercancía llegará en buen estado o sabiendo donde se encuentra en todo momento en la ruta.

Automoción: Las empresas de automoción más importantes del mundo van a invertir gran cantidad de dinero en desarrollar coches automáticos que puedan ir sin conductor y en mejorar la seguridad ante incidencias buscando patrones que puedan aplicar según se produzcan determinadas acciones. La recopilación de datos relacionados con la automoción ayudará en otras áreas como las aseguradoras. El hecho de poder conocer por ejemplo, los hábitos de conducción de las personas, podrá determinar el tipo de póliza que una aseguradora pueda o no ofrecer.

Aviación: En la aviación, la inclusión de IoT supone desde aumentar la seguridad y comodidad de los pasajeros hasta reducir costes por la automatización de procesos. Las rutas, por ejemplo, podrían calcularse al momento controlando la alteración de rutas establecidas y con ello evitar accidentes, aterrizajes de emergencia… Por otro lado, el ajuste de estas rutas eligiendo las más óptimas supondrían un ahorro de combustible. Si nos vamos a los aeropuertos: embarque, salida, entrada, controles… procesos obligados, gestionados de forma automática aumentarían la eficiencia y la facilidad para el usuario. El aeropuerto de Dubái, por ejemplo, está integrando portamaletas automáticas o servicio de limpieza inteligente.

- SALUD

Prevención, monitoreo y diagnóstico precoz de pacientes, tratamiento o control de hábitos saludables son las funciones principales entorno a las que giran las aplicaciones sobre las que IoT está trabajando en el sector de la salud.

Por otro lado se encuentran las farmacéuticas donde el IoT puede aportar beneficios como el seguimiento de los medicamentos: stocks, detección de productos falsificados, control de medicamentos con necesidades especiales…

Estudiaremos este campo con mayor profundidad en el apartado 6 Internet de las Cosas en el Campo de la Salud.

- AMBIENTES INTELIGENTES.

Ciudades inteligentes, casas inteligentes, oficinas inteligentes. Este es el sector que más rápido ha crecido. Sensores y aplicaciones que pueden hacer la vida más fácil. Cambiar la luz dependiendo de la hora del día o adaptar la temperatura a las preferencias del usuario son ejemplos que permiten mayor comodidad para él y un ahorro de energía y por ende de costes debido al apagado automático de aparatos que no se usan. Estos desarrollos tienen un alto coste y por eso, se están centrando las investigaciones en aplicaciones que puedan ajustarse a las necesidades del usuario pero también a su factor económico, por ejemplo contadores inteligentes para medir el consumo de energía.

Las ciudades inteligentes (Smart City) es un campo donde empresas e instituciones están fijando cada vez más su interés. Smart Parking, indicando al conductor donde hay un hueco libre, Smart Traffic indicando en tiempo real el tráfico en la ciudad, gestión eficiente del alumbrado o regadío de jardines. Son algunos ejemplos basados en tener la mayor cantidad de datos y que tienen como objetivo facilitar la vida al ciudadano.

En el ámbito de la seguridad, alarmas conectadas incluso a objetos valiosos que pueden controlar su movimiento y que avisan a un teléfono o a otro dispositivo.

- AGRICULTURA Y ALIMENTACIÓN

El GPS permite la trazabilidad de los animales agrícolas, sus movimientos y su detección para tener el censo real en todo momento. Por otro lado, el estado de salud de los animales se puede controlar a través de muestras con un alto nivel de fiabilidad, las regiones y los países pueden ser certificados por el uso de la IoT que, sin duda, mejorará la detección y control de brote de enfermedades contagiosas.

Se prevé que dado el aumento de las personas, en 2050 la producción de alimento deberá crecer un 70% según FAO (Organización de las Naciones Unidas para la alimentación y la agricultura). La recolección de información sobre cultivos, suelos, cambio climático, maquinaria, etc. Ayudará a alcanzar el objetivo. Los sensores y la interconexión entre ellos crearán una agricultura inteligente. Por otro lado, los agricultores serán capaces de distribuir a los consumidores sus cosechas de forma independiente lo que supone un cambio en la cadena de suministro, haciéndola más directa y abaratando costes con una garantía de identificación de cosechas que previamente habrá que negociar.

Las aplicaciones actuales de los sistemas IoT en la agricultura y alimentación está todavía muy fragmentado debido a la falta de interoperabilidad entre los sistemas (La conectividad a la red en las zonas rurales puede ser un reto), los modelos de negocios

existentes y las dudas de los usuarios. La Unión Europea ha aprobado el proyecto IoF2020[18] de cuatro años de duración en el que intervendrán trece países, para mejorar estos retos organizativos y tecnológicos.

- MEDIO AMBIENTE

Evitar la deforestación de los bosques, la mejora y/o mantenimiento de la situación de los océanos a través de la toma de datos o, el control de especies en peligro de extinción son ámbitos en los que el IoT está contribuyendo de forma positiva en el medio ambiente.

Resaltan las herramientas que IoT puede proporcionar en el campo de las energías renovables. La integración de aplicaciones de medición de eficiencia de fuentes de estas energías, de uso de redes eléctricas o consumo de energía ayudaran a equilibrar las actividades de suministro y demanda. El aumento de fuentes de energías renovables implicará un incremento en la acumulación de energía que requerirá una mejor gestión y análisis de datos. Por otro lado, la mejora y equilibrio del sector energético pueden reducir las emisiones de CO2. Según un informe de A.T.Kearney[19] realizado en 2015, el desarrollo de IoT rebajará las emisiones de CO2 en Europa en 200 millones de toneladas en 2025, un 22% de lo que falta para cumplir el objetivo de reducción para el 2030.

La necesidad de energía para que millones de dispositivos se añadan al IoT también afecta, aunque de otra manera, al medio ambiente. Se debe hacer un esfuerzo para crear un IoT con un consumo reducido que genere el menor impacto posible. En este sentido el LPWA (redes de amplio espectro y de bajo consumo) mejorará en un futuro cercano, los sensores actuales: su vida útil será de varios años y podrán ser situados a mayor distancia de la antena.

- INDUSTRIA MANUFACTURERA

Este sector es uno de los más beneficiados por la llegada del IoT. Los artículos pueden vincularse a aplicaciones IoT a través de identificadores únicos o por dispositivos inteligentes integrados en maquinarias de fábricas o almacenes de estantes permitiendo el seguimiento del producto en tiempo real en todo su ciclo de vida, desde la producción hasta el final del ciclo; de una forma eficiente, fácil y con costes bajos.

Los datos detallados de un artículo pueden monitorearse y guardarse en la etiqueta o en el sistema de información. Estos datos pueden facilitar tareas como el diseño de los productos o servicios relacionados, la comercialización o, finalmente la toma de decisiones para la eliminación del producto o su reciclaje.

[18] El proyecto IoF2020. Promovido por la UE tiene como objetivo promover y acelerar la adopción de IoT en el campo agrícola y alimentario de Europa.
Comisión Europea. 2017. Disponible en línea en: http://cordis.europa.eu/project/rcn/206761_es.html [Consulta: //2017]

[19] A.T.Kearney: Empresa de asesoría internacional.

La inmersión del IoT en la industria, no sólo manufacturera, significa una transformación. Las tareas mecánicas serán realizadas por tecnología sustituyendo la mano de obra y el funcionamiento laboral será muy diferente al que conocemos hoy. Realmente para la industria, la llegada del IoT supondrá a corto plazo un cambio en la forma de ver los negocios.

4 ECOSISTEMA Y ARQUITECTURA DEL IOT

Actores, dispositivos y la relación que se establece entre ellos, así como elementos externos como pueden ser la legislación o el tratamiento de los datos, forman el ecosistema IOT.

En un ecosistema IoT la relación entre personas, procesos, cosas y datos requiere pensar en la variedad de proveedores y usuarios que pueden participar y en una comunicación, que además de la tradicional persona-persona o persona-máquina, podrá ser máquina-máquina dado que, los objetos con los que interactuamos en este ecosistema pueden compartir y utilizar datos de otras máquinas. En la siguiente ilustración podemos ver los diferentes actores y la relación que puede establecerse entre ellos.

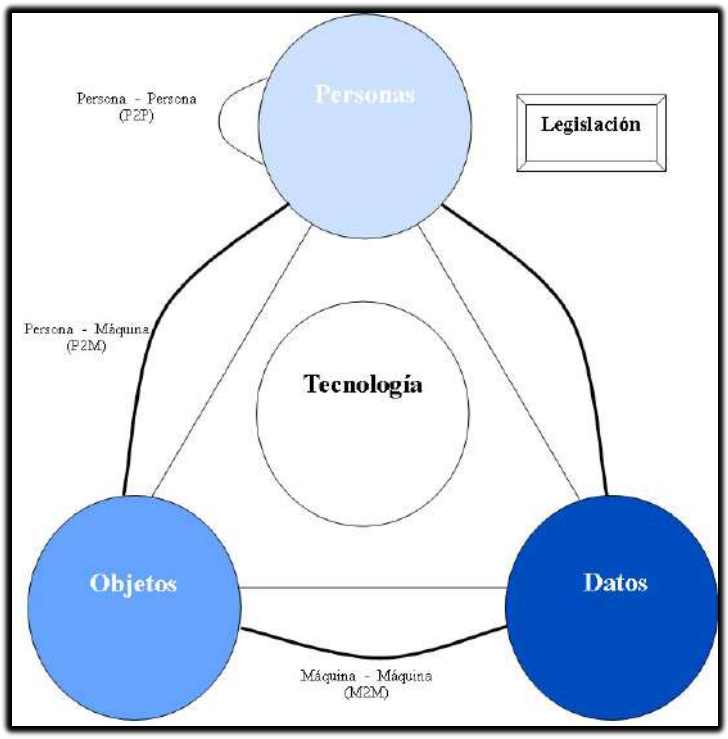

Ilustración 8: Ecosistema de IoT. Elaboración propia.

4.1 ACTORES

Se podrá definir como "actor" dentro de un ecosistema IOT a cualquier persona que de una forma u otra tengan cierto grado de responsabilidad directa dentro de alguna de las capas de la arquitectura IoT.

- Usuarios

Serán las personas que utilicen los dispositivos inteligentes y, por ende, los titulares de los datos personales y quienes entregarán la información para su posterior tratamiento y fin. Los usuarios no siempre serán los que adquirieron el dispositivo.

- Proveedores

Podemos diferenciar entre varios tipos de proveedores:

- **Fabricantes de dispositivos**: Serán las empresas que proveen los dispositivos o equipos físicos encargados de captar la información. Normalmente, además del hardware, estos proveedores modifican los sistemas operativos o el software de los dispositivos para determinar o ajustar su funcionalidad (Por ejemplo la frecuencia en la recogida de los datos). Estos proveedores también pueden recoger y procesar información de su dispositivo.
- **Proveedores de plataforma**. Proveedores de software IoT, servicios de alojamiento en la nube [20] o servidores físicos locales.
- **Desarrolladores de aplicaciones**: Terceros encargados de desarrollar aplicaciones para los fabricantes de dispositivos IoT. Normalmente a la hora de utilizar estas aplicaciones, se permite que estos desarrolladores accedan a los datos que el proveedor del dispositivo ha almacenado.
- **Integradores**: empresas que tratan directamente con el usuario final. Comercializan los servicios IoT de forma integrada (Dispositivo, aplicaciones y plataforma de alojamiento).

[20] El almacenamiento en la nube es un modelo de almacenamiento donde los datos están almacenados en espacios virtualizados normalmente ofrecidos por terceros. Su acceso será a través de un servicio web, una interfaz de programación de aplicaciones o una interfaz de usuario.
Wikipedia. Colaboradores de Wikipedia. Almacenamiento en nube. 2016 Disponible en línea en: https://es.wikipedia.org/wiki/Almacenamiento_en_nube [Consulta 10/06/2017]

4.2 ARQUITECTURA IOT

En IOT la información sigue un proceso vertical en el que fluye del medio físico a un medio virtual. El sistema estará basado en una arquitectura orientada a eventos y construida de abajo hacia arriba mencionada como una característica del IOT en el punto *3.4 Características.*

4.2.1 CARACTERÍSITICAS DE LA ARQUITECTURA IOT

- Conectividad.

La conectividad permite compatibilidad y acceso a la red, sea cual sea el medio que le rodea

- Escalabilidad

Una arquitectura deberá diseñarse para que pueda ser escalable y capaz de soportar un gran número de dispositivos.

Estas arquitecturas suelen ser de costes elevados y por tanto, se puede tomar también como un requisito el poder escalar el servidor en servidores económicos para poder conseguir una arquitectura asumible.

- Interacción

En un sistema que trate de mantener objetos inteligentes conectados, una de las principales características que se deben cumplir es la interacción que deberá establecerse entre cualquier objeto y de forma bidireccional para que puedan interactuar entre ellos.

El protocolo HTTP aun siendo el más común y útil para todos los dispositivos y capaz de ofrecer una conectividad unificada, presenta dos problemas a resaltar. Por un lado el tamaño de la memoria del programa en dispositivos pequeños y por otro, el alto nivel de energía que requiere.

Si además, tenemos en cuenta que los dispositivos pueden conectarse directamente a la red o a través de gateways necesitando en este caso, dos protocolos de comunicación, parece importante buscar protocolos de comunicación pequeños y simples con habilidad para superar firewalls.

La interacción entre sistemas o componentes se pueden dar en las siguientes capas:

- Interoperabilidad técnica: normalmente se asocia con componentes software / hardware, sistemas y plataformas que permiten una comunicación máquina a máquina. Esta comunicación se centra en protocolos y su infraestructura necesaria.
- Interoperabilidad sintáctica: Los mensajes transferidos deben tener una sintaxis y codificación definida. Cuando un protocolo lleva contenido puede utilizar sintaxis de transferencia de alto nivel.
- Interoperabilidad semántica: Se relaciona con el entendimiento a nivel humano del contenido intercambiado.
- Interoperabilidad organizativa: Capacidad de las organizaciones para comunicarse de manera efectiva aunque utilicen diferentes sistemas de información sobre diferentes infraestructuras, quizá en diferentes zonas geográficas.

➢ Energía.

Cada dispositivo que tengamos conectado deberá tener la mayor autonomía posible ya que sin energía el dispositivo no funcionará. Los retos, en un mundo inteligente, estarán en integrar los dispositivos con energías renovables e inagotables, y por otro lado en encontrar el medio por el que la energía pueda compartirse entre los diferentes dispositivos, algo que, parecen no cumplir las baterías aunque éstas sean cada vez más duraderas.

➢ Seguridad.

Aunque después profundicemos en el tema de la seguridad, cabe citarla como una característica que debe estar presente en cualquier arquitectura del IoT tanto en términos tradicionales (riesgo eléctrico, etc.) como digital (privacidad, etc.).

A falta de fijar unos criterios de valoración, se crea un nuevo paradigma de seguridad capaz de escalar sin complicaciones y en el que deben participar todos los actores implicados. Como aproximación, podemos decir que una arquitectura IoT deberá soportar entre otros requerimientos:

- Encriptación de dispositivos.
- Modelo de identidades basado en tokens[21].
- Gestión de tokens y accesos lo más remota y fácilmente posible.
- Control de accesos basados en políticas y con gestión de usuarios para sistemas basados en XACML.

[21] Tokens de seguridad: Dispostivos electrónicos encargados para facilitar procesos de autenticación. Encargados de almacenar claves criptográficas como firmas digitales, datos biométricos o huellas digitales.
Wikipedia. Colaboradores de Wikipedia. Token de seguridad. 2010. Disponible en línea en: https://es.wikipedia.org/wiki/Token_de_seguridad [Consulta 10/06/2017]

4.2.2 PARTES DE UNA ARQUITECTURA IOT

Para analizar la arquitectura IoT hemos cogido como ejemplo la propuesta de Sumit Sharma de MuleSoft[22] que divide la arquitectura en cuatro grandes grupos.

Ilustración 9: Modelo arquitectura IoT. Fuente: Sumit Sharma. 2014

4.3 COSAS / OBJETOS / DISPOSITIVOS

Sensores, actuadores y hardware para comunicar el mundo físico con el virtual forman la capa de la IOT más visible para los usuarios y la que menos espacio ocupa. Los componentes cada vez son más pequeños, lo que facilita que se pueda conectar casi cualquier cosa desde cualquier sitio y en cualquier momento.

- **SENSORES**

La RAE (Real Academia Española) define un sensor como un "*Dispositivo que detecta una determinada acción externa, temperatura, precisión, etc…, y la transmite adecuadamente*". En IoT los sensores son una de las piezas fundamentales que permiten que objetos comunes interactúen con ordenadores y recopilen información. Entre sus características podemos resaltar:

[22] Sumit Sharma de MulseSoft es una empresa creada en 2006 centrada en la creación de software para conectar aplicaciones, fuentes de datos y APIs.

- Múltiples sensores pueden unirse a un objeto, gracias a su tamaño; para medir una amplia gama de datos (variables físicas o fenómenos, por ejemplo) que transmitirán para un análisis posterior. Por ejemplo, las compañías de seguros pueden utilizar sistemas de sensores que recuperen información de las pautas de conducción de sus asegurados.
- Los sensores pueden desencadenar acciones, permitiendo la elaboración de patrones que determinen la automatización de funciones. Puede ser el caso de una alarma. Un sensor podría ser un componente M2M, un lector RFID (Radio Frecuency IDentification), o un medidor de SCADA (Supervisory Control And Data Adquisition).
- Podrán ser localizables en todo momento. Con ello se podrán realizar aplicaciones en las que se necesite saber la localización exacta de forma continua y, por otro lado poder saber el comportamiento de los consumidores o las decisiones que pueden influir en un proceso. Esta información permitirá realizar cambios sobre la marcha minimizando costes, teniendo una imagen más real de la empresa/producto y evitar imprevistos. Podemos poner el ejemplo de una empresa de logística.

Dentro de los retos que nos podemos encontrar en el desarrollo de los sensores, podemos destacar el consumo de energía y la interoperabilidad. Como hemos mencionado anteriormente, una característica a tener en cuenta en una arquitectura IOT es la energía, la lucha por intentar reducir el tamaño de los sensores hace que el factor de la energía sea cada vez más limitante. El tamaño de las baterías se reduce y con ello el tiempo de funcionamiento. El objetivo, en este punto, es encontrar la forma de que los sensores generen su propia energía para aumentar su autonomía.

Por otro lado, y más prioritario, se encuentra la necesidad de dar la mayor flexibilidad y modularidad a los componentes para asegurar la integración de éstos. La diferencia entre los sensores, obliga a que exista una plataforma que gestione los diferentes datos.

- **Actuadores.**

Dispositivos capaces de transformar energía en la activación de procesos que puedan generar un efecto sobre un proceso automatizado. Los actuadores son capaces de procesar datos, simplemente reciben una señal desde el controlador y realizan una acción. Hay tres tipos de actuadores utilizados en la IoT:

- Hidráulica: utiliza la presión del líquido para realizar movimiento mecánico.
- Neumáticos: utiliza aire comprimido a alta presión para permitir el funcionamiento mecánico.
- Eléctrico: convierte la energía eléctrica para el funcionamiento mecánico.

- **Tecnologías de sistemas micro electromecánicos (MEMS).**

Se trata de diminutos dispositivos mecánicos impulsados por electricidad. Fusiona la nano escala, los sistemas nano electromecánicos y la nanotecnología. Los MEMS pueden

actuar como sensores, actuadores o de traductor. Aunque esta tecnología todavía no se conoce al mismo nivel que los sensores.

4.3.1.1 Puntos de acceso y conectividad

Los puntos de acceso permiten la conectividad de los objetos. Conocidos como gateway o interfaces de comunicación. Establecen una conexión entre los periféricos (dispositivos y objetos) y la nube para recoger la información obtenida y poder gestionarla. La comunicación debe ser segura, robusta y tolerante a fallos. A continuación numeramos algunas de las funciones que deben cumplir:

- Deberá tener una interfaz para conectar con una LAN (Local Area Network) o WLAN.
- Debería implementar interfaces para redes Bluetooth, ZigBee …
- Consolidar datos con diferentes formatos en un formato común y entendible para Internet.

El gateway concentra toda la complejidad IP que antes recaía sobre los nodos y de esta forma se reduce el consumo, la memoria y el procesamiento de estos. Por otro lado, en muchas aplicaciones de IoT, el gateway puede integrar un interfaz de usuario para centralizar la gestión y el mantenimiento de los nodos o un servidor Web que permita al usuario conectarse a la red a través de sus dispositivos. Si analizamos las ventajas de un gateway hacia el lado de la nube, se minimiza la complejidad y el coste de una conexión directa a Internet

A continuación indicamos tres modelos de arquitectura con Gateway:

- En el primer modelo: los nodos se conectan a Internet a través del gateway a través de cables o conexión inalámbrica. El gateway tiene un software para gestionar el flujo de información o tratar lo datos.
- En el segundo modelo: los nodos se conectan a Internet que conlleva que tengan más capacidad y recursos para implementar TCP/IP y para consumir más energía. El gateway puede ser un router convencional que sólo hará tareas de gestión de de datos.
- En el tercer modelo: entre los nodos e Internet hay un interfaz con conexión PAN o cualquier otro protocolo. El gateway serviría de traductor para que entre la red PAN y la red WAN se entiendan.

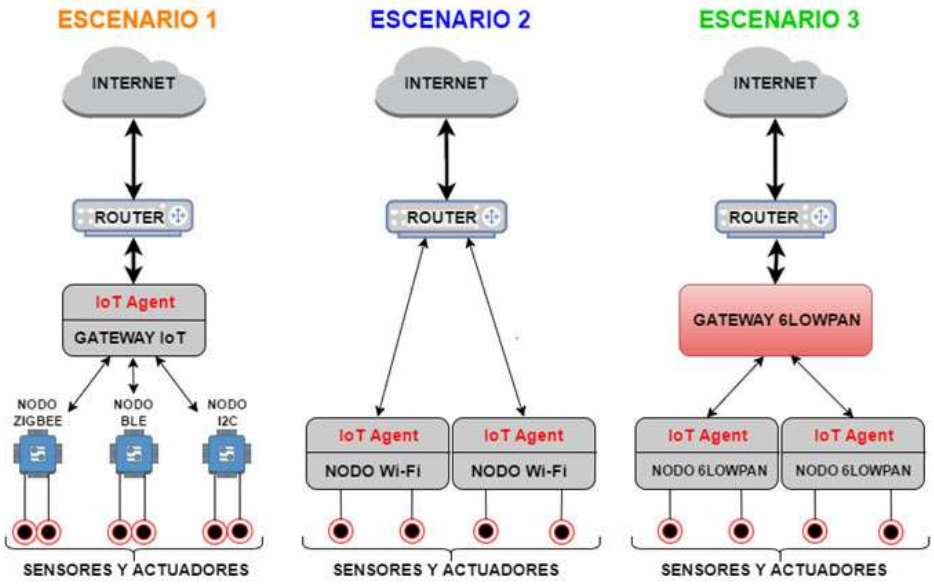

Ilustración 10: Modelos arquitectura con gateway. Fuente Ermesh

Aunque damos por hecho que en la mayoría de los sitios tendremos la posibilidad de conectarnos a internet para utilizar nuestros dispositivos, lo cierto es que la capacidad de las infraestructuras de telefonía móvil es limitada y el crecimiento de los teléfonos inteligentes está saturando la capacidad de las redes. Si sumamos millones de nuevos dispositivos que se deberán conectar, la capacidad de las redes móviles actúa como un cuello de botella al que se necesita buscar soluciones que pasan por compartir el espectro.

Protocolos y tecnologías de comunicación facilitan mover los datos al menor coste posible y con bajo consumo. Podemos mencionar entre otros a: ZigBee con un radio de acción de 10 – 100 m. interior y 1km exterior, WIFI con un radio de 70 m. interior y 300 m. exterior, entre otras.

ZigBee o RFID son algunas de las tecnologías que no utilizan IPv6. Todos los dispositivos conectados a Internet navegan con un número diferente conocido como dirección IP y por el que pueden ser identificados. Esta dirección IP sirve para establecer su conexión con el resto de la red. Este sistema funciona con los protocolos IPv4 e IPv6. Dado el número de dispositivos que van conectándose a la red y todos los que se esperan para los próximos años, las direcciones IPv4 se están agotando y esto obliga a que Internet de las cosas se implemente sobre IPv6.

Las redes inalámbricas para IoT se pueden clasificar según su alcance en redes de corto y largo alcance y, otras redes como vía satélite.

Introducimos en este punto el término: "Internet cero". Hasta ahora en los avances de la tecnología se hacía especial hincapié en que la velocidad no bajara. Actualmente muchos estándares de IoT compiten por dotar a los objetos cotidianos de capacidad para conectarse a la internet a baja velocidad sin que esto suponga una desventaja y, a un precio menor.

4.3.1.2 Procesamiento de datos

Una de las claves del IoT son los datos. El buen funcionamiento de un sistema dependerá directamente de la capacidad de gestión y el uso que se haga de ellos que pasa porque un sistema sea capaz de recoger la información solamente necesaria, almacenarla y analizarla. En este punto las plataformas en la nube adquieren toda la importancia.

Plataformas en la nube: es la capa superior desde donde se centralizan los servicios de la estructura IoT que tiene como objetivo mostrar los beneficios de una solución IoT como costes, calidad, control… Entre otros servicios de infraestructura que deben ofrecer se encuentra: Bases de datos, Integración de servicios de software, identificación de usuarios, configuración remota, obtención de informes (Análisis del funcionamiento de los componentes del sistema IoT). Se pueden distinguir tres grupos de plataformas IoT. Por un lado las plataformas para pequeños proyectos: Dweet.io, etc. Por otro, plataformas para proyectos de dimensiones más grandes: M2X y finalmente las tres grandes plataformas que ofrecen servicios completos de infraestructura para desarrolladores de diferentes ámbitos: Microsoft Azure, GoogleCloud y AWS Amazon.

Volviendo al tratamiento de la información, no finalizará en el análisis de ésta. Los datos han sido analizados con un fin, por ejemplo, lanzar alertas basadas en el cumplimiento o no de reglas (Dependiendo de una temperatura poner la calefacción o el aire acondicionado). Dentro del análisis avanzado de datos podemos destacar big data.

4.3.1.3 Relaciones del IoT con la tecnología

Internet de las cosas es un compendio de distintas tecnologías para poder dar vida e inteligencia a objetos. Sensores, actuadores, redes, gateways, protocolos de datos… desempleando cada una de ellas su función, hay sectores y tecnologías directamente relacionadas con el IoT de tal manera que sin ellas la existencia de objetos inteligentes conectados entre sí existiría sólo en nuestra imaginación.

- IOT y BIG DATA

  Big data es un concepto enmarcado en el sector de las tecnologías de la información y la comunicación, que hace referencia a la tecnología basada en el análisis masivo de

datos que no pueden ser procesados o analizados utilizando herramientas tradicionales (es decir, que generalmente tienen que ser gestionados por una plataforma específica para ellos).

Una de las características del IoT es la recolección de datos que son capaces de recoger los dispositivos pero no vale de nada generar datos si no se pueden gestionar y analizar de forma correcta, es por esto que el IoT y Big Data están estrechamente relacionados.

- IOT Y RFID

Ya hemos hablado de la tecnología RFID (Radio Frequency Identification), cuyo objetivo es el de identificar objetos de una forma rápida, con poca transmisión de información y en un entorno cercano. De tal forma que implementándolo con el IoT se puede dar identidad a cada objeto para generar datos. La RFID puede proporcionar datos sencillos sobre una cosa a medida que se escanea. La RFID de lectura / escritura puede recopilar más datos y conjuntamente con GPS puede recopilar datos adicionales como temperatura, ubicación, etc.

- IOT Y CÓMPUTO UBICUO

La computación ubicua (ubicomp) es la integración de la informática en el entorno de la persona, de forma que los ordenadores no se perciban como objetos diferenciados; apareciendo entonces en cualquier lugar y en cualquier momento y contando con características como transparencia o interconexión de dispositivos.

La computación ubicua es soportada en dispositivos no tradicionales, de pequeño tamaño o invisibles, con lo cual se mezcla con un entorno físico. Dotados de sensores para recopilar datos de su entorno, son sensibles al contexto en el que se encuentran y normalmente pueden presentarse en forma de “objeto inteligente” o dispositivo digital.

Teniendo estas características y sus capacidades en cuenta, podemos decir que Internet de las Cosas resulta una evolución de la computación ubicua.

- IOT Y COMPONENTES M2M

M2M (Machine to machine) se refiere a la comunicación entre máquinas entendiendo como máquina un dispositivo electrónico, un robot, un automóvil o cualquier cosa que no sea una persona. Esa máquina debe comunicar por Internet con un servidor que gestiona información.

Es común encontrarnos con la utilización del término M2M e IoT de manera indistinta. Esta es una idea errónea pues aunque tengan puntos en común no son lo mismo.

- IoT se enfoca a bienes de consumo, ofreciendo un servicio en un mercado globalizado, el M2M está enfocado al punto de vista técnico de las comunicaciones.
- La información capturada a través de M2M se transmite por la red que traducirá la información útil. El IoT, sin embargo interconecta sistemas M2M aislados que actúan sin intervención humana y transmite los datos por conexión IP.
- Por otro lado en M2M las cosas envían información que recolectan y en IoT las cosas envían, reciben, procesan información y realizan acciones con ayuda de soluciones de Big Data.

A continuación mostramos el esquema que tiene el M2M y el que tiene Internet de las Cosas.

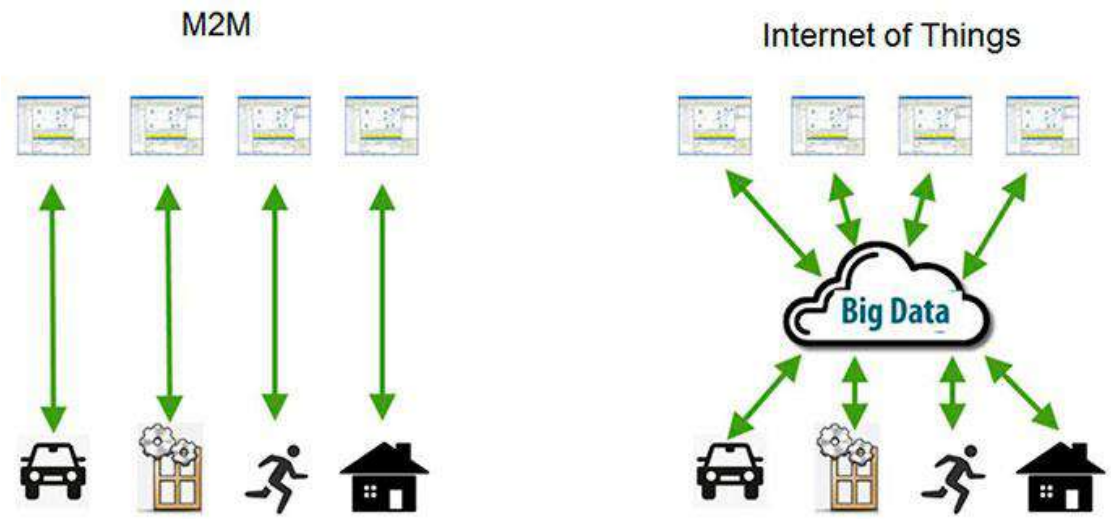

Ilustración 11: Esquema M2M e IoT[23].

Podemos decir que IoT intenta ser un bus que interconecta sistemas M2M aislados en sistemas más amplios que interactúan sin intervención humana.

[23] Fuente: Lo más nuevo. Autor Erwin. Artículo "Diferencias entre IoT y M2M Machine to Machine. 2015. Disponible en línea en: http://www.lomasnuevo.net/iot/diferencias-entre-iot-y-m2m-machine-to-machine/ [Consultado 25/04/2017]

5 IMPLICACIONES DEL USO DE INTERNET DE LAS COSAS EN EL DERECHO A LA PROTECCIÓN DE DATOS

5.1 INTRODUCCIÓN CONCEPTOS BÁSICOS

Hemos visto a lo largo de todo el trabajo las características del IoT, también las previsiones que indican que de forma inevitable Internet de las Cosas entrará en nuestras vidas y aportará grandes ventajas en personas y empresas, grandes y pequeñas de tal forma que muchos lo llegan a catalogar como una nueva revolución.

Entre los grandes desafíos que encontramos, uno de los que más preocupan a gobiernos de distintos países, organismos, empresas y a la sociedad en general, es la seguridad y la amenaza a la privacidad de los usuarios. Sin duda, el manejo de gran cantidad de datos es una de las ventajas del IoT. No sólo los datos que proporcionemos serán válidos, también lo serán los que se puedan derivar de la recopilación, análisis y cruces entre dispositivos. Patrones de comportamientos, estado de la salud física o el control de los horarios del usuario, son sólo algunos ejemplos que podemos encontrar. Esto nos hace llegar a preguntarnos si a nivel de seguridad y protección de datos ¿Estamos preparados para el IoT?

Parece necesario en este momento; analizar detenidamente la repercusión que el IoT puede tener y la que puede llegar a alcanzar, así como la revisión de las herramientas actuales a nivel legal para asegurar el cumplimiento de privacidad y derechos de los usuarios por un lado y las obligaciones de los responsables por otro.

En el siguiente punto revisaremos las leyes vigentes en este momento a nivel nacional e internacional. El trabajo que se está haciendo al respecto de la nueva tecnología para preservar los principales derechos: el derecho a la privacidad y el derecho a la protección de datos y el papel de cada actor que forma parte del ecosistema del IoT. A continuación revisaremos conceptos básicos que debemos conocer y manejar para analizar los desafíos del IoT al respecto.

5.2 DERECHOS A LA INTIMIDAD, AL HONOR Y A LA PROPIA IMAGEN

Dentro de los derechos fundamentales, la Constitución Española de 1978 considera uno de ellos el derecho a la intimidad y así queda reflejado en el artículo 18 de la sección 1ª de los derechos fundamentales y libertades públicas: *"Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".*

El Tribunal Constitucional relacionó el derecho al honor, a la intimidad y a la propia imagen con el fundamento común del principio de dignidad de la persona[24] indicando que los tres tenían rasgos comunes pero también aspectos que permiten diferenciarlos.

A continuación desglosaremos el artículo 18 de la Constitución.

5.2.1 DERECHO AL HONOR

Debemos tener presente que el honor está vinculado a las circunstancias de tiempo y lugar. Se distinguen dos aspectos. El primero consiste en la estima que cada persona tiene de sí misma; el segundo se centra en el reconocimiento de los demás de nuestra dignidad y por tanto está más relacionado con la fama y la opinión social.

5.2.2 DERECHO A LA INTIMIDAD PERSONAL Y FAMILIAR

Se vincula a la esfera más reservada de las personas, al ámbito que éstas siempre preservan de las miradas ajenas, aquél que desea mantenerse oculto a los demás por pertenecer a su esfera más privada, vinculada con la dignidad y el libre desarrollo de la personalidad. La intimidad, de acuerdo con el propio precepto constitucional, se reconoce no sólo al individuo aisladamente considerado, sino también al núcleo familiar.

5.2.3 DERECHO A LA PROPIA IMAGEN

Este derecho salvaguarda la proyección exterior de dicha imagen como medio de evitar inferencias no deseadas, de velar por una determinada imagen externa o de preservar nuestra imagen pública. Este derecho está íntimamente condicionado por la actividad del sujeto, no sólo en el sentido de que las personas con una actividad pública verán más expuestas su imagen, sino también en el sentido de que la imagen podrá preservarse cuando se desvincule del ámbito laboral propio.

El desarrollo de la protección de estos tres derechos lo realiza la L.O. 1/1982, de 5 de mayo, donde se intentan separar supuestos de intromisión ilegítima (art. 7)[25], de aquellos que no

[24] Sentencia del Tribunal Constitucional 231/88 de 2 de diciembre, establece que la privacidad, vida privada o intimidad "preserva el ámbito propio y reservado frente a la acción y conocimiento de los demás, el cual es necesario para mantener la calidad de vida mínima".

[25] Artículo 7: Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo 2 de esta ley.

puedan reputarse como tales, por mediar consentimiento o por recoger imágenes públicas (art. 8)[26]. La ley L.O. 4/1997, de 4 de agosto, se regula la utilización de videocámaras en lugares públicos por las Fuerzas y Cuerpos de Seguridad (art. 8 y 9 L.O 4/1997).

1. El emplazamiento en cualquier lugar de aparatos de escucha, filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas.
2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como una grabación, registro o reproducción.
3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo.
4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela.
5. La captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 8.2.
6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga.
7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.
8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas.

[26] Artículo 8 de la ley L.O. 4/1997:

1. No se reputarán, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la ley, ni cuando predomine un interés histórico, científico o cultural relevante.
   - En particular, el derecho a la propia imagen no impedirá:
   - Su captación, reproducción o publicación por cualquier medio, cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.
   - La utilización de la caricatura de dichas personas, de acuerdo con el uso social.
2. La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.

Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza.

5.3 DERECHO A LA PROTECCIÓN DE PROTECCIÓN DE DATOS

Redactada tomando como ejemplo la Constitución portuguesa realizada dos años antes; una primera interpretación llevó a considerar este derecho como una especificación del derecho a la intimidad, pero el Tribunal Constitucional ha interpretado que se trata de un derecho relacionado con el de la intimidad pero independiente.

Con este derecho fundamental se garantiza a la persona el control sobre sus datos, sean de carácter íntimo o no, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos sean usados para fines distintos a aquel que justificó su obtención.

Este derecho queda recogido en el Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de datos de carácter personal. Se debe destacar el Real Decreto 1720/2007 sobre el que hablaremos más delante y de forma más detallada.

5.4 DERECHO A LA PROTECCIÓN DE DATOS. NORMATIVA Y LEGISLACIÓN

En España, la Constitución de 1978 recoge en el artículo 18.4 que: "*El legislador limitará el uso de la informática para proteger los derechos fundamentales de los ciudadanos*".

El 30 de noviembre de 2000, se dicta la Sentencia 292/2000 por el Tribunal Constitucional donde se pretende limitar el uso de la informática "*para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de su derecho*". Se recoge que el Derecho a la Protección de datos, es un derecho fundamental específico e independiente de otros derechos que se recogen en el artículo 18 de la Constitución Española de 1978.

El Derecho a la Protección de Datos prevé garantizar el libre y pleno ejercicio de cualquiera de los derechos (Intimidad, honor, propia imagen, no discriminación, trabajo, etc.) mediante la protección de cualquier dato personal que pueda identificar o permitir la identificación de una persona.

Las garantías por una parte, consisten en la creación de la Agencia de protección de datos con el fin de velar por el cumplimiento de la Ley, y el Registro general de protección de

datos en el que deberán inscribirse todos los ficheros de acuerdo con la Ley. Por último se establece un régimen sancionatorio.

A nivel europeo, en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea se recoge también este derecho como *"Protección de datos de carácter personal":*

1. *Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
2. *Esos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamente legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
3. *El respeto de estas normas quedará sujeto al control de una autoridad independiente.*

Quedando la legislación aplicable:

- **Normativa Nacional.**
  - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal
  - Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.
  - Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- **Normativa Europea.**
  - 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. Posteriormente la Directiva fue modificada por la Directiva 97/66CE derogada por la Directiva 2002/58/CE.
  - Directiva 2016/679 del Reglamento General de Protección de Datos de la Unión Europea que ya está en vigor y que comenzará a aplicarse a partir de 25 de mayo de 2018.

La Constitución Español de 1978 y la Normativa de la Unión Europea prevalecen sobre las demás leyes.

Los tratados internacionales, estarán al mismo nivel que la Constitución Española ya que, el contenido del tratado será conforme a la Constitución y, en caso de no serlo se puede negociar o hacer una revisión constitucional. Tan solo hasta que el tratado esté publicado en el Boletín Oficial del Estado, la Constitución estará por encima del Tratado.

5.5 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La Unión Europea en la Directiva 95/46/CE, dice que: *"La creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales" (Considerando 62 de la Directiva 95/46).* Así como en el apartado 8.3 de la Carta de Derechos Fundamentales de la Unión Europea queda reflejado sobre el Derecho de Protección de Datos que: *"El respeto de las normas quedará sujeto al control de una autoridad independiente".*

La Agencia Española de Protección de Datos (AEPD) se creó en 1992 siguiendo el criterio organizativo y funcional propuesto en el Convenio 108 y comenzó su funcionamiento en 1994 con naturaleza independiente, presupuesto propio y plena autonomía funcional comenzando su funcionamiento en 1994.

Dentro de las funciones de Agencia Española de Protección de Datos recogidas en el Artículo 37 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD) podemos resaltar[27]:

- *Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.*
- *Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.*
- *Atender las peticiones y reclamaciones formuladas por las personas afectadas.*
- *Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.*
- *Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.*

[27] Puntos extraídos de Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal consultado en http://noticias.juridicas.com/base_datos/Admin/lo15-1999.t6.html#t6 y Guía del derecho fundamental a la protección de datos de carácter personal. Agencia Española de Protección de Datos. AEPD, 2004. Disponible en línea: http://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf [Consulta: 18/01/2017]

- *Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.*

- *Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.*

- *Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.*

5.6 DEFINICIONES

5.6.1 Persona identificada o identificable

La Lopd (y el Reglamento que la desarrolla, Real Decreto 1720/2007) considera como "*persona identificable*" a "*toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados*".

5.6.2 Datos

No todos los datos de las personas se tratan de igual forma, hay datos que son especialmente sensibles y por tanto se tratarán de distinta manera que los datos generales del usuario.

5.6.2.1 Datos de carácter personal

Se define "*datos de carácter personal*" como "*Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*" (Artículo 3.a de la Lopd y 5.1.f de su reglamento)

Entendemos por "*información concerniente a una persona identificada*" a cualquier información que nos indica a que persona se refiere sin que se tenga que realizar ninguna averiguación. Por ejemplo el Documento Nacional de Identidad. Y, por "*Información concerniente a una persona identificable*" a información que a priori no indica a que persona se refiere pero que es suficiente para averiguarlo.

Ejemplos de datos de carácter personal pueden ser nombre, apellidos, Dni, fotografías, videos, voz, huellas, etc. que hagan referencia a una persona física (identificada o identificable).

5.6.2.2 Datos especialmente protegidos.

También conocidos como "*datos sensibles*" son una categoría de datos de carácter personal que, por su importancia en la intimidad, derechos fundamentales y libertades públicas del individuo, necesitan mayor protección que otros datos. El tratamiento de estos datos está regulado en el artículo 7 de la Lopd y son:

- Datos que revelen la ideología, afiliación sindical, religión y creencias. Se establece en el apartado 2 del artículo 16 de la Constitución que, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Deberá existir un consentimiento expreso y por escrito del afectado para que puedan tratarse los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Advirtiendo al interesado sobre su derecho a no prestarlos cuando se solicite el consentimiento para recabar información sobre alguno de estos datos. Con excepción de fichero mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica religiosa o sindical, en cuanto a datos de asociados o miembros, necesitando, ante la cesión de dichos datos, precisar el previo consentimiento del afectado.
- Datos que hagan referencia al origen racial, la salud o la vida sexual. Este tipo de datos sólo podrán ser recabados, tratados y cedidos cuando la ley así lo disponga o el afectado dé su consentimiento expreso.
- Datos relativos a la comisión de infracciones penales o administrativas. Sólo podrán incluirse en ficheros de las Administraciones públicas competente o en los supuestos previstos en las respectivas normas reguladoras.

Excepciones: podrán tratarse los datos especialmente protegidos cuando dicho tratamiento resulte necesario para prevención o diagnóstico médico, prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios siempre que ese tratamiento se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a esta obligación o equivalente. También podrán utilizarse cuando sea por el interés vital del afectado o de otra persona siempre y cuando el afectado se encuentre incapacitado para dar su consentimiento.

5.6.2.3 Tratamiento de datos

El artículo 5.1.t) del RLOPD define al tratamiento de datos como "*cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*".

5.6.2.4 Fichero

Jurídicamente se define Fichero a "*todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*" Como se recoge en el artículo 3.b de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y artículo 5.1.k del Real Decreto 1720/2007

La manera en la que se lleva a cabo el almacenamiento y la organización de los datos se diferencia entre ficheros automatizados: cuando los datos personales se almacenan en soportes físicos y el acceso a éstos se hace por medio de algún tipo de aplicación o proceso automatizado. Y ficheros no automatizados que se recogen en el RLOPD 5.1.n como "*todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica*". Por ejemplo documentos que se guardan en archivadores.

Dependiendo de la titularidad de los ficheros el RLOPD distingue:

- *Ficheros de titularidad privada: "los ficheros 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.m)*
- *Ficheros de titularidad pública: "los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o 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 de derecho público". (Art. 5.l)*

5.6.2.5 Responsable del fichero o del tratamiento

El artículo 3.d de LOPD establece como Responsable del fichero o tratamiento a "*persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente*".

Se recoge en el artículo 5.1.q de RLOPD que podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

5.6.2.6 Encargado del tratamiento.

"*La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*". Indicado en el Artículo 3.g de la LOPD. Pudiendo así mismo ser también encargados del tratamiento entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados (RLOPD art. 5.1.i)

5.6.2.7 Afectado o interesado:

En el artículo 3.e de la LOPD queda reflejado como Afectado o interesado toda "*aquella persona física titular de los datos que sean objeto del tratamiento*".

5.6.2.8 Cesión o comunicación de datos

Artículo 3.i de la LOPD: "*Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado*".

5.6.2.9 Procedimiento de disociación

Artículo 3.f y artículo 5.1 de RLOPD: "*Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable*".

Si los datos personales no permiten la identificación de la persona concreta, dejan de ser datos personales, quedando al margen de la normativa sobre protección de datos.

5.6.2.10 Transferencia internacional de datos

Recogido en el art. 5.1.s) de RLOPD. Una transferencia internacional de datos significa el tratamiento de datos que supone una transmisión fuera de la Unión Europea, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de

datos por cuenta del responsable del fichero establecido en territorio español. Se crearán, en la transferencia, dos actores:

Exportador de datos: persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español y que realiza la transferencia de datos (Art. 5.1.j de RLOPD).

Importador de datos: persona física o jurídica, pública o privada, u órgano administrativo encargado de la recepción de los datos en territorio internacional. Podrá ser responsable o encargado del tratamiento o tercero. (Art. 5.1.ñ de RLOPD)

5.7 PRINCIPIOS DE PROTECCIÓN DE DATOS

En el Título II de la Lopd quedan regulados los principios de la protección de datos, núcleo central de las obligaciones del responsable del fichero y cuyo incumplimiento puede significar importantes sanciones económicas.

A continuación revisamos los principios básicos presentes en todas las fases del tratamiento de los datos:

5.7.1 DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS

Recogido en el artículo 5 de la Lopd y en los artículos 18 y 19 del Real Decreto 1720/2007.

Cuando los datos personales se soliciten directamente a su titular, el responsable del fichero deberá informar previamente, de manera expresa, precisa e inequívoca de los siguientes puntos:

a. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información.
b. Del carácter obligatorio o facultativo de sus respuestas a las preguntas que les sean planteadas.
c. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e. De la identidad y dirección del responsable del tratamiento, en su caso, de su representante.

Se recoge en el artículo 5.3 de la Lopd como excepción: "*no será necesaria la información a que se refieren las letras b, c y d si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban"*.

Por otro lado, el caso de que los datos no hayan sido obtenidos directamente del titular, queda regulado en el artículo 5.4: "*Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento de la procedencia de los datos, así como de lo previsto en las letras a, d y e*". Se tendrá en cuenta como excepciones, las recogidas en el artículo 5.5 de la Lopd: "cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados…".

5.7.2 CONSENTIMIENTO DEL AFECTADO

El tratamiento de datos personales requerirá el consentimiento inequívoco del afectado, salgo que la ley disponga de otra cosa. Este consentimiento podrá ser revocado cuando haya causa justificada.

No será necesario el consentimiento cuando:

- ✓ Los datos de carácter personal sean recogidos para el ejercicio de las funciones de las Administraciones públicas.
- ✓ Se refieran a las partes de un contrato o precontrato de una relación laboral, de negocio o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- ✓ El fin del tratamiento de los datos sea proteger un interés vital del interesado en los términos del artículo 7, apartado 6 de la Ley.
- ✓ Los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comunique los datos.
- ✓ No vulneren los derechos y libertades fundamentales del interesado.

5.7.3 CALIDAD DE LOS DATOS

Se establecen, por este principio, un conjunto de reglas que debe cumplir el responsable del fichero para que el tratamiento de los datos pueda ser considerado "leal y lícito" desde la recogida de los datos hasta la cancelación de éstos.

Estas reglas vienen recogidas en el artículo 4 de la Lopd y en los artículos 8 a 11 del Reglamento que la desarrolla. Dependiendo de la fase del tratamiento de datos establecerán:

- **Recogida de datos:** "*Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido*" (Artículo 4.1). Además, "*Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos*" (Artículo 4.7).
- **Almacenamiento de datos:** se establece que los datos deben ser almacenados de manera que, el titular pueda ejercer el derecho de acceso (punto 5.10.4.1 Derecho de acceso). Esto obliga al responsable del fichero a establecer un procedimiento de almacenamiento que permita cumplir el derecho antes mencionado en el plazo de un mes desde la recepción de la solicitud del interesado.
- **Tratamiento y mantenimiento de los datos:** los datos "*…no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos*".

Los datos serán exactos, completos y puestos al día con la situación del afectado. En caso de no ser así serán cancelados, rectificados o completados.

Cancelación de los datos: se establece que los datos de carácter personal no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario. "*Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos*" (Artículo 4.5).

5.7.4 SEGURIDAD DE LOS DATOS

A nivel europeo, en la Directiva 95/46/CE dedica el artículo 17 a esta materia con el título "*Seguridad del tratamiento*" indica que "*Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar 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*.

El artículo 9 de la Lopd establece que "*El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la*

naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural", prohibiendo expresamente el registro de datos de carácter personal *"… en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas*".

Se establecen tres tipos de fichero: básico, medio y alto, que deberán cumplir las medidas de seguridad según lo expuesto en el artículo 80 del RLOPD. La clasificación de los datos entre tipos de ficheros estará regulada por el artículo 81: *Aplicación de los niveles de seguridad*. A continuación, adjuntamos una ilustración mostrando ejemplos de tipos de datos que podrían ajustarse en uno u otro fichero.

Ilustración 12: Niveles de seguridad por tipo de fichero y correspondencia del nivel de seguridad con los datos. Elaboración propia basada en Art. 81 RDLOPD.

5.7.5 EL DEBER DE SECRETO

El responsable del fichero y toda persona que intervenga en el tratamiento de datos de carácter personal están obligados al secreto profesional respecto de los mismos y, al deber de guardarlos aún después de finalizar sus relaciones con el titular de fichero o, con el responsable del mismo.

5.7.6 CESIÓN O COMUNICACIÓN DE LOS DATOS

Se establece en el artículo 11 de la Lopd que "*los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado*". Por tanto debe cumplirse que:

El afectado dé su consentimiento previo habiéndole dado información sobre la finalidad a la que se van a destinar los datos cedidos y la finalidad del cesionario así como la actividad que desarrolla.

El objeto de la comunicación debe ser de fines relacionados directamente con las funciones de quien entrega los datos (cedente) como de quien los recibe (cesionario).

El artículo 11.2 se recogen las excepciones al consentimiento de datos y que se darán en los siguientes supuestos:

- ✓ Cuando la cesión está autorizada por la ley.
- ✓ Cuando se trate de datos recogidos de fuentes accesibles al público.
- ✓ Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- ✓ Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
- ✓ Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

- ✓ Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Además de estos puntos, la ley establece que:

- ➢ Artículo 11.3 El consentimiento podrá ser nulo si la información facilitada no sea completa o cumpla con lo regulado.
- ➢ Artículo 11.4 El consentimiento podrá ser revocable.

5.7.7 ACCESO A LOS DATOS POR CUENTA DE TERCEROS

Cuando el responsable del fichero contrata a una persona o entidad ajena a la organización para que le preste algún servicio utilizando los datos de carácter personal almacenados en sus ficheros se establece una relación jurídica denominada "*Acceso a los datos por cuenta de terceros*". En esta relación, quién preste el servicio pasará a ser "*Encargado del fichero*" manteniendo las mismas obligaciones, siguiendo estrictamente las instrucciones y devolviendo o destruyendo los datos una vez hay finalizado el servicio contratado.

Este principio viene recogido en el artículo 12 de la Lopd. En el apartado 2 se expresa que: "*la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas*".

Para evitar que por medio de este principio los datos personales vayan pasando de unas a otras personas o entidades, el artículo 21 del Real Decreto establece que el encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. Sin embargo permite la subcontratación sin autorización cuando se cumplan los siguientes requisitos:

- ✓ Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Cuando no pudiera ser, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.
- ✓ Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

- ✓ Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.
- ✓ Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en los apartados anteriores.

5.8 DERECHOS DE LOS INTERESADO RESPECTO A LOS DATOS PERSONALES

La LOPD otorga a los ciudadanos una serie de derechos para permitir que puedan controlar el uso de sus datos personales y tomar medidas cuando el tratamiento de estos datos no cumpla lo regulado en la LOPD.

En el Título III "Derecho de las personas" de la LOPD quedan regulados los siguientes derechos.

5.8.1 DERECHO A SER INFORMADO PREVIAMENTE A LA RECOGIDA DE DATOS

El artículo 5.1 de la LOPD, recoge que los interesados a los que se soliciten datos personales, deberán ser informados previamente de forma expresa, precisa e inequívoca de la siguiente información:

a. *De la existencia de un fichero o tratamiento de datos de carácter personas, de la finalidad de la recogida de los datos y de los destinatarios de la información facilitada.*
b. *De la obligatoriedad o no a dar los datos requeridos.*
c. *De las consecuencias de la obtención de datos o la negativa a facilitarlos.*
d. *De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
e. *De los datos (Identificad y dirección) del responsable del tratamiento de los datos o su responsable. Si el responsable no está dentro de la Unión Europea.*

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco.

5.8.2 DERECHO DE IMPUGNACIÓN DE VALORACIONES

Este derecho es la herramienta para que los ciudadanos puedan proteger su privacidad frente a la utilización de sus datos personales por parte de alguien para evaluar determinados aspectos de la personalidad (rendimiento laboral, crédito…) y utilice la información para tomar algún tipo de decisión que pueda afectar significativamente.

El derecho de impugnación de valoraciones queda regulado en el Título III de la Lopd, artículo 13 de la siguiente manera:

1. *Los ciudadanos tienen derecho a no verse afectados por una decisión que se base, únicamente, en un tratamiento de datos destinados a evaluar aspectos de su personalidad.*
2. *Podrán ser impugnados por el afectado, aquellos actos o decisiones que conlleven una valoración de su comportamiento cuando el fundamento principal sea un tratamiento de datos que ofrezca una definición de sus características o personalidad.*
3. *El afectado tiene derecho a obtener información del responsable del fichero, criterios de valoración y programa utilizados en el tratamiento y que dieron lugar a la decisión en que consistió el acto.*
4. *La valoración sobre el comportamiento de los ciudadanos, basa en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.*

Teniendo en cuenta las excepciones que se establecen en el artículo 36 del Reglamento que desarrolla la Lopd (Real Decreto 1720/2007): "*Cuando la decisión se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre y cuando se le otorgue la posibilidad de alegar lo que estimara pertinente y habiendo, el responsable del fichero, informado previamente al afectado".*

5.8.3 DERECHO DE ACCESO

Recogido en el artículo 15 de la LOPD. Los ciudadanos podrán dirigirse de forma gratuita al responsable del fichero que está utilizando sus datos para informarse de si sus datos están siendo objeto de tratamiento, finalidad del tratamiento que se esté realizando e información sobre el origen de los datos y las cesiones realizadas o previstas a terceros. Teniendo, por parte del responsable del fichero, el plazo de un mes desde la recepción de la solicitud para aceptarla o denegarla (Explicando los motivos en este último caso).

Se podrá optar por visualizar los datos directamente en pantalla u obtenerlos por medio de escrito, copia, fotocopia, correo electrónico u otro sistema adecuado al fichero que está tratando los datos.

Este derecho podrá ejercitarse a intervalos no inferiores a doce meses excepto si la persona interesada acredita un interés legítimo al efecto, caso en el que podrán ejercitarlo antes.

El derecho de acceso forma parte lo que se denomina Derechos Arco (acceso, rectificación, cancelación y oposición). Estos derechos están especialmente protegidos y regulados en el Título III de la LOPD y Título III del RLopd. Los derechos Arco son derechos personalísimos que significa que el ejercicio de éste, sólo puede hacerse por el titular de los datos, su representante legal o por un representante voluntario designado para ello.

5.8.4 DERECHO DE CONSULTA AL REGISTRO

Regulado en el artículo 14 de la LOPD: *"Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento"*.

El Registro General es de consulta pública y gratuita y permite, entre otras cosas, saber quién figura como responsable del fichero, su finalidad y la dirección donde debe remitir sus solicitudes.

5.8.5 DERECHO DE OPOSICIÓN

Regulado en los artículos 6.4 y 30.4 de la Lopd y en el Título III del Real Decreto 1720/2007 artículos 23 a 26 y 34 a 36. El ciudadano puede negarse a que se traten sus datos cuando:

- No sea necesario su consentimiento para el tratamiento para el tratamiento de los datos pero haya un motivo legítimo o fundado, referido a su situación personal, que lo justifique, siempre y cuando la Ley no disponga lo contrario.
- Se trate de ficheros que tengan como objetivo la realización de publicidad y prospección comercial.
- La finalidad del tratamiento sea la adopción de una decisión referida al afectado y basada en un tratamiento automatizado de sus datos personales.

Este derecho debe poder ejercerse por parte del afectado o su representante a través de un medio sencillo, ágil y gratuito que deberá facilitar el responsable del tratamiento sin que suponga un coste adicional el usuario.

5.8.6 DERECHO DE RECTIFICACIÓN O CANCELACIÓN

Regulados en Título III de la Lopd (artículo 16) y en el título III del Real Decreto 1720/2007 (artículos 23 a 26 y 31 a 33). Cuando los datos personales del usuario sometidos a tratamiento resulten inexactos, incompletos, inadecuados o excesivos podrá disponer de las siguientes opciones:

- **Derecho de rectificación**: se sustituirán los datos erróneos por los correctos, adecuando el tratamiento a la situación real de la persona interesada.
- **Derecho de cancelación**: dará lugar al bloqueo de los datos que serán conservados únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, antes posibles responsabilidades.

Una vez ejercitado cualquiera de estos dos derechos ante el responsable del fichero ya sea por escrito o por los medios que haya dispuesto para hacerlo, éste tendrá un plazo de diez días hábiles tras la recepción de la solicitud, para resolverla bien aceptando la petición del usuario, bien denegándola bajo alguno de los supuestos recogidos[28]. Debiendo comunicar sea cual fuere la resolución, al usuario.

En el caso de acepta la solicitud y de que el fabricante haya cedido los datos a terceros, se verá en la obligación de hacerles llegar la solicitud de rectificación o cancelación en un plazo de diez días y que la gestión por parte de terceros sea realizada en un plazo no superior a otros diez días tras la recepción.

5.8.7 DERECHO DE INDEMNIZACIÓN

En el artículo 19 de la Lopd queda reflejado el derecho del titular para reclamar al responsable del fichero o al encargado del tratamiento, una indemnización por los daños y perjuicios que haya ocasionado un tratamiento inadecuado de sus datos.

La reclamación del afectado deberá ser vía jurisdicción que corresponda (Dependerá de si se reclama al responsable de un fichero de titularidad pública o privada), quedando al margen la Agencia Española de Protección de Datos.

28 Los supuestos recogidos por los que el responsable del fichero puede negar el derecho de rectificación o cancelación son: 1) Quien lo solicite sea una persona distinta al titular de los datos o no esté acreditado que sea su representante. 2) Cuando así lo prevea una Ley o norma de derecho comunitario o cuando éstas impidan al responsable revelar a los afectados el tratamiento de los datos al que se refiere el acceso. 3) Cuando lo datos deban ser conservados durante plazos legales o no hayan finalizado las relaciones contractuales que justificaron el tratamiento.

5.9 REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS 2016/679

El Reglamento General de Protección de Datos 2016/679 entró en vigor el 25 de mayo de 2016 pero no comenzará a aplicarse hasta el 25 de mayo de 2018. Hasta ese momento la Directiva 95/46 y las normas nacionales que la trasponen, sigue siendo válidas y aplicables y, las Instituciones Europeas y organizaciones deben ir preparándose y adaptándose para que el Reglamento sea aplicable.

Respecto a la convivencia del nuevo Reglamento con la LOPD en España, José Luis Piñar Mañas, catedrático de Derecho Administrativo y ex director de la AEPD, apuntó para "Noticias jurídicas" (04/05/2016) que "*parece que podrá seguir siendo aplicable en lo que esté fuera del Derecho de la UE, pero suscitan dudas en materias como el registro de ficheros".*

Este Reglamento tiene como finalidad establecer según recoge en su Artículo 1:

- ✓ *Las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales.*
- ✓ *Las normas relativas a la libre circulación de los datos recogidos en el apartado 1.*

A continuación recogeremos las principales novedades del Reglamento que afectarán a la seguridad y privacidad del IoT. El Principio de Anonimización se recogerá más adelante, en el capítulo 8.6.3 al estar directamente relacionado con datos médicos.

5.9.1 RESPONSABILIDAD ACTIVA

Una de las características de este nuevo Reglamento es que se basa en la prevención por parte de las organizaciones que tratan los datos ya que entiende que, actuar sólo cuando se ha producido la infracción es insuficiente y los daños causados pueden ser difíciles de recompensar. Como medidas previsoras el Reglamento recoge:

5.9.1.1 Protección de datos por defecto

El responsable del tratamiento, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, aplicará tanto en el momento de determinar los medios como en el propio del tratamiento, medidas técnicas y organizativas apropiadas como la minimización de los datos, a fin de cumplir los requisitos del Reglamento.

Además, aplicará medidas con miras a garantizar, por defecto, que sólo sean objeto de tratamiento los datos personales necesarios para da fin específico.

5.9.1.2 Condiciones para el consentimiento

Estando ya presente la obligatoriedad del consentimiento, este nuevo Reglamento requiere que haya una declaración de los interesados o una acción positiva que indique el acuerdo del interesado. El consentimiento no puede deducirse del silencio o de la inacción de los dueños de los datos. Debiendo, el responsable, ser capaz de demostrar que el titular de los datos consintió el tratamiento.

Si el consentimiento del interesado se da en el contexto de una declaración escrita en la que se refiera a varios asuntos, la solicitud de consentimiento deberá distinguirse claramente de los demás asuntos.

El interesado podrá retirar su consentimiento en todo momento habiendo informado al usuario de ello previamente al consentimiento.

Al evaluar el consentimiento libre, se tendrá en cuenta si la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales no necesarios para la ejecución del contrato.

5.9.1.3 Realización de evaluaciones de impacto sobre la protección de datos

Recogido en el Artículo 35. Cuando sea probable que un tipo de tratamiento entrañe un riesgo para los derechos y libertades de las personas físicas, el responsable realizará, antes del tratamiento, una evaluación del impacto de las operaciones. Requiriéndose en los siguientes casos:

a) *Evaluación de aspectos personales basado en un tratamiento automatizado, como elaboración de perfiles, y sobre cuya base se tomen decisiones que puedan producir efectos jurídicos.*
b) *Tratamiento a gran escala de datos sensibles.*
c) *Observación sistemática a gran escala de una zona de acceso público.*

La evaluación deberá incluir como mínimo:

a) *Descripción sistemática de las operaciones de tratamiento previstas para el tratamiento.*
b) *Evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad así como, una evaluación de riesgos para los derechos y libertades del individuo.*
c) *Las medidas previstas para afrontar los riesgos, medidas de seguridad y mecanismos y garantías que de protección de los datos personales, teniendo en cuenta los derechos de los titulares de los datos.*

5.9.1.4 Nombramiento de un delegado de protección de datos

Artículo del 37 a 39 del RGPD 2016/679. El responsable o encargado del tratamiento designará un delegado siempre que sea necesario[29] y publicará los datos de contacto del delegado y los comunicará a la autoridad de control.

El delegado prestará atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines de tratamiento y tendrá como funciones informar y asesorar al responsable o encargado del tratamiento de los datos, supervisar el cumplimiento de lo expuesto en el Reglamento 2016/679. Y asesorar sobre la evaluación de impacto.

Además, esta figura será el intermediario entre el responsable del fichero y la autoridad de control.

5.9.1.5 Notificación de violaciones de la seguridad de los datos

El artículo 33 RGPD 2016/679 recoge que ante una violación de la seguridad de los datos personales, el responsable del fichero tendrá un máximo de 72 horas después de la constancia de ella, para avisar a la autoridad de control a menos que se considere que el delito no constituye un riesgo para los derechos y las libertades de las personas física. De cara a los dueños de los datos, en el artículo 34 queda reflejado que se deberá comunicar de una violación de la seguridad al interesado cuando sea probable que dicha violación entrañe un riesgo para los derechos y libertados del titular describiendo en lenguaje claro la naturaleza de la violación y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d)[30]. Por otro lado, la comunicación no será necesaria si el responsable ha tomado y aplicado medidas de protección sobre los datos, si ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto

29 Casos en los que se ha de designar un delegado de protección de datos, registrados en el punto 1 del Artículo 37: a) Cuando el tratamiento lo lleve a cabo una autoridad u organismo público excepto tribunales. b) Cuando las actividades principales conlleven un tratamiento de datos que requieran una observación habitual y sistemática de interesados a gran escala. c) Cuando las actividades del responsable o encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y datos relativos a condenas e infracciones penales.

30 La comunicación deberá como mínimo:

a) Describir la naturaleza de la violación de la seguridad, categorías y número, si fuera posible; de interesados afectados y categorías y número de registros de datos afectados.
b) Comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto que pueda dar más información.
c) Describir posibles consecuencias de la violación de la seguridad de los datos.
d) Describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos, incluyendo si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

riesgo para los derechos o cuando suponga un esfuerzo desproporcionado, caso en el que se podrá optar por una comunicación pública.

5.9.1.6 Promoción de códigos de conducta y esquemas de certificación

Artículos del 40 al 43. Los estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del Reglamento, teniendo en cuenta las características de los distintos sectores de tratamiento y las necesidades de microempresas y pequeñas y medianas empresas.

Asociaciones y otros organismos, en representación de los responsables y encargados del tratamiento de datos, también podrán elaborar códigos de conducta o ampliar los ya existentes. También podrán adherirse a códigos, asumiendo compromisos vinculantes y exigibles. Si el proyecto de código, modificación o ampliación es aprobado por las organizaciones competentes y no se refiere a actividades de tratamiento en varios Estados miembros, las autoridades de control registrarán y publicarán el código. Si se refiere a actividades en varios países, lo presentará por el procedimiento del artículo 63[31].

Respecto a la certificación. Las autoridades de control, el Comité y la Comisión, promoverán a nivel de la Unión Europea, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados, teniéndose, al igual que en los códigos de conducta, las diferentes necesidades de los sectores.

Los códigos de conducta contendrán mecanismos que permitan efectuar un control obligatorio del cumplimiento de sus disposiciones por aquellos que se comprometan, de forma voluntaria, a aplicarlo, sin prejuicio de las funciones y los poderes de las autoridades.

La certificación será expedida por los organismos de certificación[32].

[31] El mecanismo de coherencia tendrá como fin contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí, y en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido.

[32] Se expone en el Artículo 43 que los Organismos de certificación serán acreditados por la autoridad de control competente, por el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo con arreglo a la norma en ISO/IEC 17065/2012.

Por otro lado, dichos organismos de certificación necesitarán para ser acreditados, demostrar su independencia y control competente con el objeto de la certificación. Tienen procedimientos establecidos para la expedición, la revisión y la retirada de certificaciones, sellos y marcas y han demostrado que sus procedimientos no dan lugar a un conflicto de intereses

5.9.2 DERECHO AL OLVIDO

O derecho de supresión, recogido en el Artículo 17 del nuevo Reglamento: El interesa tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación los datos dentro de las siguientes circunstancias:

a) *Los datos no sean ya necesarios para los fines recogidos.*
b) *El consentimiento sea retirado por parte del interesado.*
c) *El interesado de oponga al tratamiento.*
d) *Los datos hayan sido tratados ilícitamente.*
e) *Los datos deban suprimirse para el cumplimiento de la obligación legal establecida en el Derecho de la Unión de los Estados miembros que se aplique al responsable del tratamiento.*
f) *Los datos se hayan obtenido en relación la oferta de servicios de la sociedad de la información mencionados en el artículo 8 aptdo. 1.*

Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo anterior, a suprimir los datos, el responsable adoptará las medidas razonables, incluidas las técnicas, para informar a los responsables que estén tratando los datos.

El derecho al olvido no se aplicará cuando el tratamiento sea necesario:

a) *Para ejercer el derecho a la libertad de expresión e información.*
b) *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.*
c) *Por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, letras h) e i) y apartado 3*[33].

[33] Artículo 9: Queda prohibido el tratamiento de datos personales que revelen origen étnico o racial, opiniones políticas, convicciones religiosas, datos relativos a la salud… Exceptuando entre otros casos:
h) El tratamiento necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, presentación 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 y sin perjuicio de las condiciones y garantías contempladas en artículos del mismo Reglamente.
i)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, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular del secreto profesional.
El artículo completo se puede consultar en el BOE, en línea en https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2016-80807 [Consulta 09/01/2017]

d) Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.
e) Para la formulación, ejercicio o defensa de reclamaciones.

5.9.3 DERECHO A LA PORTABILIDAD

Recogido en el Artículo 20, recoge que: *"El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado"*. Aplicándose sin perjuicio del derecho de olvido y siempre y cuando: "*el tratamiento esté basado en el consentimiento o contrato, el tratamiento se haga por medios automatizados y la transmisión sea técnicamente posible*".

5.10 ANÁLISIS DEL DICTAMEN SOBRE PROTECCIÓN DE DATOS EN IOT DEL GRUPO DE TRABAJO 29.

Las autoridades europeas de protección de datos conocidas como Grupo de Trabajo del Artículo 29 (GT29), aprobaron en 2014 el primer Dictamen sobre internet de las cosas con el fin de "contribuir a la aplicación uniforme del marco legal de protección de datos respecto a la IoT". Catalogado como la Opinión 8/2014, de 16 de septiembre. La Agencia Española de Protección de Datos con la Autoridad francesa, han liderado la elaboración del documento que contempla las perspectivas de beneficios económicos y sociales y también, identifica y alerta de los riesgos que pueden existir dentro del ecosistema del IoT.

El dictamen se centra en tres desarrollos específicos del IoT actualmente en uso y bajo las actuales leyes de protección de datos que veremos a continuación. No obstante, los principios y las recomendaciones pueden ser aplicados a otros desarrollos IoT y no son excluyentes entre ellos.

- ✓ **Wearables**: Se refiere a ropa de diario y complementos que los usuarios pueden llevar como relojes, gafas, etc. Que puede integrar cámaras, micrófonos y sensores para grabar y transferir datos al fabricante del dispositivo.

  Estos objetos son susceptibles de ser adoptados rápidamente por la utilidad extensible ofrecida por los objetos cotidianos de los que apenas se diferencian estéticamente.
- ✓ **Dispositivos que registran actividad de la persona**: diseñados para personas que quieren registrar información sobre sus hábitos y estilos de vida como rastreadores de sueño, seguimientos de actividad…

  Estos objetos pueden recopilar datos y analizarlos para inferir en información relacionada con la salud pues, debemos tener en cuenta, que los datos en bruto que el

dispositivo recoge, serán tratados y convertidos en otros datos visibles. En la mayoría de los casos, como veremos más adelante, sólo se muestran estos últimos datos, pero el fabricante o proveedor del servicio tiene derecho a más.

- ✓ **Domótica**: Objetos que contienen sensores de movimiento pueden detectar y registrar cuando el usuario está en casa, patrones de movimiento y quizá, desencadenar acciones previamente determinadas. Normalmente estos dispositivos están constantemente conectados y por tanto pueden transmitir en todo momento datos al fabricante.

La domótica plantea desafíos específicos de privacidad y protección de datos.

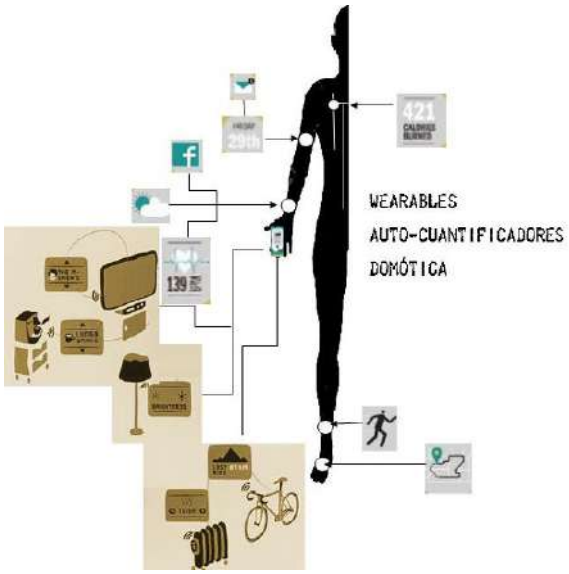

Ilustración 13: Desarrollos sobre los que se centra el Dictamen del Grupo de Trabajo 29. Diseño propio.

5.10.1 DESAFÍOS EN PRIVACIDAD

El GT29 considera que la IoT plantea una serie de desafíos de privacidad y protección de datos nuevos además de los tradicionales que se ven amplificados según el procesamiento de datos. Por ello, es de relevancia la aplicación del marco jurídico de la UE y ha emitido una serie de recomendaciones prácticas.

5.10.1.1 La falta de control y asimetría de la información

En esta interacción de servicios, aparece la necesidad de dar servicios de forma discreta. La comunicación entre objetos puede activarse por defecto o de forma automática sin que el usuario lo sepa. La interacción entre objetos, objetos y dispositivos individuales, entre individuos y otros objetos y entre objetos y sistemas back-end, dará lugar a la generación de flujos de datos nuevos difíciles de controlar, en las que las herramientas clásicas usadas para garantizar la protección y derechos de los usuarios perderán eficacia.

Todo esto puede hacer que el usuario pierda el control de sus datos y la difusión de éstos, llegando a terceros sin que él lo sepa si el recabado y utilización de esos datos no se hace de una forma transparente y segura.

La combinación del IoT con otros avances tecnológicos en los que se hace presente el problema de la falta de control como el Big Data, hace que este problema sea mucho más difícil de resolver.

5.10.1.2 Calidad del consentimiento del usuario

En el Grupo de Trabajo 29 considera que en muchos casos el usuario puede no ser consciente del tratamiento de sus datos por parte de dispositivos inteligentes. La falta de información puede hacer difícil demostrar el consentimiento válido según la legislación comunitaria y por ello no puede ser considerado como una base legal para el tratamiento de los datos.

¿Es fácil distinguir un reloj normal de uno conectado? ¿Es real un consentimiento libre de la utilización de los datos?

Muchos de los dispositivos inteligentes no podrían distinguirse de dispositivos reales pese a llevar micrófonos, cámaras, sensores de movimientos… tecnología que puede compartir datos del usuario sin que sea consciente, entonces ¿Cómo podrá consentir el usuario que esto ocurra o no? El GT29 piensa que podría resolverse previendo una señalización adecuada que fuera realmente visible a los titulares de los datos.

Sobre la segunda pregunta, opina que el consentimiento libre y la posibilidad de renunciar a características de los dispositivos del IoT es más un tema teórico que real. ¿Es entonces válido en virtud de la legislación comunitaria?

Parece que los sensores utilizados en IoT no se diseñan para dar información y obtener un consentimiento del interesado y que los mecanismos clásicos para obtenerlo pueden ser difíciles de aplicar en IoT y por tanto "de baja calidad" por la falta de información y no ser ajustado a las preferencias del usuario.

Las nuevas formas para obtener un consentimiento válido deben ser estudiadas por todas las partes del ecosistema IoT y deben extenderse a mecanismos de consentimiento a través de los propios dispositivos.

5.10.1.3 Inferencias derivadas de los datos y de su reproceso

La cantidad de datos recogidos y los avances en técnicas de análisis de datos y cruces puede dar lugar al uso de datos para fines secundarios totalmente distintos del fin inicial. Datos sin significado aparente, pueden dar lugar a información relevante para otro fin.

Los *Quantified self* utilizan sensores básicos para recoger datos "En bruto" y extraer después información sensible para tratar y mostrar a los usuarios finales. Un dispositivo, por ejemplo, que cuente el número de pasos puede informar al usuario de su condición física.

Por todo ello, se puede dar el escenario en el que un usuario puede estar de acuerdo y dar su consentimiento para el intercambio de datos con un propósito y no estarlo con cierta información secundaria que podría usarse con otro fin. Es importante, establece el documento, que las partes interesadas de la IoT aseguren que los datos se van a utilizar para fines compatibles con el propósito original e informen de ese propósito al usuario.

5.10.1.4 Trazar de forma intrusiva patrones de comportamiento y perfiles

Diferentes dispositivos pueden recoger pequeñas piezas de información. La comunicación entre los dispositivos puede hacer que esas pequeñas piezas, tras su análisis revelen hábitos, preferencias o, patrones de comportamientos o formas de vida detallados de un individuo.

Igual que con el uso de circuitos cerrados de televisión en espacios públicos, la conducta de las personas se vieron influenciadas, con el IoT puede ocurrir lo mismo en terrenos más íntimos de los usuarios como sus propios hogares o lugares de trabajo. Se cree que esto podría presionar a los individuos para evitar comportamientos no habituales que eviten la detección de comportamientos fuera de los patrones creados o llegar a una tendencia intrusiva en la vida privada y la intimidad de las personas que debería ser especialmente prevenido y vigilado.

5.10.1.5 Limitaciones en la posibilidad de permanecer en el anonimato cuando se utilizan servicios

Es complicado hacer compatible el anonimato con aplicaciones IoT en el área de la salud, por ejemplo. Objetos en las proximidades de los usuarios pueden identificarse con direcciones MAC y el uso de múltiples sensores de dispositivos con direcciones MAC pueden dar lugar a huellas digitales únicas que se podrán relacionar con usuarios específicos que podrán usarse para múltiples fines. Estos, para el GT29, son sólo ejemplos de cómo permanecer en el anonimato y guardar la vida privada de los usuarios será más difícil según vaya entrando la IoT en nuestras vidas.

Este punto implica importantes preocupaciones respecto a la protección de datos y la privacidad. Datos no anónimos se pueden combinar con otros datos no anónimos y algunos sensores pueden ser vulnerables a los ataques de identificación o suplantación del individuo.

5.10.1.6 Riesgos de seguridad

El GT29 considera que el IoT plantea retos relacionados con la combinación entre los problemas de seguridad de los dispositivos y la optimización de recursos. Por un lado no se sabe con claridad cómo los fabricantes conjugarán la disponibilidad del procesamiento de los datos con la optimización de recursos y la implementación de medidas de seguridad. Por otro, dispositivos menos seguros conectados entre sí y diferentes niveles de procesamiento originados por diferentes grupos de interés obliga a una coordinación que puede dar lugar a puntos débiles y vulnerabilidades, violaciones de datos y una percepción negativa del individuo en relación con la seguridad del IoT. Además el almacenamiento de datos se hará sobre infraestructuras de proveedores y por tanto, la seguridad en el IoT deberá no sólo ser cosa de los dispositivos sino extenderse a enlaces de comunicación, infraestructura de almacenamiento y otros elementos de su ecosistema.

5.10.2 APLICACIÓN DE LA LEGISLACIÓN COMUNITARIA PARA EL TRATAMIENTO DE DATOS PERSONALES DE LA IOT

Mientras se cumplan las condiciones de su vigencia establecidas en el artículo 4 de la Directiva 95/46/CE, el marco jurídico para evaluar los problemas de privacidad y protección de datos dentro del escenario del IoT serán esa misma Directiva así como las disposiciones específicas de la Directiva 2002/58/CE.

De acuerdo con el artículo 1.4 (a) la legislación nacional de un Estado miembro es aplicable al tratamiento de datos establecido en el territorio de ese Estado. La ley nacional de un Estado también es aplicable en los casos en que el tratamiento no esté establecido en el territorio comunitario, pero hace uso de "equipos" [34] situados en él (Artículo 1.4 (c)).

Aplicando estos artículos en el entorno del IoT, cuando un responsable del tratamiento no está en la UE pero ha participado en el desarrollo, distribución o funcionamiento del dispositivo, seguirá estando sujeto a la legislación de la UE. Es importante por tanto, saber los diferentes actores y su papel, involucrados en el IoT para calificar su estado legal.

5.10.2.1 El concepto de dato personal

El Grupo de Trabajo amplia la orientación sobre el tratamiento de Datos Personales que se da en el artículo 2 de la Directiva 95/46/CE. En el contexto del IoT puede darse el escenario en el que el individuo sea identificado sobre la base de datos que se originan en el

[34] En IoT "equipo" serán todos los objetos que se utilizan para recopilar y procesar datos, dispositivos terminales de usuarios como teléfonos inteligentes o en los que software o aplicaciones previamente instaladas.

"objeto inteligente" recoge en su base de datos incluso, estos datos pueden trazar patrones de comportamiento de éste.

Los datos relativos a personas que vayan a ser tratados tras la implementación de técnicas que aseguren el anonimato, pueden tener que ser tratados como datos personales si tenemos en cuenta que, la mayoría de datos tratados de forma automática conllevan un riesgo de suplantación de identidad. En este punto, el Grupo de Trabajo hace referencia a un reciente dictamen sobre técnicas de anonimato.

5.10.2.2 Partes interesadas de la IoT

El concepto de tratamiento de datos y de responsable de datos, se pueden encontrar en los puntos 5.6.2.3 y 5.6.2.5 respectivamente de este trabajo. Si nos trasladamos a sistemas complejos de múltiples actores, muchos escenarios implicarán responsables y encargados con diferentes grados de autonomía y responsabilidad.

La aplicación de la IoT implica la intervención combinada de múltiples partes interesadas que conlleva la necesidad de una asignación precisa de responsabilidades legales entre ellos en lo que respecta al tratamiento de datos personales del interesado dependiendo de las características de sus intervenciones. A continuación se detalla la responsabilidad de diferentes partes del ecosistema IoT.

- ***Fabricantes de dispositivos***

Además de ser los proveedores de los artículos físicos, pueden desarrollar o modificar su sistema operativo, integrar un programa que garantice su funcionalidad o cuándo, a quién y con qué fines se recogen estos datos. Por ello a efectos de la legislación de la UE se califican como responsables del tratamiento.

- ***Plataformas sociales***

Aunque los usuarios sean los que elijan que datos compartir en sus redes sociales, este proceso normalmente suele llevarse a cabo de forma automática después de configurar la aplicación. La capacidad de compartir, por tanto, pertenece a la configuración predeterminada como estándar de aplicaciones proporcionadas por el fabricante.

Los usuarios que suban datos procesados por las redes sociales para fines distintos de los que se hayan acordados, actuarán como responsables del tratamiento de datos en su propio derecho en virtud de la legislación y cuyas consecuencias se recogen en el Dictamen WP9 sobre redes sociales.

- ***Terceros desarrolladores de aplicaciones***

Muchos sensores contienen APIs para facilitar el desarrollo de aplicaciones de terceros. La instalación de estas aplicaciones a menudo consiste en proporcionar al desarrollador de la aplicación un acceso a los datos a través de esa API. Cuando estos datos no son completamente anónimos, esos accesos suponen una transformación del artículo 2 de la Directiva 95/46/CE (Punto XXX), por lo que el desarrollador de la aplicación que ha decidido este acceso a los datos debe ser considerado como un responsable del tratamiento de ellos.

- ***Otros terceros***

Terceros que no son fabricantes ni desarrolladores pueden utilizar dispositivos IoT para recoger y procesar información sobre los individuos sin tener control sobre el tipo de datos recogidos. Estos terceros son calificados también como responsables del tratamiento para el proceso concreto de esos datos en la medida en que los recogen y analizan para fines que han decidido ellos mismos.

- ***Plataformas de datos IoT***

Teléfonos inteligentes y tablets son utilizados por los usuarios como pasarelas de datos recogidos en diferentes dispositivos IoT. Los fabricantes han desarrollado plataformas para alojar estos datos para centralizar y facilitar su gestión.

Estas plataformas también pueden calificarse como responsables del tratamiento para la legislación de la UE.

- ***Titulares de datos***

Los suscriptores y usuarios del IoT son los titulares de los datos. Si estos datos se utilizan para fines únicamente personales o domésticos, estarán bajo la "*extinción doméstica*" de la Directiva 95/46/CE. El modelo de negocio de la IoT implica que los datos del usuario se transfieren sistemáticamente a fabricantes, desarrolladores y terceros y por tanto esa "*extinción doméstica*" será de aplicación limitada en el IoT.

El tratamiento de los datos también puede extenderse a personas que no son usuarios ni suscriptores del IoT. La aplicación de la legislación de la UE no está condicionada por la propiedad del dispositivo, sino por el tratamiento de los datos personales.

5.10.3 OBLIGACIONES DE LOS RESPONSABLES DE FICHEROS

El Grupo de Trabajo 29, en su Dictamen del 16 de septiembre recoge las obligaciones en el contexto de la IoT que, obviamente, no excluye la aplicación de otras disposiciones.

5.10.3.1 Aplicación sobre privacidad en internet

El artículo 5.3 de la Directiva 2002/58/CE se aplica a situaciones en las que un actor almacena o dispone de acceso a la información ya almacenada en un dispositivo IoT. El hecho de que el propietario de un dispositivo IoT y la persona cuyos datos sean almacenados sean diferentes personas, pueden dar lugar a una aplicación distribuida del artículo 5(3).

Los dispositivos IoT serán calificados como "Equipo Terminal" a efectos de la disposición y es obligación que el usuario o suscriptor dé su consentimiento al acceso y almacenamiento de datos a no ser que sea obligado para llegar a dar el servicio que desea. Este consentimiento deberá darse después de que el responsable del fichero haya dado una información completa y clara y debe ser previo al acceso de la información del dispositivo.

El requisito de consentimiento está dirigido al fabricante del dispositivo y las partes interesadas que quieran tener acceso a estos datos agregados en bruto almacenados en esta infraestructura y a cualquier responsable del tratamiento que desee almacenar datos adicionales.

5.10.3.2 Fundamentos para el tratamiento

Los responsables que hemos visto en el punto 1.1.2.2 deberán cumplir uno de los requisitos del artículo 7 de la Directiva para el tratamiento de datos personales para que este sea legítimo.

En la práctica el GT29 dispone tres fundamentos jurídicos relevantes en el tratamiento de datos:

- Primer fundamento jurídico: hay que resaltar el principio de consentimiento (Punto 2.4.2 del trabajo).
- Segundo fundamento jurídico: Dispone que el procesamiento es legítimo cuando es necesario para el cumplimiento de un contrato en el que una parte sea el interesado. Este fundamento está limitado por el criterio de "necesidad", que requiere una relación directa y objetiva entre el propio tratamiento y el propósito de la relación contractual.
- Tercer fundamento jurídico: Permite el tratamiento de datos cuando éste es necesario para la satisfacción del interés perseguido por el responsable del tratamiento o por terceros a los que se den los datos, excepto cuando sobre esos intereses prevalezcan derechos fundamentales y libertades de los afectados.

El tratamiento de los datos personales de un individuo en el Contexto de la IoT afectará probablemente, de mayor forma a sus derechos fundamentales a la intimidad y protección de datos que en un contexto sin dispositivos IoT. Estas situaciones pueden suceder cuando los

datos que se recojan afecten a la salud del usuario, su ubicación, intimidad o patrones de comportamiento.

Teniendo en cuenta la importancia de una interferencia en el tratamiento de los datos, es obvio que dicho tratamiento apenas se justifica por el interés económico que un actor pueda tener del procesamiento del IoT.

5.10.3.3 Calidad de los datos.

En el punto 2.4.3 hablamos sobre la calidad de los datos en la Lopd. También sobre ello se recoge en el artículo 6 [35]de la Directiva 95/46/CE.

En relación con la IoT y debido a que los sensores están diseñados para no ser invasivos, es decir, para que pasen desapercibidos en la mayor medida de lo posible, adquiere mayor relevancia cumplir el principio de equidad[36] e informar a todas las personas de la vecindad geográfica o digital, de los dispositivos conectados cuando se recogen los datos relacionados con ellos o su entorno.

Así mismo, y dado que los usuarios deben saber con qué fines se recogen sus datos, las partes de la IoT deben tener una visión general y completa de su modelo de negocio antes de recolectar datos para cumplir con el principio de limitación de la finalidad[37] y para recoger sólo datos estrictamente necesarios: principio de minimización de datos[38].

Sobre este último principio, algunas opiniones reflejan que dentro del IoT, puede suponer una limitación de oportunidades y una barrera para la innovación relacionada con el análisis de datos. Respecto a esto, el GT29 insiste en la importancia de este principio para la protección de los derechos y los datos del individuo ya que este principio implica que cuando los datos no son necesarios se debe ofrecer al usuario la posibilidad de usar el servicio de forma anónima.

Respecto a la duración de los datos también mencionado en el apartado 2.4.3 del presente trabajo. El GT29 especifica dentro del marco del IoT que los datos personales

[35] En el artículo 6 los Estados miembros disponen que los datos personales sean: a) Tratados de manera leal y lícita. b) Recogidos con fines determinados, explícitos y legítimos y no tratados posteriormente de manera incompatible. c) Adecuados, pertinentes y no excesivos en relación a los fines. d) Exactos y actualizados cuando sea necesario respecto a los fines por los que fueron recogidos o tratados posteriormente, sean suprimidos o rectificados. e) Conservados de forma que permita la identificación durando un tiempo no superior al necesario para los fines o el tratamiento posterior.

[36] El principio de equidad requiere específicamente que los datos personales no deben ser recogidos y procesados sin que el individuo realmente sea consciente de ello.

[37] Limitación de la finalizad implica que los datos sólo pueden ser recogidos con fines determinados, explícitos y legítimos siendo, cualquier otro tratamiento incompatible con estos propósitos, ilegal en virtud de la legislación comunitaria.

[38] Principio de minimización de los datos: los datos recogidos sobre el titular de los datos deben ser los estrictamente necesarios para la finalidad específica determinada previamente por el responsable del tratamiento.

comunicados por un usuario cuando se suscribe a un servicio específico en el IoT deben eliminarse en el momento en el que el usuario pone fin a su suscripción. La información borrada por el usuario en su cuenta no debe mantenerse y, si el usuario deja de utilizar un servicio por un tiempo definido, se deberá informar en el perfil del usuario indicando que está inactivo y después de otro tiempo reglamentario se deberán eliminar los datos.

5.10.3.4 Tratamiento de datos sensibles

En particular los dispositivos auto-cualificadores que recogen datos sobre el bienestar de los usuarios, aunque no sean datos de salud como tales; pueden proporcionar información acerca de ésta ya que los datos se registran a lo largo del tiempo pudiendo derivar inferencias. Los responsables del tratamiento deberían anticipar este posible cambio en la calificación y tomar las medidas oportunas para cumplir lo dispuesto sobre el tratamiento de datos sensibles.

5.10.3.5 Requisitos de transparencia

En el punto 2.4.1 indicábamos la información que el responsable del fichero debe dar al dueño de los datos. También en los artículos 10 y 11[39] de la Directiva 95/46/CE se recoge.

En concreto, dentro del marco del IoT, dependiendo de las aplicaciones, esta información podría proporcionarse en el objeto en sí utilizando la conectividad inalámbrica para transmitir la información, o el uso de localización efectuadas por un servidor, para informar a los usuarios que se encuentran cerca del sensor.

5.10.3.6 Seguridad

Si los fallos de seguridad que resultan son el resultado de un diseño inadecuado o falta de mantenimiento de los dispositivos, la responsabilidad caerá directamente sobre el responsable del tratamiento. Por ello, el GT29 aconseja que se lleven a cabo evaluaciones de seguridad de los sistemas como un todo y la implementación de la certificación de dispositivos y la armonización con las normas de seguridad internacionalmente reconocidas.

El IoT implica una compleja cadena de suministro con múltiples partes interesadas que asumen diferentes responsabilidades, por ejemplo, los subcontratistas que diseñan y fabrican los componentes de hardware sin realmente tratar con datos, no pueden ser responsables si

[39] Artículo 10. Información en caso de obtención de datos recabados. Se recoge en este artículo la información que debe proporcionar el responsable del fichero al dueño de los datos.
Artículo 11. Información cuando los datos no han sido recabados del propio interesado.
Ambos artículos se puede encontrar en línea consultando en https://www.urjc.es/images/proteccion_datos/B.4-cp--Directiva-95-46-CE.pdf [Consulta 2870272017]

se produce una infracción en la protección de datos pero jugaran un papel fundamental en el mantenimiento de la seguridad del ecosistema IoT. Otro factor son los dispositivos. Diseñados para acceder directamente por internet lo que facilita el acceso a intrusos, sus componentes se caracterizan por los recursos limitados de energía y potencia y su vulnerabilidad a ataques físicos o escuchas. En algunos objetos, los valores que son observados pueden ser manipulados, estos dispositivos deben recibir una protección adecuada ya que pueden impactar indirectamente en decisiones relacionadas por ejemplo, con la salud.

El GT29 subraya las prácticas de seguridad basadas en restricciones de la red, la desactivación por defecto de funcionalidades no críticas, la prevención del uso de fuentes de actualización software que no sean de confianza como formas de limitar el impacto y alcance de posibles violaciones de datos. También hace hincapié en la previsión de soluciones alternativas de soporte en las ocasiones en las que un fabricante deja de darlo sobre un dispositivo. Por último, resalta la necesidad de una política adecuada de notificación de violaciones de datos que ayude mediante el conocimiento a contener los efectos negativos del diseño del software y sus vulnerabilidades.

5.10.4 DERECHOS DE LOS INTERESADOS

Las partes interesadas deben respetar los derechos de los interesados citados en el punto 5.8 "*Derechos de los interesados respecto a los datos personales*". Entendiendo por "interesados" cualquier persona cuyos datos personales sean tratados.

A continuación vamos a mencionar las particularidades más importantes que considera el Dictamen respecto a los derechos de los interesados dentro del marco del IoT.

5.10.4.1 Derecho de acceso

Aunque normalmente los usuarios muestran más interés por conocer los datos ya interpretados que los datos en bruto, la importancia de conocer estos últimos radica en entender lo que el fabricante del dispositivo puede saber acerca de ellos, la capacidad para transferir datos a otros responsables o interrumpir servicios de datos. En la teoría, la posibilidad de elegir ante esta información se ve limitada por los fabricantes de los dispositivos.

Generalmente los dispositivos mandan primero datos al fabricante del dispositivo y es éste el que hace que sean accesibles para el usuario vía portal web o aplicación. Este diseño permite ofrecer servicios que el dispositivo da, pero también impedir que los usuarios elijan libremente el servicio que interactúa con el dispositivo de tal forma, que si los usuarios quisieran interrumpir los servicios o transferir los datos a otro responsable no tendrían otra posibilidad que dejar de utilizar el dispositivo o acceder sólo a una versión degradada de los datos ya almacenados, una actitud que impide el ejercicio efectivo del derecho de acceso.

El GT29 considera que las partes interesadas en el IoT deben tomar medidas para que se cumpla tanto este derecho como el derecho de portabilidad, ofreciendo a los usuarios la posibilidad de utilizar otro servicio sin que éstos tengan que estar provistos necesariamente por el fabricante del dispositivo. Para ello, proponen los estándares de interoperabilidad como una herramienta útil.

5.10.4.2 Derecho de oposición o cancelación

Los esquemas de retirada deben cubrir según el Dictamen:

- *Los datos recogidos por un objeto específico (Por ejemplo solicitando que la estación meteorológica deje de recoger datos de humedad, temperatura y sonidos).*
- *Un tipo específico de datos recogidos por cualquier objeto (Por ejemplo, un usuario debe poder desactivar de cualquier dispositivo la grabación de sonido).*
- *Un tratamiento de datos específicos (Por ejemplo, un usuario debe poder hacer que su reloj y su podómetro dejen de contar pasos).*

El GT29 ha especificado que los interesados deben tener la posibilidad de retirar su consentimiento en cualquier momento sin tener que salir del servicio provisto. Actualmente, para ello se está tratando de dar al usuario más control en las funciones de administración de consentimiento mediante, por ejemplo sticky-policies o privacy proxies[40].

También considera que se debe dar la opción al usuario de permitir que objetos nuevos funcionen como los originales desactivando la opción de "conectado" ante la posibilidad de que los Wearables acaben sustituyendo a los objetos sencillos existentes.

5.11 LEGISLACIÓN VIGENTE ENTRE ESTADOS UNIDOS Y EUROPA

En 1998 Estados Unidos y la Unión Europea llegaron a un acuerdo sobre protección de datos creando un marco de "puerto seguro" (Safe Harbor) que permitía la transferencia de datos entre ambos para empresas que firmaran actuar bajo este marco siempre y cuando se cumplieran una serie de principios de privacidad.

En 2015 el Tribunal de Justicia de la UE anuló este marco pues consideraban que en la práctica el nivel de protección de esas empresas no podía comprobarse y por tanto resultaba insuficiente. Abriéndose paso el acuerdo Privacy Shield o "Escudo de privacidad" que se publicaría en 2016 (Decisión de ejecución (UE) 2016/1250.

Con este acuerdo se establece un sistema de auto-certificación mediante el cual las empresas de EEUU se comprometen a cumplir un conjunto de principios de privacidad que se

40

revisará entre la Comisión Europea, el Departamento de Comercio de EEUU y entidades de control y protección de datos de estados miembros de la Unión Europea. El acuerdo también recoge obligaciones y garantías de un control no masivo e indiscriminado de personas físicas europeas, lo que quiere decir que las empresas europeas que transfieran datos de usuarios europeos a empresas en Estados Unidos no tendrán que solicitar autorización previa a la Agencia de Protección de Datos sino verificar que la empresa a la que transfieren datos esté adherida al acuerdo y comunicar la transferencia. El certificado deberá ser renovado anualmente, verificando que cumplen con lo establecido en la Lista Shield con regularidad para verificar que se continúa dentro de los parámetros de cumplimiento.

Las principales obligaciones son:

- Principio de notificación y opción. La empresa deberá informar a sus usuarios sobre sus políticas de privacidad y el tratamiento de los datos personales.
- Garantizar la obtención del consentimiento expreso y explícito a la finalidad concreta por parte del titular de los datos, en especial de los datos sensibles. Así como el principio de oposición (opto ut) y el derecho de acceso, corrección, modificación y eliminación de información personal inexacta o tratada en incumplimiento de los principios establecidos.
- Limitar el tiempo de almacenamiento de datos al tiempo que sirvan para cumplir la finalidad concreta para la que se dio el consentimiento.
- Tomar las medidas de seguridad técnica y organizativa en la recogida, almacenamiento y tratamiento de datos.

Actualmente tras el decreto de Trump que indica que las agencias como FBI o NASA “deberán asegurarse de que no aplican la protección de la Ley de Privacidad a personas que no son ciudadanos de EE UU ni residentes legales” pone en riesgo este acuerdo.

Aunque la Comisión Europea sostiene que esta protección está blindada ante este decreto (Según la interpretación de las dos normas vigentes), pidió a EE UU que explicara ciertos comportamientos como órdenes judiciales secretas para vigilar el traspaso de datos entre empresas o la información que páginas de empresas de EE UU estaban dando a las usuarias indicando que podían verse obligadas a compartir datos personales en respuesta a peticiones de la las autoridades, incluidas las relacionadas con la seguridad nacional”[41].

[41] Artículo de El País: “Un decreto de Trump amenaza el acuerdo de protección de datos con la UE” Fecha de publicación 24/03/2017. Disponible en línea en : http://economia.elpais.com/economia/2017/03/24/actualidad/1490387414_940802.html [Consulta 27/04/2017]

6 INTERNET DE LAS COSAS EN EL CAMPO DE LA SALUD

Los ecosistemas conectados cambiarán el futuro de la asistencia sanitaria.

William King

En el punto *3.5 Campos de aplicación* hablamos brevemente del IoT en el campo de la salud. En este punto profundizaremos sobre el Internet de las Cosas de la salud.

Hay multitud de términos con los que se refieren a la tecnología relacionada con el campo de la salud: Internet de las Cosas de la salud, medicina digital. IoHT (Internet of Healthcare Things) como nos referiremos a partir de ahora, es la convergencia e integración de datos recogidos a través de una amplia gama de fuentes de datos, dispositivos médicos equipados con sensores, actuadores y etiquetas RFID entre otros.

6.1 POR QUÉ IOT EN EL CAMPO DE LA SALUD

El sistema de salud de los países está bajo constante presión para reducir el coste de la atención, mientras debe atender a necesidades de una población cada vez más insalubre y con un aumento de la edad media. En una situación de crisis como la de los últimos años donde particularmente en España, el gasto público en Sanidad y Educación han crecido alrededor de 10.000 millones de euros menos que el PIB desde el 2011, los factores que incrementan el gasto sanitario son:

- Incremento de la demanda de servicios debido a un aumento de enfermedades crónicas y un progresivo envejecimiento de la población. Actualmente las enfermedades crónicas son la causa del 60% de las muertes a nivel mundial y el 75% del gasto sanitario. 388 millones de personas morirán en los próximos 10 años por una de estas enfermedades.
- Aumento de gastos de infraestructuras y recursos humanos.
- Avances en tratamientos y técnicas diagnósticas.

En este tiempo en el que el sistema sanitario asistencial está redefiniéndose, el presupuesto se reduce y la demanda de servicios aumenta. Desde la Comisión Europea se promueve la sanidad electrónica como un medio para garantizar la continuidad de los tratamientos y para mejorar la sostenibilidad de los sistemas sanitarios. Los avances que

puede aportar el IoHT, pueden ayudar a hacer frente al aumento del gasto sanitario mejorando el funcionamiento de sistemas sanitarios donde el paciente puede gestionar su salud con un nuevo modelo de interacción, el diagnóstico precoz y mayor control de tratamientos y menor número de hospitalizaciones. Citamos como ejemplo una investigación de la firma de seguridad Zingbox (2016) donde se muestra que actualmente, los hospitales de Estados Unidos tienen un promedio de 10 a 15 dispositivos conectados por cama en centros donde puede haber hasta 5000 camas. Según la estimación realizada por esta misma empresa, las tecnologías IoHT podrían ahorrar 63.000 millones de dólares en costes de atención sanitaria durante 15 años y una reducción de entre el 15% y el 30% en los costes de los equipos médicos.

6.2 CARACTERÍSITICAS TÉCNICAS IoT SALUD

La arquitectura de dispositivos inteligentes para la salud no varía demasiado de la arquitectura para dispositivos de otras áreas. Inteligencia descentralizada es el principal objetivo en la construcción de dispositivos médicos inteligentes al igual que en otro tipo de dispositivos para mejorar el procesamiento de datos operativos a nivel local, además del servidor central.

Una arquitectura básica en este tipo de dispositivos puede dividirse en tres capas como mostramos en la ilustración.

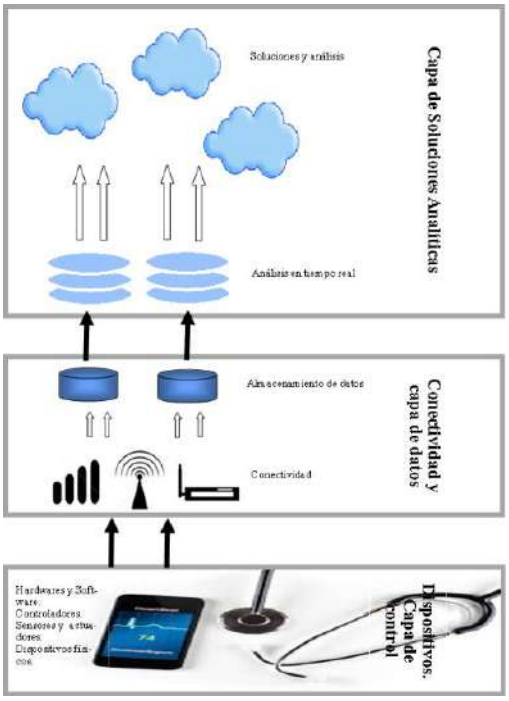

Ilustración 14: Ejemplo de arquitectura IoHT. Elaboración propia

- **Sistemas locales y capa de control**: Estos dispositivos normalmente son activados con sensores para medir parámetros de funcionamiento, controladores para la toma de decisiones en tiempo real basados en los datos recibidos e interfaces de red para compartir con otros equipos los datos.

  Codificadores, actuadores y dispositivos de cifrado realizarán las transformaciones de datos para transmitirlos y analizarlos. Igual que en el Internet de las cosas de cualquier área, en la salud uno de los mayores desafíos que nos encontramos es la interoperabilidad.

  En el ámbito de la medicina, tanto para la interoperabilidad sintáctica, referida a la estructura de la comunicación, como para la interoperabilidad que hace referencia al significado de la comunicación; se han desarrollado y apropiado estándares para varios propósitos relacionados con mensajería, terminología, documentos, esquemas conceptuales, aplicación y arquitecturas.

  En mensajería, por ejemplo; se han desarrollado estándares que definen el formato y la estructura de elementos de datos para facilitar la comunicación entre diferentes sistemas clínicos. Podemos citar algunos de ellos:

- HL7 V2.X, HL7 V3 para intercambiar datos demográficos, clínicos y administrativos.
- DICOM (Digital Imaging & Communications in Medicine) que define la forma para comunicar imágenes diagnósticas y datos asociados a éstas.
- ASC-X12 para intercambiar tramitaciones, elegibilidad de pacientes y pagos de prestaciones.
- IEEE 1073 que decide mensajes para intercambiar datos con equipos de instrumentación biomédica.

Respecto a la terminología, se han desarrollado vocabularios y códigos para etiquetar conceptos clínicos que pueden ir desde enfermedades a laboratorios pasando por diagnósticos, técnicas, procedimientos… Los más importantes:

- Clasificación Internacional de Enfermedades CIE-10 que define un catálogo de diagnósticos y procedimientos para fines estadísticos, facturación, costos y tramitaciones.
- LOINC para pruebas de laboratorio, métricas y observaciones clínicas.
- SNOMED CT, conceptos biomédicos y sus descripciones, relaciones y gramática para construir expresiones clínicas.

No obstante, aún hay multitud de estándares que pueden dificultar las decisiones de interoperabilidad entre sistemas con los que un centro sanitario debe interactuar. Urge por tanto, definir y establecer correctamente políticas, estándares y guías a implementar.

La compatibilidad y la integración de la electrónica impulsan el uso de soluciones a nivel de dispositivo. Éstos, son capaces de adquirir datos biométricos del cuerpo del paciente y transmitirlo siempre en un entorno seguro a una capa superior.

- **Conectividad y capa de datos**: Esta capa se centra en la recogida de datos desde el dispositivo y el almacenamiento de éstos en almacenes predefinidos.
  En este sector, la conectividad juega un papel importante. La posibilidad de utilizar tecnologías RFID, NFC, Bluetooth, ZigBee, etc. para monitorización de parámetros médicos aumenta el campo de aplicación de los dispositivos. Podemos destacar por escenarios:
  - Redes de gestión hospitalaria: ofrece los servicios típicos de transferencia de información como intranet, email, conectividad web… y una amplia variedad de aplicaciones médicas que proporcionan recuperación y procesamiento de la información del paciente, transferencia de imágenes y video, etc.
  - Redes de atención domiciliaria, servicios de tele asistencia. Dispositivos de telemetría portables de control de parámetros como pulsímetros, básculas, etc. cuentan con conectividad WI-FI o Bluetooth, siendo capaces de avisar en caso de detectar algún tipo de anomalías.

- Redes ubicuas de atención sanitaria: que permiten la atención y asistencia del paciente independientemente de su ubicación contarán con dispositivos que actúan como pasarelas y/o routers.

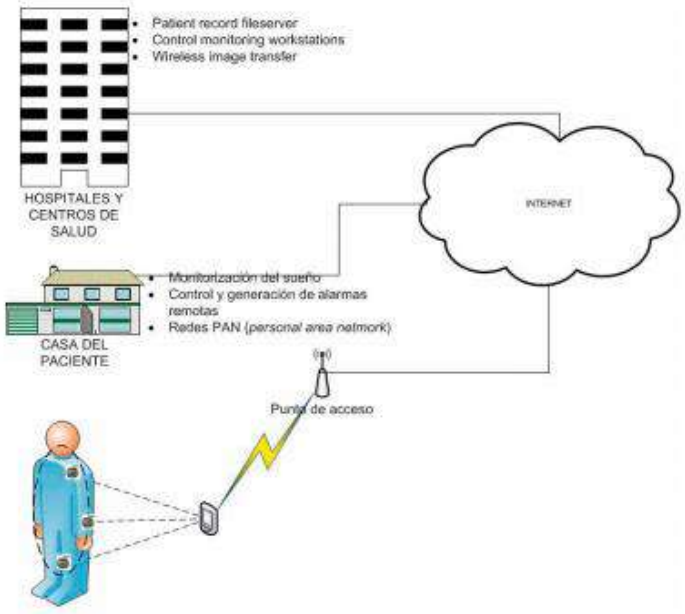

Ilustración 15: Escenarios de aplicabilidad de redes de comunicación en entornos sanitarios. Autor: Unidad de Investigación en Telemedicina y e-Salud Instituto de Salud Carlos III

- **Capa de soluciones analíticas**: El servidor central recoge los datos de los dispositivos a través de la red y sus componentes. Este servidor con algoritmos incorporados analizan los datos en tiempo real para proporcionar información como el diagnóstico, predicción de la enfermedad o aplicación de medidas preventivas. Permitiendo soluciones como monitorización remota o intervenciones y tratamientos de enfermedades crónicas

6.2.1 BODY AREA NETWORKS (BAN)

Los sistemas BAN consisten en redes de sensores para el cuidado de la salud junto con una infraestructura de red, evitando la necesidad de un sistema de salud administrado de forma manual. Caracterizadas por:

- ✓ Los nodos de la red son sensores o dispositivos de telemetría que recogen los parámetros biológicos y los envían al router o Gateway con un grado de alcance de un metro.
- ✓ El router/Gateway será típicamente un Smartphone que recopilará la información detectada por los sensores para transmitirla posteriormente al centro de control.
- ✓ Las pacientes tendrán más control sobre su salud al utilizar este tipo de tecnología. Existen dos tipos de interfaces: El interfaz de red de corto alcance, conecta dispositivos de telemetría con el router o Gateway. El interfaz de red de largo alcance, que permite la conectividad entre el router con el centro de control por red inalámbrica o cableada. Al buscar la mayor ubicuidad posible en el cuidado de las pacientes, se necesita que las redes tengan independencia, por tanto se recomendará en la mayoría de los casos que las interfaces de red de las BAN's sean inalámbricas y de esta manera integrar el m-healthcare con soluciones móviles.

6.2.2 RFID EN ENTORNOS SANITARIOS

Es obligado, dentro del estudio del IoHT, pararnos en el RFID en entornos sanitarios que permiten la identificación y localización de los pacientes o registros médicos además de diversas e importantes funcionalidades que se aplicarán después en ámbitos como la seguridad y el cuidado del paciente, aplicaciones farmacéuticas o gestión de material, suministros y dispositivos.

La importancia de la inmersión de tecnología RFID en el campo de la salud radica mayormente en los siguientes aspectos:

Control de los medicamentos en el ámbito de las farmacéuticas. Tanto en Estados Unidos como en Europa, preocupa el incremento de la falsificación de productos en el mercado. El etiquetado de los medicamentos más relevantes ha impulsado la regulación de RFID dentro del sector farmacéutico donde se realizará una trazabilidad de los medicamentos desde su fabricación hasta su llegada a la farmacia.

Mayor control de dispositivos en los centros de salud. Se estima que el coste por robo de equipamientos y bienes en un hospital estadounidense puede acercarse a los 4000 US$ anuales. Los elementos que se quedan olvidados en el cuerpo de los pacientes tras una operación son de uno por cada 10.000 intervenciones[42]. Este hecho, además de poner en riesgo la salud del paciente provoca pérdidas monetarias debido a las pérdidas económicas y el aumento de tiempo de hospitalización. La integración de pequeños chips en dispositivos

[42] Dato sacado del informe de vigilancia tecnológica realizado por Madridmasd disponible en línea en: http://www.madrimasd.org/uploads/informacionidi/biblioteca/publicacion/doc/VT/_VT13_RFID.pdf [Consulta: 19/05/2017]

médicos, pueden ayudar a controlar dónde están en todo momento evitando robos o pérdidas. La tecnología RFID en gasas o instrumental quirúrgico permiten su etiquetado y conocer la localización de éstos. Su inventariado puede ayudar a controlar que no haya errores como dejar un bisturí dentro del cuerpo del paciente al que han operado.

Pacientes fuera del entorno sanitario. Para pacientes que aún fuera del entorno sanitario siguen necesitando cuidados pueden llevar un brazalete o un objeto identificativo a través de etiquetas RFID accesibles desde un lector portátil. En caso de urgencia el tiempo de acceso a información importante se reducirá notablemente. Además, poder consultar los movimientos del paciente puede ayudar a que el sanitario cuente con más información y acelerar los protocolos de actuación.

6.3 BENEFICIOS Y BARRERAS EN IOHT

6.4 BENEFICIOS IOT EN EL SISTEMA DE SALUD

La conexión de pacientes, profesionales, máquinas y sistemas dinámicos, garantizan un sistema sanitario efectivo ante la vigilancia médica. A continuación mostramos un esquema de los beneficios que aporta el Internet de las Cosas en este sector. Estos beneficios se centran en mejorar la calidad de vida del paciente.

Ilustración 16: Beneficios IoHT. Elaboración propia.

El informe de 2017 realizado por Bankinter[43] extrae los principales beneficios que el internet de las cosas puede aportar en el campo de la salud. Podemos dividir los beneficios en campos a los que afectará directamente teniendo en cuenta que esos campos están estrechamente ligados:

- Pacientes
  - ✓ Empoderamiento: el paciente podrá gestionar y mejorar de forma pro activa su salud gracias a la información que diferentes dispositivos le puedan aportar.
  - ✓ Satisfacción del paciente: el aporte de datos de cada paciente en tiempo real podrá darle una atención más personalizada y por tanto de mejor calidad.
  - ✓ Acceso remoto: el acceso a aplicaciones relacionadas con la salud de fácil uso, ampliará el espectro de población que pueda utilizarlas.
  - ✓ Bienestar individual: evitar que los pacientes deban trasladarse o crear alternativas a pruebas que pueden resultar invasivas para ellos mejora sin duda el bienestar individual.
  - ✓ Conciencia de la salud: Wereables y dispositivos de prevención darán conciencia a las pacientes sobre su estado de salud. La posibilidad de crear objetivos aportará motivación para modificar comportamientos de salud.
  - ✓ Resilencia: Los pacientes podrán adaptarse mejor a situaciones adversas relacionadas con su salud.

- Atención médica
  - ✓ Prevención: se fomentarán los cuidados de salud a través de la prevención de enfermedades.
  - ✓ Cuidado continúo: el análisis en tiempo real mejorará sin duda el cuidado a los pacientes en todo momento adaptándose a las variaciones que puedan sufrir. Aportará además ayuda a familiares y cuidadores de los pacientes.
  - ✓ Atención personalizada: la gran cantidad de datos mejorará la toma de decisiones de tratamientos más personalizada y ajustada a las necesidades del paciente.
  - ✓ Detección: los dispositivos pueden ayudar a la detección de patologías y acortar el tiempo hasta llegar a un diagnóstico de las mismas. La inteligencia Artificial, la mejora en el diagnóstico de imágenes y la gran cantidad de datos donde poder comparar mejoran el diagnóstico.
  - ✓ Errores médicos: expertos consideran que la tasa de errores médicos puede verse reducida con la utilización de tecnología en la salud basándose en que los errores fortuitos estarán controlados.

[43] Informe Bankinter realizado en 2017 realizado por la Fundación Innovación Bankinter basado en la reunión de diciembre de 2016 del Future Trends Forum. Disponible en línea en: https://www.fundacionbankinter.org/documents/20183/97216/Salud++Digital+ES/5f5bd348-ca10-49de-8bfe-2ba368a2e269 [Consulta 19/05/2017]

- Sistema sanitario
  - ✓ Base de datos: permitirán analizar con precisión y en tiempo real cada caso. Se reducirán las posibilidades de pérdida de información y se mejorará el acceso a todo el historial clínico del paciente.
  - ✓ Investigación y desarrollo: el IoHT para el I+D+I supondrá una herramienta de gran ayuda. Acceso a más casos de estudio, más datos sobre cada caso. Realización de estadísticas o informes en los que basar el estudio o sacar muestras de población.
  - ✓ Costes de la atención sanitaria: permitirá reducir el coste global de asistencia sanitaria.
  - ✓ Feedback financiación: mayor capacidad de obtener información de utilidad para los inversores y vincular inversiones en salud pública con los beneficios financieros.
  - ✓ Estabilidad política: la salud de la sociedad de un país está vinculada al crecimiento sostenible de su economía, proporcionando bases para el desarrollo de sistemas estables.

6.4.1 BARRERAS IOHT

Actualmente existen una serie de barreras cruciales para acelerar los beneficios de la Salud Digital. En la figura podemos ver un resumen por actores del ecosistema.

Ilustración 17: Barreras IoHT por grupos. Elaboración propia.

A continuación repasaremos las barreras más importantes con las que el IoHT se puede enfrentar:

- Datos: la tecnología debe desarrollar estándares que destruyan los silos de información existentes. Actualmente hay una necesidad de mejorar el acceso a la información sobre el historial médico o de enfermedades de los pacientes.
- Inversión: los inversores consideran que se necesitan nuevos modelos de financiación para fomentar la innovación además de una coordinación entre inversiones públicas y privadas. También consideran que los organismos reguladores deberían compartir información de forma pública, de esta forma; al contar con mayor información a la hora de tomar decisiones, se reduciría la incertidumbre respecto al retorno de la inversión de proyectos.
- Cultura e incentivos: Culturalmente, existe una resistencia al cambio que aumenta si se trata del tema de la salud. Es necesario que el sistema sanitario pueda medir lo que ofrecen a los pacientes para promover un cambio en el sistema de Salud. A mayor tecnología biomédica mayores protocolos de seguridad. Los médicos deberán aprender de bioseguridad y tecnología. Es necesario insistir en este aspecto ya que una parte importante y que se debe cubrir necesariamente es cualquier medida de seguridad al alcance de los usuarios, ya sean pacientes o profesional médico.

- Liderazgo: la inmersión del IoT en la salud a ritmos acelerados hace que haya cierta carencia por parte de los profesionales para medir y analizar los resultados en salud en las innovaciones tecnológicas.
- Incertidumbre política y regulatoria: Es necesaria una coordinación y un entendimiento entre todas las partes implicadas en el ecosistema para desarrollar estrategias y políticas regulatorias, así como revisar el valor y los intereses de la innovación.

6.5 LÍNEAS DE APLICACIÓN DE IOHT

6.5.1 DISPOSITIVOS PARA EL BIENESTAR PERSONAL

También conocidos como Wereables, son dispositivos destinados a la monitorización de la actividad física, un fomento de la vida saludable y el bienestar personal que se incorporan en alguna parte de nuestro cuerpo interactuando de forma continua con el usuario y con otros dispositivos para realizar alguna función concreta. Directamente no tienen que ver con el campo de la salud, pero de forma indirecta ayudan a mejorarla y los datos que se almacenan y el análisis que se haga de ellos posteriormente, si pueden dar información acerca del estado de salud del usuario.

Relojes, zapatillas con GPS y pulseras que controlan nuestro estado de salud son ejemplos de este tipo de dispositivos que hasta ahora estaban enfocados a personas jóvenes y deportistas y, donde actualmente se han introducido nuevos perfiles de usuarios como personas mayores o pacientes que los utilizan como ayuda en el seguimiento y tratamiento de patologías. Este cambio ha forzado cambiar el enfoque a fabricantes y diseñadores de estos dispositivos.

Aunque las principales agencias reguladoras, FDA[44] y EMA[45] no les exige una certificación especial, dado que no son de uso médico y no son invasivas y por tanto no requieren una aprobación concreta, la información que recogen puede ser útil si se interpreta bien sobre todo en pacientes que ingresan de urgencias. Los médicos ven en estos dispositivos aliados para: facilitar el establecimiento de objetivos concretos, progresivos y adaptados a las

[44] FDA (Food and Drug Administration): Es la agencia del gobierno de los Estados Unidos encargada de la regulación de alimentos, medicamentos y cosméticos. Disponible en línea en: https://es.wikipedia.org/wiki/Administraci%C3%B3n_de_Alimentos_y_Medicamentos [Consulta 15/06/2017]

[45] EMA: Agencia Europea de Medicamento encargada de evaluar las solicitudes de autorización de comercialización de medicamentos en la Unión Europea. Disponible en línea en: https://es.wikipedia.org/wiki/Agencia_Europea_de_Medicamentos [Consulta 15/06/2017]

características individuales de cada paciente; aumentar la motivación y mejorar la efectividad de planes de tratamientos. También se empiezan a emplear en ensayos clínicos para ver si las terapias que se prueban, sumadas a un estilo de vida favorable funcionan, este es el caso del realizado en el Hospital Mount Sinai (EEUU) que estudiará durante tres años como los hábitos de vida influyen en la salud cardiovascular.

Sin embargo los médicos temen por algunos obstáculos. Por una parte se preguntan hasta qué punto son fiables y si son útiles más allá de un uso en la población sana y por otro, ante ensayos clínicos largos y en relación a los pacientes, se preguntan: ¿Cuánto dura una persona cumpliendo con los parámetros de su monitor? ¿Cuándo lo deja? ¿Por qué lo abandona? Encontrar respuesta a estas preguntas es básico para los médicos ya que la modificación de hábitos tiene que persistir en el tiempo y no sólo estar sujeto a la moda o a alcanzar un objetivo. James Fogarty, profesor de Ingeniería y Ciencias de la Computación en la Universidad de Washington explica que "*Entre las razones habituales para dejar a un lado el dispositivo se halla el que una vez que saben lo que tienen que hacer, no necesitan apoyos; no les gusta lo que el dispositivo revela de ellos; se sienten mal por incumplir las expectativas; o no quieren que otros sepan lo que hacen*" Artículo de La Razón, 2017.

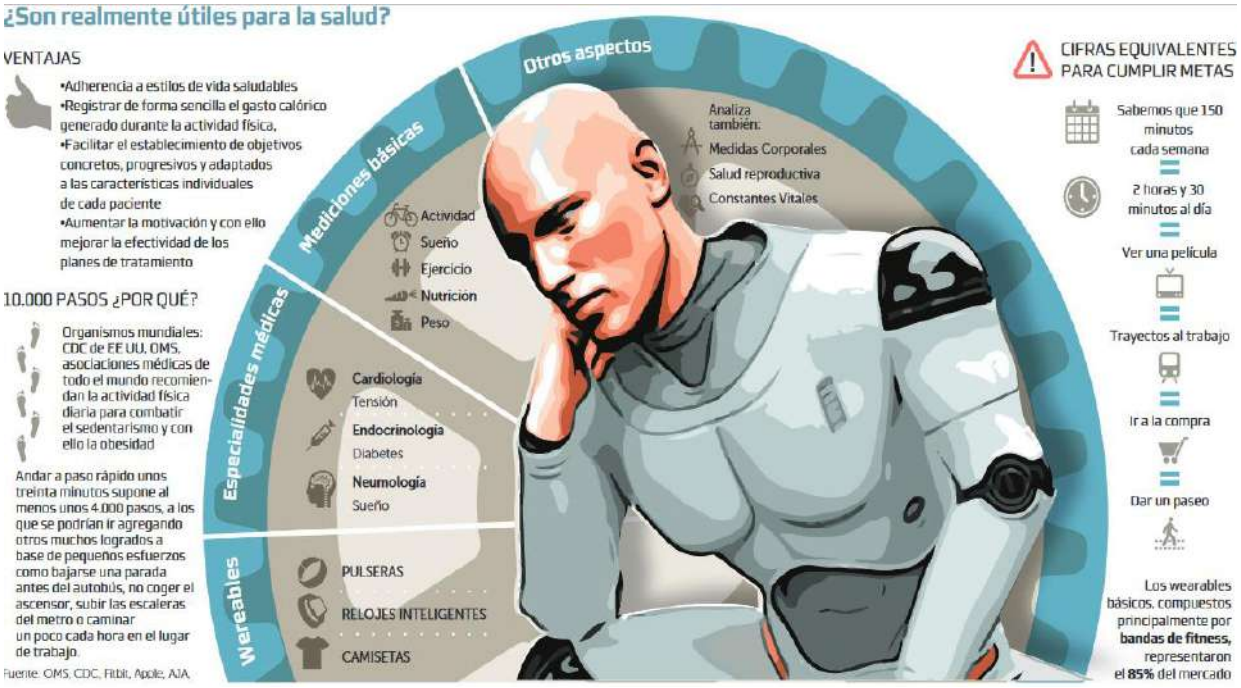

Ilustración 18: Wearables para la salud. Fuente OMS 2015

6.5.2 IMPRESIÓN 3D

Actualmente las prótesis e implantes representan el campo que más está creciendo, ya que la impresión 3D posibilita crear modelos más anatómicos, compatibles y personalizados a un bajo coste. Como ventajas, la impresión 3D permite en prótesis movibles, dotarlas de mayor naturalidad y mejor funcionamiento integrando robótica y electrónica. La forma de crearlas conlleva unos minutos y el trabajo se hace directamente desde una radiografía o resonancia. La aplicación se hace cada vez con más frecuencia y para crear modelos o réplicas exactas del cuerpo humano. Esto supone un gran paso para la cirugía ya que los cirujanos podrán practicar intervenciones complejas a escala real con mayor probabilidad de éxito. La impresión 3D avanza y lo próximo será el intento de reproducir un órgano.

Para saber cómo resisten al paso del tiempo, habrá que integrar sistemas de seguimiento, diagnóstico y control de fallo dentro de los productos médicos 3D, con el fin de proteger la salud del paciente. Estos seguimientos de los productos médicos puede verse apoyado por radiofrecuencia (RFID) y los códigos QR parecen sistemas poco eficientes de seguimiento y propensos a errores o fallos en la eficiencia.

En línea con las prótesis y yendo más allá en la innovación. El IoT ha permitido con la impresión 3D y los dispositivos wearables, crear una startup especializada en la rehabilitación ósea y muscular. Un proyecto reconocido, utiliza las impresoras 3D para crear férulas a medida del paciente que inmovilizan el miembro fracturado e incorporan un sistema de electro-estimulación que, conectado al móvil y a una app propia le permite seguir la rehabilitación desde casa, lo que reduce en 30 por ciento el tiempo de recuperación y los costes de las bajas laborales. La mayoría de los audífonos y muchas piezas dentales se hacen con impresión 3D. La última novedad, una pastilla impresa en 3D para tratar las crisis epilépticas. Avances que nos facilitarán la vida en los que hay que poner atención en especial en la gestión de imágenes y la anonimización de éstas en su tratamiento.

6.5.3 PREVENCIÓN Y PRONÓSTICO TEMPRANO.

No son pocas las veces que habremos oído la importancia del diagnóstico precoz para combatir con éxito ciertas enfermedades. También sabemos que muchas de ellas se presentan sin síntomas aparentes o con síntomas que bien pueden relacionarse con otros problemas de salud más comunes. Sea como fuere y aunque parece que estamos mejorando en la responsabilidad de hacernos revisiones periódicas, todavía la mayor parte de la población acudimos al médico sólo cuando nos duele algo. La necesidad de pruebas entonces, demora el diagnóstico. Las listas de espera y los tiempos son problemas a resolver por los sistemas sanitarios, que pueden mejorarse con la implantación de tecnología IoT.

Sensores y dispositivos que al detectar un problema o valor alterado lancen un aviso o, desencadenen el suministro de una dosis médica es un hecho. El avance en este campo está dando como resultado multitud de dispositivos para prevenir enfermedades. Podemos poner ejemplos como el cepillo de dientes inteligente*: Grush*[46] *creó un cepillo de dientes inteligente incorporando un chip Intel al cepillo. El chip recopila información como en qué parte de la boca está el cepillo, la fecha y la hora en que se utilizó y cuánto tiempo se dedicó a cada pieza dental. También se analiza qué dicentes suelen olvidarse de cepillar, si no se ha cepillado un diente, la aplicación envía una notificación y se inicia un proceso para identificar el posible deterioro futuro. Los datos se envían en tiempo real a una aplicación móvil para poder ver la información en pantalla. El cepillo está orientado para niños, por eso lleva un juego de puntos donde dan puntos según te lavas los dientes. Los niños juegan y los padres saben cómo es la higiene bucal de sus hijos. (*Recogido de IBM DeveloperWorks 2016*)*

Start Analytical Services y la Universidad de Queensland, en Australia después, desarrollaron aplicaciones a través de las cuales se podría diagnosticar el asma o la neumonía en los pacientes con un análisis del sonido de cuatro o cinco toses. Para ello se compararía el sonido con una base de datos de 1000 perfiles. Otra app con bastante éxito en las pruebas es Priori, desarrollada por la Universidad de Michigan, tiene como objetivo predecir episodios bipolares en los pacientes y alertar a los cuidadores o médicos en caso de que sea necesario.

Aplicaciones para detectar si una persona sufre Alzheimer, un problema cardiovascular, dispositivos que analizando comportamientos puedan indicar si hay un trastorno depresivo… los nuevos dispositivos son múltiples y los objetivos para los que están creados también. En la siguiente ilustración podemos hacernos una idea de todos los dispositivos que pueden ayudarnos en la prevención de enfermedades.

[46] Se puede ver el artículo de forma más detallada en el artículo de IBM developerWorks disponible en línea en: https://www.ibm.com/developerworks/ssa/cloud/library/cl-grush-smart-toothbrush-bluemix-trs/index.html [Consultado 13/05/2017]

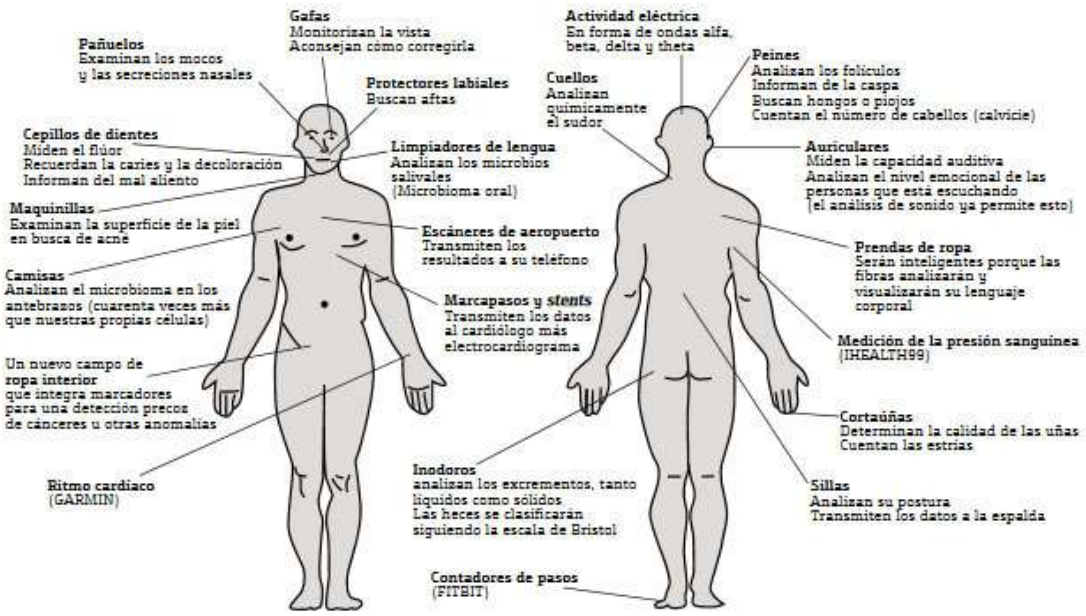

Ilustración 19: Aplicaciones Internet de la Salud. Fuente: http://quantifiedself.com/

6.5.4 ATENCIÓN CLÍNICA

Para pacientes con enfermedades crónicas, la aparición de dispositivos que miden un gran número de variables que pueden ir desde la temperatura hasta las horas necesarias de sueño o las dosis de medicación, ayudan a médicos, pacientes y cuidadores en la toma de decisiones rápida y de una forma más cómoda para los enfermos. El médico podría ajustar las dosis de las medicinas o cambiar el tratamiento en tiempo real sin necesidad de que el paciente tuviera que acudir a la consulta. Con la recopilación de datos se podría facilitar, además, estadísticas que relacionen medicación con mejoría en la salud ayudando a los facultativos a toma de decisiones más personalizadas y ajustadas con los enfermos.

Además de pacientes crónicos, la telemonitorización puede ayudar a sustituir la hospitalización por una hospitalización domiciliaria en postoperatorios o rehabilitación. Esto evitará más desplazamientos prescindibles o transferir el diagnóstico, seguimiento y terapias al hogar del paciente.

6.5.5 INTERVENCIÓN REMOTA

La empresa Telcare creó el primer glucómetro móvil que permite transmitir los resultados de un análisis a un centro médico para recibir asistencia instantánea on-line. El dispositivo tiene una ranura para insertar un papel con una gota de sangre, conexión wi fi y una pantalla por la que enviar los datos. Aplicaciones envían resultados de las analíticas al teléfono móvil del médico para que contacte con el paciente por correo electrónico con la interpretación.

La posibilidad de poder hacer ciertas pruebas o análisis de forma independiente mejoran la calidad del sistema sanitario para con el paciente, el hecho de no tener que desplazarse a centros sanitarios para realizarlas supone una reducción en las listas de espera y un tratamiento más eficaz y más rápido respecto al tiempo empleado.

Podemos definir como "Ingeribles", aunque se puedan utilizar otras vías para introducirlos en el interior del cuerpo como cirugía o vía rectal), son los dispositivos que pueden medir datos en el interior del cuerpo. Tecnología que se trata y realiza mediciones que transmite a un servidor externo durante el tiempo que esté dentro de nuestro organismo. A continuación mostramos el funcionamiento de estos dispositivos:

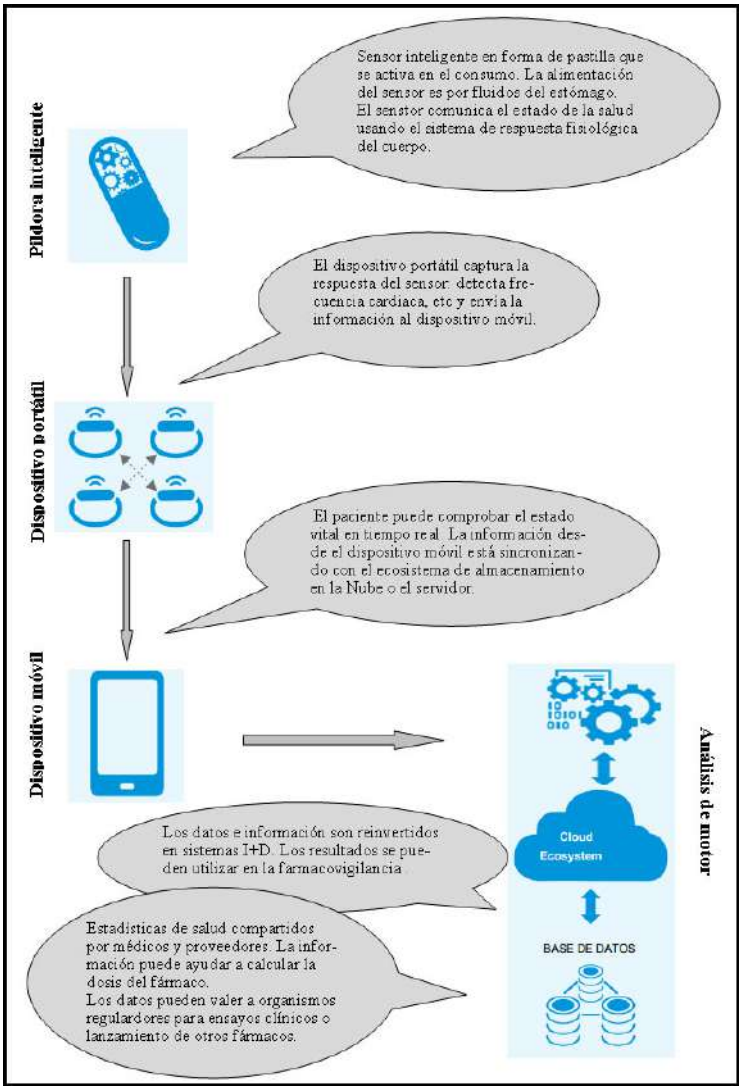

Ilustración 20: Funcionamiento píldora inteligente basada en figura Nextgen pharma [47].

Las posibilidades con estos dispositivos se disparan. Se prevén dos tipos de dispositivos: permanentes, que pueden quedar introducidos en el cuerpo de forma continua y los que tendrán un paso temporal por nuestro cuerpo. Datos en tiempo real obtenidos de sensores permiten a los facultativos administrar fármacos o cambiar las dosis y evaluar la respuesta en caso de emergencia, el dispositivo compuesto por una batería, una luz y dos minicamaras que puede ser una alternativa a la colonoscopia para pacientes que no hayan podido realizarla ya está aprobada por la FDA para su uso en EEUU. El dispositivo se conecta a una grabadora que el paciente puede llevar en el cinturón. Pruebas médicas como estas

[47] Disponible en línea en: http://www.wipro.com/documents/nextgen-pharma-takes-smart-strides-with-internet-of-things.pdf [Consulta 30/03/2017]

podrán ser completadas con algoritmos que crucen datos recogidos en otros dispositivos del paciente.

La toma de valores que antes se realizaba exclusivamente en entornos sanitarios, puede ser recogida y mandada por los dispositivos o puede que cuidadores, familiares o los propios pacientes deban realizar alguna operativa. Seguimiento de los pacientes en tiempo real sin necesidad de desplazamiento. Telemedicina. Todos estos dispositivos, orientados mayormente a enfermos crónicos o personas con movilidad reducida, permiten mejorar la autonomía del paciente, la autoestima y la movilidad. Ayudan a evitar el aislamiento social y aportan un apoyo a los cuidadores y las familias. Por otro lado ayuda a reducir costes por la hospitalización o el traslado si existe esa necesidad.

En este punto es un factor importante, el abaratamiento de los dispositivos y entornos fáciles de utilizar por toda la población pero en especial por personas mayores no familiarizadas con la tecnología. De forma indirecta aparece como reto la extensión de las redes de datos a entornos personales y domiciliarios.

6.5.6 FARMACIA

El IoT de la salud está estrechamente relacionado el sector farmacéutico. El crecimiento que se prevé en este sector es enorme, sobre todo en el campo de la transmisión de datos médicos y el seguimiento de pacientes. Tanto, que está llevando a replantear el diseño de los ensayos clínicos y la forma de recoger los datos durante el desarrollo clínico y la post-comercialización.

La posibilidad de monitorizar mediante sensores productos farmacéuticos tienen beneficios como:

- Identificar productos que requieren especiales condiciones de almacenamiento o transporte.
- Seguimiento de medicamentos originales que cumplen estándares de calidad, esto permitirá la detección de productos falsificados.
- Etiquetas inteligentes sobre medicamentos pueden informar a los pacientes de dosis, fecha de caducidad y un aseguramiento de la autenticidad del medicamento. Por otro lado, si lo complementamos con un gabinete de medicina inteligente que revise la información que pueden enviar las etiquetas, se podrá revisar y avisar al paciente de dosis prescritas, intervalos para la toma de los medicamentos y el cumplimiento del tratamiento por parte de paciente.
- Control de stocks.

Actualmente ya existen proyectos y colaboraciones muy interesantes. Novartis junto con Qualcomm están desarrollando un inhalador que puede enviar información de quien lo

utilice. Novartis quiere monitorizar cada inhalación su medicamento para tratar el enfisema. Desde los dispositivos móviles los pacientes podrán hacer el seguimiento de su tratamiento y los médicos podrán acceder a los datos a través de la web. Por otro lado, Novartis conjunto con Google están trabajando para crear una lente de contacto inteligente que pueda monitorear la glucosa en sangre de los niveles de líquido en el ojo de un paciente y comunicárselo por WI FI al médico o farmacéutico. Y hablando de anteojos, Microsoft está desarrollando unas gafas especiales que permitan a los farmacéuticos ver los registros de los pacientes y la información de la prescripción.

6.5.6.1 Venta a distancia de medicamentos

La venta a distancias de medicamentos quedó regulara en el Real Decreto 870/2013 por el que se regula la venta a distancia de medicamentos de uso humano no sujetos a prescripción médica. Excluye, por tanto los medicamentos sujetos a prescripción, los preparados y los medicamentos veterinarios. Por otro lado, la venta por internet sólo podrá realizarse en una farmacia física y con la intervención de un farmacéutico titular.

La página web que venda este tipo de medicamentos deberá cumplir con unas obligaciones específicas, seguridad, accesibilidad, cifrado de datos, diferenciación inequívoca de la parafarmacia o la prohibición de la publicidad.

La receta electrónica supone ahorro de tiempo para el paciente y reducir las listas de espera para el médico que deba extender las recetas. El avance puede ser mayor, el botiquín inteligente podrá avisar a la farmacia de si en realidad no le queda más medicación, incluso si el paciente la toma o no correctamente.

Del lado de los laboratorios, la competitividad de las farmacéuticas se verá beneficiada por el Internet de las Cosas. Podemos resaltar los siguientes beneficios:

- Ahorro de costes.
- Mejora de la calidad: con los sistemas inteligentes el control de los medicamentos, su calidad y la tasa de error se reducirá drásticamente en fases de prueba. Los informes y sistemas de análisis de datos podrán ajustar los efectos secundarios mejorando la calidad de los medicamentos.
- Mejor adherencia cumplimiento: los dispositivos aportarán información en tiempo real a través de la monitorización. Las excepciones pueden ser respondidas de forma rápida y esto puede ayudar en los estudios o informes de regulación. La presentación de informes de eventos adversos pueden ser minimizados a través de alertas de predicción.
- Mejor planificación y menor tiempo de comercialización: Los datos obtenidos mediante los dispositivos en tiempo real se pueden utilizar para la toma de decisiones o la generación de ideas de negocio. Datos como cambios en la investigación de

fármacos, eficacia, adopción, resultados… pueden ser útil durante el lanzamiento del medicamento, aportar ideas para la decisión de precios del medicamento y el desarrollo

6.6 HOSPITAL CON EL IOHT

Habitaciones, quirófanos, urgencias, consultas. Salas de recuperación, rehabilitación, radiología. Farmacia, pasillos, lavandería, cocina, almacenes de artículos sanitarios, despachos administrativos, dirección, laboratorios… espacios con diferentes niveles de accesibilidad. Pacientes ingresados, pacientes externos, familiares, personal sanitarios de diferentes áreas y clasificaciones: médicos, enfermeras, estudiantes, administrativos, personal de dirección, limpieza, seguridad, proveedores… con diferentes restricciones de acceso. La tela de araña de un hospital es grande y compleja. Diversidad de situaciones, de espacios y de personas, de tareas que hay que realizar y de variables a tener en cuenta hacen que se convierta en un reto organizativo sensible a fallos, deficiencias e ineficacias. El momento por el que la economía mundial está atravesando no ayuda a este entramado, el aspecto económico influye directamente en la calidad y competitividad de los hospitales que repercute, a su vez; en la calidad de la atención sanitaria recibida por los pacientes en un entorno donde los fallos en esta atención pueden traer graves consecuencias.

Digitalizar, informatizar y automatizar pueden ser claves para mejorar el sistema. Algunas claves ya llevan tiempo aplicándose como la informatización de historias clínicas, la receta electrónica, pruebas diagnósticas… Otras serán de más fácil aplicación con la llegada del Internet de las Cosas y no sólo hablamos de las directamente relacionadas con la medicina, cualquier actividad informatizada con soporte tecnológico ayudará a la disminución de errores humanos y facilitará, en el caso de haberlos, encontrar la razón y evitarlos. Aunque pueda parecer que hablamos de un futuro lejano, no es así. El IoHT ya ha llegado a los hospitales. Una investigación de la firma de seguridad **Zingbox** afirma que actualmente los hospitales de Estados Unidos tienen un promedio de 10 a 15 dispositivos conectados por cama en centros donde puede haber hasta 5000 camas. Según la estimación realizada por esta misma empresa, las tecnologías IoHT podrían ahorrar 63000 millones de dólares en costes de atención sanitaria durante 15 años y una reducción de entre el 15% y el 30% en los costes de los equipos médicos.

Como ejemplo de hospitales punteros en la integración de la nueva tecnología podemos citar al Humber River Hospital de Toronto. Este hospital ha ido integrando diferentes dispositivos, algunos incluso de la industria, para hacer de él un hospital automatizado. Por sus pasillos hay un despliegue de plataformas sobre ruedas, estos vehículos monitorizados capaces de entregar el 75% de los suministros, van por los pasillos, abren y

cierran ascensores, advierten a la gente para que se retire e informan al personal cuando han entregado sus cargas.

El flujo de trabajo en el laboratorio es otro ejemplo, las peticiones se envían al laboratorio y el laboratorio envía uno de los vehículos a los que nos hemos referido antes con tubos y una impresora de código de barras, de esta forma cuando se extraiga la sangre se podrá sacar el código de barras. Los tubos se envían al laboratorio. El tiempo de respuesta se ha reducido y también los errores con las muestras. El flujo de medicamentos es parecido, se envían a la farmacia electrónicamente, un sistema de robótica recoge y envasa los medicamentos organizados en sobre con un código de barras. Los sobres se envasan y se envían por vehículos a los puestos de enfermería que les corresponden.

Signos vitales que se trasmiten desde monitores hasta el registro médico sin papel y reajustando los datos. Las camas cuentan con terminales de cabecera con funciones para el bienestar de los pacientes que van desde el acceso a internet hasta el acceso a sus registros hospitalarios algo que da cierto empoderamiento a los pacientes. Los terminales también se pueden utilizar por los médicos para acceder a los datos del paciente o insertar nuevos. Los teléfonos muestran alertas y alarmas, actúan como un sistema de llamada a enfermeras. Tienen cámaras que permiten la videoconferencia con el paciente, lector de barras por si se ha olvidado y tiene que consultar medicamentos o muestras de laboratorio y son capaces de mostrar tiras de ritmo cardiaco. El hospital cuenta con un sistema de localización de tiempo real para saber dónde encontrar a profesionales y pacientes en todo momento pero también sillas de rueda si se necesitaran.

Este hospital no es un caso aislado, el hospital Karolinska Solna de Estocolmo además de carritos automatizados cuenta con una red de tubos neumáticos en todo el hospital. Por ellos viajan medicamentos, bolsas de sangre, materiales. Así los laboratorios están conectados y el tiempo de demora en pruebas y consultas se reduzca considerablemente.

Los elementos inteligentes que puede haber en un hospital para que su eficacia y el rendimiento de sus trabajadores mejore pueden ser cientos y aunque a la larga aportará múltiples beneficios, puede suponer un aumento elevado de presupuesto. A continuación citaremos algunas tecnologías que se considera, deberían incorporarse a los hospitales del futuro:

- Tecnología hardware y software para monitoreo de ingreso y egreso de personal ajeno al hospital.
- Impresoras 3D para permitir imprimir con alta precisión prótesis personalizadas.
- Robots de toma de imágenes que se adapten a cada paciente.

- Interfaces Naturales de Usuario[48] de interacción para la salud, basados en dispositivos optoelectrónicos que permiten acceder a la información digital sin necesidad de contacto, de forma intuitiva que no implica abandonar la zona estéril pero previene de infecciones por contacto. Ahorrando también tiempo y recursos.
- Drones para traslado urgente de órganos para trasplantes, sangre, antídotos específicos…
- Recopilación de toda la información asistencia, social y económica en un sistema de big data para realizar estudios que permitan la prevención y el diagnóstico precoz, al tiempo que cuentan con una herramienta de análisis de costes.
- Telemedicina que permitirá una optimización del tiempo disponible para consultas del facultativo sin que el paciente deba salir de casa así como la posibilidad de que los facultativos puedan acceder a la telemonitorización domiciliaria.
- Tecnología de hardware y software de Radio Frequency Identification –RFID-, para múltiples tareas, por ejemplo en el caso de pacientes, para saber en tiempo real donde se encuentra o en qué punto del centro se lleva a cabo un procedimiento que se deba realizar. Se evita al máximo el secuestro de pacientes neonatos y pediátricos, algo más frecuente de lo que parece. Evitan la sustracción en el interior dela institución y tienen censados los implementos. Además ayudan para el control de medicamentos en farmacia y salas de enfermería.
- Hardware y software en cada cama de las habitaciones de los pacientes con los cuales saber si el paciente se intenta levantar de su cama o si ocurre cualquier problema en tiempo real.
- En España el Colegio Oficial de Ingenieros de Telecomunicaciones demanda una normativa para que los centros sanitarios sean diseñados como edificios inteligentes con el objetivo de mejorar la asistencia, humanizar la estancia y ahorrar costes. Por ejemplo: en un hospital con 900 camas que atiende a 110.000 pacientes al año, integrar un sistema inteligente permite reducir el tiempo medio de permanencia en urgencias entre dos y dos horas y media a menos de sesenta minutos.

Queda claro que integrar los avances tecnológicos en nuestros sistemas hospitalarios aportarían grandes ventajas que influirían sin lugar a dudas en nuestra salud y en el bienestar de la población. Aún con ello no nos podemos olvidar de las amenazas que pueden existir en un hospital inteligente. Además de las amenazas existentes en cualquier dispositivo inteligente, la Agencia Europea de Seguridad de las Redes y de la Información publicó en 2016 un estudio sobre las principales amenazas dentro de los hospitales inteligentes donde destacaban el malware como el principal factor de riesgo.

[48] Interfaces de interacción natural para la salud. Tecnología que permite acceder a la información digital sin necesidad de contacto. Más información en http://www.tedcas.com/es [Consulta 24/04/2017]

6.7 REGULACIÓN PROTECCIÓN DE DATOS EN IOHT

La protección de estos datos es un derecho fundamental recogido por el TFUE[49] en su artículo 16[50] y en la Carta de Derechos Fundamentales, artículos 7 y 8. El RDLOPD en el artículo 5.1.g define los datos de carácter personal relacionados con la salud como "*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"* que únicamente pueden ser objeto de tratamiento con el consentimiento expreso del titular y teniéndose en cuenta que pueden tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido.

A nivel nacional, en España no existe una regulación expresa sobre el Internet de las Cosas de la salud, pudiéndose aplicar las normas que se muestran en el siguiente cuadro:

NORMAS DE APLICACIÓN A NIVEL NACIONAL
Ley 16/2003 de Cohesión y Calidad del Sistema Nacional de Salud.
Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y el Real Decreto 1720/2007 que desarrolla la misma.
Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
Ley 14/1986, General de Sanidad
Ley 41/2002 de Autonomía del Paciente
Ley 34/1988, General de Publicidad
Real Decreto Legislativo 1/2007, de la Ley General para la Defensa de los Consumidores y Usuarios.
Real Decreto, de 7 de febrero por el que se establecen normas para garantizar la asistencia transfronteriza.

Ilustración 21: Normas de aplicación a nivel nacional. Elaboración propia

[49] TFUE: Tratado de Funcionamiento de la Unión Europea.
[50] Artículo 16 del TFUE:
- "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
- El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes."

Aunque los servicios de salud en general se rigen a nivel de cada estado miembro, se considera a la telemedicina (Parte del IoHT) como un servicio de salud y a la vez un servicio de la sociedad de la información por lo que los aspectos legales se rigen por:

- El principio de libre prestación de servicios.
- La normativa de comercio electrónico.
- Directiva de derechos de los pacientes en la asistencia transfronteriza.

La Directiva sobre el comercio electrónico de la UE /31/CE de 2000 establece el marco legal para los servicios de sociedad de la información, que incluyen cualquier servicio prestado normalmente a distancia, por vía electrónica y a petición individual de un destinatario de servicios. Entendiéndose por "A distancia" que el servicio es proporcionado sin estar las partes en el mismo lugar al mismo tiempo.

6.7.1 PRIVACIDAD DE DATOS

Respecto a la privacidad de los datos, la Directiva de protección de datos proporciona un marco vinculante de la UE para proteger la privacidad del paciente. Los operadores del IoHT deben evaluar sistemáticamente los aspectos de la privacidad de datos cada vez que se presten servicios de salud electrónica teniendo en cuenta también la legislación nacional. Productos y servicios de salud digital tienen más probabilidades de implicar el tratamiento de la información de salud del paciente. El procesamiento de dicha información personal se rige a nivel de la UE bajo la Directiva de Protección de Datos 95/46/CE, modificada y la ePrivacy/58/CE[51], la Directiva 95 de 2002, modificada (E-privacidad). En las directivas anteriores se establecen requisitos específicos para proteger los derechos del individuo a la intimidad y asegurar que las comunicaciones y las redes sean seguras.

Art. 9 Tratamiento de categorías especiales de datos personales.

1 Queda prohibido el tratamiento de datos personales que revelen "… datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física".

El apartado 1 no será de aplicación cuando concurra entre otras en las siguientes circunstancias:

- *El interesado dio su consentimiento explícito para el tratamiento de dichos datos personales.*
- *En el ámbito del Derecho laboral y de la seguridad y protección social.*

[51] ePrivacy/58/CE : Disponible en línea http://www.boe.es/buscar/doc.php?id=DOUE-L-2002-81371 [Consulta 18/03/2017]

- *El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.*
- *Para fines de medicina preventiva o laboral, capacidad laboral o diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas.*
- *Para fines de archivo en interés público, investigación científica o histórica o fines estadísticos.*

6.7.2 ASISTENCIA TRANSFRONTERIZA

Aún con la falta de normativa expresa que regule la práctica profesional de la medicina a distancia de nuestro país y volviendo al Reglamento Europeo, en Europa se aprobó la Directiva 2011/24/UE relativa a los derechos de los pacientes respecto a la asistencia transfronteriza, transpuesta al Ordenamiento Jurídico Español mediante el Real Decreto 81/2014 de 7 de febrero y que regula varios puntos[52]. A continuación citamos los más importantes:

- Recibir tratamiento en otro Estado miembro y ser reembolsado bajo determinadas condiciones.
- Tener acceso a una copia de su historial médico por escrito o por medios electrónicos.
- Telemedicina.

La Directiva de Salud con la asistencia transfronteriza, reconoce la protección de los datos personales de salud como una responsabilidad compartida del Estado miembro de afiliación y el Estado miembro de tratamiento donde:

- Estado miembro de tratamiento velará porque el derecho a la intimidad esté protegido conforme a las medidas nacionales de aplicación de las disposiciones de la Unión de la protección de datos personales (Directiva 95/46/CE).
- Estado miembro de afiliación debe proporcionar al paciente una adecuada, correcta y actualizada información sobre la transmisión de sus datos personales a otro Estado miembro. Esta parte debe garantizar la recepción segura de datos y proporcionar el

[52] La normativa de asistencia sanitaria transfronteriza regula los siguientes puntos:
- El reembolso de los gastos en la asistencia sanitaria transfronteriza.
- La telemedicina.
- El reconocimiento de recetas en otro Estado miembro.
- La identificación del médico prescriptor/control profesional.
- El acceso a la historia clínica del paciente.
- Los “Puntos nacionales de contacto”, que son centros de información sobre el ejercicio profesional.

nivel adecuado de protección de datos cuando se procesa, a raíz de su legislación nacional de protección de datos[53].

Aún con todo esto, nos encontramos con preocupaciones respecto al uso de los servicios de la salud electrónica transfronteriza que se están abordando. La actuación ante fallos en el tratamiento y el conflicto de cuestiones de jurisdicción en las que pueden derivar es una de ellas. Otra preocupación importante es que las normas éticas y profesionales de los médicos no están armonizadas entre todos los países miembros, lo que significa que un médico en un estado miembro puede estar practicando acciones con una ética diferente a un médico de otro estado. La aplicación y extensión de la normativa en telemedicina debe estar alineada con las normas deontológicas de las profesionales sanitarias que deberán adaptarse. La Ley de Autonomía del Paciente (Ley 41/2002) deberá adaptarse para recoger nuevas premisas de las nuevas tecnologías como el intercambio de información sensible, el acceso por parte del paciente a la información y su consentimiento, la transmisión de documentación, etc.

6.7.3 ANONIMIZACIÓN DE DATOS

El Reglamento general de protección de datos, de 26 de abril de 2016 (en adelante RGPD) refleja en el artículo 4:

Para el procesamiento de la información sensible, se estipula una protección especial en la que sea obligatoria que los datos sanitarios incluyan cualquier número, símbolo o dato asignado al paciente que le identifique de manera inequívoca a efectos sanitarios, información de pruebas o exámenes de una parte del cuerpo o sustancia corporal. También deberá ir así identificado información sobre enfermedades, riesgo de padecerlas, historial o estado fisiológico o biomédico independientemente de la fuente.

A nivel europeo, la LOPD no concreta los atributos clínicos que componen el grupo de datos de la salud relativa a los derechos de los pacientes en la asistencia tal que permita identificarlos para procesos de anonimización. Por su parte, el RDLOPD en el artículo 5.1.g define los datos de carácter personal relacionados con la salud como *"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".*

El artículo 4.5 recoge el principio de seudonimización de la forma siguiente: "*El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y*

[53] Dictamen del Supervisor Europeo de Protección de Datos, 2009 DO C 128/03, párrafo 22.

esté sujeta a medidas técnicas organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

No debemos confundir este principio con el concepto de "Datos disociado" definido en el art. 5.1.e del RLOPD . En este último "*no permite la identificación de un afectado o interesado*", por tanto la información queda desvinculada de la persona, mientras que el principio de seudonimización se sustituyen los datos identificativos por un código o clave, si bien sería posible la vinculación de la información a la persona afectada con información adicional.

6.7.4 PRODUCTO SANITARIO

En función de si una aplicación es una aplicación en salud y si se trata o no de un producto sanitario se establecerá quién es el responsable ante un error de dicha aplicación aunque la normativa vigente en la actualidad no prevé regulación específica para las Apps en salud.

El marco regulatorio de los dispositivos médicos es diferente en EEUU que en Europa, revisaremos, en este caso, el marco Europeo. Independientemente del país, los dispositivos médicos se clasifican en los siguientes grupos:

- Clase I: dispositivos que presentan un grado muy bajo de riesgo.
- Clase II: dispositivos que tengan un grado de riesgo moderado.
- Clase III: dispositivos que presentan un elevado potencial de riesgo.
- Clase IV: dispositivos considerados críticos en materia de riesgos.

Un "producto sanitario" debe cumplir con la Directiva 93/42/CEF y sus modificaciones posteriores (Real Decreto 1591/2009 en España) antes de salir al mercado. La Comisión Europea publicó en 2012 cuatro preguntas con las que saber si una app es un producto sanitario. Si se contesta afirmativamente a las siguientes preguntas se trataría de un producto sanitario y por tanto previo a su comercialización debería obtenerse el marcado "CE". Las preguntas serían:

- *¿Es un programa informático?* Si la app no se ajusta a determinadas reglas de programación ni está compuesto de declaraciones e instrucciones para resolver una función o tarea se trata de un documento digital y no de un dispositivo médico.
- *¿Genera o modifica datos?* Si la aplicación almacena datos no se trata de un producto sanitario. Para que lo sea la modificación de datos debe tener un propósito médico.

- *¿Está pensada para beneficiar a pacientes individuales?* Si está enfocada a manejar datos a poblaciones o si ofrece recomendaciones genéricas no estaremos ante la definición de un producto sanitario.
- *¿Está diseñada para ser usada como un producto sanitario?* Para ello debe incorporar alguna de estas funcionalidades:
  - Diagnóstico, prevención, seguimiento, tratamiento o alivio de una enfermedad, diagnóstico, control o tratamiento o compensación de una lesión o discapacidad.
  - Regulación o apoyo de la concepción.
  - Exploración o modificación de un proceso o estado fisiológico.
  - Proporción de información para fines médicos de muestras que deriven del cuerpo humano.

El 5 de abril de 2017 se adoptaron dos nuevas regulaciones de la UE sobre dispositivos médicos: Reglamento (UE)2017/746 sobre dispositivos médicos de diagnóstico in vitro (IVDR) y Reglamento (UE)2017/745 sobre dispositivos médicos (MDR). Con esta nueva Directiva que entrará en vigor 5 y 3 años respectivamente de su entrada en vigor, se derogan las Directivas 90/385/CEE y 93/42/CEE.

Por nuestra parte nos centraremos en el Reglamento (UE)2017/745 sobre dispositivos médicos (MDR) quedando como producto sanitario: "*cualquier instrumento, dispositivo, equipo, programa informático, material u otro artículo, utilizado solo o en combinación, incluidos los programas informáticos destinados por su fabricante a finalidades específicas de diagnóstico y/o terapia que intervengan en su buen funcionamiento, destinado por el fabricante a ser utilizado en seres humando 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.*
- *Regulación de la concepción".*

Los agentes encargados de la regulación deben asegurar que los dispositivos médicos cubren al menos los siguientes requisitos:

- Cumplen los requisitos esenciales. (Protección contra radiación, riesgo eléctrico, infección bacteriana, riesgo de energía, incluyen la información del fabricante, etc.)
- Están fabricados de acuerdo a una ruta de conformidad apropiada.
- Llevan la marca CE.
- Están sujetos a vigilancia o reporte por parte del mercado.

Las Normas ISO aplicables a dispositivos médicos son ISO 13485: referida al sistema de gestión de la calidad aplicable para dispositivos médicos y la ISO 14971 que especifica los requisitos de un sistema de gestión de la calidad cuando una organización precisa demostrar su capacidad para proporcionar productos sanitarios y servicios relacionados.

6.8 AMENAZAS Y DESAFIOS RESPECTO A LA PROTECCIÓN DE DATOS Y PRIVACIDAD

La protección de datos está sin duda directamente relacionada con el IoT. La cantidad de información que los objetos inteligentes son capaces de recopilar es una de las características que se resaltan de la nueva tecnología.

En este punto de nuestro trabajo, la pregunta al respecto de la privacidad es ¿Realmente supone una amenaza mayor de la que ya existía? Hay dos opiniones al respecto: por un lado y de forma minoritaria, están quienes opinan que estamos en presencia de un avance tecnológico que no trae consigo distintas amenazas a las que ya existían en materia de privacidad, el aumento de ataques es fruto del avance tecnológico en general más que de la llegada del IoT según esta opinión, un camino por el que toda novedad relacionada con la tecnología pasa. El tráfico de datos en la red, por otro lado, no será realmente mayor que el ya existente pues el almacenamiento de grandes cantidades de información en la nube o el Big Data se pueden utilizar de forma independiente a los dispositivos obteniendo si cabe la misma información.

La otra opinión, apoyada por organismos gubernamentales como no gubernamentales y expertos en derecho, defiende que el IoT constituye una nueva amenaza para la privacidad y la protección de datos personales con desafíos específicos y distintos a los ya existentes entre otras razones, porque antes los ataques se producían más debido a un intento del usuario por mantener un rol activo y ahora, con la llegada del IoT eso da igual porque constantemente hay intercambio de datos entre más variedad de actores de los que había tradicionalmente Estos intercambios de información pueden ser transparentes o no para los usuarios y obligan, por otro lado a que los dispositivos estén constantemente conectados, muchas veces a redes públicas con más facilidad para el intrusismo o, que los tentáculos del IoT llegan a áreas de aplicación mucho más sensibles como puede ser la salud o la conducción de un vehículo donde los datos serán mayores en cuanto a cantidad, calidad y sensibilidad, lo que significa que las inferencias que pueden extraerse de ellos son más grandes y más sensibles y su identificación más probable o incluso necesaria[54].

Pese a las herramientas en el marco regulatorio vigentes y futuras estudiadas ya en el punto 5, el IoT es con todo algo novedoso, donde podemos plantear una gran variedad de desafíos sin tener la certeza de que lo planteado se dé y, debido a que actualmente vivimos una etapa expansionista y de transición del IoT que hace que avance a una velocidad mucho

[54] Opinión del 36th International Conference of Data Protection and Privacy Commisisioners, 2014) que se puede encontrar en línea en: http://www.privacyconference2014.org/English/aboutconference/Documents/Resolution/Declaraci%C3%B3n-de-Mauricio-sobre-el-Internet-de-las-Cosas.pdf [Consulta 15/04/2017]]

mayor que los entornos regulatorios y las políticas relacionadas; surjan desafíos que hoy por hoy no podemos anticipar.

El primer ordenador personal fue promovido como un lugar para almacenar recetas de cocina. Cuando apareció el Ipad fue necesario sugerir como podría ser utilizado. El Internet de las Cosas no aparece para cubrir un problema específico. No se pone en juego su utilidad sino que los propósitos sólo podrán ir viéndose con el tiempo o, cuando la ubicuidad sea total y los aparatos inteligentes estén en todas partes y haya una accesibilidad real ya que a medida que el IoT se integre, será utilizado por más personas con distintos perfiles y objetivos. Será ahí cuando podamos hablar de amenazas y desafíos de una manera más completa. Hasta entonces, la identificación del mayor número de problemas y preocupaciones posibles puede hacer que estemos mejor preparados para enfrentarnos a los retos que no podemos anticipar, bien sean tecnológicos, sociales o ambientales.

Los riesgos asociados a la evolución del IoT varían en función de la tarea a la que esté destinado el dispositivo o por la dependencia que se tenga de él. Nunca serán igual los riesgos a tener en cuenta a la hora de implementar una lavadora inteligente que cualquier dispositivo destinado a la salud de las personas, no obstante, si habrá amenazas comunes a ambos. Algunas de ellas, relacionadas con cómo se va a afrontar la gestión de esta gran revolución como por ejemplo la eliminación de todos los desechos electrónicos con una obsolescencia planificada mientras se cumple el Convenio de Basilea[55] o la ubicación física de tanta información; parece que cuentan con más tiempo para su resolución. Otras, relacionadas con fallos o, mayoritariamente con la seguridad y privacidad de los datos requieren ser abordados antes de que ocurra la adopción masiva del IoT.

Debido al objetivo de este trabajo, nos centraremos en las amenazas que tengan que ver con la privacidad y protección de la información de los usuarios debido a deficiencias en el ciclo de vida de los dispositivos, ataques malintencionados o el mal uso que podamos dar a los dispositivos entre otros y, proponemos para un trabajo futuro el análisis de otros importantes desafíos como la estandarización o la interoperabilidad.

6.8.1 ¿CUÁNTO VALEN NUESTROS DATOS?

Hay quien está de acuerdo en que las usuarias no somos conscientes del valor que tienen nuestros datos aunque el Foro Económico Mundial (WEF) se refirió a ellos como un nuevo tipo de activo. Para Alex Pentland, profesor de Toshiba de Artes y Ciencias de los

[55] El Convenio de Basilea es un tratado ambiental global adoptado el 22 de marzo de 1989 y que entró en vigor el 5 de mayo de 1992. Regula estrictamente el movimiento transfronterizo de desechos peligrosos y estipula obligaciones a las Partes para asegurar el manejo ambientalmente racional de los mismos. Se puede encontrar más información en: http://www.basel.int/TheConvention/Overview/History/Overview/tabid/3405/Default.aspx [Consulta 03/05/2017]

Medios en el MIT, cuanto más invadida se sientan las personas por la cantidad de datos recogidos de su vida, mayor será la sensación de ser cada vez más espiado. Será entonces cuando tomen conciencia de todos los datos que hay de ellas y se preguntarán si realmente es tan bueno que una empresa recopile información sobre los entrenamientos, la hora en que se va a la cama o cuando recoge a sus hijas del colegio[56].

¿Hay que llegar hasta ahí para proteger nuestros datos? Los ingresos por Internet han crecido fuertemente en los últimos diez años, este dato se relaciona con el aumento de la recolección de información. Uno de los elementos que hacen que Internet sea un gran negocio es la publicidad y dentro de ella la publicidad personalizada, dirigida a un público que se sabe de antemano, estará interesado en ella. Para llegar hasta ahí se necesita contar con datos de clientes como hábitos o intereses. Amazon, por ejemplo ofrece productos a un cliente en función de su histórico. Empresas como Axciom utiliza múltiples fuentes para llegar a más de 1000 características de los clientes y la información básica: edad, ubicación, detalles del hogar y a más de 3500 datos específicos de comportamiento como los hábitos de compra. Los intermediarios de datos ganan vendiendo datos compilados en listas completas o bases de datos a los vendedores. The Guardian sacó en 2014 una calculadora para saber el valor de nuestros datos cuando los ministros británicos se planteaban cambiar la ley para que HM Revenue and Customs[57] pudiera vender datos a terceros.

[56] Entrevista a Alex Pentland en línea en https://hbr.org/2014/11/with-big-data-comes-big-responsibility. [Consulta 06/05/2017]

[57] HM Revenue and Custooms o HMRC es un departamento no ministerial del Gobierno de Reino Unido encargado de la recaudación de impuestos, pagos de algunas formas de apoyo estatal y la administración de otros regímenes reguladores. https://en.wikipedia.org/wiki/HM_Revenue_and_Customs [Consulta 05/05/2017]

Ilustración 22: Calculadora del valor de los datos. Fuente The Guardian (2015).

El punto de vista de los más positivos es que el intercambio de información ayuda a las economías y mejora nuestras propias experiencias. Internet es un servicio mayormente gratuito, y compartir datos es el precio que pagamos. Otros creen que el uso de información sin consentimiento es una violación de privacidad. Sea como sea lo que se hace necesario con un presente y futuro de dispositivos conectados intercambiando datos casi continuamente; es tomar conciencia de la importancia que tienen nuestros datos para poder seleccionar cuales queremos facilitar y cuáles no, si realmente la funcionalidad que nos va a proporcionar el dispositivo que los solicita merece darlos y la importancia de conservar la privacidad de nuestros datos en todo momento.

6.8.2 PRIVACIDAD FRENTE A DESARROLLO

Si hacemos una búsqueda en Internet sobre las amenazas y los desafíos del Internet de las Cosas, en todos los artículos y trabajos que saldrán como resultado, ocupando los primeros puestos estará la privacidad y seguridad de los datos. Parece que en la parte teórica está clara la preocupación, sin embargo a nivel práctico todavía es una asignatura pendiente para empresas y fabricantes. Muchas de ellas anteponen la rentabilidad del producto a su fiabilidad, seguridad o privacidad. Un estudio realizado por 25 reguladores de protección de datos de todo el mundo, examinó dispositivos inteligentes como medidores de electricidad, termostatos, relojes… obteniendo, que seis de diez dispositivos IoT no dicen adecuadamente a los clientes cómo usan su información personal[58]. Con más de 300 dispositivos revisados el informe mostró que:

- El 59% de los dispositivos no explicó adecuadamente a los clientes cómo su información personal fue recopilada, utilizada y divulgada.
- El 68% no explicó correctamente cómo se almacenaba la información.
- El 72% no explicó cómo los clientes podían eliminar su información del dispositivo.
- El 38% no incluyó datos de contacto fácilmente identificables si los clientes tuvieran problemas de privacidad.

Desde la aparición de legislaciones sobre protección de datos de carácter personal o privacidad, emergieron algunas opiniones que veían este concepto como un lastre y una amenaza para el progreso de las tecnologías. Puede verse así, la inversión en seguridad y privacidad puede hacer que no haya una aparición indiscriminada de dispositivos con una mínima seguridad aunque no suficiente, que la regulación de la cantidad de datos que se pueden recoger se base en el principio de minimización puede limitar las funcionalidades o los datos que los dispositivos puedan dar o, que los costes de la fabricación y mantenimiento de un objeto inteligente aumenten lo que conlleva que la comercialización de objetos inteligentes no esté al alcance de todos los fabricantes.

Ahora bien, también puede darse el caso de que los consumidores pierdan la confianza en los dispositivos o que no utilicen todo el potencial que ofrecen cansados de oír casos de hackers, ciberataques o robo de datos o, que tras problemas de privacidad no controlados, existan continuas reclamaciones o denuncias hacia los fabricantes de productos. El World

58 Datos de informe de ICO (Information Commissioner´s Office). Privacy regulators study finds Internet of Things shortfalls. 2016. Disponible en línea en: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/privacy-regulators-study-finds-internet-of-things-shortfalls/ [Consulta 02/05/2017]

Economic Forum[59] (2016) ha estimado que el impacto económico total si no se alcanza la confianza de los usuarios puede llegar a 3 billones de dólares en 2020 en pérdida de productividad y crecimiento. "*Incluso* – señala – *un número pequeño de ataques destructivos reduce el nivel* de *confianza, obligando a gobiernos a reaccionar a través de nuevas regulaciones y frenando el ritmo de innovación tecnológica. Como resultado, el mundo dejará de capturar parte del potencial estimado en 10-20 billones de dólares ligado a soluciones de Big Data o movilidad*"[60]

Podemos por tanto pensar que sólo con políticas de privacidad durante todas las etapas del tratamiento de los datos (denominado privacy by desing) se generará la confianza necesaria para que el producto tenga éxito.

Los principales riesgos para la privacidad tienen origen en la revelación de información personal sin autorización, lo que puede dar lugar a un mal uso de éstos.

6.8.3 VECTORES DE ATAQUE PARA LA SEGURIDAD Y PRIVACIDAD DE LOS DATOS

La seguridad en el IoT comprende desde problemas físicos al desconocimiento del usuario en la utilización de los objetos. Algunos de los principales riesgos para la privacidad son provocados por vulnerabilidades de aplicaciones web, fugas de datos por deficiencias de software, falta de previsibilidad ante la violación de datos o transferencias de datos no seguras. La identificación de vectores de ataque de privacidad para buscar soluciones y aumentar la seguridad es uno de los primeros pasos para minimizar cualquier amenaza.

El mayor problema que nos encontramos en este punto es la variedad de sistemas heterogéneos que dificulta unas reglas comunes para el mantenimiento del dispositivo. Por otro lado, la duplicidad de labores (Fabricantes que se encargan también del software) sin la experiencia suficiente hace que se lancen al mercado productos con problemas que se resuelven después o no se resuelve, que carecen de actualizaciones y que finalmente corren el riesgo de quedarse obsoletos y con una seguridad incompleta.

6.8.3.1 Seguridad en la transmisión de datos

En un mundo de objetos conectados es obligado cubrir la seguridad en las comunicaciones ya sean inalámbricas, redes cableadas o cualquier otra forma de transmisión. Cualquier dato que viaja por un canal de comunicación es sensible a sufrir ataques a la

[59] Word Economic Forum (WEF): fundación sin fines de lucro compuesta por los principales líderes empresariales, líderes políticos internacionales y periodistas e intelectuales que analizan los problemas actuales más apremiantes a nivel mundial.
[60] Artículo de AOTEC. Internet de las cosas, una realidad palpable. 2016. disponible en línea: http://www.aotec.net/noticias/noticia.asp?ent=2463 [Consulta 28/05/2017]

confidencialidad de las comunicaciones, en especial canales inalámbricos y públicos por la falta de control de los usuarios que los utilizan.

Un ataque en la transmisión de datos sin que éstos estén correctamente encriptados puede provocar:

- La irrupción del servicio. Los dispositivos se quedarían sin red y muchos no podrían funcionar. Imaginemos si esto pasara en una cadena de montaje o en cualquier dispositivo industrial.
- El acceso a toda la información que viaje por el canal de comunicación lo cual no se limitaría a que el intruso conozca datos de los usuarios, sino también podría provocar que éste se hiciera con el control del dispositivo sin darnos cuenta.

6.8.3.2 Seguridad del software

El uso de versiones ajustadas de un sistema operativo sobre distintos dispositivos, interfaces web administradas desde dispositivos remotos, apps que se pueden descargar desde el móvil para la gestión de los dispositivos o servicios en la nube son elementos comunes a diferentes dispositivos de tal forma que la vulnerabilidad en cualquiera de ellos deja una puerta abierta al acceso de información y el control de un gran número de objetos.

Al haber brechas de seguridad en el software o descargar alguna aplicación maliciosa, se puede acceder a la información del usuario y al igual que antes, poder hacerse con el control del dispositivo sin que éste se dé cuenta.

El periódico El Mundo, publicaba el pasado marzo (2017) una noticia por la que, según WikiLeaks, la CIA podría grabar conversaciones secretas recogidas por medio de 'televisiones inteligentes'. Un programa llamado "'Ángel", instalado en "televisiones inteligentes", pondría la televisión infectada en un modo "off falso". El consumidor ve la televisión como apagada pero realmente está grabando conversaciones que posteriormente envía a través de Internet a un servidor secreto de la CIA que por el momento no ha confirmado ni desmentido la noticia[61].

6.8.3.3 Seguridad del hardware

Este tipo de ataque existía antes de la llegada del IoT, sin embargo no suele ser usual ya realizarlo requiere altos conocimientos en los sistemas y se necesitan sistemas especializados. Una forma posible de ataque podría ser acceder a la memoria del dispositivo, de esta manera se tendría acceso a información sensible y claves almacenadas y se podría

[61] Fuente: artículo publicado por el periódico El Mundo con fecha del 08/03/2017. Autor Pablo Pardo. Disponible en línea: http://www.elmundo.es/internacional/2017/03/08/58bf1e0de5fdea49618b45a9.html [Consulta 07/06/2017]

producir, como ejemplo, el reseteo del dispositivo perdiendo todos los datos almacenados o modificando los dispositivos con valores de fábrica. Imaginemos que el dispositivo está encargado de bajar las persianas a las seis de la tarde y sufre un reseteo, las persianas no se bajarán pues habrá perdido esa orden. Es un ejemplo sin demasiada trascendencia, pero si lo trasladamos por ejemplo a una máquina de respiración asistida de un hospital, la criticidad porque no se den este tipo de ataques aumenta.

6.8.4 RETO I: PRIVACIDAD EN EL FLUJO DE INFORMACIÓN.

En este punto analizaremos las amenazas y retos que presenta el Internet de las Cosas teniendo en cuenta que cuando hablamos del tratamiento de datos solemos pensar que éste se reduce al análisis. En un sentido más amplio podemos distinguir entre las siguientes etapas dentro del tratamiento de datos en un ecosistema IoT:

- Recogida de datos: Es la etapa inicial que requiere de una tecnología que extraiga los datos personales de un sujeto que haya interactuado con ella y que no tiene porqué ser el dueño del dispositivo. Esta interacción puede haber sido activa o pasiva, decir con o sin consentimiento o conocimiento de ello. Recogidos los datos, son transferidos a través de redes.
- Procesamiento de datos: El proveedor del servicio analiza y cruza los datos recogidos para obtener el resultado que necesita. A veces este resultado son algoritmos de comportamiento, otro la creación de un perfil de usuario que recoja sus características, hábitos, gustos… que normalmente van ligados a preferencias de consumo o conductas.
- Entrega de datos: los datos que son obtenidos en la etapa anterior, son entregados al mismo usuario o a terceros (En este caso será una comunicación o transmisión de datos).

6.8.4.1 Desafíos en la etapa de recogida de datos

El consentimiento es el eje principal en el que se articula la legitimación para llevar a cabo un tratamiento de datos. El consentimiento es una responsabilidad del fabricante y deberá ser libre, inequívoco, informado y específico.

Para analizar los desafíos producidos en la etapa de recogida de datos partamos del siguiente ejemplo: *Una marca ofrece en su gran tienda, bombillas inteligentes que pueden conectarse a la wi fi de la casa. Las bombillas se encuentran expuestas en la zona de*

iluminación entre otras bombillas, su precio es asequible y ahorra en gasto de luz[62]*. La tienda por otro lado tiene otros objetos relacionados con el hogar como mobiliario, ropa de cama, material de cocina…*

Imaginemos entonces que un consumidor adquiere una de estas bombillas. El primer problema que nos encontramos es que muchos "objetos inteligentes" pueden no ser identificados como tal, este problema irá aumentando a medida que estos objetos se vuelvan más familiares, dejen de ser una novedad y puedan adquirirse más fácilmente. Si no sabemos distinguir entre dispositivos inteligentes y objetos simple, difícil que podamos ser conscientes de lo que el uso del dispositivo va a conllevar. La señalización adecuada es una propuesta ya realizada como hemos visto anteriormente pero todavía regulada.

Quizá a partir de ahora objetos que llevan implantada una tecnología deberán ir acompañados en su caja de un papel informativo donde se identifiquen las políticas de privacidad o de códigos de activación a través de internet como si del prospecto de un medicamento se tratara. Los dispositivos inteligentes, los sensores que los componen, no están preparados para dar una información real ni completa que pueda obtener un consentimiento válido por parte del consumidor.

Al llegar a casa, nuestro consumidor lee que debe registrarse en una web para dar su consentimiento de privacidad y descargarse una aplicación a un dispositivo móvil desde donde podrá gestionar el uso de su bombilla a través de un teléfono inteligente. Independientemente la bombilla funcionará colocándola y conectándola a la Wi Fi.

El consumidor podría haber utilizado el dispositivo sin consentimiento alguno. *En este caso pongamos que se registra en la web,* entonces ha aceptado un consentimiento de forma indirecta en el que se indicaba que: "*… sus datos serían almacenados con finalidad fiscal, contable, etc. Así como para el envío de información comercial de otros productos de iluminación"*. Pero en el que no está indicado el acceso a sus datos teniendo en cuenta que una característica de los dispositivos IoT es que simplemente por el hecho se der conectados a internet, envían automáticamente información a sus fabricantes como, por ejemplo, hora en que los encendieron y los apagaron. Por tanto nuestro consumidor ha aceptado que puedan tratar datos sobre él y que puedan mandarle publicidad de los productos sin saber la alternativa a no aceptar alguna de las dos cosas (Por ejemplo no querer recibir publicidad) y sin saber si por el mero hecho de no querer dar ese consentimiento, en la tienda le hubiera devuelto el dinero al no poder utilizar el producto. El consentimiento libre, por tanto queda en entredicho. Actualmente el usuario suele verse obligado a aceptar el consentimiento a falta de posibilidades de renunciar a ciertas características del dispositivo.

[62] Ejemplo basado en las bombillas inteligentes de IKEA y productos de LuzWifi, bombillas inteligentes. Los productos se pueden consultar en las páginas web de las marcas: http://www.ikea.com/es/es/ y http://www.luzwifi.com/ [Consulta 15/05/2017]

Normalmente la información que se da sobre el dispositivo es extremadamente larga y compleja en términos de forma que hace imposible un consentimiento significativo. Se suma además, que estos consentimientos suelen informar de la finalidad de los datos que se recogen pero no de los que tras su tratamiento podrían obtenerse de tal forma que el usuario puede no saber realmente la información que está cediendo. Fuera de este ejemplo, objetos del IoT estarán formados por varios sensores que proporcionen funcionalidades suplementarias que no interfieren en el uso del objeto como tal, es importante que se tenga en cuenta que cada uno de estos sensores puede recoger información y por tanto el consentimiento debería ser independiente y el uso de cada una de las funcionalidades suplementarias optativo de tal forma que se pudiera dar el consentimiento para algunas y para otras no sin perjuicio para el usuario.

Con la inmersión de objetos inteligentes en nuestro día a día, nos encontramos con "consentimientos" que pueden resultar no válidos por no darse con la suficiente claridad o no informar de forma completa. Hay que buscar alternativas que aseguren que los usuarios realmente son conscientes del objeto adquirido, en nuestro caso por ejemplo, haciendo que sólo si el consumidor declara haber entendido la información dada por el fabricante la bombilla pueda funcionar.

Planteamos una serie de propuestas para minimizar los problemas expuestos:

- Proporcionar información suficientemente comprensible y clara para los usuarios finales que será responsabilidad de los fabricantes de los dispositivos.
- Empleo de las PIAS (Privacy Impact Assessments): este tipo de evaluaciones de impacto serán como una auditoría que puedan revisar cómo afectan o pueden comprometer la privacidad sus productos. Estas herramientas tienen como objetivo:
    - Garantizar la conformidad con los requisitos legales, reglamentarios y normativos aplicables para la privacidad.
    - Determinar los riesgos y efectos.
    - Evaluar las protecciones y los procesos alternativos para mitigar los posibles riesgos de privacidad.

- Aplicación de los principios de Privacy by desing y Privacy by default que dará mayor protección durante todo el ciclo de vida del objeto. Hasta ahora una serie de controles técnicos con el fin de garantizar el cumplimiento de la normativa más que para velar por los derechos de las usuarias.
- Información del uso de los datos agregados, en lugar de los datos en bruto.

6.8.4.2 Desafíos en la etapa de procesamiento de datos

Los desafíos en la etapa de procesamiento de datos de un objeto inteligente son múltiples, si podemos conectarlo con otro dispositivo las amenazas se pueden multiplicar. A medida que vayamos conectando dispositivos aumentaremos estos desafíos debido al

aumento de datos recogidos, al aumento de datos que se pueden obtener y al aumento de puntos sensibles a fallos fortuitos o ataques de privacidad que puedan suceder.

Seguiremos con nuestro ejemplo anterior. *El consumidor ha colocado las bombillas tecnológicas, se ha registrado y se ha bajado la app para poder controlar el producto desde su móvil. Con esa app el consumidor puede decidir la intensidad de luz que puedan dar las bombillas, programe las horas de encendido / apagado o programarlas para que la bombilla se pueda ir apagando gradualmente. Para utilizar esta app se solicitan otros datos como estado civil, edad, fecha de nacimiento o profesión, tipo de habitación donde está cada bombilla (Baño, cocina, dormitorio…). Esta app da la opción de registrar varias bombillas de diferentes sitios.*

Dado que los fabricantes del dispositivo han contratado a una empresa informática China para hacer esa app, terceros recogerán datos que no necesitarán de consentimiento al establecerse un "Acceso a los datos por cuenta de terceros". Muchos de estos datos suelen pedirse por norma general y los consumidores suelen responder por inercia y a veces por obligación.

El código de buenas prácticas y en particular la responsabilidad de recabar información siguiendo la norma de minimización de datos no parece que se suela cumplir por parte de los actores encargados de recoger los datos. En nuestro ejemplo, *tras varios meses utilizando estas bombillas, el fabricante sabe las horas en las que suele estar en casa, los lugares en los que suele pasar más tiempo, la hora en la que se va a la cama. Puede relacionar cruzando datos de otros usuarios el tipo de intensidad o la cantidad de consumo dependiendo de si las consumidoras están en paro, son autónomas o trabajan por cuenta ajena o la media de luces encendidas en una casa por rango de edad.*

Realmente son muchos los datos que pueden saber a partir de algo tan insignificante como unas bombillas. Si por ejemplo el usuario adquiriera un sistema de persianas inteligentes que subieran o bajaran dependiendo de diversas variables, cabría la posibilidad de poder saber analizando las horas de encendido de una bombilla en una habitación y los horarios de subida y bajada de una persiana, cuánto de luminosa es la habitación de la casa.

La minimización de datos realmente, puede ayudar a proteger contra riesgos relacionados con la privacidad. En primer lugar, porque los almacenes de datos más grandes presentan un objetivo más atractivo para los ladrones de datos dentro o fuera de la empresa, y aumenta el daño potencial para esos "ladrones de datos". En segundo lugar, cuanto mayor es la cantidad de datos que una empresa recoge, mayor es el riesgo de que sean utilizados de forma ilícita o diferente a las expectativas del cliente. La regulación actual no menciona nada sobre la minimización de datos y aunque en el Reglamento General de Protección de Datos 2016/679 se recoge como una medida previsora, es muy difícil establecer una línea entre datos necesarios y no necesarios en un mundo donde los objetos van a estar conectados y los

datos pueden compartirse ya que datos no necesarios para el fin de un objeto puede serlo para el de otro.

El IoT presenta otro desafío. No siempre los propietarios son los que vayan a utilizar el dispositivo. El artículo 5.3 de la regulación vigente exige al responsable obtener el consentimiento del usuario del dispositivo. El artículo tiene lógica, el dueño de una empresa puede poner un dispositivo en el sitio de cada trabajador o trabajadora para controlar si cumple su jornada laboral, en este caso no tiene sentido que el dueño dé el consentimiento al fabricante pues serán los trabajadores y las trabajadores los que den sus datos. En Inglaterra….

El ejemplo anterior es sencillo y puede parecer obvio sin embargo, si lo trasladamos a otros ámbitos puede resultar cuanto menos más complicado de cumplir y es que, si volvemos al ejemplo de las bombillas:

- ✓ *¿Qué pasaría si el comprador instalara las bombillas en casa y meses después pusiera el piso en alquiler?* En ese caso el cambio de usuario del dispositivo seria transparente para el fabricante. Debería ser el dueño quién informara al inquilino al entrar de la existencia de estas bombillas y entonces ¿Firmar otro consentimiento anulando el anterior? (Los datos del registro serían los del dueño de la casa). El dueño de la casa, en este caso debería informar de los cambios y nuevos consentimientos al fabricante y se debería crear un nuevo registro para la app. En el Internet de las Cosas se necesitan más derechos para los usuarios pero también nuevas responsabilidades y métodos faciliten el llevarlas a la práctica ¿Sería real que al alquilar una casa se tuviera que firmar un consentimiento por cada objeto inteligente y transmitírselo al fabricante de cada dispositivo?
- ✓ *¿Si en la casa conviven más personas?* Cumpliendo el artículo 5.3. Todas las personas que vivan en la casa deberían dar su consentimiento ya que se podrán medir datos de todas ellas.

Estas son sólo algunas de las situaciones que se pueden dar debido a la cantidad de objetos cotidianos que podrán conectarse a la red. La teoría puede ser analizada pero habrá que revisar a la larga si está adaptada al mundo en que vivimos o no. ¿Es real que cualquier persona vaya a informar al fabricante, cambiar registros o informar y solicitar el consentimiento a todas las personas que pasen por casa y se conviertan en usuarios de unas bombillas, persianas, lavadoras….?

Puede darse el caso de que no sean ciertos los datos introducidos, el exceso de información solicitada puede dar lugar a que el consumidor se canse de responder o no ponga interés en la respuesta si la pregunta le parece que no está relacionada con el objetivo del dispositivo. *En nuestro caso, imaginemos que el comprador ha introducido datos en la app que considera poco importantes de forma aleatoria: estado civil, profesión… o que la casa sea de alquiler y en ese caso los datos recogidos por las bombillas o la app no estén directamente relacionados con el dueño*. En ese caso cualquier dato obtenido posteriormente que tenga que ver con algún dato inexacto tendrá menos o ninguna validez.

Este punto será más o menos importante dependiendo del fin del dispositivo, evidentemente para dispositivos que tengan que ver con la salud, que lo usen diferentes personas no debería darse nunca. Otro caso en el que puede ser importante que varias personas puedan usar un dispositivo es cuando los datos son cedidos por ejemplo a la policía (Este caso lo revisaremos después). Por defecto la información no está protegida con una clave de acceso o algún otro mecanismo de autenticación y si lo tiene, normalmente por una mala praxis de los usuarios, usuario y contraseña están almacenados y se puede acceder sin problemas. En este aspecto el GT29 recomienda una entrada de doble seguridad. Quizá también interesante podría ser guardar un registro de quién ha accedido y manipulado los datos.

Al tratar los datos para poder analizarlos y obtener información que resulte interesante, éstos deberán ser "anónimos" de tal formar, que no se sepa quién es la dueña de los datos. Control de datos de comportamiento, control del tráfico, grabaciones de cámaras de seguridad, Direcciones d Mac de múltiples, etc. son algunos de los datos que pueden obtener de nosotros. Con el IoT será cada vez más complicado resultar anónimo. Este hecho conlleva el riesgo de poder identificarnos: casa, salud, coche… y facilitar uno de los ataques más comunes en el IoT: la suplantación del usuario.

6.8.4.3 Desafíos en la etapa de entrega de datos

Ahora pongamos que los creadores de la app, ceden esos datos obtenidos a una empresa eléctrica y un día nuestro comprador empieza a recibir ofertas de tarifas por horario que, casualmente; mejor se ajustan a su consumo o, publicidad sobre otros productos del centro comercial donde le vendieron las bombillas.

- ✓ En el primer caso la cesión de los datos a la compañía eléctrica no debería haberse realizado sin consentimiento pero, por un lado ¿Cómo saber que consentimiento deberían haber solicitado de datos que ni siquiera el usuario sabe que tienen de él? Por otro lado, la empresa informática que ha cedido los datos es china, puede tener otra regulación respecto a la protección de datos y entonces saber si es legítimo o no el cede de esos datos se hace muy complejo.
    - ✓ En el segundo caso, dado que se han utilizado los datos para fines que no tienen que ver con la finalidad del producto en sí, podríamos decir que el uso no es lícito.

La cesión de datos en el IoT resulta uno de los desafíos más difíciles de resolver. La gran cantidad de actores que pueden tener acceso a alguno de los datos recogidos por el objeto y las diferentes zonas en las que se encuentren con sus respectivas legislaciones son las principales causas. La gestión de datos a terceros, está recogida en la regulación actual sin embargo de cara al aumento de dispositivos IoT, algunos expertos opinan que requiere una

revisión y análisis profundo ya que puede darse el caso de que un fabricante ceda los datos a un tercero y otro fabricante diferente ceda datos del mismo cliente al mismo tercero. El tercero podría hacer uso de los datos llegados por el mismo canal sacando datos "de grano fino" que le pudieran aportar información adicional y no directa con los objetivos de la cesión.

Poder saber a quién pertenece una serie de datos en IoT no es complicado. Direcciones Mac por ejemplo es una forma de poder trazar los movimientos del afectado.

Los principales riesgos para la privacidad del individuo es la toma de su información personal sin que él la haya utilizado ya que puede dar lugar a un uso indebido de ésta como generación de perfiles o el rastreo de una persona en base a datos sobre rutinas.

- El rastreo o trazabilidad es un ataque a la intimidad de la persona. Se trata de un ataque en el que pueden vigilar y seguir los movimientos de la persona en tiempo real, imaginemos en el caso de las bombillas que, *la app instalada en el móvil solicita acceder a la ubicación de la persona para calcular el tiempo que tarda en llegar y activar las luces a la hora calculada*. Puede resultar muy complicado, ante un ataque o uso indebido, que este dato sea anónimo.
- La generación de perfiles o suplantación de usuarios: a través de los datos se realiza una reconstrucción de actividades y movimientos de una persona durante un periodo de tiempo con el fin de obtener información sobre hábitos y costumbres.

Retomemos nuestro ejemplo. *Pasa el tiempo, el usuario de las bombillas sabe que tiene que hacer una actualización de la app que se descargó en el móvil y cuando se decide a hacerlo, después de haber pasado algo de tiempo y por tanto, de haber tenido sus datos más expuestos a un ataque,* tras la actualización le muestra una nueva funcionalidad, un sensor capaz de dar orden a las bombillas para que se enciendan o se apaguen dependiendo de si detectan o no movimiento durante un tiempo elegido por el usuario.

El problema de mantener actualizados los dispositivos IoT es que normalmente cuando la usuaria se da cuenta de que debe actualizarlo es cuando necesita usarlo por tanto suele dejarlo para un momento más tranquilo. Aún con todo es una responsabilidad del usuario hacerlo y cubrir la seguridad de sus datos aunque algunas expertas opinan que se podría facilitar esta tarea obligando a actualizar por ejemplo, no pudiendo utilizar el dispositivo si la versión que tiene ha quedado obsoleta.

Al usuario de nuestro ejemplo no le convence demasiado la nueva funcionalidad, de hecho no quiere instalarla. Actualmente no habría obligación por parte del fabricante de dar una alternativa de uso, por ejemplo actualizar su app sin usarla, haciendo que el dueño del dispositivo tuviera que elegir entre seguir utilizando una app obsoleta con los riesgos que implica o aceptar la nueva funcionalidad. El Grupo de Trabajo de la EU recomienda que los fabricantes ofrezcan alternativas respecto a las funcionalidades y facilitando el mantenimiento seguro de los dispositivos.

6.8.5 RETO II: FLUJOS TRANSFRONTERIZOS

Que datos que recogen los dispositivos IoT se envíen a través de límites jurisdiccionales, como por ejemplo dispositivos que recojan datos en una jurisdicción y lo transmitan a otra para su tratamiento; es algo que no se puede evitar. Esto puede convertirse en un problema porque ¿Qué pasaría si los datos recogidos fueran considerados como sensibles y estuvieran sujetos a diferentes jurisdicciones? ¿Y si las leyes de protección donde reside el titular de los datos fueran incompatibles con las leyes de la jurisdicción donde se almacenan los datos?

Estas situaciones se denominan: flujos de datos transfronterizos. Y muchas de las preguntas que pueden surgir se han abordado en el Reglamento 2019/679 RGPD y en el GT29.

Los dispositivos IoT podrán conectarse automáticamente a otros dispositivos y sistemas y transmitir información a través de fronteras sin que el usuario sea consciente de tal forma, que puede convertirse en responsable de cumplir con los requisitos aplicables a los flujos de datos transfronterizos sin que lo sepa.

Los principios de transferencia revisados anteriormente se aplicarán a las transferencias dentro de España o en el Espacio Económico Europeo. Transferencias de datos personales a países fuera del área económica europea se permitirán en las siguientes circunstancias:

- Esos países ofrecen “protección adecuada” para la seguridad de los datos.
- Si la transferencia se lleva a cabo en virtud de un Tratado del que España forma parte.
- Si está destinado a proporcionar o solicitar la cooperación internacional judicial.
- Si se requiere a transferencia de las cuestiones médicas graves, si se refiere a las transferencias internacionales de dinero.
- Si el interesado consiente de manera inequívoca.
- Si la transferencia es necesaria para ejecutar, en interés de la persona afectada, un contrato entre el responsable del tratamiento y un tercero.
- Si la transferencia es necesaria para proteger un interés público.
- Si la transferencia sea necesaria para la aplicación, ejercicio o defensa de un derecho.
- Si la transferencia se realiza desde un registro público para un propósito legítimo y a un destinatario legítimo, siguiendo las instrucciones de una persona legitimada.

En cualquier otro caso, la transferencia al exterior de los territorios no adecuadas debe ser autorizada por la AEPD.

6.8.6 RETO III: DISCRIMINACIÓN DE DATOS

En Estados Unidos, algunos planes de seguro médico están incentivando a los participantes para que permitan que la aseguradora acceda a los datos de su dispositivo de registro de actividad física a cambio de primas más bajas. Podemos pensar que esto es positivo si somos, claro; personas que podemos acceder a tener uno de esos dispositivos y si es así, si cumplimos con los baremos que la aseguradora ha puesto para lograr un incentivo a parte del que nos dé por ceder nuestros datos. Imaginemos un esquema de precios que castiga a las personas que no pueden dormir lo suficiente o a los hábitos alimenticios de los trabajadores más pobres. En ese caso, esta práctica deja de ser tan positiva y se convierte en discriminatoria. Y la opción de ceder los datos podría dejar de ser tan libre dependiendo de los incentivos financieros o, habiendo cedido los datos voluntariamente, lo que podría dejar de ser tan libre serían nuestras conductas modificadas para conseguir los incentivos.

Si hablamos del IoT la utilización de datos de forma discriminatoria está cada vez más presente sin saber cómo se podrían utilizar las diferentes combinaciones de datos para discriminar en el futuro. Por ejemplo coches que dan datos de hábitos de conducción y geolocalización pueden ser facilitados y podría ser beneficioso por ejemplo para una rápida asistencia en un accidente, pero si se utilizan en una empresa de transportes para monitorear el trabajo de sus conductores sin que éstos puedan elegir ser o no observados, sería otra forma de utilizar datos de forma discriminatoria. En el punto en el que estamos, el IoT permite poner sensores que cubran prácticamente toda la oficina para controlar los hábitos de sus trabajadores. Se plantea en este punto diversas preguntas éticas a las que no se han dado respuesta: ¿Un trabajador puede ser castigado por los datos recopilados a través de un objeto de IoT? ¿El jefe debe comunicar a sus empleados la existencia de sensores que rastrean su comportamiento?

Muchos objetos inteligentes están compuestos por sensores que suelen asociarse con una situación operativa específica y por eso, con los datos recogidos permite un alto grado de especificidad a la hora de relacionar los datos con una persona o un grupo hasta poder asociar el dispositivo con la usuaria de éste.

La cantidad de datos que consentimos en cada objeto inteligente, crea flujos de datos continuos sin intervención humana. Con la ayuda de Big Data se pueden analizar cantidades enormes de datos, buscar correlaciones estadísticas y semánticas, crear un perfil y determinar grupos de usuarios con características similares. Cabe la posibilidad de que estos algoritmos categorizaran injustamente a los usuarios y explotar sus características. Hace poco leíamos en un artículo[63] de prensa la historia de un hombre que dejó una crítica en internet sobre el

[63] Noticia de GIZMODO. Autor: Matías S. Zavia. Los riesgos del IoT: un vendedor inutiliza la puerta del garaje de un cliente por una opinión negativa en Amazon. 2017. Disponible en línea en:

producto que se había comprado. El producto era un mando para abrir la puerta de su garaje y que estaba dando fallos técnicos. Un portavoz de la marcha respondió al comentario, pero también dejó inutilizado el mando desde la parte del servidor.

6.8.7 RETO IV: DISPOSITIVOS UTILIZADOS PARA ACCIONES LEGALES

Los datos que damos a nuestros dispositivos IoT, una vez cruzados y analizados, pueden dar tal cantidad de información que pudiera parecer como si de nuestro diario personal se tratara.

Cada vez hay más casos en la que los datos que recogen los dispositivos pueden servir como prueba en un procedimiento legal; no parece que este proceder vaya a desaparecer, al contrario, es probable que se utilice cada día más. En principio esto puede no parecer un riesgo ante nuestros datos. Una mujer presentó los datos de su dispositivo de actividad física en una demanda por lesiones personales, lo que puede parecer que no entraña riesgo puede cambiar si no son los dueños de los datos recogidos los que los utilizan. Algunos abogados han utilizado en un juicio por divorcio los datos de los dispositivos de peaje instalado en los coches para demostrar que un cónyuge engañaba a otro. El sensor recoge los datos de cualquier conductor que use ese coche. ¿Quién puede acceder y usar la información recogida? ¿Para qué?

"*Las mentiras socialmente aceptables de antes serán más difíciles o casi imposibles porque estarás constantemente acechado y bajo monitoreo a través de Internet*", asegura Pamela Wright, presidenta de innovación para los Archivos Nacionales de EE.UU. "*Oye, tú dijiste que te fuiste de fin de semana, pero tu cama dice que dormiste bien ocho horas el sábado por la noche…*". Este tipo de escenarios plantea si los fabricantes de dispositivos deberían incluir en ellos, tecnologías como el cifrado de datos o, si se debe facilitar el uso de los datos en un procedimiento judicial previo aviso a las usuarias. ¿Es necesario desarrollar estándares que especifiquen requisitos de diseño para que los datos de la IoT soporten la cadena de custodia de los datos en los procesos judiciales? ¿Se deberían establecer regulaciones que protejan al consumidor de ciertos dispositivos de la IoT?

Lo que parece necesario, de cualquier forma es buscar un equilibrio entre los beneficios económicos y sociales y la defensa de la privacidad para asegurar el control y la libre disposición de los datos personales de la sociedad.

En España el uso de conversaciones telefónicas grabadas sin permiso del usuario y sin una orden no valen como prueba en un juicio al ser recogidas sin el conocimiento de una de las

http://es.gizmodo.com/los-riesgos-del-iot-un-vendedor-inutiliza-la-puerta-de-1794002365 [Consulta: 14/05/2017]

dos partes. Con la llegada del IoT y objetos inteligentes al alcance de nuestra mano, se deberá revisar qué información puede utilizarse como prueba y qué no por suponer un allanamiento de nuestra intimidad. Una vez decidido eso, que la información recogida por estos elementos pueda resultar válida también es un punto que debe analizarse con detenimiento. Muchos de estos objetos pueden utilizarse por varias personas incluso sin el conocimiento de ellas mismas, la información que puede obtenerse por tanto, no siempre podrá demostrarse que está relacionada con una persona en particular.

Parece por tanto, que salvo en algunos casos en los que el uso del dispositivo esté completamente restringido a su dueño, su utilización en procedimientos legales puede, lejos de aportar "claros" en un juicio; abrir nuevas incógnitas que dificulten su objetivo.

6.8.8 DISPOSITIVOS DE IOT UTILIZADOS PARA AGENCIAS DE APLICACIÓN DE LA LEY Y LA SEGURIDAD PÚBLICA

Los dispositivos de la IoT podrán ayudar en la aplicación de la ley y la seguridad pública. Muchos comercios minoristas han optado por poner cámaras de seguridad. On-Star Corporation puede proporcionar datos de los sensores que se encuentran alojados en los coches de policía para saber dónde están o para desactivarlos de forma remota. En el Condado de Nassau (New York), la policía utiliza una red de sensores de sonido llamada ShotSpotter [64] para detectar y localizar la fuente exacta de un disparo en los barrios donde han sido desplegados. Todos estos ejemplos son beneficiosos y sin duda, mejoran la seguridad pública. Sin embargo todos estos dispositivos pueden suponer un arma de doble filo.

El uso de las tecnologías IoT preocupan a algunos defensores de los derechos civiles. En la actualidad, entre la disponibilidad de tecnología y el riesgo de ataques terroristas como argumento, está surgiendo una omnipresencia de las actividades de monitoreo de los datos, las políticas sobre su conservación y destrucción, los usos secundarios que los gobiernos pueden darles y la potencial exposición accidental de los datos a actores maliciosos. La línea entre la utilización o acceso a nuestros datos por seguridad y un control excesivo limitando nuestras libertades es muy fina y muy subjetiva dependiendo de quién la mire. En un artículo[65] publicado por el diario británico The Guardian (2016), se narraba como James Clapper, director de la Inteligencia de EEUU declaraba en el Senado como parte de una declaración sobre las amenazas a las que tendrá que hacer frente EEUU: *"En el futuro, los servicios de inteligencia*

[64] ShotSpotter: Dispositivo sensor que avisa automáticamente cuando se produce el sonido de un disparo y permite triangular la ubicación del mismo. Se puede encontrar más información en http://www.shotspotter.com/ [Consulta 18/06/2017]

[65] THE GUARDIAN. US. intelligencie chief: we might use the internet of things to spy on you. 2016. Disponible en línea en: https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper [Consulta 16/05/2017]

podrán usar el IoT para la identificación, vigilancia, monitorización, localización y seguimiento para reclutar u obtener acceso a redes o credenciales de usuario"

iPhone y su sistema operativo iOS 8, Apple Corporation eliminó un método de acceso tipo "puerta trasera" que existía en sus versiones anteriores. La función de puerta trasera permitía a la policía acceder a los datos del teléfono móvil de un usuario. Apple eliminó esa característica y ahora encripta el contenido interno sin tener forma de permitir el acceso sin la autorización del propietario. Al fin parece simplemente estar cumpliendo el derecho de consentimiento pero para agencias federales de seguridad, esto hace que sea más difícil procesar los comportamientos criminales. La controversia está servida. En este trabajo se ha mencionado la encriptación como una medida para mejorar la seguridad de los dispositivos ¿Cómo se puede equilibrar esto con el legítimo acceso a los datos del usuario en interés de la seguridad pública? ¿Es legítimo que todas las usuarias estemos bajo la posibilidad de que revisen nuestra información por el bien de la seguridad pública sin saberlo?

6.8.9 DESAFÍOS ESPECIFÍCOS EN EL USO DEL INTERNET DE LAS COSAS MÉDICO

Si bien es reconocido que la expansión de la IoT traerá beneficios y mejoras en el campo de la asistencia sanitaria, también implica ciertas preocupaciones que se solapan.

En el punto anterior se analizaron los desafíos más importantes a los que se enfrenta el Internet de las cosas. En objetos inteligentes relacionados con la salud, aparecen nuevos retos y otras amenazas adquieren mayor relevancia. A continuación revisaremos alguno de los puntos más importante.

6.8.9.1 Sobrecarga

Existe un peligro de sobrecargar a los médicos con demasiados datos que les alejen de su misión de tratar pacientes y el trato personal médico – paciente se pierda entre información. Malcolm Glandwell en su libro Blink ilustraba como el hecho de disponer de demasiados datos puede llevar a los médicos a tomar decisiones erróneas.

Algunos médicos están empezando a plantear el problema de almacenar gran cantidad de información de los pacientes. Consideran que puede tener más sentido en proyectos de investigación o estadísticas pero a la hora del diagnóstico y tratamiento, el profesional puede perderse en un sinfín de datos buscando uno concreto o desechando los que no son válidos, con el tiempo empleado para ello. Por otro lado, se plantea si vale la pena tener datos de personas sanas o se corre el riesgo de "padecer cierto síndrome de Diógenes con la información". La línea entre los datos sanitarios importantes y los que no lo son es subjetiva, la

ampliación de datos a integrar en el historial médico de un paciente puede suponer demasiados detalles de la vida del paciente que pueden intercambiarse sin consentimiento entre entidades públicas que pueden tener objetivos comunes pero donde haya información que debiera proceder compartirse. Un ejemplo puede ser el caso de las adopciones, Servicios Sociales puede acceder al historial clínico de la mujer que solicita la adopción si bien en este historial pueden haberse introducido datos que no tienen relación directa con el objetivo final.

6.8.9.2 Fallos fortuitos

Ciertos objetos, como muchas otras herramientas de la tecnología formarán parte de nuestra cotidianidad casi de forma inevitable, la entrada del IoHT puede generar desconfianza a médicos y pacientes. Un fallo fortuito de gran impacto podría provocar en la sociedad cierta resistencia a utilizar los dispositivos médicos conectados a las redes, lo que retrasaría su despliegue y normalidad en años o décadas.

La aparición de nuevas tecnologías hace necesario una reforma en el modelo de contratación pública, ya que las normas de contratación y pliegos de condiciones no se adecúan a la aparición de situaciones tecnológicas. Igualmente se hace necesario introducir en la formación de las profesionales conocimientos sobre la utilización de nueva tecnología y seguridad en los dispositivos.

En 2013 la FDA admitió que fallos en los desfibriladores de emergencia podrían haber provocado "cientos de muertes". Las máquinas, colocadas en lugares públicos, se usan para reanimar a personas que han sufrido un ataque al corazón o fuertes arritmias. Pacientes que necesitaban someterse a ciclos de radIoTerapia recibieron sobredosis masivas de radiación (Aproximadamente cien veces la cantidad prevista), el software de los aparatos tenía un fallo y producía errores al unir los datos procesados y sus resultados. La FDA informó que entre 2005 y 2012 recibió hasta 45.000 informes de incidencias por equipos que no funcionaron correctamente en EEUU. En España el número de casos es notablemente menor, sin embargo no hay registro donde poder consultar las consecuencias de estos problemas[66].

En muchos de estos casos existe una gran dificultad en demostrar que el error ha sido del dispositivo médico y controlar el número de dispositivos defectuosos. La mejor medida de reducir estos fallos es la previsión. Trabajar desde el principio poniendo la seguridad como prioridad saldrá más barato a la larga. De nuevo la importancia de la "Seguridad pro defecto".

[66] Ejemplos recogidos del artículo "Dispositivos médicos: cuando un fallo en la tecnología te puede costar la vida". Fecha de publicación: 16/06/2014 por Eldiario.es disponible en línea en: http://www.eldiario.es/hojaderouter/tecnologia/medicos-pifias-radiacion-salud_0_275772495.html [Consulta 15/05/2017]

6.8.9.3 Ataques malintencionados

Queda claro que integrar los avances tecnológicos en nuestro sistema sanitario aportaría grandes ventajas que influirían sin lugar a dudas en nuestra salud y en el bienestar de la población. Aún con ello no nos podemos olvidar de las amenazas que pueden existir. Además de las amenazas existentes en cualquier dispositivo inteligente, la Agencia Europea de Seguridad de las Redes y de la Información publicó en 2016 un estudio sobre las principales amenazas dentro de los hospitales inteligentes donde destacaban el malware como el principal factor de riesgo.

Cada nuevo dispositivo, indica el informe, es un objetivo potencial para un ataque. Y estos ataques son importantes ya que está en juego la vida de los pacientes y la privacidad de sus datos personales. Dentro de las amenazas resaltamos:

- Ataques basados en ingeniería social. En este tipo de ataques engañan a empleados para que revelen datos y clave de acceso a los sistemas de información. Por ejemplo un empleado que abre un archivo contaminado y se ejecuta un programa que toma el control del dispositivo.

- Manipulación de dispositivos médicos. Es inquietante que hackers puedan tomar el control de dispositivos médicos y aunque no sea usual, siempre que el dispositivo esté conectado a la red cabe esa posibilidad. Los hackers pueden usar los dispositivos como puerta de entrada al sistema o incluso pueden llegarse a plantear situaciones de ransomware.

- Robo de equipamiento. El robo de dispositivos inteligentes dentro de un hospital es una realidad. La gravedad aumenta si el dispositivo robado contiene datos de pacientes.

- El ramsonware se da cuando cibercriminales toman el control de aspectos fundamentales del sistema informático de un hospital y exige un rescate a cambio de liberar los datos de los pacientes. Este es actualmente uno de los más preocupantes ataques ya que dejan el hospital parado completamente.

- DDOS Ataques de denegación de servicio. Estos ataques persiguen inutilizar los sistemas de información del hospital a través de un envío masivo de tráfico a los servidores para que éstos se saturen y dejen de prestar servicio.

La responsabilidad para evitar las amenazas vistas pasa por llevar las mejores prácticas en materia de seguridad y de crear un plan de formación para empleados sobre medidas de seguridad ya que una de las asignaturas pendientes en la docencia de los profesionales es mejorar la formación de estas nuevas tecnologías. Responsabilidad tiene también los

fabricantes de dispositivos inteligentes a la hora de incorporar la seguridad en el mismo diseño del producto.

6.8.9.4 Enfermos psicosomáticos

Cedric Notredame[67] en referencia a los avances del Big Data y el Internet de las Cosas en el ámbito de la salud, decía que en el futuro habría posibilidades de convertirnos en enfermos psicosomáticos. Parece algo liviano, pero plantea una pregunta importante: ¿El exceso de información conlleva peligro de toxicidad? ¿Estamos preparados para tantos datos sobre nuestra salud? Ahora mismo, cuando nos hablan de algún posible problema de salud es fácil que caigamos en la tentación de buscar en internet información: síntomas, tratamientos o historias de otros pacientes. Partiendo de la base de que no deberíamos y lo hacemos, puede que consultemos en Medline Plus[68] que es una fuente fiable, o puede que consultemos otros sitios donde más que obtener información nos desinformen. En algunos países se han creado listados de páginas "amigas" donde poder consultar información médica con fiabilidad. Esta puede ser una solución aunque algunos profesionales opinan que no sólo vale con consultar páginas de confianza, hay también que entender que la medicina es compleja y está llena de matices que pueden hacer que los diagnósticos varíen y los pacientes que consulten no lo tengan en cuenta. Actualmente esto ocurre con frecuencia pero con el Internet de las Cosas puede verse acentuado. Imaginen, en el caso anterior, si además podemos disponer en nuestros dispositivos de gran cantidad de datos relacionados con nuestra salud sin saber si tienen o no relación con el problema indicado: frecuencia cardiaca, niveles en sangre, peso… La cantidad de datos y la posibilidad de obtener información derivada de estos aún sin saber de su veracidad, puede hacer que sustituyamos al profesional médico por búsquedas en Internet o que aumente la automedicación dentro de la población.

El acceso a mucha información no siempre está relacionado con un beneficio. Pongamos el caso de un enfermo de anorexia que compra un reloj wereable que puede decirle las calorías que come en el día y las que pierde con el tiempo de ejercicio ¿Sería correcto que lo usara? Como para el resto de tecnología como móviles, ordenadores, etc., no hay una regulación que valore quién puede hacer uso o no, es algo más bien basado en la ética y la responsabilidad bien de los mismos usuarios, bien de sus responsables pero en un día a día de objetos conectados ¿Será llevadero?

6.8.9.5 Interrupciones intencionadas

Los dispositivos médicos conectados a las redes son tan vulnerables como cualquier otro objeto conectado pero, cuando un dispositivo de red se conecta a una persona, las

[67] Cedric Notredame, bioinformática del Centro de Regulación Genómica de Barcelona. Artículo 2013 disponible en http://blogthinkbig.com/curarnos-con-nuestro-smartphone/ [Consulta 25/06/2015]
[68] Medline Plus: enciclopedia médica promovida por la Biblioteca Nacional de Medicina y los Institutos Nacionales de Saludo de los Estados Unidos

consecuencias de los ciberdelitos cometidos utilizando ese dispositivo podrán ser especialmente personales y graves. Aunque los estudios indican que los ataques dirigidos a personas con la intención de hacerle un daño físico son poco probables, existe una alta probabilidad de que se produzcan ataques que podrían causar interrupciones generalizadas.

Actualmente la atención del desarrollo y producción de dispositivos médicos se centra en cubrir las preferencias de los fabricantes y las necesidades de los pacientes. Es importante que los fabricantes y la Administración Pública implementen un conjunto de estándares de seguridad o de prácticas recomendadas específicas para el IoHT. Un enfoque coordinado en el que puedan extrapolarse los resultados y desarrollar sinergias.

Falta de interoperabilidad técnica, legal y administrativa de los diferentes servicios. Desde el punto de vista técnico, es la mayor dificultad. Los usuarios de estas herramientas (profesionales y pacientes), deberían estar capacitados para el uso correcto de cualquier plataforma tecnológica o sistemas similares en cualquier parte donde lo pudieran encontrar.

6.8.9.6 La protección de la privacidad

La privacidad y confidencialidad de la información es una de las cuestiones claves a superar para el éxito del IoT y en particular del IoHT. Anteriormente ya explicamos en el punto de riesgos del IoT los desafíos que se presentaban.

En este punto hablaremos de riesgos particulares dado que la información que el IoHT maneja es información sensible teniendo en cuenta que los riesgos vistos en el punto antes mencionado no entran en conflicto con éstos.

Los datos personales relacionados con la salud son considerados de gran confidencialidad en todos los países. La divulgación no autorizada de una determinada condición médica, diagnóstico o cualquier otro tipo de información confidencial podría tener efectos negativos en la vida de los afectados. La necesidad de una serie de políticas y regulaciones que definan cómo cumplir con la protección de la información médica confidencial se hace necesaria. Una mala praxis en este ámbito puede tener consecuencias negativas.

En el contexto de la IoHT, datos que se deben proteger especialmente son:

- Información de Identificación personal: información personal identificable como fechas de nacimiento o números de seguridad social.
- Datos clínicos: los historiales médicos electrónicos con información del paciente o sus tratamientos.
- Datos de hábitos y comportamientos: los datos sobre comportamientos de ciudadanos, vigilancia, consultas en Internet, aportaciones en redes sociales o los

hábitos de compra ya que ayudan a elaborar formas de comportamiento humano de forma precisa.

- En el campo de la genética se incide más en su sensibilidad ya que con el genoma completo de una persona se podría descubrir las enfermedades futuras. Las consecuencias en este sentido podrían ser extremadamente perjudiciales para el dueño de los datos, objeto de discriminación o publicidad destructiva.

La encuesta PwC sobre el estado global de la seguridad de la información "Global State of Information Security Survey 2015" muestra que los incidentes relacionados con la seguridad de la información denunciados por proveedores del sector sanitario aumentaron en 2014 un 60%, casi el doble que el resto de sectores. May Wang, ingeniero en Zingbox afirma "En los últimos tres años el sector de la salud ha sido hackeado más veces que el sector financiero. Y cada vez más incidencias de hacking están dirigidos a dispositivos médicos". La misma investigación también mostró que una parte de los sistemas de salud expuestos utilizan sistemas operativos obsoletos, lo que puede hacerlos mucho más vulnerables. Más del 3% de los dispositivos utilizaban Windows XP, el sistema operativo Microsoft retirado que ya no recibe actualizaciones de seguridad. Más adelante revisaremos este punto con mayor profundidad.

6.8.9.7 Riesgo de pérdida de intimidad

Los datos sobre salud son datos sensibles y por ello tienen normas más restrictivas que aseguran su privacidad. Hoy en día en el autobús, por la calle o en cualquier lugar público, vemos a personas utilizando sus dispositivos móviles para poner música, hablar por teléfono con el "manos libres". Quizá no vaya más lejos que un problema de educación pero ¿Sabemos las consecuencias que pueden tener? Con el Internet de las Cosas, dispositivos médicos podrán dar datos sobre nuestra salud y algunos expertos se preguntan si no pondremos en riesgo nuestra intimidad sin darnos cuenta de las consecuencias.

Imaginemos un dispositivo que nos pone en contacto con nuestro médico. Si caemos en estas "malas costumbres" puede que alguna persona de nuestro alrededor se entere de la conversación o, imaginen que la app lanza un mensaje cada vez que el paciente debe tomarse una medicación: "Es hora de su dosis de….". En ese caso todas las personas que estuvieran alrededor podrían saber lo que nos pasa. Puede importarnos o no, pero al menos debemos poder elegir. Imaginemos que el medicamento que nombra es un antidepresivo y que lo oye la persona que hay sentada al lado en la oficina que resulta ser el jefe y por ese motivo no decidiera renovar el contrato a la persona.

Es importante que sepamos las características de los dispositivos inteligentes, de esta forma podremos desactivar las funcionalidades que queramos como los avisos de voz.

En Ohio hubo un incendio en casa de un hombre mayor y enfermo que había sufrido un implante de corazón artificial. Los policías encargados del caso consiguieron una orden de

registro para poder acceder a los datos almacenados en el dispositivo médico que, dio detalles del funcionamiento del marcapasos y de su ritmo cardiaco antes, durante y después del fuego. El cardiólogo confirmó que los datos no eran acordes con una persona que escapaba de un fuego y veía arder su casa. El hombre finalmente fue acusado. Este caso ha sido el primero en el que se acceden a datos de dispositivos médicos por parte de las fuerzas de seguridad[69].

Desde que las amenazas de ataques terroristas crecieron, todos los países han revisado y planeado modificar sus leyes, viendo como punto importante poder acceder a nuestros datos. Fiscales, policía local y gobiernos están interesados en recabar la mayor información posible de dispositivos médicos inteligentes, juguetes o cualquier objeto del IoT. En España, por ahora, la se podrá acceder a información sensible cuando suponga un riesgo para la seguridad pública. El problema de esto es que la línea que separa la libertad de la seguridad parece ser fina y difuminada, el debate está abierto y al margen de que sea legal o no que puedan acceder a dispositivos médicos que puede, estén implantados en nuestros cuerpos, lo que es cierto es que al saber esto, las personas intenten evitar cualquiera de estos dispositivos, por tener la sensación de poder ser espiado continuamente.

6.8.9.8 Identificación y responsabilidad de los actores

A la hora de identificar posibles responsabilidades derivadas de la utilización de dispositivos del IoHT, o de alguna forma de ejercer la medicina por un medio no presencial, aplicar las normas generales puede convertirse en algo complejo por la cantidad de actores involucrados en el diagnóstico, opinión, tratamiento o intervención.

El tratamiento de pacientes con estos dispositivos, hace que además de los profesionales médicos, entren en juego profesionales de telecomunicación e informática encargados de asegurar el mantenimiento de equipos y del material así como de mantener sistemas seguros, ser transparentes en las prácticas y cumplir con los derechos de usuarios. Fabricantes de dispositivos, sensores o el proveedor de comunicaciones electrónicas pueden tener responsabilidades ante fallos fortuitos de los sistemas o problemas de privacidad.

Múltiples factores que suponen múltiples fuentes pueden dar lugar a que un daño en la salud del paciente pueda provenir desde un diagnóstico equivocado dado por el profesional, a un error de almacenamiento provocado por las nuevas tecnologías o un error del paciente al introducir los datos.

Revisamos a continuación algunos casos que pueden darse y la responsabilidad sobre los actores que intervienen.

[69] Artículo: "Pacemaker data used to help indict alleged arsonist" de Nakedsecurity. Fecha 03/02/2017 disponible en línea en: https://nakedsecurity.sophos.com/2017/02/03/pacemaker-data-used-to-help-indict-alleged-arsonist/ [Consulta 18/05/2017]

- Escenario 1. *Se realiza una consulta a distancia entre el médico y el paciente*. En este caso el médico asumirá la responsabilidad del diagnóstico, opinión, tratamiento e intervenciones médicas directas.
- Escenario 2. *Han participado, en el tratamiento del paciente, actores no médicos como cuidadores o familiares en la recolección de datos, pruebas o vigilancia o el mismo paciente*. En este caso, el médico ha debido, previamente, asegurar que la formación y competencia de estos actores sean adecuadas para garantizar la seguridad del paciente. Se debe asegurar también de que ha entendido la importancia de su papel en el proceso y cumple con su responsabilidad a la hora de: introducir los datos de forma correcta, hacerlo con la frecuencia que se ha estipulado o en la fecha/hora prevista, hacerlo en las condiciones óptimas (En ayunas, tras ejercicio, etc.) e informar al médico si no se han cumplido alguna de estas premisas.

  En este punto, sin embargo, se abre una discusión ya que el médico puede asegurarse del entendimiento por parte del paciente del funcionamiento de los dispositivos o la importancia de su uso correcto, pero no se puede quitar la responsabilidad al fabricante de éste de asegurarse de que las instrucciones sean claras y fáciles de seguir por cualquier paciente que pueda hacer uso de él. Por ello, las entidades de regulación pertinentes deberán realizar una revisión adecuada del dispositivo antes de que éste salga al mercado.

- Escenario 3. *Un paciente hace uso de una cápsula inteligente para tomar parámetros de salud. Por el resultado se inscribe un tratamiento erróneo al paciente que hace que aparezcan nuevos problemas de salud.* En estos casos, la responsabilidad de un tratamiento erróneo con diversas consecuencias cae en un vacío legal en parte, por la dificultad que existe para demostrar que el fallo fue debido al dispositivo.

Una de las ventajas del IoHT es que hacen que el paciente sea más activo a la hora de cuidar su salud y dispongan de mayor cantidad de datos sobre ella. El hecho de poder realizar pruebas médicas o controles sin necesidad de acudir al hospital o utilizar dispositivos médicos que implican una responsabilidad respecto a la seguridad y utilización hacen que organizaciones sanitarias estén cambiando su enfoque de trabajo opinando que implicar a los pacientes supone obligaciones no sólo para los profesionales, sino también para los pacientes ya que el éxito de un tratamiento no dependerá únicamente del acierto del profesional, sino de la conducta y responsabilidades del paciente: buen uso de recomendaciones, consejos o tratamientos, utilización responsable de los recursos sanitarios, etc. Por ahora no se está estudiando ningún cambio respecto a la responsabilidad de los pacientes.

6.8.9.9 Robo de identidad

Cuando una persona se hace pasar por otra utilizando sus credenciales de salud: nombre, número de seguridad social, etc. Se dice que se produce un “Robo de identidad médica”. Este hecho suele estar relacionado con la prestación de servicios o productos de

atención médica como recibir un tratamiento, defraudar a las aseguradoras presentando falsas reclamaciones o comprar medicamentos entre otros. Este tipo de hechos pueden ser con o sin el consentimiento del dueño real de los datos.

El robo de identidad puede producir daños de diferentes tipos, por un lado nos encontramos con las pérdidas monetarias que puede causar: a los pacientes si se trata de un seguro privado porque pueden hacer que las primas aumenten o que deban asumir costes por pruebas que no necesitaban y a las aseguradoras ya que pueden perder dinero y reputación. Por otro lado y más graves son las consecuencias en la salud del paciente. Cuando una persona obtiene atención médica en nombre de otra persona, la información médica del usuario fraudulento se integra con el historial del paciente real haciendo que no quede reflejado el estado real del paciente, es lo que se conoce como "historial médico mixto". Ambos (Afectado y usurpador), pueden verse perjudicados entonces, por ejemplo si su tipo de sangre es diferente, las alergias de uno de los pacientes se trasladan al otro o se le niega a uno un medicamento al que el otro puede ser alérgico. En el historial del paciente puede quedar reflejados medicamentos que no haya tomado o enfermedades que no hayan tenido, datos en definitiva, incorrectos. Según la MIFA[70], el 20% de las víctimas de estos robos reciben un tratamiento o un diagnóstico equivocado o sufren retrasos para ser asistidos debido a la confusión que se genera sobre su historial.

Con dispositivos inteligentes que mandan datos para cruzar con otros y obtener información, el hecho de que cualquier dato mandado sea alterado, puede dar lugar a una propagación de información errónea que puede resultar peligrosa si se trata de datos sanitarios. Esta información además, puede pasar a formar parte de estadísticas o estudios con resultados equivocados.

Ponemon Institute[71] estimó que el número de casos aumentó de 1.5 millones en 2012 a más de 1.8 millones en 2013 en Estados Unidos. El aumento no es preocupante pero con la inmersión del Internet de las Cosas en el sector de la salud, se prevé que el número de casos crezca: la digitalización de los historiales médicos de los pacientes la información personal se vuelve más vulnerable a los ataques externos. Los dispositivos wereables y dispositivos médicos transportables son los dispositivos más sensibles a este tipo de actos ya que son más fáciles de perder o robar, el uso rutinario puede hacer que el usuario no sea consiente de los riesgos de su pérdida cometiendo algunas imprudencias como guardar las contraseñas para poder acceder de forma más rápida.

[70] Medical Identity Fraud Alliance (MIFA): cooperativa público-privada que une a todas las partes interesadas en el desarrollo de soluciones y prácticas de prevención, detección y resolución del fraude de identidad pública. Para más información, disponible en línea en: http://medidfraud.org/ [Consulta 15/06/2017]

[71] Ponemon Institute se encarga de realizar investigaciones independientes sobre privacidad, la protección de datos y la política de seguridad de la información.

En la telemedicina o asistencia médica a distancia facilitan este tipo de robos de datos y más si se hacen con consentimiento (Personas de una misma familia). El profesional no tiene por qué ver al paciente, como pueden ser los casos en los que el médico mande por mail una prescripción, en ese caso se pierde la seguridad de estar hablando con él o con otra persona.

En Estados Unidos los datos médicos, según el FBI, se venden entre el 20 y 70 dólares mientras que las tarjetas de crédito se venden por 5 dólares. Esto se debe a dos factores: detectar el fraude y robo de identidad médica es mucho más difícil que detectar el fraude financiero y, una vez descubierto, cancelar las tarjetas sanitarias y revisar los historiales médicos no suelen ser procedimientos rápidos. Víctimas de "Robo de identidad médica", han tardado hasta tres meses en poder arreglar el problema.

En este punto nos planteamos:

El historial clínico de un paciente es un derecho de éste en sí. El paciente también tiene derecho a acceder a la documentación de la historia clínica y a obtener copia de los datos que recoja. Este derecho no puede interferir con el derecho de terceras personas a la confidencialidad de los datos que constan en sus historias ni en comentarios subjetivos que pueden hacer los profesionales sobre sospechas de actitudes o hábitos sin que por ello se justifique observaciones peyorativas carentes de valor asistencial), esta información queda recogida en el Artículo 12.1 del Decreto 38/2012, de 13 de marzo y de acuerdo con lo dispuesto en el artículo 18 de la Ley 41/2002 de 14 de noviembre.

Los centros sanitarios están obligados a disponer de un procedimiento que garantice el derecho de acceso a la propia historia clínica. Actualmente un paciente puede solicitar su historial clínico desde la página de su comunidad adquiriendo previamente un certificado para poder acceder a la página de solicitud del historial, el procedimiento es poco intuitivo y no adaptado a cualquier paciente. También lo puede hacer acercándose a Atención al Paciente de cualquier centro, donde deberá rellenar una solicitud y una vez el centro informe de que ya está disponible la copia del historial, tiene un plazo de seis meses para retirar el historial una vez esté en el centro si bien, sólo se indica que si en el plazo de un mes el centro no se ha puesto en contacto con el paciente puede llamar a pedir información sin indicar plazos.

En el Artículo 16 de la Ley Orgánica 15/1999, apartado 1 queda reflejada la obligación del responsable del tratamiento de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días teniendo en cuenta que "*Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto la Ley y, en particular, cuando tales datos resulten inexactos o incompletos*" (Art. 16.2)

El sector sanitario precisa un método que consiga identificar de forma inequívoca y segura a cada paciente en cada uno de los dispositivos inteligentes. Debe mejorar la seguridad del paciente dentro de todo el ciclo de la atención sanitaria protegiendo su identidad médica.

6.8.9.10 Necesidad de nueva legislación

Todos los actores coinciden en la necesidad de nuevas normas que se adapten a la nueva tecnología, se ha dicho en varios puntos de este trabajo. Igualmente en el campo de la sanidad, una regulación que vaya por delante de lo que puede suceder adquiere mayor relevancia pues en ello puede ir la vida o salud de personas.

Parece que España en este aspecto tiene una asignatura pendiente o al menos debe mejorar la nota. Un informe de la Comisión Europea indicó en 2014 que existe un déficit legislativo que impide la expansión de los registros sanitarios sumado a problemas relacionados con la interoperabilidad, el acceso y el intercambio de datos de salud entre regiones u otros Estados miembros.

6.8.9.11 Pérdida de autonomía de los pacientes

Recientemente, un laboratorio mostró la cantidad de información sobre fisiología femenina que puede dar la temperatura corporal si se hace un seguimiento minuto a minuto[72]. Con ella se puede saber el momento de ovulación, del comienzo del ciclo menstrual, las probabilidades de quedar embarazada en una hora determinada o si el embarazo tendrá o no éxito. Este rastreo de temperatura se hace con un dispositivo del tamaño del botón de unos pantalones vaqueros que por un lado tiene un sensor que se llevará presionado a la piel. El botón puede estar en la muñeca sujeto con una banda de sudor, o se puede meter en una correa del sujetador. La temperatura es precisa y la resolución como la frecuencia de muestreo puede ser configurada por el usuario. Los botones no necesitan cargarse, pero los datos almacenados deben ser leídos cuando la memoria se llene. Una interfaz sencilla permitirá exportar los datos para que cualquier persona pueda realizar estadísticas, gráficos, jugar con ellos… El botón y un lector de datos cuestan aproximadamente $100.

Parece interesante al menos para los expertos que no saben bien lo que están buscando, pero las direcciones a donde van creen que son prometedoras. Ahora bien, ¿Y para las usuarias puede ser útil? ¿Necesario? Dependiendo de las circunstancias lo será para unas y para otras no.

Muchos de estos dispositivos aportan gran información para expertos y equipos de investigación, en estudios de valores en conjuntos de la población, pero de forma individual puede que no aporte tanto. La novedad de estos dispositivos hace que por el precio, no sean accesibles a todas las personas por el momento pero dentro de un tiempo, cuando el IoT esté más integrado en nuestra rutina sí y cuando esto pase, tendremos que hacer uso de nuestro

[72] QUEANTIFIEDSELF. Azure Grant. Hot Stuff: Body Temperature Tracking Ovulatory Cycles. 22017. Puede encontrarse el artículo completo en http://quantifiedself.com/2017/04/hot-stuff-body-temperature-tracking-ovulatory-cycles/ [Consulta]12/05/2017]

control para no caer en una atención excesiva de nuestra salud. ¿Estamos preparados para diferenciar qué dispositivos necesitamos y cuáles no?

Aunque esta pregunta se puede trasladar a cualquier campo del IoT, toma mayor importancia dentro de la salud y más concretamente en los dispositivos que sirven para prevenir cualquier tipo de enfermedades. El IoT va a ofrecer desde pañuelos que analicen si hay una infección en la mucosa hasta peines que indican el nivel de caspa, si hay piojos o el grado de calvicie. Corremos el riesgo de rodearnos de dispositivos que nos den información en cada cosa que hacemos, meternos en un bucle de interés constante por nuestra salud y acostumbrarnos a un sobre-control que todavía no sabemos dónde nos puede llevar. Muchos dan la posibilidad de actuar para conseguir objetivos, en principio eso es algo positivo, hace que las personas tengamos mayor campo de decisión en nuestra salud pero a la larga, un exceso de objetivos por cumplir puede hacer que no lleguemos a alguno y entonces puede ser peor la sensación de fracaso. No se puede olvidar que algunas aplicaciones y/o servicios responden a una lógica de negocios basado en resultados económicos que pueden intentar cambiar o establecer tendencias para su beneficio a través de opiniones o consejos. Por ahora es sólo una hipótesis pero el aumento del desequilibrio de poder entre empresas y pacientes está ahí.

La novedad de estos dispositivos hace que por el precio, no sean accesibles a todas las personas por el momento pero dentro de un tiempo, cuando el IoT esté más integrado en nuestra rutina sí y cuando esto pase, tendremos que hacer uso de nuestro control para no caer en una atención excesiva de nuestra salud.

Muchos de estos dispositivos aportan gran información para expertos y equipos de investigación, en estudios de valores en conjuntos de la población, pero de forma individual puede que no aporte tanto.

Parece que no hay dudas en que los hábitos de la sociedad cambiaran, los Wearables están haciendo que mejoremos nuestra forma física, nuestros hábitos de vida y en general nuestra salud. Ahora bien, ¿Qué pasará si alguien necesita un pañuelo? ¿Un peine? ¿Protector labial? ¿Cualquier cosa que lleve un chip para recoger datos? ¿Se tendría que cambiar el usuario? ¿Los datos recogidos no serían los nuestros y la información resultante podría estar alterada? Entonces: ¿Nos dirigimos a una sociedad “Individualista” en la que cada uno, debe tener sus dispositivos?

Por otro lado, los pacientes pueden acabar siendo esclavos de los objetos que usan para facilitarles la forma de vida. Organizar nuestras actividades en base a cuánto le queda a un dispositivo de batería o ir o no ir a algún lugar dependiendo de si cuenta con wi fi o no, puede ocurrir. El acceso es la barrera principal en el uso efectivo del IoHT, según la última encuentra del Eurobarómetro, existe una brecha cuando se trata de acceso de banda ancha a Internet en casa, en Holanda, por ejemplo un 86% tienen acceso en su casa frente a u n 48% en Rumania y el 46% en Grecia. En España en 31 provincias, entre el 30% y el 65% de su

población no pueden acceder a internet a través de banda ancha fija a los 30 Mbps en 2017. En la siguiente ilustración mostramos el mapa de zonas sin Wi Fi en España.

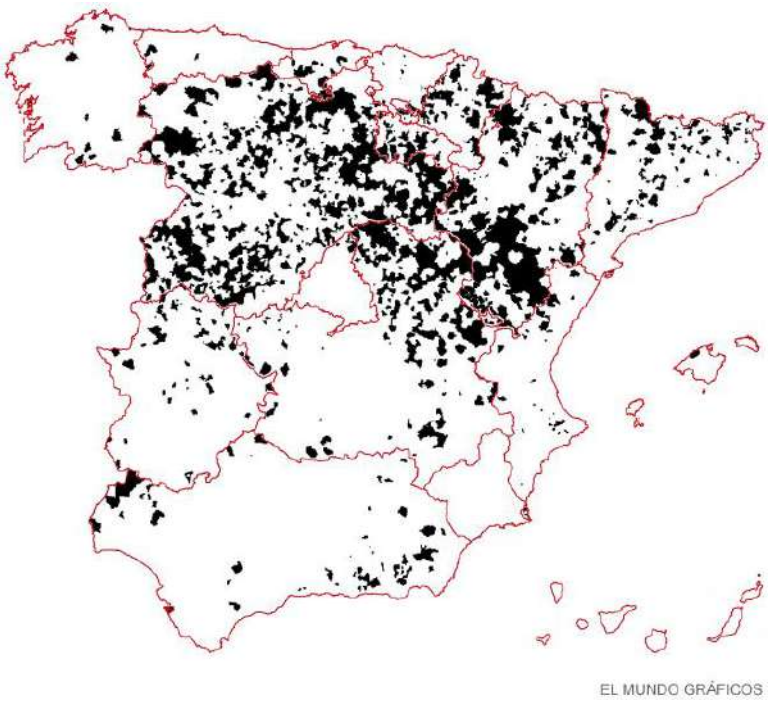

Ilustración 23: Mapa de la conexión deficiente a Internet[73]

A medida que vamos utilizando más objetos inteligentes, corremos más el riesgo de que esto ocurra. En algunos lugares de EEUU ya se está proponiendo establecer un "Día sin internet" de pruebe, de cara a saber gestionar si esto ocurriera y es que, cada vez es mayor la dependencia a las redes.

Cuando se estableció la posibilidad de usar cámaras de seguridad en algunas calles de grandes ciudades, se pudo comprobar que a veces las personas por el hecho de saber que nos están vigilando cambiamos nuestros patrones de comportamiento. Los objetos conectados pueden hacernos sentir "bajo la mirada" de alguien y cambiar nuestra forma de actuar bien porque intentemos cambiar nuestros patrones de cara a posibles ataques, bien porque intentemos por todos los medios llegar a los objetivos establecidos por el dispositivo.

[73] Artículo "Cero G, el mapa de la España sin Wi Fi" Infografía Álvaro Matilla. Periódico El Mundo, publicado el 24/04/2017 En línea http://www.elmundo.es/sociedad/2017/04/24/58fa3de946163f36758b4639.html [Consulta 14/05/2017]

6.9 RECOMENDACIONES PARA LOS ACTORES DEL ECOSISTEMA IOT

6.9.1 RECOMENDACIONES COMUNES A TODAS LAS PARTES INTERESADAS

Es importante la realización de Evaluaciones de Impacto en la Privacidad (PIA) antes que se inicie la aplicación basadas en la privacidad y el Marco de Evaluación de Impacto de Protección de Datos. Estas evaluaciones de impacto podrían ponerse a disposición del público creando Marcos Específicos de PIA.

Los dispositivos y aplicaciones deben diseñarse con el fin de informar a los titulares de los datos de forma clara y sencilla. Es importante que la información dada para obtener el consentimiento sea comprensible y vaya más allá de la política de privacidad estándar de la página web.

Cada actor de un ecosistema IoT debe aplicar los principios de privacidad desde el diseño y la privacidad por defecto. Los usuarios y responsables de los datos deben ser capaces de ejercer sus derechos y tener un control de sus datos.

Los actores deberán trabajar conjuntamente con los organismos de normalización con el objetivo de un protocolo común sobre recogida y tratamiento de datos. En este intento de colaboración, los fabricantes deben permitir a las entidades responsables y encargadas locales que permitan a los usuarios tener una idea clara de sus datos y su tratamiento.

Todas las partes interesadas trabajaran bajo el principio de minimización de los datos. Dado que muchas de las partes interesadas no tienen necesidad de tener datos en bruto en los dispositivos, cada parte deberá borrar los datos en bruto en cuanto hayan extraído la información relevante. Esta eliminación debe tener lugar en el punto de recogida de datos de los datos en bruto.

6.9.2 RECOMENDACIONES A FABRICANTES DE DISPOSITIOVS Y DESARROLLADORES. SEGURIDAD POR DEFECTO.

Las buenas prácticas de seguridad deben darse en todas las partes del IoT, desde la etapa de investigación y toma de requisitos hasta que el objeto llega al mercado. Un estudio de los requisitos de seguridad y privacidad que se han de cumplir y la posterior verificación de que se están cumpliendo, aunque puede parecer que elevará el coste del producto final, puede evitar gran parte de los problemas de seguridad del IoT.

La seguridad por defecto, “security by design” es la clave para minimizar las amenazas de ataques.

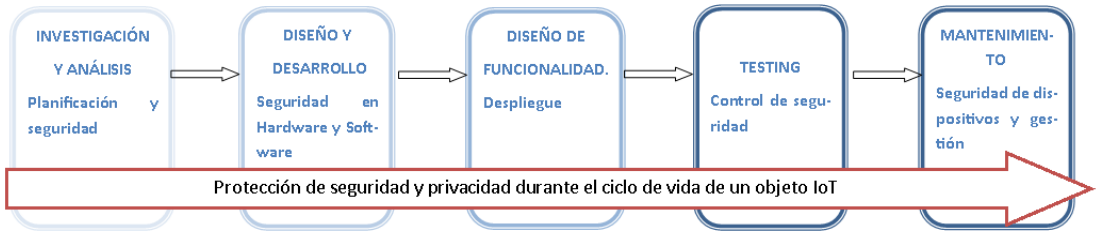

Ilustración 24: Ciclo de vida de Seguridad. Elaboración propia basada en esquema de Buiding a Trusted.

En la ilustración anterior vemos las fases por las que pasa la creación de un objeto inteligente. Analizaremos las medidas de seguridad y privacidad que se recomienda, se cubran en cada fase.

- Fase de diseño: Tener en cuenta la seguridad y reforzarla durante la fase de diseño evita tratar de reforzar la seguridad en cualquier otra fase lo que siempre resultará mucho más costoso y difícil ya que los dispositivos IoT no suelen disponer de suficiente memoria y procesamiento. Si se toma la seguridad como una característica más de los dispositivos IoT se podrán evitar problemas futuros.

- Fase hardware y software:
  - Hardware: utilizar componentes que cumplan las normas de seguridad vigentes y comprobar que el funcionamiento de cada componente es correcto o tener en cuenta la función y las condiciones en las que tendrá que funcionar evitarán tener que reemplazarlos a posteriori. Contar además con microcontroladores que detecten alteraciones o ataques de ingeniería inversa.
  - Respecto al software, se recomienda elegir un sistema operativo probado con garantía de funcionamiento. Aplicar todas las medidas de seguridad recomendadas como el principio de menor privilegio y de permisos. Por último se recomienda hacer un análisis de vulnerabilidades y asegurarse de poder realizar futuras actualizaciones que mejoren el software.

- Fase en la funcionalidad y despliegue: En esta fase se podrá instalar y configurar el dispositivo para obligar a los usuarios a tener que modificar los valores por defecto, esta acción es recomendada a los usuarios para mejorar la privacidad pero de esta forma se obliga a hacerlo. Por otro lado, verificar que se realiza un cifrado en los tipos de comunicaciones y en los datos asegurará el dispositivo de ataques

malintencionados y secuestros de datos. También debe estar cifrada la copia de seguridad. Tener una copia ayuda, en caso de ataque, a poder restablecer el dispositivo más rápido.

- Fase testing: su complejidad dependerá de las características del dispositivo. Si un objeto debe funcionar en temperaturas bajas se deberá probar, por ejemplo, pero si no es lo previsto, esa prueba podría evitarse. Esta fase requiere una batería de pruebas diseñadas específicamente para el objeto probando todas las fases anteriores: funcionamiento del hardware de forma correcta, acceso e instalación a actualizaciones, debilidades de ajustes o configuración, etc. Si el dispositivo no pasa esta fase, es recomendable volver a la fase en la que se encontró el error para trabajar en resolverlo. Además de pruebas de caja blanca se recomiendan pruebas de caja negra para confirmar que el dispositivo actúa o trata los datos de forma correcta.

- Fase de mantenimiento: Si la privacidad ha estado presente en la fase de software y de testing, no debería haber problemas con el mantenimiento del software ya que en ambas fases se comprobó que se podrían hacer actualizaciones. Por otro lado la fase de mantenimiento requiere una mayor responsabilidad por parte de los usuarios, para ello es necesario que los fabricantes de dispositivos informen de forma correcta y completa a éstos.

6.9.2.1 Fabricantes de dispositivos

Los fabricantes de dispositivos deberán informar a los usuarios de sobre los datos recogidos y su tratamiento. Deberá informar también a los demás actores involucrados cuando el usuario retire el consentimiento o se oponga al tratamiento de los datos.

Todos los dispositivos se tendrán que haber sometido a un proceso de seguridad por diseño y dedicar componentes a esa seguridad. Las herramientas que el fabricante ofrezca al usuario serán intuitivas y fáciles en su uso. Deberá al menos, facilitar las siguientes herramientas:

- ✓ Herramientas para que el usuario pueda leer, editar y modificar los datos brutos y agregados, almacenados en un formato que permita la portabilidad.
- ✓ Herramientas para notificar a los usuarios que existe una actualización y para que actualicen los dispositivos. Si este dispositivo se vuelve obsoleto se deberá informar al usuario y otros actores que puedan verse afectados por la vulnerabilidad del dispositivo.

Así mismo los dispositivos deberán tener las siguientes funcionalidades:

- ✓ Los dispositivos IoT deberán llevar una función para programar o desactivar de forma fácil y rápida sensores.

- ✓ Se deberá limitar la huella dactilar del dispositivo por medio de interfaces inalámbricas cuando no se utilicen o deban utilizar identificadores aleatorios como MAC para escanear redes WIFI con el fin de evitar identificadores que puedan ser utilizados para el seguimiento.
- ✓ Deberá tener un parámetro de ajuste que pueda distinguir a las personas que utilizan el dispositivo.

6.9.2.2 Desarrolladores de aplicaciones

Deberán seguir un enfoque de Privacidad por Diseño (PbD) y recoger los datos solamente necesarios para prestar el servicio ofertado. Además de ello deberá prestar atención a los datos recogidos y a los que se podrán deducir de ellos que podrían convertirse en datos sensibles.

El desarrollador deberá facilitar herramientas para que los usuarios puedan descargar los datos en un formato estándar y utilizable. La solicitud de datos deberá facilitar el ejercicio de los derechos de los dueños de los datos y se les recordará frecuentemente que el dispositivo sigue recogiendo datos al margen de que el desarrollador tenga o no acceso directo al dispositivo.

6.9.3 PLATAFORMAS SOCIALES

Las aplicaciones sociales con dispositivos IoT deberán preguntar a los usuarios y controlar la información antes de ser publicada, no convirtiéndose esta información por defecto en pública o, que aparezca en motores de búsqueda.

6.9.4 ORGANISMOS DE NORMALIZACIÓN Y PLATAFORMAS DE DATOS

Estos organismos deberán trabajar en el formato de datos tanto en bruto como agregados con el menor número de identificadores fuertes que aseguren el anonimato del usuario. Estos formatos deberán facilitar la transferencia entre los actores del ecosistema IoT. También deberán ser claros para que los usuarios sepan qué se va a hacer con sus datos.

Es importante que trabajen en estándares certificados y en el desarrollo de protocolos de cifrado y comunicación adaptados a las especificaciones del IoT que garanticen el cumplimiento de los derechos de los usuarios.

6.9.5 RECOMENDACIONES A USUARIOS. CULTURA DE SEGURIDAD

Por todo lo expuesto hasta ahora podemos entender que entre todos los responsables de la seguridad del IoT están los usuarios, principales interesados en que se protejan sus datos e intimidad.

Tomar conciencia de los riesgos que conlleva el IoT, la cantidad de datos directos e indirectos que proporcionamos y la importancia de tener una buena cultura de seguridad que nos haga ser responsables en la medida de lo posible de nuestros dispositivos de IoT es una pieza fundamental en la previsión de amenazas. También es una asignatura pendiente ya que se asocia el eslabón más débil de la seguridad con el entorno de usuario.

El consentimiento de los usuarios respecto al tratamiento de sus datos deberá ser libre sin que sean penalizados económicamente o vean degradado el acceso a herramientas de su dispositivo si deciden no utilizarlo o no utilizar un servicio específico. El usuario también tiene derecho a administrar su dispositivo y a ejercer sus derechos reflejados en la LOPD.

Dado que quien utilice el dispositivo IoT no tiene porqué ser siempre el usuario, éste deberá informar a quién use el dispositivo que sus datos son recogidos, respetando su derecho a no ceder sus datos.

La concienciación, precaución y la formación otorgan al usuario la capacidad de identificar los problemas y reaccionar adecuadamente contra ellas. En la actualidad, sin embargo; la ingeniería social es una de las técnicas más elaboradas y complejas y aunque se están realizando campañas informativas y cursos para enseñar seguridad a los usuarios, debemos tener en cuenta el espectro de edad de las personas que utilizarán el IoT. Nos referimos a personas mayores que tendrán algún objeto inteligente en casa (Se relaciona más con IoT médico) pero a los que no les resultará sencillo llevar su mantenimiento.

A continuación recogemos las principales recomendaciones a los usuarios frente a dispositivos inteligente.

- **Investigar y aprovechar el historial en medidas de seguridad del dispositivo IoT:** Antes de adquirir el dispositivo podemos comprobar si la empresa ha tenido problemas con dispositivos anteriores. Con una simple búsqueda por Internet podremos saber el nivel de compromiso con la seguridad en sus productos o, si ha tenido problemas al respecto en el pasado.
- **Utilización correcta de contraseñas:** el empleo de contraseñas predeterminadas no son seguras y es la principal amenaza para los dispositivos IoT. Utilizar contraseñas como frases largas, caracteres especiales, letras mayúsculas y minúsculas y números. Contraseñas difíciles de adivinar y que sean diferentes para cada uno de servicios (mail, redes sociales, banca…), aumentan la seguridad.

- **Mantener el software actualizado**: Realizando las actualizaciones oportunas podremos eliminar problemas descubiertos en versiones anteriores. El GT29 ya resaltó la importancia de facilitar estas actualizaciones para que se apliquen correctamente.
- En los dispositivos obsoletos por la falta de actualizaciones y parches, debemos **limitar el riesgo** mediante el uso de tecnologías alternativas o el bloqueo de la ejecución de programas no autorizados.
- **Deshabilitar las características y funcionalidades que no deseemos utilizar**: A menudo los dispositivos traerán funcionalidades o características que no siempre hagan falta. Es recomendable desactivar los servicios o puertos no necesarios para reducir posibles puntos de entrada de infecciones.
- Se recomienda **desactivar la función Universal Plug and Play** (UPnP)[74], para no estar expuesta a infecciones de malware y el acceso remoto si no es necesario, para no facilitar al intruso el control a distancia de nuestros dispositivos.
- **Restringir el acceso directo a los dispositivos:** La manipulación directa de los dispositivos también pueden suponer un riesgo. Es conveniente reiniciar de forma controlada los dispositivos de forma periódica, ya que pueden borrarse malware. Por otro lado, donde muchos dispositivos realizan un escáner diarios por sensores, es especialmente importante que si se llega a bloquear o apagar y dejara de hacer su función, tuviéramos herramientas que nos ayudasen a darnos cuenta y relanzar el dispositivo.
- **Conexión de red**. Es importante conectar los dispositivos IoT a una WI-Fi segura con protocolos como WPA2[75]. No obstante, no todos los dispositivos requieren lo mismo para funcionar. Cabe preguntarse ¿El dispositivo necesita conectarse a internet? ¿Necesita acceder a la misma red a la que se conecta el resto de dispositivos? Es recomendable que la red que configuremos para el dispositivo no sea mayor que la que necesite, una red pequeña es más administrable y por tanto más segura.

[74] Universal Plug and Play (UPnP) es un conjunto de protocolos de comunicación que permite a los periféricos en red, como computadoras personales, descubrir de manera transparente la presencia de otros dispositivos en la red y establecer servicios de red, compartición de datos y entretenimiento.
[75] WPA2 Wi-Fi Protected Access 2 es un sistema para proteger las redes inalámbricas, creado para corregir las. vulnerabilidades detectadas en WPA.

6.9.6 RECOMENDACIONES PARA MEJORAR LA SEGURIDAD EN IOHT

6.9.6.1 Seguridad cero

Maximizar los beneficios de los dispositivos médicos inteligentes requiere encontrar un equilibrio entre el control que podría dar a los dispositivos un enfoque seguro desde el diseño del dispositivo, y la flexibilidad que necesitan profesionales y pacientes. En ocasiones esta flexibilidad crea vulnerabilidades de seguridad debido a cambios de configuraciones o características de seguridad ya que la adición de éstas después del lanzamiento del producto no suele tener éxito. Si nos referimos además a dispositivos relacionados con la salud, el periodo de tiempo entre la aparición de una brecha de seguridad y su solución, puede traer graves consecuencias que afecten de forma masiva.

Partiendo de que hasta el producto más seguro puede tener errores, la industria de dispositivos médicos, dada la gran importancia de sus repercusiones, debe adoptar las mejores prácticas de otros sectores de la tecnología, colaborar con investigadores de seguridad informática y crear una conciencia pública en lo que afecta a la seguridad de los dispositivos. La cooperación y coordinación de todos los actores es fundamental para evitar agujeros negros donde se produzca una pérdida de seguridad que, tratándose de la salud, puede tener efectos importantes. La seguridad debe ser clave desde el diseño del dispositivo hasta el mantenimiento de éste ya en el mercado pasando por cada una de las partes de su ecosistema y cada una de las capas de su arquitectura como se mencionó en el punto 6.9.2: “Recomendaciones a fabricantes de dispositivos y desarrolladores. Seguridad por defecto”.

6.9.6.2 Identificación de los actores

Ante prácticas se seguimiento de la salud de un paciente a través de dispositivos IoT, se recomienda la existencia de un reconocimiento presencial previo por parte del profesional. Posteriormente, debería ser estrictamente necesario que tanto profesional como paciente dispongan de algún elemento de identificación fiable salvo en determinadas situaciones de urgencia.

En España hay cierto vacío sobre las medidas para identificar a profesionales y pacientes en el ámbito de la medicina a distancia. La información legal mínima que debe ofrecer el profesional queda regulada en la Directiva 200/31/CE, relativa a los aspectos legales de la sociedad de la información: Nombre, dirección geográfica de donde está establecido quien presta el servicio y el organismo de registro son datos que deben proporcionarse así

como, los profesionales deberán acreditar su título profesional y el organismo y el Estado donde se encuentren colegiados.

Se recomienda que las contraseñas en dispositivos médicos (Realmente en cualquier dispositivo IoT) no se memoricen en el dispositivo ni para los profesionales ni para los pacientes. En caso de los profesionales porque la pérdida del dispositivo (Por ejemplo para acceder al historial de paciente o a aplicaciones del hospital) puede dar lugar a que otras personas puedan entrar en esas aplicaciones. En los centros, puede que personas ajenas al centro sanitario accedan a los ordenadores de forma ilegal. Para los pacientes y teniendo en cuenta que una de las razones principales por las que el usuario se muestra reacio a la utilización de dispositivos IoHT es la facilidad para perderlos, la razón por la que los accesos a los dispositivos deben controlarse son obvias, a esta le sumamos el robo de dispositivos que podría dar la posibilidad de caer en otra amenaza, el robo de identidad.

6.9.6.3 Recomendaciones aplicaciones médicas

Gran parte de las apps se realizan en Estados Unidos y sólo se publican en inglés. Aunque en Europa está empezando a aumentar los desarrollos de estas aplicaciones, hasta ahora no era demasiada su aportación en el mercado. En 2013 se creó el primer Directorio Europeo de Aplicaciones de Salud para poner orden en el mercado de las aplicaciones médicos móviles distinguiendo las seguras y reguladas en el entorno europeo.

Se establecen una serie de recomendaciones que deben cumplir las aplicaciones móviles divididas en cuatro bloques tal y como se muestra en la siguiente ilustración.

Ilustración 25: Recomendaciones para apps médicas. Fuente: Agencia de Calidad Sanitaria de Andalucía.

1. Diseño y pertinencia. En este bloque recoge recomendaciones relacionadas con aquellos aspectos de diseño que debe tener en cuenta una app de salud. Sus contenidos y servicios deben estar orientados para que puedan ser usados de forma eficiente, efectiva y satisfactoria por el mayor número de personas, sin necesidad de que estas tengan que recurrir a adaptaciones especiales. Para ello, la app de salud debería basarse en principios de Diseño Universal, sus contenidos y servicios someterse a un testeo por usuarios potenciales y, una vez desarrollada, definir de forma clara a quién va destinada, su finalidad y objetivos.
2. Calidad y seguridad de la información. Estas recomendaciones están orientadas a reforzar la credibilidad de los contenidos de la app, al informar sobre quiénes son sus responsables, las fuentes de información en las que se basa, sus fuentes de financiación, así como la existencia de posibles conflictos de intereses.
3. Prestación de servicios. Este bloque se compone de recomendaciones sobre los servicios proporcionados por la app de salud: guías de manejo que permitan entender la aplicación, mecanismos de contacto para posibles consultas y aspectos relacionados con el comercio electrónico y el uso eficiente del ancho de banda para descargas o la publicidad.

4. Confidencialidad y privacidad. Las recomendaciones de este bloque tratan de abordar las garantías exigibles a la app de salud en materia de protección de datos, habida cuenta del carácter especialmente protegido de la información sobre salud, así como los mecanismos de seguridad que implementa una app para garantizar la privacidad y confidencialidad de la información.

6.9.6.4 Regulación para dispositivos médicos y formas de control de su uso

El progreso tecnológico en general y en el sector sanitario en particular, no siempre va acompasado de un desarrollo normativo que la dote de seguridad jurídica para todos los agentes de su ecosistema (pacientes, profesionales sanitarios y proveedores). Es importante revisar las regulaciones existentes para crear nuevas reglas que promuevan la seguridad y la innovación. Ante esto algunos fabricantes se preocupan de que las nuevas reglas creen capas innecesarias de burocracia y retrasen el acceso del paciente a las nuevas tecnologías.

En Estados Unidos, en la mayoría de procesos de regulación, se revisa el nuevo dispositivo antes de que salga al mercado para determinar si es similar a uno ya existente – con los mismos riesgos y beneficios para el tratamiento del mismo problema – La FDA clasifica el producto propuesto y revisa sus riesgos, beneficios e investigaciones sobre el producto de tal forma que el dispositivo puede ser vendido en el mercado pero no ha sido "aprobado" por la FDA. Los fabricantes prefieren utilizar viejas tecnologías que no aportan innovación pero obtendrán la aprobación reglamentaria. Por ello, se piensa que un incentivo regulatorio como un proceso de aprobación abreviado que fomentara la seguridad por diseño y la capacidad para reparar sistemas después de ser desplegados, ayudaría a fomentar la innovación. En Europa, los procedimientos para la aprobación de dispositivos son más cortos y menos restrictivos aunque existe un debate sobre la necesidad de nuevas normas.

Dejando a un lado la regulación y la división de opiniones entre los que piensan que no se necesita más y los que piensan que es necesaria una regulación estricta, actualmente la atención del desarrollo y producción de dispositivos médicos se centra en cubrir las preferencias de los fabricantes más que las necesidades de los pacientes. En la mayoría de los países, los gobiernos y las empresas privadas no representan adecuadamente el interés del público en cuestiones médicas a la hora de lograr un equilibrio entre eficacia, facilidad de uso y seguridad. Es importante que ambos implementen un conjunto de estándares de seguridad o de prácticas recomendadas específicas para el IoHT. Un enfoque coordinado en el que puedan extrapolarse los resultados y desarrollar sinergias. Foros de colaboración independientes de reguladores e industria que proporcionen una interpretación clara de la normativa y lleguen a acuerdos sobre cómo se puede dar la innovación y la eficacia protegiendo el interés público. Sabiendo que es fundamental crear un debate público, especialmente con pacientes y familiares que conviven con la enfermedad y saben cómo un dispositivo podría afectar su calidad de vida.

Por el momento en Estados Unidos NH-ISAC (Intercambio de Información Nacional de Salud y el Centro de Análisis), parece que no cumple con esa función ya que se centra en dar solución a amenazas pero no de coordinar grupos de interés y en Europa, aunque consideran que es importante una buena comunicación entre actores, todavía no se ha hecho nada al respecto.

La identificación de los dispositivos médicos que vamos a utilizar también es importante, utilizar un objeto catalogado como dispositivo médico asegura haber pasado mayores controles de seguridad y regulación mientras que otros dispositivos aunque estén destinados al mismo fin han podido saltarse ese cribado. Apps o dispositivos no regulados dan información sin asegurar ser fiables, precisos o seguros. *Ponemos de ejemplo los nuevos dispositivos para bebés que analizan la temperatura, posición y frecuencia cardiaca del bebé para ayudar a los padres. En un artículo del periódico ABC, se informaba que el centro Children´s Hospital de Filadelfia denunció que la utilización de estos dispositivos creaba alarma entre los padres, colapsando las urgencias porque el dispositivo alertaba de que algo iba mal lo que conlleva la posterior batería de pruebas, análisis, esperas en urgencias, etc. Cuando la realidad es que este tipo de dispositivos no están regulados por la FDA y por tanto se debe cuestionar la seguridad y calidad de estos diseños*[76]. Algunas plataformas como Play Store están dándose cuenta de que la información que den esas Apps, pueden alarmar a las usuarias y están comenzando a informarles antes de la descarga de la aplicación. ¿Es suficiente?

Se abre un debate sobre cuánto debe la ley limitar el uso de dispositivos inteligentes relacionados con la salud. Nos preguntamos, en este trabajo, cuál podría ser la mejor manera de controlar el uso de este tipo de dispositivos ¿Deberán ir con receta médica? ¿Controlar la edad de compra? ¿Se reducirá entonces el beneficio de la prevención de la salud que estos dispositivos pueden proporcionar? ¿Coartará la libertad de los consumidores de saber y gestionar sus propios datos? Como siempre para este tipo de dispositivos, parecer ser: "depende". Depende del tipo de datos y cómo pueda afectar a la salud de los usuarios, depende de los objetivos de los dispositivos. Sea cual sea la respuesta, parece clave puede ser que los usuarios sepamos de sus limitaciones y aprendamos a usarlos con la responsabilidad y concienciación correcta.

[76] Se puede leer el artículo completo en: ABC – TECNOLOGIA. A. Martínez. Los dispositivos inteligentes para bebés, en peligro de colapsar las urgencias de hospitales por falsas alarmas. 2017. Disponible en el siguiente enlace: http://www.abc.es/tecnologia/informatica/hardware/abci-dispositivos-inteligentes-para-bebes-peligro-colapsar-urgencias-hospitales-falsas-alarmas-201702082154_noticia.html [Consulta 22/05/2017]

7 CONCLUSIONES

En este trabajo se ha querido dar a conocer el estado del arte de "Internet de las cosas". Aunque en el siglo pasado algunos ya auguraban que objetos conectados acabarían existiendo, hasta hace unos años nos podía resultar extraño pensar en coches que pudieran conducir solos o medicamentos que pudieran sustituir a pruebas médicas más invasivas. Esto ya es una realidad. Los avances tecnológicos lo han hecho posible y aunque la cantidad de objetos inteligentes en el mundo no ha crecido tanto como se auguraba en un primer momento, el número de dispositivos sigue creciendo y se sigue trabajando para dar solución a desafíos que en un futuro puedan ralentizar el crecimiento de éstos, como pueden ser el ahorro de energía para que las baterías duren el mayor tiempo posible, o alternativas para que las redes soporten el flujo de millones de dispositivos conectados.

Las áreas de aplicación del Internet de las Cosas son amplias. Desde el medio ambiente hasta "Ciudades inteligentes", será inevitable la utilización de algún objeto del IoT. Cada vez resulta más extraño llevar un reloj que solo nos dé la hora, como en su momento comenzó a resultarlo llevar un móvil que sólo sirviera para llamar por teléfono. Empresas privadas y públicas, gobiernos de distintos países, están fomentando su uso dado los beneficios que el IoT trae consigo como es el caso de dispositivos de Internet de las Cosas médicas.

En el Iot en el campo de la salud hemos profundizado en este trabajo, revisando las ventajas que estos dispositivos pueden suponernos: mejora de la calidad de vida, independencia y autonomía de los pacientes, reducción de costes sanitarios… un cambio en la relación entre el médico y el paciente y un mayor control del paciente sobre su salud son dos de los aspectos más importantes que supone la inmersión del IoT en el campo de la medicina y el aumento de información que se podrán tratar y a los que podremos acceder.

La información y la protección de los datos de los usuarios y su privacidad es, precisamente, una de las amenazas más importantes del IoT en cualquier área de aplicación. El aumento de datos y su tratamiento y el aumento de actores que puedan acceder a ellos hace que haya que prestar atención a este desafío por parte de todas las partes implicadas.

- Pérdida de autonomía por parte de los usuarios. Objetos conectados facilitarán la vida de las personas, a la vez corremos el riesgo de volvernos esclavos de esos objetos necesitando constantemente acceso a redes, enchufes para cargar la batería etc.
- Pérdida de control de nuestros datos. Conocer dónde están o para qué están siendo usados y tener la opción de cancelar, actualizar, en resumen utilizar nuestros derechos sabiendo la forma en que podemos hacerlo.
- Derecho a decidir. El uso de estos dispositivos puede hacer que nos convirtamos en "dependientes" de sus proveedores o fabricantes si no ofrecen alternativa a sus productos o actualizaciones.

- Robo de identidad. Cada vez es mayor la cantidad de datos que diversos objetos pueden dar de nosotros, a su vez muchos de ellos pueden bien por características del dispositivo bien porque se cruzan con otros datos, identificar a los dueños de la información. Esta es una gran amenaza ya que pueden sacarse patrones de comportamiento que hagan peligrar nuestra intimidad o faciliten el robo de nuestra identidad.
- Sobrecarga de datos. La sobrecarga de información puede hacer que nuestros comportamientos cambien. Tener acceso constantemente a estos datos puede resultar una presión para nosotros y vernos influenciados por ellos.
- Control de dispositivos. El acceso a nuestros datos puede hacer que hackers accedan a nuestros dispositivos y se hagan con el control afectándonos sin que nos demos cuenta. Hasta el dispositivo más "corriente" obtiene información de nosotros y es vulnerable de ser hackeado.
- Usos "poco éticos" de nuestra información. La cantidad de datos que puede dar un dispositivo puede hacer que, aun usándolos de forma legal, puedan ser poco éticos. Esto puede ocurrir con las aseguradoras, por ejemplo, si realizan una discriminación de datos, o las fuerzas de seguridad que podrán acceder a los registros de los objetos.
- Rastreo y seguimiento del individuo.

Son múltiples las amenazas de pérdida de información y múltiples las consecuencias que pueden tener, en este caso, relacionado con dispositivos médicos, nuestra salud puede estar en juego. La necesidad de abordar las amenazas que el IoT supone para la seguridad de nuestros datos es prioritaria. En este trabajo se ha profundizado en las herramientas legales vigentes para minimizarlas. Dado el rápido avance de las tecnologías se está trabajando para adaptar el marco legal al Internet de las Cosas aunque parece que esta última va más lenta. Nuevos Reglamentos también revisados en este trabajo entrarán en vigor en 2018 abordando nuevas amenazas de los objetos conectados que, conjunto con el GT29 de la Unión Europea, abogan por ser proactivos ante las amenazas y aplicar medidas de prevención por parte de los actores implicados en el ecosistema IoT. Sea como sea las autoridades deben tener presente que muchos de los problemas están por llegar y dependerán del uso de los dispositivos y la cantidad de personas usándolos, por ello no debemos bajar la guardia.

Tras la realización de este trabajo mi conclusión personal es que el Internet de las Cosas es un avance inminente al que debemos acostumbrarnos estemos o no preparados.

- El IoT necesita afrontar necesariamente desafíos técnicos si se quieren utilizar gran cantidad de dispositivos conectados tal y como dicen la predicciones. En algunos aspectos se está trabajando en ello, buscando soluciones o alternativas a las ya existentes. Los gobiernos no pueden olvidar que fomentar el IoT requiere la responsabilidad de crear la infraestructura necesaria para poder utilizarlo. Es su

responsabilidad asumir ese reto teniendo en cuenta la cantidad de lugares que no tienen acceso a internet o lo tienen muy limitado.

- Respecto a la protección de datos, en primer lugar creo necesario que toda la sociedad adquiera conciencia de la importancia que tiene que sus datos estén protegidos y las consecuencias que puede entrañar que no lo estén. Debemos saber los derechos que tenemos sobre la protección de datos, las responsabilidades y donde acudir en caso de que no se cumplan. Creo que por ahora defender la privacidad de nuestros datos es algo a lo que no damos la suficiente importancia o prioridad, asumiendo ciertos comportamientos (Como la cesión de datos que no tienen que ver con el fin) y esto puede hacer que no estemos preparados para la llegada del IoT donde precisamente la protección de datos es una de las grandes amenazas. Por otro lado, después de analizar el marco legal vigente y futuro, creo que aunque se esté haciendo un buen trabajo al respecto, es necesario que las empresas se preocupen y no sólo hagan actos de buena fe. Es necesaria la inversión en seguridad hardware y software y un uso de los datos ético. La sociedad debe entender que la seguridad y la privacidad de los usuarios debe estar por encima del beneficio económico y, respecto a cuerpos de seguridad del estado, no traspasar la línea entre la seguridad y el control.
- Aún con lo dicho en el punto anterior, me resulta complicada la idea de conseguir que todos los derechos de las usuarias respecto a la protección de datos se cumpla cuando el número de objetos conectados crezca y esté por todas partes. Imaginemos una casa inteligente de alquiler y que el dueño deba informar, solicitar el consentimiento a sus inquilinos e informar al fabricante de su nevera inteligente, lavadora inteligente, persianas... Ciudades con sensores y cámaras se llenarán de carteles indicando que nos están grabando, por ejemplo. Si las predicciones se cumplen corremos el riesgo de caer en una tela de araña de informaciones, consentimientos, solicitud de datos, registros, contraseñas…
- El IoT puede crear una brecha mayor de desigualdad entre la sociedad. La explosión de estos nuevos dispositivos y el intento de integración en todas las áreas pueden hacer que nos olvidemos de sectores de la población que no están familiarizados con este tipo de objetos. Ancianos o personas que no tengan conocimientos informáticos podrían resultar perjudicados por al no utilizarlos o ser más vulnerables a ataques o pérdida de datos ya que una de los factores que implica la seguridad de estos objetos es la responsabilidad por parte de los usuarios.
- La realización de este trabajo, el avance de la tecnología y todos los nuevos dispositivos que se están creando relacionados con el IoT me hacen preguntarme si estaremos demasiado preocupados en buscar objetos nuevos que puedan fabricarse que en ir haciendo que nos adaptemos a los ya existentes. La irrupción de dispositivos conectados en el campo de la salud, por ejemplo, hará que médicos, pacientes, cuidadores y demás profesionales, deban cambiar su forma de trabajar o actuar. Se deberá replantear por ejemplo, la forma de los sanitarios de trabajar en un hospital

inteligente enseñando qué hacer ante problemas tecnológicos. ¿Estamos proyectando a largo plazo sin fijarnos en el momento actual del IoT?

Es obvio que las ventajas que el IoT trae son múltiples no podemos por el miedo a las nuevas amenazas identificadas o todavía por venir, no utilizar los avances tecnológicos siempre que podamos. Tenemos experiencia en afrontar este tipo de "revoluciones tecnológicas", ya lo hicimos con la llegada de Internet (guardando las distancias entre lo que supone uno y tro). Las líneas sobre las que hay que trabajar son claras y pasan por una puesta en común y un trabajo conjunto de todas las partes interesadas: gobiernos, fabricantes de dispositivos, desarrolladores, usuarias… Interesante también como un nuevo modelo de trabajo. Quizá, por todos los riesgos expuestos anteriormente, creo difícil la integración de forma masiva del IoT a corto plazo si bien tampoco creo que esta integración vaya a ocurrir, por tanto, podemos de forma progresiva adaptarnos a la llegada de objetos inteligentes trabajando de forma paralela en aspectos como la regulación, seguridad, concienciación del uso, etc.

8 BIBLIOGRAFÍA

BRUNO CENDÓN. *El Origen Del IoT*. 2017. Disponible en línea: http://www.bcendon.com/el-origen-del-iot/ [Consulta: 21/01/2017]

CISCO. The Internet of Things: Reduce Security Risks with Automated Policies. 2015. Disponible en línea en: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/security-risks.pdf [Consulta 01/05/2017]

IJESC Articulo de investigación Vol. 6 Núm. 5. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. 2016. Disponible en línea en: http://ijesc.org/upload/8e9af2eca2e1119b895544fd60c3b857.Internet%20of%20Things-IOT%20Definition,%20Characteristics,%20Architecture,%20Enabling%20Technologies,%20Application%20&%20Future%20Challenges.pdf [Consulta 16/04/2017]

JUAN CAZILA, ROBERTO JUNCO. Descubriendo Internet of Things. Segunda edición. 2015. Disponible en línea en: http://www.mazbit.com/cisco/temp/2014-12-16_iot_ebook_es/2014-12-16_iot_ebook_es.pdf [Consulta 02/05/2016]

INTERNET SOCIETY . Karen Rose, Scott Elddridge, Lyman Chapin. The Internet of things: an overview. 2015. Disponible en línea en: https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf [Consulta 01/05/2017]

DEFENSOR DEL PUEBLO DE NAVARRA. Francisco Javier Enériz Olaechea, Juan Luis Beltrán Aguirre. La protección de los datos de carácter personal. 2012. Disponible en línea en: http://docplayer.es/7023462-La-proteccion-de-los-datos-de-caracter-personal.html [Consulta 12/01/2017]

SMART ACTION. Policy paper on IoT future Technologies. 2014. Disponible en línea en: https://www.smart-action.eu/fileadmin/smart-action/publications/Policy_Paper_on_IoT_Future_Technologies.pdf [Consulta 01/05/2017]

THE ECONOMIST. The Internet of things business index 2017. 2017. Disponible en línea en: https://www.eiuperspectives.economist.com/sites/default/files/EIU-ARM-IBM%20IoT%20Business%20Index%202017%20copy.pdf [Consulta: 14/04/2017]

LA PIEDRA DE SISIFO. Autor: Marcos Martínex. “El primer objeto conectado a internet fue una tostadora”. 2016. Disponible en línea: http://lapiedradesisifo.com/2016/12/19/iot-tostadora/ [Consulta: 21/01/2017]

Muycanal, Verónica Cabezudo “La historia de Internet of Things”. 2014. Disponible en línea: http://www.muycanal.com/2014/03/01/historia-internet-of-things [Consulta: 21/01/2017]

CISCO, the network (Cisco´s Technology News Site), Kevin Maney. "Kevin Ashton, father of the Internet of Things & Network Trailblazer". 2014. Disponible en línea: https://newsroom.cisco.com/feature-content?articleId=1558161 [Consulta: 21/01/2017]

CISCO. Dave Evans. Internet de las cosas. Cómo la próxima evolución de Internet lo cambia todo. 2011. Disponible en línea: http://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf [Consulta: 18/01/2017]

SORAYA PANIAGUA. "Un poco de historia sobre Internet de las Cosas". 2012. Disponible en línea: http://www.sorayapaniagua.com/2012/04/15/un-poco-de-historia-sobre-internet-de-las-cosas/ [Consulta: 21/01/2017]

SHAWN DUBRAVAC, CARLO RATTI. Internet de las Cosas: ¿Evolución o revolución? Parte 1. 2015. Disponible en línea: https://www.aig.com/content/dam/aig/america-canada/us/documents/brochure/aig-iot-spanish-report.pdf [Consulta: 01/05/2017]

CASAGRAS. RFID and the inclusive model for the Internet of Thisgs. 2009. Disponible en línea en: https://docbox.etsi.org/zArchive/TISPAN/Open/IoT/low%20resolution/www.rfidglobal.eu%20CASAGRAS%20IoT%20Final%20Report%20low%20resolution.pdf Consuta: [12/01/2017]

TICBEAT. Reducir el uso de energía en transmisores del Internet de las Cosas. 2015 Disponible en línea: http://www.ticbeat.com/tecnologias/reducir-el-uso-de-energia-en-transmisores-del-internet-de-las-cosas/ [Consulta: 01/05/2017]

PWC. The Wearable Life 2.0 Connected living in a wearable world. 2016. Disponible en línea en: http://www.pwc.com/us/en/industry/entertainment-media/assets/pwc-cis-wearables.pdf [Consulta: 23/01/2017]

TICBEAT: Alberto Iglesias Fraga. 2017 Internet de las Cosas: 8400 millones de dispositivos conectados cuando acabe 2017. Disponible en línea en: http://www.ticbeat.com/innovacion/internet-de-las-cosas-8400-millones-dispositivos-conectados-2017/ [Consulta: 23/01/2017]

OASYS (OUTSORUCING AUTOMATION SYSTEMS). Situación actual y retos de futuro del mercado del IoT en España y Europa. 2017. Disponible previo registro Oasys [Consulta: 25/01/2017]

HUAWEI. Creación de un mundo IoT fiable y gestionado. 2017. Disponible en línea en: http://huaweispain15.com/notas/libro-blanco-ciberseguridad-IoT.pdf [Consulta: 01/05/2017]

Antonio J. Jara, Latif Ladid, Antonio Skarmeta. The Internet of Everything throught IPv6: An Analysis of Challenges, Solutiones and Opportunities. 2013. Disponible en línea en:

https://pdfs.semanticscholar.org/962f/e4c4069ac2540368fad56d7a863abdd15a77.pdf [Consulta 09/05/2017]

ARANCA. Dr Yogesh Shelke & Arpit Sharma. 2016. Internet of medical things. Disponible en línea en: http://context.aranca.com/hubfs/Aranca_Reports/Internet_of_Medical_Things_IoMT_Aranca_Special_Report.pdf [Consulta 25/03/2017]

GAMALTO SECURITY TO BE FREE. A safer Internet of Things. 2016. Disponible en línea en: http://www.gemalto.com/brochures-site/download-site/Documents/iot-security-ebook.PDF [Consulta 02/05/2017]

CENTRO DE ESTUDIOS EN LIBERTAD DE EXPRESIÓN Y ACCESO A LA IINFORMACIÓN. Carlos Cortés. El Internet de las cosas: Más Internet que otra cosa. Disponible en línea en: https://es.scribd.com/document/284623102/Internet-de-las-Cosas [Consulta 14/01/2017]

EUROPA PRESS. La inversión IoT en España alcanzará los 23.000 millones en 2020, según IDC. Disponible en línea: http://www.europapress.es/economia/noticia-inversion-iot-espana-alcanzara-23000-millones-2020-idc-20170405142959.html [Consulta: 25/01/2017]

POLITÉCNICA. Seguridad en el Internet de las cosas. 2015. Disponible en línea en: http://www.cait.upm.es/vigilancia_tecnologica/pluginfile.php/228/mod_resource/content/2/Seguridad%20Internet%20de%20las%20Cosas%20%28versi%C3%B3n%20Final%29.pdf [Consulta 17/01/2017]

THE ECONOMIST INTELLIGENCE UNIT. Jessica Twentyman. The Internet of Things business index 2017. 2017. Disponible en línea: https://www.eiuperspectives.economist.com/sites/default/files/EIU-ARM-IBM%20IoT%20Business%20Index%202017%20copy.pdf [Consulta: 28/01/2017]

EUROPEAN COMMISSION, JOINT RESERACH CENTRE. Ricardo Neisse, Gianmarco Badini, Gary Steri, Vincent Mahieu. 2016. Informed consent in Internet of Things: the Case Study of Cooperative Intelligent Transport System. [Consulta: 15/05/2017]

EVERIS. The Truth of IoT ecosystem. 2016. Disponible en línea: http://newsletter.everis.com/marketing/Documents/Newsletter%20Marketing/IoT/files/assets/common/downloads/The%20Truth%20Of%20IoT%20Ecosystem.pdf [Consulta: 28 /01/2017]

THE VALLEY. IoT: el futuro de las aplicaciones en los negocios. 2016. Disponible en línea: https://thevalley.es/blog/iot-futuro-las-aplicaciones-los-negocios/ [Consulta: 11/04/2017]

UNBLOGENRED.ES. El ecosistema de Internet de las cosas sigue creciendo: en 2017 recibirá un 15% más de inversión. 2016. Disponible en línea: http://www.unblogenred.es/el-ecosistema-de-internet-de-las-cosas-sigue-creciendo-en-2017-recibira-un-15-mas-de-inversion/ [Consulta: 11/04/2017]

TELEFÓNICA. Internet de Todo. 2017. Disponible en línea: https://www.openfuture.org/es/new/internet-de-todo-el-futuro-del-iot [Consulta: 25/01/2017]

ATKEARNEY. Thomas Kratzert, Hervé Collignon, Michael Broquist, Julien Vincent.The Internet of Things: a new path to Eurpoean prosperity. 2015 Disponible en línea: https://www.atkearney.com/documents/10192/7125406/The+Internet+of+Things-A+New+Path+to+European+Prosperity.pdf/e5ad6a65-84e5-4c92-b468-200fa4e0b7bc [Consulta: 13 /04/2017]

RICARDO VEGA. 6 Características clave del Internet de las cosas. 2015. Disponible en línea: https://ricveal.com/blog/6-caracteristicas-clave-del-internet-de-las-cosas/ [Consulta:21 /03/2017]

WEBMASTER CHAKRAY. 5 Requerimientos de una arquitectura IoT. 2016. Disponible en línea: http://www.chakray.com/5-requesitos-de-una-arquitectura-iot/ [Consulta 21/003/2017]

JOSÉ ANDRÉS LÓPEZ. Sensores (Sensors) vs Actuadores (Actuators). 2015. Disponible en línea: http://www.tuataratech.com/2015/06/sensores-sensors-vs-actuadores-actuators_8.html [Consulta 21/03/2017]

MONOLITIC. Plataformas en la nube para IoT. 2016. Disponible en línea: https://es.slideshare.net/Monolitic/plataformas-en-la-nube-para-iot Consulta 21/03/2017]

ERMESH. E. Rico. Características principales de un Gateway para Internet de las Cosas. 2017 Disponible en línea en: http://www.ermesh.com/caracterisiticas-gateway-internet-de-las-cosas/ [Consulta 21/03/2017]

EXPANSIÓN. ¿Qué impacto tendrá el Internet de las Cosas en el medio ambiente? 2015. Disponible en línea: http://www.expansion.com/economia-digital/innovacion/2015/12/10/566995ed22601d6c0b8b4650.html [Consulta 21/03/2017]

TELEFÓNICA BUSINESS Solutions. 5 maneras en las que el IoT está ayudando al medio ambiente. 2016. Disponible en línea en: https://iot.telefonica.com/blog/5-maneras-en-las-que-el-iot-esta-ayudando-al-medio-ambiente [Consulta 21/03/2017]

WHITEWALL ENERGY. José González. IoT en la industria de las energías renovables. 2016. Disponible en línea en: http://whitewallenergy.com/es/blog/iot-en-la-industria-de-las-energias-renovables/ [Consulta: 22/03/2017]

AGROINFORMACIÓN.COM. Proyecto europeo para mejorar la productividad y sostenibilidad de la agricultura por Internet. 2016. Disponible en línea en: http://www.agroinformacion.com/proyecto-europeo-mejorar-la-productividad-sostenibilidad-la-agricultura-internet/ [Consulta: 26/03/2017]

INCIPY. Internet of things (IoT) en la transformación digital de las empresas. 2016. Disponible en línea previo registro en:

http://www.fundacionseres.org/Lists/Informes/Attachments/987/150923%20internet-of-things.pdf [Consulta 18/03/2017]

C&WNETWORKS. IPV6: Un eslabón clave en el despliegue de Internet de las Cosas. 2016. Disponible en línea en: https://www.cwnetworks.com/blog_es/ipv6-un-eslabon-clave-en-el-despliegue-de-internet-de-las-cosas/ [Consulta 23/03/2017]

EVALUANDO SOFTWARE. Campos de aplicación de Internet of Things o Internet de las cosas. 2015. Disponible en línea: http://www.evaluandosoftware.com/campos-de-aplicacion-de-internet-of-things-o-internet-de-las-cosas/ [Consulta 28/03/2017]

REPORTEDIGITAL. Fernando Santamaría. Panorama del Internet de las Cosas en la Industria 4.0. 2016. Disponible en línea: http://reportedigital.com/iot/internet-cosas-industria-4-0/ [Consulta: 22/03/2017]

AGENCIA ESTATAL BOLETÍN OFICIAL DEL ESTADO. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. 2016. Disponible en línea en: https://www.boe.es/doue/2016/119/L00001-00088.pdf [Consulta 19/01/2017]

NOTICIAS JURÍDICA. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, realtio a la protección de las personas físicas. 2016. Disponible en línea en: http://noticias.juridicas.com/base_datos/Privado/574082-regl-2016-679-ue-de-27-abr-proteccion-de-las-personas-fisicas-en-lo-que.html#a7 [Consulta 19/01/2017]

ISONOR GRUPO. HERRERO & ASOCIADOS. El nuevo Reglamento (UE) 2016/679 General de Protección de Datos entrará en vigor en 2018. Disponible en línea en: http://www.grupoisonor.es/noticias/el-nuevo-reglamento-ue-2016679-general-de-proteccion-de-datos-entrara-en-vigor-en-2018 [Consulta 21/01/2017]

BOLETION OFICIAL DEL ESTADO. Protección de Datos de Carácter Personal . Edición actualizada en 2016. https://es.scribd.com/document/255797175/BOE-055-Proteccion-de-Datos-de-Caracter-Personal-pdf [Consulta: 10/01/2017]

JAVIER PARDO FALCON. Los Derechos del Artículo 18 de la Constitución Española en la jurisprudencia del Tribunal Constitucional. 1992. Disponible en línea: https://dialnet.unirioja.es/descarga/articulo/79453.pdf [Consulta 27/01/2017]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Protección de Datos: Guía para el Ciudadano. 2015. Disponible en línea en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO.pdf [Consulta 27/02/2017]

ABEL LOZOYA DE DIEGO, MARÍA TERESA VILLALBA DE BENITO Y MARÍA ARIAS POU. Taxonomía de información personal de salud para garantizar la privacidad de los individuos. 2016. Disponible en línea: http://www.elprofesionaldelainformacion.com/contenidos/2017/mar/16.pdf [Consulta 14/04/2017]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Nota informativa: Las Autoridades europeas de protección de datos aprueban el primer Dictamen conjunto sobre Internet de las Cosas. 2014. Disponible en línea: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2014/notas_prensa/common/sep_14/140924_NP_AEPD_Dictamen_IoT.pdf [Consulta 14/04/2017]

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA VOL. 4 NÚM. 2. Paula Jervis Ortiz. 2015. Disponible en línea en: www.rchdt.uchile.cl/index.php/RCHDT/article/download/37509/40366 [Consulta 15/04/2017]

INTEL SECURITY. La Internet de las Cosas en la atención sanitaria: oportunidades y riesgos. 2015. Disponible en línea: https://www.mcafee.com/mx/resources/.../rp-healthcare-iot-rewards-risks-summary.pd... [Consulta: 01/05/2017]

IFT. INSITITUO FEDERAL DE TELECOMUNICACIONES. María Elena Estavillo Flores.Internet de las Cosas: retos para su desarrollo. 2016 Disponible en línea: www.comenor.org.mx/Documentos/2016/12.pdf [Consulta 01/05/2017]

ESTHER MARÍA NODA CAMACHO. Internet de las Cosas: Beneficios y privacidad, un difícil equilibrio. 2013. Disponible en línea en: http://docplayer.es/19451537-Titulo-internet-de-las-cosas-beneficios-y-privacidad-un-dificil-equilibrio.html [Consulta 04/05/2017]

EUROPEAN COMMISSION. Article 29 Data protection working party. Opinion 8/2014 on the on Recent Developments on the Internet of Things. 2014. Disponible en línea en: www.dataprotection.ro/servlet/ViewDocument?id=1088 [Consulta 04/05/2017]

CSIRT-CV. Seguridad en Internet de las Cosas. Estado del arte. 2014. Disponible en línea en: http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf [Consulta 04/05/2017]

COMISIÓNEUROPEA. IoT Privacy, Data Protection, Information Security. 2015 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1753 [Consulta 04/05/2017]

REVISTA INGE CUC, Vol. 8, Núm 1. Alejandro Cama, Emiro De la Hoz, Dora Cama. Las redes de sensores inalámbricos y el Internet de las Cosas. 2012. Disponible en línea en: https://dialnet.unirioja.es/descarga/articulo/4869014.pdf [Consulta: 13/03/2017]

RIVER PUBLISHERS SERIES IN COMMUNICATIONS. Varios colaboradores. Internet of Thingscomperging Technologies for smart Environments and Integrated Ecosystems. 2013. ISBN:978-87-92982-96-4 (E-Book) Página 204. Disponible en línea en: http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf [Consulta: 07/04/2017]

FUNDACIÓN DE LA INNOVACIÓN BAKINTER. Eva López Suárez. Cynthia Gregsamer, Javier Corsini Ramírez. El Internet de las Cosas. En un mundo conectado de objetos inteligentes.

2011. Disponible en línea en: http://www.belt.es/expertos/imagenes/XV_FTF_El_internet_de_las_cosas.pdf [Consulta: 14/04/2017]

NOTICIAS JURÍDICAS. Carlos FH. Contenido y novedades del Reglamento general de protección de datos de la UE (Reglamento UE 2016/679 de 27 de abril de 2016. 2016. Disponible en línea en: http://noticias.juridicas.com/actualidad/noticias/11050-contenido-y-novedades-del-reglamento-general-de-proteccion-de-datos-de-la-ue-reglamento-ue-2016-679-de-27-de-abril-de-2016/ [Consulta 15/04/2017]

DIARIO OFICIAL DE LAS COMUNIDADES EUROPEAS. Directiva 95/46/CE del Parlamento Europeo y del Consejo. 1995. Disponible en línea en: http://www.wipo.int/edocs/lexdocs/laws/es/eu/eu188es.pdf [Consulta 15/04/2017]

EY BUILDIGN A BETTER WORKING WORLD. Cybersecurity and the Internet of Things. 2015. Disponible en línea en: http://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the-internet-of-things/$FILE/EY-cybersecurity-and-the-internet-of-things.pdf [Consulta 01/05/2017]

DELF UNIVERSITY OF TECHNOLOGY. Jeroen van den Hoven. FACT SHEET – ETHICS SUBGROUP IoT – Version 4.0. 2012. Disponible en línea en: https://pdfs.semanticscholar.org/d887/01968142b7b34198895ec923ed4c12c784d7.pdf?_ga=2.161077624.479968101.1497381763-1672350341.1497381763 [Consulta 15/04/2017]

LA RAZÓN.ES. Pilar Pérez. <<Wearables>> saludables: Los médicos comienza a <<prescribir>> dispositivos tecnológicos. 2017. Disponible en línea en: http://www.larazon.es/atusalud/salud/wearables-saludables-los-medicos-comienzan-a-prescribir-dispositivos-tecnologicos-BF14555884 [Consulta 24/05/2017]

IBM developerWorks. DE qué forma ha construido Grush un cepillo de dientes inteligente utilizando la arquitectura IoT de IBM Cloud Architecture Center. 2016. Disponible en línea en: https://www.ibm.com/developerworks/ssa/cloud/library/cl-grush-smart-toothbrush-bluemix-trs/index.html [Consulta 26/05/2017]

HARVARD BUSINESS REVIEW STAFF. With Big Data Comes Big Responsability. 2014. Disponible en línea en: https://hbr.org/2014/11/with-big-data-comes-big-responsibility [Consulta 18/04/2017]

CENTRO DE ESTUDIOS DE CONSUMO. Isabel Koutsourais Fernández. Nuevas modalidades de servicios médicos. E-HEALTH y M-HEALTH: fronteras legales y espacios de ejercicios. 2015. Disponible en línea en: https://blog.uclm.es/cesco/files/2015/04/Nuevas-modalidades-de-servicios-m%C3%A9dicos.pdf [Consulta 02/04/2017]

U.S. DEPARTMENT OF HOMELAND SECURITY. Version 1.0. Strategic principles for securing the Internet of Things (IOT). 2016. Disponible en línea en: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf [Consulta 16/04/2017]

WIPRO APPLYING THOUGHT. Akash Shrivastava. Nextgen pharma takes "Smart" strides with internet of things. 2015. Disponible en línea en: http://www.wipro.com/documents/nextgen-pharma-takes-smart-strides-with-internet-of-things.pdf [Consulta 30/03/2017]

HIBERUS LEGALTECH. Susana González Ruizsanchez. Datos personales en EEUU tras el escudo de privacidad: Privacy Shield. 2016. Disponible en línea en: https://www.hiberus.com/legaltech/blog/datos-personales-eeuu-privacidad-privacy-shield/ [Consulta: 30/05/2017]

TELEFÓNICA. Grupo de Ciberseguridad de IoT. "Alcance, escala y riesgo sin precedentes: asegurar el Internet de las Cosas". 2016. Disponible en línea en: https://www.telefonica.com/documents/23283/5538439/Telef%C3%B3nica_Security_IoT_Spanish.pdf/5137cc8e-e572-44c8-aecd-2f29f3f236be [Consulta 23/04/2017]

MADRIDMASD. Autores: Javier I. Portillo García, Ana Belén Bermejo Nieto y Ana M. Bernardos Barbolla. Informe de vigilancia tecnológica. Tecnología de identificación por radiofrecuencia (RFID): aplicaciones en el ámbito de la salud. 2016. Disponible en línea en: http://www.madrimasd.org/uploads/informacionidi/biblioteca/publicacion/doc/VT/_VT13_RFID.pdf [Consulta 17/05/2017]

BAKINTER. Autora: Lorena Carrillo. 2017. Disponible en línea en: https://www.fundacionbankinter.org/documents/20183/97216/Salud++Digital+ES/5f5bd348-ca10-49de-8bfe-2ba368a2e269 [Consulta 19/05/2017]

DLA PIPER. Data protection laws of the workd. 2014.

BDV Big Data Value Association. Big data technologies en cuidado de la salud. Necesidades, posibilidades y retos. 2016. Disponible en línea en: http://www.bdva.eu/sites/default/files/Big%20Data%20Technologies%20in%20Healthcare.pdf [Consulta 27/05/2017]

ETHICS INF TECHNOL. David Wright. A framework for the ethical impact assessment of information technology. 2010. Disponible en línea: https://www.researchgate.net/publication/225629433_A_framework_for_the_ethical_impact_assessment_of_information_technology [Consulta 27/05/2017]

IJESC. Keyur K Patel, Sunil M Pater. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. 2016. Disponible en línea en: http://ijesc.org/upload/8e9af2eca2e1119b895544fd60c3b857.Internet%20of%20Things-IOT%20Definition,%20Characteristics,%20Architecture,%20Enabling%20Technologies,%20Application%20&%20Future%20Challenges.pdf [Consulta 16/04/2017]

BECK EJ, GILL W. and DE LAY PR.Protecting the Privacy, Confidentiality and Security of Personally Identifiable Health Information: extended bibliography. 2014. Disponible en línea en: http://journals.co-action.net/index.php/gha/article/downloadSuppFile/32089/31942 [Consulta 18/05/2017]

REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA Y SALUD. Transformación digital del sector salud. 2016. Disponbile en línea: http://www.seis.es/imagenes/REVISTAS/118.pdf [Consulta 22/05/2017]

SASHA MARSCHANG, EPHA. Health inequalities and eHealth. 2014. Disponible en línea en: file:///C:/Users/Teresa/Downloads/eHealthInequalitiesreportEHSG%20(1).pdf [Consulta 20/05/2017]

LITMOS HEALTHCARE DIVISION. Amit Garg, CISSP, PMP, MBCI. 2016. El Internet de las Cosas: Impactos en la Salud. Seguridad y privacidad. Disponible en línea en: https://www.litmos.com/healthcare/demo/ [Consultado 27/05/2017]

JORNADAS APDIS UNIVERSIDAD DE COIMBRA. Julio Alonso Arévalo. Aplicaciones móviles en medicina y salud. 2016 Disponible en línea: https://gredos.usal.es/jspui/bitstream/10366/130118/1/Aplicaciones%20m%C3%B3viles%20en%20medicina%20y%20salud.pdf [Consulta: 30/05/2017]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Guía del derecho fundamental a la protección de datos de carácter personal. 2004. Disponible en línea: http://www.agpd.es/portalwebAGPD/common/FOLLETO.pdf [Consulta: 18/01/2017]

NOTICIAS JURÍDICAS. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Portal de búsqueda disponible en línea: http://noticias.juridicas.com/base_datos/Admin/lo15-1999.t6.html#t6 [Consulta: 18/01/2017]

JULIO CÉSAR MIGUEL PÉREZ. ISBN: 978-84-9964-560-5. Páginas 272. 2015 4ª Edición actualizada. Protección de datos y seguridad de la información.

FREESCALE. David Niewolny. 2013. How the Inteernet of Things Is Revolutionizing Healthcare. Disponible en línea en: https://cache.freescale.com/files/corporate/doc/white_paper/IOTREVHEALCARWP.pdf [Consulta 27/05/2017]

T6.2 JASEHN – proyecto de la versión 2. El marco legal y orientación sobre la protección de datos en Servicios de Información Transfronterizo de salud (CBeHIS). 2016.

PAN ERUOPEAN NETWORKS: GOVERNMENT. Smart cities & IOT. 2016. Disponible en línea en: http://www.theinternetofthings.eu/sites/default/files/GOV18%20R%20van%20Kranenburg%206007_ATL.pdf [Consulta 24/05/2017]

COGNIZANT. How the Internet of Tings is transforming medical devices. 2016. Disponible en línea en: https://www.cognizant.com/whitepapers/how-the-internet-of-things-is-transforming-medical-devices-codex1945.pdf [Consulta 14/05/2017]

COMISIÓN EUROPEA. 2014. Green paper on mobile Health ("mHealth"). Disponible en línea en: https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth [Consulta 28/05/2017]