Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

Privacy of Things: La protección de datos en la era de la interconexión digital.

Trabajo fin de estudio presentado por:	Álvaro Miguel Morandeira
Tipo de trabajo:	Trabajo de Fin de Máster
Director/a:	Nicomedes Rodríguez Gutiérrez
Fecha:	21/07/2022

Resumen

En este Trabajo de Fin de Máster (TFM), elaborado bajo el ámbito de estudio del Máster Universitario de Protección de Datos de la Universidad Internacional de la Rioja, se realizará un análisis en profundidad de uno de los retos actuales más importantes para la defensa efectiva de la protección de datos, la masificada interconexión digital que está sufriendo la sociedad actual, así como las posibles problemáticas o riesgos que esta puede ejercer sobre la protección de nuestros datos personales. Este fenómeno, tan extendido hoy en día, penetra e infiere diagonalmente en la esfera privada de las personas de formas que no podían preverse jurídicamente hace menos de diez años. Con cada nuevo avance, o desarrollo tecnológico, activamente implementado en nuestra sociedad, especialmente en cuanto a los llamados dispositivos de uso personal "Wearables" o asistentes personales como "Alexa" o "Siri" al servicio de multinacionales privadas, los ciudadanos se ven frecuentemente inmersos en un incómodo dilema puesto ante ellos: el acceso a facilidades y servicios de última generación para la mejora de nuestro día a día, o la certeza de una preservación segura de la integridad total de nuestros derechos a la privacidad y la protección de nuestros datos personales.

Palabras clave: Internet of Things, Protección de Datos, Privacidad, Seguridad, *Privacy by design, Privacy by default.*

Abstract

In this Master's Thesis (TFM), prepared under the scope of study of the Master's Degree in Data Protection of the International University of La Rioja, an in-depth analysis will be made of one of the most important current challenges for the effective defence of data protection, the massive digital interconnection that today's society is undergoing, as well as the possible problems or risks that this may pose to the protection of our personal data. This phenomenon, which is so widespread nowadays, penetrates and intrudes diagonally into the private sphere of individuals in ways that could not have been legally foreseen less than ten years ago. With every new technological advance, or development, actively implemented in our society, especially regarding the so-called wearable devices or personal assistants such as "Alexa" or "Siri" in the service of private multinationals, citizens are often immersed in an uncomfortable dilemma placed before them: access to state-of-the-art facilities and services for the improvement of our day-to-day life, or the certainty of a secure preservation of the full integrity of our rights to privacy and protection of our personal data.

Keywords: Internet of Things, Data Protection, Privacy, Security, *Privacy by design, Privacy by default*.

Índice de contenidos

1. Introducción

Los recientes avances de las tecnologías de la información y la comunicación (TIC) nos han empujado a vivir en un ambiente de revolución e innovación constantes; los procesos que hace algunos siglos tardaban décadas en generalizarse, e integrarse en el ADN de la sociedad, hoy en día requieren simplemente de años, o en algunos casos meros meses, para implementarse de forma efectiva. En el seno de este actual fenómeno, es innegable el esencial componente humano presente para su creación, sin embargo, no puede discutirse que el papel protagonista de su despliegue debe atribuirse necesariamente a las nuevas tecnologías, y a su rápida evolución como elemento esencial en el día a día sociedad contemporánea. Y es en el ojo del huracán de este continuo proceso de expansión y gestación de nuevas tecnologías donde encontramos el fenómeno conocido como «Internet de las Cosas» (Internet of Things, o referido por sus siglas inglesas IoT).

Hemos llegado a un punto en el que no es frecuente ver expresiones de sorpresa al afirmar abiertamente que nadie puede escapar hoy en día a la digitalización (Sebastian 2022), este fenómeno que nos rodea, y se extiende hasta las capas más profundas de nuestra intimidad, no es sino una consecuencia del concepto de «Internet de las Cosas», que por sí mismo está llegando a propiciar lo que algunos ya se refieren como la próxima gran trasformación en la evolución de Internet, asi como uno de los agentes de la “cuarta revolución industrial” (Barrio Andrés 2020)

Sin embargo, hemos posicionado al IoT como protagonista, pero aún no hemos definido en que consiste de forma concisa. Según algunos autores, el llamado IoT se considera como el fenómeno tecnológico que ha supuesto una evolución, desde una red interconectada de sistemas, a una red de objetos inteligentes interconectados. Estos objetos no solo pueden comunicarse entre sí, e interactuar a través de internet, sino que pueden ser controlados y monitoreados de forma remota por el usuario o alternativamente por otros dispositivos. Estas conexiones pueden llegar a crear “ecosistemas” interconectados, en donde múltiples objetos inteligentes pueden llegar a automatizar gran parte de los elementos, en las actividades cotidianas, de formas increíblemente variadas; desde la preparación del desayuno, hasta la

gestión de la agenda semanal de un gran empresario. Las limitaciones se encuentran únicamente hasta donde el software y el hardware implementado le permita llegar al sistema.

1.1. Justificación del tema elegido

La selección de este tema para la elaboración de este Trabajo de Fin de Máster se ha seleccionado, no solo por el apasionante estudio que puede hacerse sobre este campo tecnológico tan innovador y práctico desde la lente que proporciona el derecho, sino por la sustancial cantidad de problemáticas que esta implementación encuentra en su desarrollo de manera simultánea con el mantenimiento de un respeto a nuestro derecho fundamental a una protección de datos y una privacidad adecuados. Pues, a pesar de que la reciente normativa en materia de protección de datos, tanto europea como nacional, se configure de tal manera que pueda ser efectiva en su aplicación independientemente de los posibles avances tecnológicos, principio acuñado en el marco jurídico internacional como "neutralidad tecnológica"(Remolina Angarita 2014), en la práctica se nos presentan múltiples retos para adaptar las previsiones legales existentes a los siempre cambiantes escenarios tecnológicos.

1.2. Problema y finalidad del trabajo

Con la normalización de la interconexión digital se nos pueden suscitar múltiples preguntas: ¿Qué supondrá para nuestros derechos, y más concretamente nuestro derecho fundamental a la protección de datos, la generalización de un entorno conocido por ser históricamente hostil para los mismos?¿Cómo podremos protegernos ante una realidad que proporciona tantas puertas de acceso a nuestra vida privada, como dispositivos inteligentes hayamos incorporado a nuestro día a día?¿Qué puede deparar el futuro para una realidad que se actualiza a un ritmo muy superior al derecho que la ordena, a pesar de la búsqueda de una verdadera neutralidad tecnológica? Todas estas cuestiones no poseen simples respuestas, pero en este estudio, propiciado por la elaboración de este trabajo de fin de máster de la Universidad Internacional de la Rioja, intentaremos ofrecer argumentos suficientes para que todo lector pueda formar su propia opinión fundamentada al respecto.

1.3. Objetivos

La irrupción del IoT en la sociedad es un fenómeno indiscutible, sin embargo, su correcta implementación y regulación bajo los marcos legales vigentes en materia de protección de

datos supondrán desarrollar los correctos argumentos jurídicos que las fundamenten, asi como abordar ciertas medidas, tanto de técnicas y organizativas, para paliar los posibles riesgos que esta nueva tecnología supone.

Por tanto, el objetivo perseguido en el siguiente trabajo será el de encuadrar la posición del IoT en el marco normativo vigente, analizar sus posibles riesgos y amenazas para el derecho fundamental a la protección de datos y la privacidad de los usuarios, proponer las debidas medidas y soluciones adecuadas para con los riesgos inherentes y previsibles extraídos, y finalmente intentar dilucidar cual es el rumbo que podría tomarse en un futuro para integrar adecuadamente este nuevo fenómeno tecnológico que marcará un antes y un después en la forma que han realizado históricamente la obtención y tratamiento de datos.

2. Introducción al concepto de Internet of Things.

El término de IoT ha sido objeto de debate desde su primera concepción en 1999 por el tecnólogo Kevin Ashton para la multinacional Procter & Gamble, desde ese entonces se partió de la concepción de que se trataba de objetos interoperables identificables de forma única con tecnología de identificación por radiofrecuencia (RFID), confeccionándose en forma de sistemas donde objetos del mundo físico podrían conectarse a internet, automatizando la recogida de datos mediante sensores (Barrio Andrés 2020). Sin embargo, esta definición no tardo en evolucionar y desarrollarse, algunas definiciones contemporáneas han indicado que el Internet de las cosas (IoT) es una red conectada a dispositivos, en la que éstos se conectan de forma inalámbrica a través de sensores inteligentes (Pretz 2013), otras que se trata de un superconjunto de dispositivos, con capacidad de conexión, que son identificables de forma única mediante las técnicas existentes de comunicación de campo cercano (NFC) (Li, Xu and Zhao 2015). Tambien podemos encontrar la relevante descripción proporcionada en el Dictamen 8/2014 sobre la evolución reciente del Internet of Things , publicado en 2014 por el prestigioso Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, que define el concepto como "*una infraestructura en la que miles de millones de sensores integrados en dispositivos comunes y cotidianos - "cosas" como tales, o cosas vinculadas a otros objetos u objetos o individuos - están diseñados para registrar, procesar, almacenar y transferir datos y, al estar asociados con identificadores únicos, interactuar con otros dispositivos o sistemas utilizando las capacidades de la red*"(Article 29 Data Protection Working Party 2014).

Sin embargo, a día de hoy podemos afirmar que la obtención de una definición exacta y única es altamente improbable, debido a los constantes avances tecnológicos en la matrería, y a la perspectiva desde la cual sea definida. Por tanto, debemos aceptar que se trata de un concepto en proceso de constante de formación y las definiciones que expongamos aquí estarán indudablemente sujetas a diversos cambios y correcciones en el futuro.

Pese a este estado de cambio y redefinición constante, si nos viéramos obligados a clarificar de forma simplificada a día de hoy el IoT, deberíamos comenzar exponiendo su concepción básica: concretándose en la capacidad que adquieren determinados objetos cotidianos de estar equipados con capacidades de identificación, detección, conectividad en red, y procesamiento de datos que les permitan cumplir una determinada función predefinida,

permitiéndoles a su vez comunicarse entre sí y con otros dispositivos y servicios a través de Internet, para lograr algún objetivo útil (Whitmore, Agarwal and da Xu 2015)

Si nos detenemos un momento en esta última definición podemos encontrar varios componentes considerados como elementos nucleares del IoT, sin los cuales un determinado sistema perdería la capacidad de englobarse dentro de este fenómeno. Primeramente, es esencial para su correcta definición la existencia de un conjunto compuesto y plural de dispositivos u objetos cotidianos, ya que lo que define a un sistema es que no esté conformado únicamente por un solo componente. Seguidamente estos dispositivos deben tener cierta capacidad de procesamiento, es cierto que no todos ellos deben necesariamente poseer esta caracteristica, ya que ciertos componentes de un sistema pueden actuar como meros sensores o herramientas al servicio de otros componentes; sin embargo, deben existir varios dispositivos que sean capaces de procesar una concreta información. A continuación, siguiendo la aguda observación de Cassimally, debemos asegurarnos de que se da un determinado intercambio de información a través de internet entre los distintos componentes, para que los dispositivos que lo conforman "trabajen en el mundo de los datos"(McEwen and Cassimally 2014), ya que sin él no habría una verdadera comunicación por medio de la red, y no estaríamos hablando de un sistema de IoT sino de un sistema cerrado. Partiendo de este último concepto, debemos aclarar que para que un sistema trabaje de forma coordinada cada uno de sus elementos debe cumplir una función concreta dentro del proceso, en donde la suma de todos permita alcanzar el objetivo pretendido. Finalmente, debemos atender a este objetivo pretendido y útil, ya sea el realizar un determinado servicio o ejecutar una función productiva preestablecida; si el sistema no buscara realizar una función final el sistema carecería de propósito. Como podemos observar, todos estos elementos son considerados como esenciales para poder hablar de un sistema integrado en el IoT, si faltara alguno de ellos es probable que no pudiéramos ajustarnos a los requisitos funcionales de un sistema de estas características.

La filosofía original detrás de este fenómeno es evidente, su concepción surgió de la problemática generada por el tiempo requerido para introducir y trasferir ciertos datos en una cadena productiva, cuya automatización podría reducir y optimizar. Se planteó sí la eficiencia de un proceso concreto no podría aumentarse de obtener la información en cuanto a su estado, productividad y eficiencia directamente de los objetos que lo componen, permitiendo

de esta manera un seguimiento a tiempo real de la capacidad y las características de un proceso o servicio. Este planteamiento no solo podría solucionar evidentes problemas de la introducción manual de los datos, como son los errores en su incorporación o retrasos en su trasmisión, sino que consecuentemente se traduciría en un aumento considerable de la producción y en una posible reducción de costes a largo plazo.

No podemos pasar por alto que muchas de las tecnologías que establecieron los cimientos de los sistemas de IoT ya existían previa su adhesión a los mismos, y estaban siendo utilizadas individualmente en procesos industriales, este era el caso de las redes interconectadas de sensores, las redes de comunicación de campo cercano (NFC)[1], o las redes de identificación por radiofrecuencia (RFID)[2] (Li, Xu and Zhao 2015).Por tanto, podemos afirmar que el IoT, tal y como se configuró en su origen, representó una evolución del uso de ciertas tecnologías preexistentes, tanto en el número y los tipos de dispositivos involucrados en un sistema, como la interconexión de estas redes de dispositivos a través de Internet, con el fin de obtener una eficiencia de los resultados perseguidos en sus distintas disciplinas de aplicación. (Whitmore, Agarwal and da Xu 2015)

A pesar de su origen, la tecnología basada en sistemas de IoT es utilizada hoy en día en aplicaciones tremendamente diversas, y se implementa en sectores muy variados y diferenciados entre sí. Podemos encontrar dispositivos y sistemas interconectados, que utilizan la tecnología IoT formando parte de infraestructuras inteligentes en redes de plantas energéticas, midiendo el consumo y hábitos de los ciudadanos; en sistemas públicos competencia del estado, como en plantas depuradoras o sistemas de transporte público, o en controles de acceso a zonas limitadas o restringidas del entramado urbano en aplicación de planes ecológicos sectoriales, como se da en la Comunidad de Madrid con estrategia de sostenibilidad ambiental “Madrid 360”. Todas estas medidas podemos observar que tienden,

[1] La NFC es un estándar de comunicación de corto alcance en el que los dispositivos son capaces de establecer una comunicación por radio entre sí cuando se tocan o se acercan unos a otros. La tecnología NFC se integra con frecuencia en los teléfonos inteligentes, que son capaces de intercambiar datos entre sí cuando se juntan (Li, Xu and Zhao 2015)

[2] La identificación por radiofrecuencia (RFID) es una tecnología de comunicación de corto alcance en la que una etiqueta RFID se comunica con un lector RFID a través de campos electromagnéticos de radiofrecuencia. Las etiquetas pueden contener diferentes formatos de datos, pero el más utilizado para las aplicaciones de IoT es el Código Electrónico de Producto, o EPC. Un EPC es un identificador universalmente único para un objeto. (Li, Xu and Zhao 2015)

directa o indirectamente, a hacer de la ciudad un entorno inteligente interconectado, con el fin de mejorar en la medida de lo posible la vida de sus habitantes.

Otro más que notable dominio de aplicación de los sistemas de IoT se da en el sistema sanitario, a través de máquinas inteligentes de monitorización de pacientes ingresados u operados, supervisión a tiempo real del desarrollo de enfermedades crónicas y tratamientos de larga duración, asistencia en intervenciones quirúrgicas de alta precisión, sistemas de control de acceso restrictivo en sus instalaciones excepto a personal autorizado, e infinidad de sistemas auxiliares de gestión y administración que pretenden mejorar la calidad de vida de los ciudadanos a través de la automatización de tareas e interconexión de sistemas hospitalarios y de centros de salud.

Finalmente, no podemos olvidarnos de las aplicaciones más conflictivas y debatidas en los foros legales actuales, nos referimos a las aplicaciones personales y sociales, que abarcan desde los ámbitos más íntimos y privados, hasta los más públicos y masificados. Hablamos de dispositivos en hogares inteligentes o viviendas automatizadas que analizan y asisten en nuestros hábitos y rutinas (Article 29 Data Protection Working Party 2014), automatizaciones que recopilan nuestros gustos o tendencias de búsqueda para ofrecernos contenido personalizado, vinculaciones de nuestros perfiles sociales en las plataformas más conocidas a dispositivos de uso personal y cotidiano como los moviles, o los wearables con capacidades de geoposicionamiento para alertarnos de eventos cercanos que puedan ser de interés para el usuario (Guo et al. 2012) . Estos fines, desarrollados en un contexto social, pueden considerarse aquellos que más impacto pueden alcanzar en el día a día de las personas y sus datos, ya que simultáneamente se convierten en fuentes de tratamientos potencialmente constantes e individualizados de datos personales, y consecuentemente en puertas a nuestra intimidad y privacidad. Es por ello por lo que en este estudio serán estas aplicaciones, personales y sociales, sobre las que centremos nuestro foco de análisis, requiriendo a su vez de un minucioso estudio para conseguir preservar los beneficios de estas nuevas tecnologías, minimizando los posibles riesgos a nuestros derechos fundamentales.

3. Internet of Things a la luz del marco normativo del RGPD y LOPDGDD.

3.1. Estudio Legislativo

Como algunos autores han puesto de manifiesto, el Internet de las Cosas ha actuado como punto de encuentro de tres disciplinas clave de gran relevancia para la sociedad: la tecnológica, la económica y la referente al derecho; desarrollándose en su núcleo diversos conflictos generados por los evidentes intereses contrapuestos y dispares de los agentes implicados en este fenómeno, trasformando en una "tormenta perfecta" cualquier consecuencia a gran escala derivada de su aplicación (Barrio Andrés 2020; McEwen and Cassimally 2014).

Esta relevancia jurídica propiciaría que desde 2014 el antiguo Grupo de Trabajo del Artículo 29, mediante su Dictamen 8/2014 liderado por la Agencia Española de Protección de Datos (AEPD) junto con la Autoridad francesa (CNIL), realizase un análisis en profundidad en cuanto a las implicaciones del entonces vigente ordenamiento de protección de datos sobre el IoT; extrayendo de la actualmente derogada 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos los elementos nucleares de su regulación y limitaciones legales.

Desde este estudio, ya podía preverse la complejidad regulatoria que se daría en un fenómeno tan multidisciplinar como el IoT, por ello, hoy en día centrándonos en el ordenamiento Español podemos considerar como pertenecientes al marco juridico sectorial regulatorio del IoT los siguientes cuerpos normativos acorde a su disciplina:

Disciplina	Cuerpos Normativos
Sector Publico	Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
	Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
Ciberseguridad	Ley 36/2015, de 28 de septiembre, de Seguridad Nacional
	Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas
	Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información
Comercio electrónico y servicios de Internet	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
Competencia	Ley 3/1991, de 10 de enero, de Competencia Desleal.
Defensa de Consumidores	Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias
Propiedad industrial	Ley 24/2015, de 24 de julio, de Patentes
Propiedad Intelectual	Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia

Protección de datos	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos
	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
Publicidad	Ley 34/1988, de 11 de noviembre, General de Publicidad
Telecomunicaciones	Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Figura 1. Compendio de Normativas Sectoriales con contenido de Protección de Datos. (Fuente: Elaboración Propia)

Sin embargo, debido al eje central y objeto de estudio de nuestro trabajo, nos limitaremos en su mayor parte a analizar en profundidad los elementos regulatorios presentes en el reciente Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos (RGPD), junto a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) que lo complementa en nuestro país; así como algunos preceptos presentes en directivas europeas como la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, actualizada posteriormente mediante la Directiva 2009/136/CE, y traspuesta en nuestro ordenamiento mediante la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSICE).

3.1.1. Evolución legislativa

Como hemos comentado anteriormente, los dos elementos normativos de mayor relevancia en el sector de la protección de datos en referencia a los sistemas de IoT, son el RGPD y la LOPDGDD, no obstante, este marco juridico no ha sido el primero en configurar los límites y ejercicio del derecho fundamental a la protección de datos, ni en coordinar principios y medidas aplicables al fenómeno que hoy se conoce como IoT.

Para poder encuadrar la evolución legislativa del actual derecho a la protección de datos, y más concretamente del derecho fundamental a la privacidad desde donde evolucionaría, debemos remontarnos a finales del siglo XIX y relocalizarnos en Estados Unidos. Sería en este país donde se gestaría una verdadera noción legal de derecho a la privacidad, concretamente a raíz del trabajo de los juristas norteamericanos Samuel Warren y Louis Brandéis, en su artículo titulado "*The Right to privacy*" en 1890. Sería en este texto donde Warren y Brandéis extrajeron, del entonces vigente ordenamiento estadounidense, los principios reguladores para combatir las posibles intromisiones de terceros en la vida privada de los individuos. Sin embargo, no sería hasta casi un siglo después cuando en 1974, tras múltiples informes jurídicos y coincidiendo con la dimisión del presidente Richard Nixon a raíz del incidente conocido como Watergate, acerca de un sistema de grabación y espionaje ilícito de comunicaciones, el legislador estadounidense adoptaría el llamado "*Privacy Act",* configurando efectivamente la primera legislación norteamericana especifica consagrada para regular el uso ilícito de información de los ciudadanos por parte de los organismos gubernamentales.

Desviando nuestra vista al territorio europeo, algunas organizaciones internaciones como el Consejo de Europa, indudablemente inspirado por los debates y trabajos emitidos desde Estados Unidos en torno a la noción de privacidad, incluyó en sus textos internacionales un reconocimiento del derecho de toda persona al respeto de su vida privada y familiar, como refleja el Convenio Europeo de derechos Humanos de 1950 en su Art. 8. Sin embargo, no sería hasta principios de los años 70 cuando países europeos tomaron interés por la regulación sobre el uso y el tratamiento de datos. Algunos países, como Suecia y Alemania, fueron los pioneros en elaborar leyes nacionales de protección de datos, en 1973 y 1977 respectivamente, convirtiéndose en los primeros países europeos con una legislación dedicada en la materia. Siguiéndoles brevemente Francia en 1978, asi como España y Portugal en 1976 y 1978 respectivamente, incluyendo en sus textos constitucionales menciones al derecho de la protección de datos personales. Concretamente podemos encontrar este precepto en el Art. 18 CE , tras consagrar los derechos a la intimidad, el honor, la propia imagen, la inviolabilidad del domicilio y el secreto de las comunicaciones, dispone en su párrafo cuarto que «limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

Posteriormente, hubo otros cuerpos normativos que materializaron una preocupación por una protección de datos uniforme en todo el territorio europeo, fruto de esto surgió en 1981 el llamado Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108), que se constituyó como el primer instrumento internacional legalmente vinculante destinado a organizar la protección de datos de carácter personal.

Tras este largo camino legislativo, finalmente en 1995, la Comisión Europea adopto, tras un complejo proceso de negociación, la que hoy se conoce como Directiva de Protección de Datos 95/46/CE, con dos objetivos en mente: garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas en lo que respecta al tratamiento de los datos personales, y prohibir a toda restricción a la libre circulación de datos personales entre Estados miembros. A pesar de este importante avance, dicha normativa pecaría de múltiples defectos que se traducirían en una aplicación nacional irregular en todo el territorio de la UE, debido principalmente a las limitaciones y diferencias institucionales de los países europeos en ese momento (Cazurro Barahona 2020). Poco después de la promulgación de esta directiva, el reconocimiento individualizado de la Protección de datos de carácter personal quedaría fuera de toda duda mediante la promulgación en 1999 de la Carta de los Derechos Fundamentales de la Unión Europea, la cual contiene en su Art. 8 un reconocimiento expreso del derecho a la protección de datos personales, finalmente diferenciado en un texto internacional del derecho al respeto de la vida privada y familiar.

En suma, debido a todas las irregularidades acaecidas con la última Directiva 95/46/CE, y con objeto de asegurar un marco normativo uniforme y directamente aplicable a todo el territorio europeo, sería en 2016 cuando se implementaría el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Además, con la introducción de este reglamento se pretendió reforzar los derechos de los titulares de los datos, asi como uniformar conceptos y contenidos que actualizasen los obsoletos mecanismos de protección tras el avance de las nuevas tecnologías y el uso masivo de Internet (Cazurro Barahona 2020).

Centrándonos específicamente en los antecedentes dirigidos a esbozar el marco jurídico regulador del IoT, además de la legislación ya presentada en materia de protección de datos,

encontramos múltiples instancias de iniciativas promovidas tanto por la Comisión Europea, como por otros organismos de corte internacional. Estas iniciativas de cooperación entre estados europeos, asi como entre terceros países, han desembocado en diversos informes de interés tales como el "Informe preliminar sobre Investigación sectorial sobre el Internet of Things" con el fin de comprender mejor el sector del IoT, su panorama competitivo, sus tendencias en desarrollo y los posibles problemas de competencia desleal que en su seno puedan darse; asi como fomentar que la industria europea participe activamente en el desarrollo del ecosistema de IoT emergente que según informa "*se espera que crezca significativamente en los próximos años […] y sus ingresos se dupliquen entre 2020 y 2025*"(European Commision 2021).

A su vez, no podemos ignorar los dictámenes emitidos a nivel europeo en materia de IoT por parte del GT29 en los últimos años; que si bien no componen el grueso del marco normativo directamente aplicable, si ofrecen una perspectiva increíblemente útil en el estudio de las implicaciones del mismo. Concretamente podemos acudir en primer lugar al "Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes" publicado en 2013, y con el que se inicia un estudio preliminar sobre desarrollo de estas novedosas técnicas de tratamiento bajo el espectro de la protección de datos, el marco jurídico aplicable a las mismas, asi como las implicaciones y recomendaciones a tener en cuenta en el desarrollo, distribución y uso de aplicaciones en dispositivos inteligentes. Por otra parte, un año después encontraríamos la publicación del "Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos", en donde de forma mucho más directa y focalizada se abordan los elementos normativos más incidentes en este campo y se identifican todos aquellos posibles riesgos y consecuencias sobre la protección de datos en el ecosistema de las tecnologías de IoT, ofreciendo en el proceso recomendaciones y posibles soluciones a las mismas.

Finalmente, podemos encontrar otras iniciativas adyacentes a la propia normativa, centradas en promover desde el consenso, el dialogo y la interacción entre las partes involucradas tanto en el sector público, como en el privado; así como textos informativos y aclaratorios emitidos recientemente por la entidad de control española, la AEPD. En cuanto a las primeras iniciativas mencionadas estas encontramos ejemplos como la Fundación de la Alianza para la Innovación del Internet de las Cosas en 2015, cuyos objetivos principales son la creación de un ecosistema que proporcione el despliegue de IoT para las empresas europeas, propiciando a con ello

beneficios para todos los ciudadanos europeos; a su vez aspira a cooperar con otras regiones del mundo para garantizar la abolición de las posibles barreras al desarrollo del mercado de IoT, preservando y velando al mismo tiempo por la privacidad y la protección del consumidor (Barrio Andrés 2020). A su vez, atendiendo a las comunicaciones y artículos emitidos por la AEPD encontramos varios de ellos que, inspirados por los dictámenes previos emitidos por el GT29 en 2013 y 2014, exploran y definen ciertos elementos aproximando sus posibles consecuencias y riesgos a los profesionales de la privacidad y a la población en general (Agencia Española de Protección de Datos 2020a; 2020c; 2021b; 2021c)

3.1.2. Las delimitaciones del RGPD y la LOPDGDD

A pesar de lo que hemos podido ver, es indudable que el evento singular más destacable y relevante en los últimos años, desde el punto de vista del IoT, ha sido la publicación del reciente RGPD y su subsecuente ley complementaria nacional, la LOPDGDD. Según el mismo, se asegura de dejar reflejado en su Art. 3.1 y 3.2 RGPD que deberán atenerse, y quedar vinculados a sus contenidos y obligaciones, todas las empresas y organizaciones que traten datos de ciudadanos que se encuentren en la Unión Europea, se localicen o no dichas empresas simultáneamente en el territorio europeo, incrementando efectivamente su alcance territorial de aplicabilidad. Aspirando a paliar la marcada disparidad normativa entre los estados miembros, propiciada por la anterior directiva europea, y eliminando definitivamente la tendencia empresarial de adherirse a la normativa más beneficiosa en detrimento muchas veces de los derechos de los ciudadanos, fenómeno conocido como "fórum shopping". (Dimitrov 2017)

Como hemos podido observar, ya desde su origen el RGPD ha sido concebido para fortalecer y reforzar los derechos de las personas físicas residentes en el territorio europeo ante posibles tratamientos llevados a cabo sobre sus datos personales, tratamientos entre los que encontramos materializadas las aplicaciones prácticas de las tecnologías del IoT, a pesar de no ser mencionadas expresamente. Concretamente, el RGPD define en su Art. 4.2 que será considerado como tratamiento de datos *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no"*; pudiéndose calificar acertadamente como tratamientos sujetos a la normativa europea las operaciones automatizadas sobre los datos de los interesados, llevadas a cabo por uno o un conjunto de dispositivos inteligentes interconectados vía internet, así

como la comunicación bidireccional de dichos datos entre los propios dispositivos y el proveedor de servicios, como ya estableció el GT29 en su dictamen sobre esta materia, bajo la entonces vigente Directiva 95/46/CE (Article 29 Data Protection Working Party 2014).

Por todo ello, una vez encuadrados tanto el ámbito territorial, como el relativo a su aplicabilidad sobre el objeto de estudio, debemos aclarar ciertos conceptos circundantes y objetivos que han sido pilares en cuanto a la elaboración y entrada en vigor de esta normativa. Como bien es sabido hasta ahora, la protección de datos personales estaba concebida antes de la entrada del reglamento como una obligación meramente formal, donde salvo en contadas ocasiones, era percibida como un obstáculo y una carga al avance tecnológico, económico y empresarial en las organizaciones. Sin embargo, esta filosofía es contraria a los principios rectores del nuevo reglamento, mediante el cual se aspira a entender la protección de datos como una oportunidad más de negocio, con increíble valor estratégico. Consolidándose a través de su previsión y desarrollo en las distintas organizaciones la fidelidad de los clientes actuales, y erigiéndose como un factor diferenciador en el mercado, a través de la incorporación de una verdadera cultura de la privacidad integrada en sus procesos productivos, de servicios y sistemas organizativos. Desechándose, por tanto, el llamado "*compliance en papel*" carente de resultados garantistas efectivos para los interesados, y centrándose en la evasión de sanciones por los operadores responsables del tratamiento.

De entre todo el articulado contenido en el RGPD, existe una clasificación concreta de elementos normativos que, ya sea por su aplicabilidad general a todo tipo de tratamientos, o por su concreta configuración especifica, ejercen una especial incidencia en los tratamientos integradores del IoT. Comenzando por los llamados principios del tratamiento, contenidos en el Art. 5.1 RGPD, estos principios actuarán como obligaciones para todo responsable de tratamiento, que deberá guiarse por su contenido de manera estricta, y aplicarlos a todo tipo de tratamientos de datos personales.

En primer lugar, se nos presenta el principio de licitud, lealtad y transparencia que aplicado bajo el umbral de las tecnologías de IoT podríamos entenderlo como la diligencia de llevar a cabo tratamientos amparados bajo la más estricta licitud en sus bases legales, informando a los interesados de todas aquellas características, conjuntos de datos y finalidades que caracterizarán nuestro tratamiento mediante dispositivos de IoT, así como todos los derechos legalmente establecidos que se encuentran a su disposición junto a la forma propuesta de

ejercicio. Uno de los mayores factores a tener en cuenta por el IoT en torno a este principio es el evitar y prevenir la posibilidad que se recojan o sometan a tratamiento datos personales sin que el interesado sea realmente consciente de ello (Article 29 Data Protection Working Party 2014).

A continuación, encontramos los principios de limitación de la finalidad y minimización de datos respectivamente. Estos principios de tremenda relevancia para las tecnologías de IoT son considerados conceptos totalmente independientes, pero aun podemos encontrar ciertos elementos comunes en el establecimiento de una restricción directa y limitativa a la libre actuación de un responsable en sus funciones en cuanto al tratamiento indiscriminado de datos. Haciendo referencia el primero en cuanto a las finalidades explicitas, legitimas y determinadas para los tratamientos de datos que se vayan a realizar, debidamente delimitadas e informadas en su inicio; y la segunda en cuanto a la mínima recolección de datos para alcanzar esas finalidades, quedando excluido cualquier tratamiento sobre una finalidad no declarada expresamente, o sobre un dato recabado ilícitamente o desconocido para el interesado; estableciendo un freno al posible conocimiento excesivo que pueden llegar a ostentar algunos responsables de tratamiento sobre una persona física. (Palma Ortigosa 2018)

Seguidamente, se hace referencia a otros principios de aplicación general, como el principio de exactitud de los datos, convidando a todo responsable a garantizar de manera proactiva la exactitud de los datos de los interesados almacenados y tratados bajo su ámbito de control. Así como el principio de limitación de los plazos de conservación, el cual no solo actúa como garante de que los datos no serán almacenados durante periodos de tiempo que excedan las necesidades y finalidades del tratamiento perseguido, sino que, tras la finalización de estos plazos derivados de políticas internas u obligaciones legales preestablecidas, el responsable deberá suprimir o finalmente destruir diligentemente dichos datos mediante las técnicas adecuadas.

Por tanto, podemos entender a modo de síntesis y al tenor de estos principios, que el tratamiento sobre datos exactos esenciales, recopilados de manera licita y leal, para llevar a cabo finalidades de tratamiento debidamente informadas (Palma Ortigosa 2018) debe ser una constante de atención prioritaria en relación a los tratamientos llevados a cabo bajo las tecnologías del IoT.

Después de estas concreciones, podemos encontrar dos de los principios de mayor incidencia en cuanto a los riesgos que conllevan los tratamientos del IoT, y su posible prevención. Hablamos de los principios de integridad y confidencialidad, referidos a la seguridad de los datos, y a la responsabilidad proactiva, tambien llamado accountability, que deberá adoptar todo responsable del tratamiento. En cuanto al primero de ellos, dedicaremos gran parte del apartado cuarto al estudio y prevención de los posibles riesgos asociados a estos tratamientos en referencia a su disponibilidad integridad y confidencialidad, sin embargo, podemos adelantar que este principio se verá altamente complementado, como veremos, por las medidas de seguridad exigidas en el Art. 32 RGPD destinadas a preservarlo. De la misma forma, encontramos una intrínseca relación entre el principio sobre la seguridad de los datos y la responsabilidad proactiva que acompaña a todo responsable, puesto que una de las funciones y objetivos de dicha proactividad es la prevención, idealmente desde el diseño y por defecto, de los posibles riesgos e incidencias sobre los datos de los interesados, siendo garante tanto de su protección como del respeto en su tratamiento de todos los principios contenidos en este art. 5 .1 RGPD.

Una vez analizados estos principios debemos acudir al artículo inmediatamente posterior, el Art. 6.1 RGPD, destinado a concretar las posibles bases aplicables a las tecnologías del IoT, que justificarán la licitud del tratamiento a realizar dentro del marco normativo. En este caso, debemos analizar cual de las distintas bases de tratamiento serían las más adecuadas para justificar el tratamiento realizado mediante dispositivos pertenecientes al IoT de captación, recepción, trasmisión y procesamiento de datos interconectados entre sí, asi como a la nube simultáneamente. Esta pregunta ya fue planteada por el GT29 en múltiples dictámenes, bajo la aplicación de la pasada directiva 95/46/CE, en donde se planteó cuáles eran los fundamentos jurídicos pertinentes que debían regir los tratamientos en el uso de dispositivos inteligentes interconectados; a lo cual la respuesta ofrecida se mantuvo constante en el tiempo a pesar del desarrollo de una tecnología tan novedosa.

Inicialmente se advierte que la base o fundamento más adecuado para esta clase de dispositivos o plataformas suele ser generalmente el consentimiento de los interesados (Art. 6.1.a RGPD), entendiendo esta vía como la más optima y adecuada independientemente de las categorías de los datos objeto de tratamiento. Este consentimiento debe ser, acorde a los requisitos extraídos del art. 7 RGPD y a las recomendaciones entradas de los trabajos del GT29,

especifico, expreso, informado, libre y revocable (Grupo de Trabajo sobre Protección de Datos del Artículo 29 2011). Proporcionando a los interesados todos los aspectos necesarios sobre el tratamiento que se pretende realizar para poder formar una opinión precisa del mismo, teniendo el usuario la opción de aceptar o rechazar el tratamiento libremente, sin opciones únicas; estableciéndose dicha manifestación de voluntad individualmente para a cada uno de los tratamientos específicos sobre un dato o tipos de datos concretos, ofreciendo en todo momento la opción de ser retirado libremente por el interesado, y finalmente considerándose invalido todo consentimiento tácito recabado en el proceso (Grupo de Trabajo sobre Protección de Datos del Artículo 29 2013).

Sin embargo, esta base del tratamiento no es considerada como la única disponible para los operadores y responsables del tratamiento para poder recabar y procesar datos personales en el entorno de las tecnologías del IoT. Como acertadamente ya puntualizó el GT29, también existen otras bases que, si bien encuentran su justificación en tratamientos más específicos, su aplicabilidad es innegable en determinados contextos. Nos referimos concretamente a los tratamientos motivados por la ejecución de una obligación contractual, Art. 6.1.b RGPD, y a los derivados de la satisfacción de un interés legítimo perseguido por el responsable del tratamiento o por aquellos terceros a quienes se cedan los datos tratados, Art. 6.1.f RGPD.

En cuanto a los tratamientos cuya fundamentación jurídica depende de la existencia de una relación contractual previa, debiendo inferirse que dicha relación se verá limitada por el criterio de necesidad ajustado al contrato firmado entre las partes, requiriendo de una relación directa y objetiva entre el propio tratamiento perseguido y los fines previstos del cumplimiento contractual que se espera del responsable (Article 29 Data Protection Working Party 2014). Podemos ejemplificar esta situación cuando un usuario otorga su consentimiento para la instalación de una aplicación bancaria de pago “contactless” en su reloj inteligente, aceptando todos aquellos permisos necesariamente informados para su uso en dichos dispositivos “wearables”, y posteriormente realizar un pago mediante dicho sistema, la entidad bancaria no tiene por qué solicitar el consentimiento específico para revelar su nombre y número de tarjeta o cuenta bancaria al beneficiario del pago en la transacción, ya que el tratamiento y trasmisión de esos datos se consideran necesarios para ejecutar el contrato de compraventa en el que el pago se enmarca.

Por otro lado, si nos centramos en aquellos tratamientos cuya base legitimadora es un interés legítimo perseguido por el responsable del tratamiento debemos considerar detenidamente que no se vulneren o prevalezca intereses o derechos de los interesados, como podría considerarse su derecho fundamental a la intimidad personal en el contexto de un tratamiento de datos personales. Para poderse entender dicho interés como legítimo este debe considerarse legítimo, ser articulado clara y específicamente, ponderándose mediante una evaluación de impacto de forma recomendada; y representar una necesidad real y actual para el interesado (Grupo de Trabajo sobre Protección de Datos del Artículo 29 2014). A modo ejemplificativo podemos plantearnos una res de dispositivos interconectados, entre los que pueden encontrarse cámaras de videovigilancia, parquímetros, sensores, instalados por un ayuntamiento con la finalidad de restringir el acceso de cierto tipo de vehículos contaminantes a determinadas zonas centrales de la ciudad. En este caso el ayuntamiento recabará y procederá al tratamiento de la información de la matrícula de los vehículos para determinar unos criterios diferenciadores previamente predefinidos: tipo de combustible del vehículo, año de matriculación, tipo de motor, categoría medioambiental del modelo… para determinar mediante los mismos la tarifa de acceso a pagar por el conductor amparado por un interés legítimo. No obstante, se requiere cautela para cualquier tratamiento que exceda dichos parámetros y finalidades concretas para el tratamiento a realizar, ya que un tratamiento adicional podrá requerir de otra base legitimadora al no encontrarse amparada bajo el umbral del interés legítimo.

Sin embargo, a pesar de poder fundamentar un interés legítimo como base jurídica de ciertos tratamientos posteriores o adyacentes a los principales, ejecutados por los dispositivos interconectados, debemos puntualizar que solo se podrá recurrir a las misma siempre que los mismos no impliquen el tratamiento de categorías especiales de datos de carácter personal, englobadas bajo la definición del Art. 9.1 RGPD. Ya que, de llevarse a cabo dichos tratamientos sobre categorías especiales de datos, únicamente podremos recurrir al consentimiento de los interesados o, en casos muy determinados, el cumplimiento de un vínculo contractual como base legitimadora.

Enlazamos, de esta manera, con otro de los elementos centrales para un potencial tratamiento realizado mediante tecnologías IoT, siendo esta la prohibición generalizada de cualquier tratamiento sobre categorías especiales de datos personales, definidas y reguladas

como ya hemos indicado bajo los preceptos del Art. 9.1 RGPD. Enfocadas dichas categorías especiales, dentro del IoT, a todo aquel tratamiento mediante dispositivos inteligentes, capaces de revelar el posible origen étnico o racial, la opinión política o la afiliación sindical, datos de caracter genético o biométrico, o aquellos relativos a la salud o la orientación sexual de una persona física. Desde wearables que pueden medir nuestras constantes vitales, hasta dispositivos de medición de los niveles de azúcar en sangre, conectados a nuestro teléfono, destinados para personas diabéticas, es indudable que los tratamientos sobre categorías especiales de datos van a estar cada día más a nuestro alcance. Pero, no cabe olvidar que para que sean legítimos, dichos tratamiento deben encuadrarse en alguno de los apartados del Art. 9.2 que levantan la prohibición general aplicada fuera de sus premisas. En este caso la primera de ellas, Art. 9.2.a), es la más accesible y recomendable para un uso general de estas tecnologías sobre categorías especiales de datos.

Ademas de los conceptos ya analizados, no debemos olvidar de resaltar uno de los requisitos que requerirán de una mayor atención por parte del responsable para su cumplimiento, la trasparencia en el tratamiento de los datos tratados. Este derecho se encuentra localizado en el Art. 12 RGPD, y vincula a todo responsable del tratamiento a tomar las medidas adecuadas y necesarias a la hora de informar adecuadamente a todo interesado, propietario de los datos, de todos aquellos elementos de interés relativos al tratamiento de forma clara, concisa, sencilla y de fácil acceso. Englobando dentro de esta información a proporcionar al interesado todos aquellos requisitos incluidos en los Art.13 y 14 RGPD. Para las tecnologías del IoT, la configuración de este requisito de trasparencia dependerá, en mayor medida, de la naturaleza de los servicios o aplicaciones que se ofrezcan al interesado a través de las mismas, pero podemos indicar que cierta información como: la identidad del responsable del tratamiento, los fines del tratamiento, los destinatarios de los datos, las medidas para desconectar el dispositivo y así limitar ciertos tratamientos, o la existencia de los derechos de acceso a la información tratada y oposición al tratamiento compone los elementos esenciales que se suelen considerar en estas comunicaciones (Article 29 Data Protection Working Party 2014).

Otro de los principios que considerados centrales para esta clase de tecnologías, es el concepto de privacidad desde el diseño (privacy by design) y la privacidad por defecto (privacy by default) reguladas en el Art. 25 RGPD. Ambos conceptos deben erigirse como pilares infranqueables a la hora de diseñar y comercializar, no solo los dispositivos denominados

inteligentes, sino tambien todas las plataformas, aplicaciones, servicios o tratamientos posibles que se realicen mediante dichos dispositivos. Si consultamos la guía elaborada por la AEPD en la materia, nos resalta la necesidad de utilizar una mentalidad definida en torno a la gestión del riesgo y la responsabilidad proactiva del responsable, con la finalidad de establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida tanto del dispositivo como del propio dato personal (Agencia Española de Protección de Datos 2019). Para ello se deberían impulsar una evaluación de impacto previa (Art. 35.1 RGPD), ya que nos encontramos con un tratamiento realizado en mediante tecnologías ciertamente innovadoras, y a raíz de sus resultados aplicar unas medidas y objetivos implementados desde la fase de diseño, hasta la fase final de producción de los dispositivos y subsecuente tratamiento de datos.

Finalmente, no podemos avanzar sin hacer una breve referencia al fundamento legal que justificará una adecuada seguridad del tratamiento de datos en el seno de estas redes de dispositivos; hablamos por supuesto de las medidas técnicas y organizativas presentes en el Art. 32 RGPD. En el mismo se establece que, acorde al estado de la técnica, los posibles costes, así como la naturaleza y posibles finalidades del tratamiento, entre otros factores a tener en cuenta, tanto el responsable como su encargado adoptarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. En concreto cuando hablamos de tratamientos realizados mediante por IoT los riesgos presentes en los mismos demanda el mantenimiento de un nivel de seguridad bastante exigente, razón por la cual analizaremos en profundidad las posibles medidas disponibles en esta clase de dispositivos interconectados en un apartado posterior, y valoraremos su idoneidad para el nivel de riesgo presente en diversos tratamientos de esta índole.

A pesar de todos estos principios aplicables de forma adaptiva a los tratamientos pretendidos estos dispositivos inteligentes, hemos de admitir que la legislación en materia de protección de datos no hace ninguna mención específica sobre las tecnologías del IoT en sus textos normativos. Sin embargo, sí podemos extraer una mención indirecta para todos aquellos responsables de los tratamientos realizados por estos dispositivos en entornos exclusivamente personales acudiendo al considerando 18 RGPD. En el mismo se nos indica que en el caso de realicen tratamientos de datos personales, llevados a cabo en el ámbito personal o doméstico de los interesados, también serán de aplicación todos los contenidos de

dicho reglamento a las personas responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas (Unión Europea 2016) . De esta manera, quedan vinculados todos aquellos tratamientos, realizados en entornos personales o domésticos por redes o dispositivos interconectados, que en ausencia de este considerando se encontrarían exentos debido a la excepción general domestica contenida en el Art.2.2.d RGPD. La relevancia de esta mención es muy destacable hoy en día, puesto que cada vez más hogares optan por la instalación de estos dispositivos inteligentes, acorde a un estudio realizado por la Asociación Española de Domótica e Innatica (CEDOM), habiendo sufrido dicho sector un crecimiento del 15% solo en el año 2019 (Asociación Española de Domótica 2020).

3.1.3. Sujetos y responsables involucrados jurídicamente relevantes

Hemos hablado repetidamente de las obligaciones vinculadas a la posición de responsable del tratamiento, pero ahora debemos adentrarnos en las diversas identidades que pueden tomar estos responsables en aquellos tratamientos enmarcados por tecnologías o redes del IoT. Esta clasificación de posibles responsables, o corresponsables en su caso, es relevante de plantear ya que sus particulares características, y relaciones con posibles encargados del tratamiento, condicionarán las posibles responsabilidades de las distintas organizaciones que intervienen en una red de dispositivos interconectados tan compleja en ocasiones como las presentes mediante el IoT.

Por definición las aplicaciones del IoT conllevan la intervención combinada de múltiples partes interesadas, desde fabricantes de dispositivos que conforman estas redes, hasta los desarrolladores de las aplicaciones que actúan de interfaz en estos dispositivos. El hecho de conformarse estas redes en donde intervienen múltiples responsables exige, acorde al criterio del GT29, la necesidad de asignar de forma acertada y concreta las distintas responsabilidades jurídicas que se asignarán a cada uno de ellos, en relación con las características del tratamiento, y las singularidades de sus particulares intervenciones. (Article 29 Data Protection Working Party 2014)

En primer lugar, podemos identificar ciertos intervinientes especialmente vinculados con las capacidades, los funcionamientos, y la seguridad en los sistemas de las maquinas que llevan a cabo estos tratamientos, los fabricantes de los dispositivos. Dentro de este grupo deben excluirse todas aquellas empresas que simplemente se limitan a vender estos dispositivos a

los interesados; tomando como característica necesaria para su inclusión el formar parte en el diseño, la fabricación, o la programación de los sistemas o mecanismos presentes en alguno de estos dispositivos interconectados en la red para poder ser considerados como responsables. En este caso, la besa de la responsabilidad reside en que la mayoría de los fabricantes recogen y someten a tratamiento datos personales recabados los dispositivos, mediante condiciones y finalidades preestablecidas por dichos fabricantes. Ya sea a través de un servicio adyacente proporcionado tras la fabricación del dispositivo, como ocurre con la aplicación y plataformas digitales del asistente Alexa® proporcionadas por Amazon®; o a través de ciertos tratamientos de recopilación de datos con fines de "calidad y mejora de la eficiencia de los dispositivos" una vez son utilizados por los interesados o consumidores finales.

A continuación, encontramos otro tipo de responsables en los llamados desarrolladores de aplicaciones y proveedores de servicios online. En este caso estos responsables no participan en el diseño o fabricación de un dispositivo, sino que diseñan y producen aplicaciones o servicios que harán uso de funcionalidades presentes en estos dispositivos. Este sería el caso de ciertas aplicaciones de "fitness & wellness" desarrolladas por estudios independientes para instalarse en dispositivos "wearables" como los relojes inteligentes, siendo el caso por ejemplo de la aplicación de gestión de datos de salud Da Fit® desarrollada por la empresa CRREPA® con conectividad para relojes inteligentes y descargable a partir de la tienda digital de Google®. Como nos indica el GT29, la base del tratamiento para el uso de estas aplicaciones es necesariamente el consentimiento de los interesados, diligentemente recabado en el momento previo a su instalación en los dispositivos del IoT, debiendo ser claro, especifico, y proveniente de un usuario debidamente informado como veíamos en puntos anteriores.

Ademas de estos desarrolladores, en el entorno digital podemos identificar a los llamados administradores de plataformas IoT, ostentando a su vez la posición de responsables del tratamiento. En este caso, se entiende como administradores a aquellas empresas que dirigen, gestionan y mantienen plataformas vinculadas a través de cualquier tipo de conectividad a dispositivos inteligente, los cuales de forma automática, mediante el funcionamiento del mismo dispositivo o manualmente por sus usuarios, son recolectados, procesados y analizados datos personales de los interesados que las frecuentan. Cuando estas redes sociales, accesibles desde dispositivos inteligentes, someten a tratamiento datos

personales con finalidades determinadas por ellas mismas, se les puede reconocer como responsables del tratamiento en el entorno del IoT (Article 29 Data Protection Working Party 2014).

Finalmente encontramos un grupo relativamente amplio de responsables, concretándose en todos aquellos terceros que no se pueden adherir a ninguna de las tres categorías anteriores, no ostentando la posición de fabricantes o desarrolladores, pero sin embargo, pudiendo hacer uso de los dispositivos de la IoT para acceder o recopilar información y datos personales de los interesados, y someterlos a tratamiento. Este es el caso, por ejemplo, de las entidades aseguradoras que ofrecen junto a la póliza de sus clientes un podómetro o cualquier otro dispositivo inteligente, sobre el cual, aparte de ser el fabricante el que potencialmente realice tratamientos de datos, sería a su vez considerado como responsable la empresa aseguradora, siempre que tenga acceso o almacene los datos que recojan dichos dispositivos sobre sus clientes o cualquier interesado.

Por último, no podemos finalizar este apartado de sujetos relevantes sin antes hacer mención del importante papel que ostentan los encargados de tratamiento en estas redes de tratamiento inteligente. Siguiendo los criterios del GT29, entendemos como encargado de tratamiento a toda entidad jurídica independiente del responsable que realiza un determinado tratamiento de datos personales por cuenta de este (Grupo de Trabajo sobre Protección de Datos del Artículo 29 2010). En cuanto a las redes de dispositivos IoT, el mismo GT29 afirma que se consideran sistemas complejos, con multitud de actores, en donde responsables y encargados pueden intervenir conjuntamente para ciertos tratamientos, y de manera autónoma para otros; pudiéndose dar diferentes grados de responsabilidad para estos encargados. A modo general, deberemos atender a lo contenido en el Art. 28 RGPD, asi como a las características de los tratamientos concretos, debiendo concretar la posición de cada uno de los actores intervinientes acorde a su papel como responsable o encargado en el funcionamiento de la red de dispositivos.

3.2. Riesgos normativos, vacíos legales, y posibles inclusiones futuras

Como ya hemos traído a colación anteriormente, no son muchos los casos en los que la ley hace referencia directa a ciertas tecnologías de manera específica o concreta, de hecho, ni en el RGPD ni en la LOPDGDD se hace ninguna mención directa a los tratamientos realizados en

el marco de las tecnologías de IoT. Es comprensible que una ley pretenda o aspire a alcanzar el fenómeno conocido como "neutralidad tecnológica", caracterizado por una serie de objetivos cuya finalidad es asegurar tanto la máxima aplicabilidad del marco normativo a todo tipo de tecnologías disponibles, independientemente de sus desarrollo y evolución presente o futura, como evitar dentro de lo posible su obsoletismo frente al cambiante estado del arte tecnológico; garantizando de esta manera que los cuerpos normativos perduren en el tiempo y no exijan cambios permanentemente por cuestiones tecnológicas (Remolina Angarita 2014). Simultáneamente, uno de los consecuentes beneficios de esta corriente consiste en prevenir la posible dependencia tecnológica, de una disciplina determinada, en cuanto a un cuerpo normativo concreto, asegurando la libertad de las organizaciones de optar por la tecnología más apropiada y conveniente a sus necesidades sin que dicha selección exceda los posibles límites de la regulación legal (Rios 2013).

Por tanto, si la neutralidad tecnológica trae consigo múltiples beneficios cual puede ser el fundamente para sugerir desde este estudio la necesidad de una regulación explicita y más ajustada a las necesidades y riesgos generados por el uso de estas nuevas tecnologías de IoT. En primer lugar, la abrumadora escala de dicha industria en la sociedad actual; estudios recientes realizados por Cisco Systems indican que el número de dispositivos conectados a redes IP triplicará a la población mundial en 2023, estimando que habrá aproximadamente 3,6 dispositivos conectados a la red per cápita en 2023, frente a los ya alarmantes 2,4 dispositivos registrados en 2018 (Cisco 2020). La mera escala de este fenómeno reclamará, por si sola, algún tipo de ordenación normativa de carácter expreso en materia de protección de datos, con objeto de paliar la abrumadora avalancha de incidencias que probablemente traerá consigo, debido a los elevados riesgos inherentes que conllevan los tratamientos sobre datos personales bajo estas tecnologías.

A pesar de ello, no queremos inferir que la regulación existente no cubre las necesidades legislativas necesarias para encuadrar estos tratamientos de manera correcta; todo lo contrario, reconocemos las valiosas funciones que el reglamento, la LOPDGDD, la legislación sectorial y las iniciativas adyacentes a la propia normativa poseen en la dura tarea de definir, relacionar y vincular estas tecnologías a los estándares de protección pretendida a nivel europeo para todo tipo de tratamientos. Sin embargo, no podemos evitar echar en falta cierta regulación específica para todas aquellas situaciones y medidas específicas que, por las

características de la tecnología y los riesgos asociados a la misma, se dan de manera recurrente en esta materia.

Existen, desde el punto de vista de este autor, dos propuestas actuales que podrían considerarse adecuadas en solventar las cuestiones sobre la falta de regulación reflejada anteriormente. En primer lugar, proponemos la inclusión de ciertos elementos regulatorios de las tecnologías IoT en la reciente propuesta del nuevo Proyecto de Ley General de Telecomunicaciones, la cual pretende hacer un gran hincapié en impulsar un ecosistema de ciberseguridad en sus contenidos. El principal contrargumento de esta idea yace en que el proyecto de ley sectorial ya se encuentra en una fase bastante avanzada de tramitación, a la espera de su revisión por parte del senado, y con un amplio apoyo parlamentario; por lo que es altamente improbable que se realicen modificaciones a su contenido que no se hayan reflejado hasta el momento.

Otra de las propuestas que consideramos más viable y directa se basa en la regulación de un Reglamento de desarrollo de la actual LOPDGDD que refleje, entre su articulado, una regulación específica para esta clase de redes de dispositivos. De la misma forma que el Real Decreto 1720/2007, por el que se aprobó el Reglamento de desarrollo de la ya derogada Ley Orgánica de protección de datos de carácter personal 15/1999, complementó los contenidos de esta en cuanto a diferentes materias y atribuciones, puede un nuevo reglamento de desarrollo completar la actual LOPDGDD, incluyendo entre sus títulos uno dedicado en exclusiva para dispositivos y componentes que implementen tecnologías inteligentes como las IoT. Pero de nuevo nos encontramos con la improbabilidad de su tramitación, ya que, a diferencia de la situación con la antigua directiva y su Ley orgánica de trasposición, el nuevo reglamento y su correspondiente ley orgánica actúan de una manera mucho más simbiótica y complementaria que sus predecesoras en sus respectivas materias regulatorias, prescindiendo de esta manera de la necesidad de un reglamento añadido, exceptuando su posible idoneidad para contadas materias actualmente no reguladas en profundidad.

Aparte de estas dos propuestas, existen algunas alternativas menos probables, como son la posible mención expresa de una regulación explicita de ciberseguridad, enfocada en estas nuevas tecnologías, en la reciente tramitación de la Directiva NIS 2 de seguridad de las redes y sistemas de información en la Unión Europea (Portal de la Administración Electrónica 2022). O la posible regulación de una hipotética “Ley sobre dispositivos pertenecientes al Internet de

las Cosas", que proceda a ordenar expresamente la materia, sin depender de su inclusión en otro cuerpo normativo de una materia más general, y posiblemente más extensa, como pueden ser las telecomunicaciones.

En cualquier caso, solo el tiempo determinará cual será el destino normativo de una posible regulación en cuanto a las tecnologías IoT, y los tratamientos de datos que se derivan de ellas, siendo probable que la mera escala de este fenómeno se considere motivo suficiente a ojos del legislador para demandar una solución expresa en nuestro ordenamiento. La única cuestión a tener en cuenta en ese caso será mediante qué medidas de armonización se decidirán aplicar para con la actual legislación en materia de protección de datos en esta nueva futura legislación en nuestro ordenamiento.

4. La problemática de la seguridad en la era de la interconexión digital

4.1. Riesgos para la privacidad en los dispositivos interconectados

Según la Estrategia Europea de Datos, publicada en febrero de 2020, el previsible incremento en el volumen global de datos se verá quintuplicado desde 2018 hasta 2025, recogiéndose a su vez el cambio en las formas en la que los datos serán tratados, estimando que para 2025 el 80% de los datos globales serán procesados, directa o indirectamente, a través de dispositivos vinculados a las tecnologías IoT, frente al 20% que se procesaba en 2018 (Comisión Europea 2020). De ello podemos extraer, con total seguridad, que los tratamientos realizados mediante dispositivos vinculados al IoT no harán más que incrementar en número; aumentando exponencialmente junto a un crecimiento los riesgos inherentes, para los datos de los interesados, ya presentes en la actualidad en el uso de estas tecnologías.

Aun con esta perspectiva, no excesivamente esperanzadora, debemos detenernos brevemente a analizar cuáles son concretamente estos riesgos inherentes y como pueden repercutir en los tratamientos de datos realizados a través de tecnologías IoT. Con el objetivo de poder plantear soluciones efectivas desde el diseño y por defecto de aplicación general, teniendo en cuenta las particularidades de cada tratamiento, para que puedan tomarse en consideración simultáneamente antes de comenzar la fase de diseño de un posible dispositivo, asi como aplicarse en tratamientos que ya se estén llevando a cabo por los sujetos responsables.

Con el fin de adquirir cierta perspectiva de los tratamientos más demandados en los hogares promedio, y por tanto enfocarnos en aquellos riesgos merecedores de una mayor atención, debemos consultar previamente las aplicaciones, finalidades, o servicios a los cuales más frecuentemente se destinan estas tecnologías fuera del ámbito empresarial o industrial. Como podemos ver en un estudio llevado a cabo por la Comisión Europea en cuanto a las finalidades de las categorías de dispositivos inteligentes distribuidos a la población europea en 2021, observamos que los electrodomésticos inteligentes constituyen la mayor categoría de productos distribuidos, seguido por aquellos dispositivos destinados al confort o el control

de la iluminación y seguido por categorías secundarias como el entretenimiento o la seguridad (European Commision 2021).

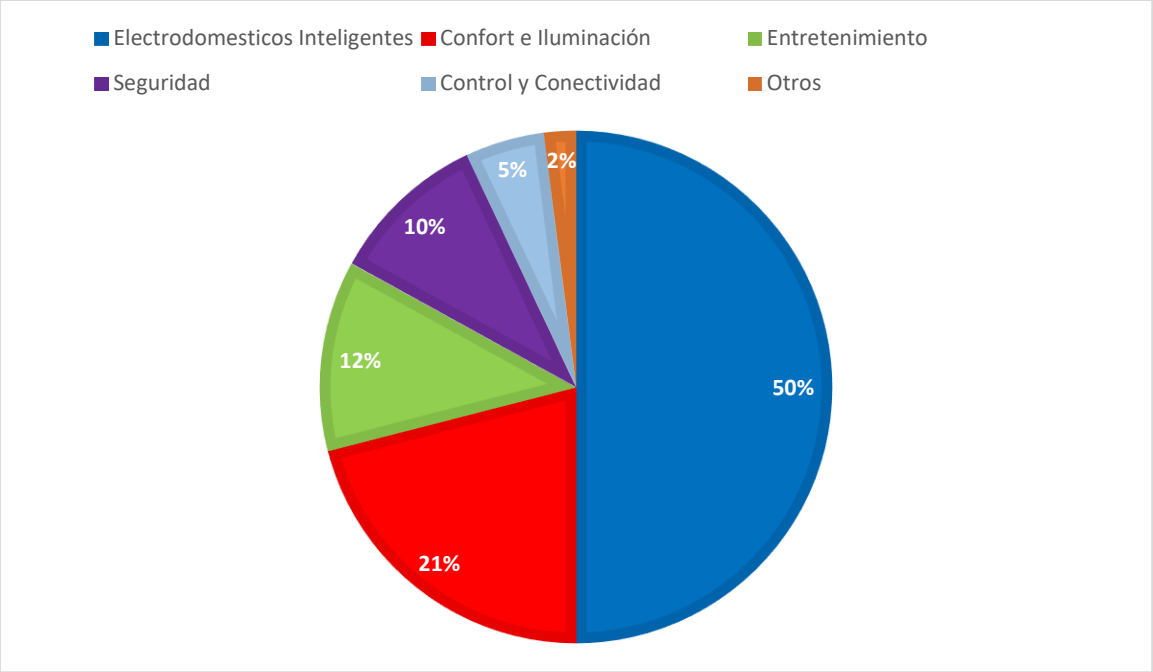

Figura 2. Distribución de los productos de los encuestados por categoría de dispositivos domésticos inteligentes. (Fuente: https://ec.europa.eu/competition-policy/system/files/2021-06/internet_of_things_preliminary_report.pdf)

Como podemos ver, aun a día de hoy el grueso de los tratamientos levados a cabo por esta clase de dispositivos se centran en aquellos vinculados a nuestra rutina diaria, ya sea simplificándola mediante el uso de electrodomésticos inteligentes, o participando en ella mediante nuevas formas de entretenimiento. La intromisión de estas tecnologías en la privacidad de nuestro día a día conlleva que todos los responsables implicados en dichos tratamientos accedan a un volumen muy extenso de información personal, la cual acorde a la AEPD puede ser adquirida u obtenida a través de distintos procesos: en primer lugar identificamos todos aquellos datos que son proporcionados y facilitados al responsable por los propios usuarios o interesados antes o durante el uso del dispositivo, seguidamente identificamos todos aquellos datos que son observados o captados por los distintos componentes o sensores de los propios dispositivos, a continuación localizamos aquellos datos derivados y extraídos de la información originalmente facilitada por el interesado u obtenida por el dispositivo, y finalmente se encuentran los datos inferidos, extraídos a partir

del procesamiento analítico de un conjunto amplio de datos procedentes de varios usuarios o fuentes, tambien conocidos como “Big Datta”(Agencia Española de Protección de Datos 2020a).

Está claro que, una vez desglosada esta clasificación, no cabe duda acerca de la ingente cantidad de datos que potencialmente se encuentran a disposición de los responsables del tratamiento, en algunos casos sin que realmente sea consciente el propio interesado, permitiendo a los mismos construir perfiles de usuario muy detallados a través de estas redes. Y es destacable como a pesar de ello, acorde a un reciente informe publicado por la entidad Kaspersky, el 43% de las empresas no protege completamente su infraestructura IoT, debido entre otros motivos a que temen que los productos de ciberseguridad puedan afectar al rendimiento del IoT, o a la potencial dificultas de su implementación (Kaspersky 2022). Y ciertamente, al no disponer de unos estándares de seguridad generalizados, como es el caso de otro tipo de redes de información o telecomunicaciones, el riesgo de que se produzca un acceso no autorizado por algún tercero, comprometiendo la seguridad de la información contenida en toda la red, es altamente probable.

Por ello hemos procedido a recopilar aquellos riesgos, en cuanto a la privacidad de los interesados, más comúnmente reconocidos tanto por el GT29 como por la propia AEPD (Article 29 Data Protection Working Party 2014; Agencia Española de Protección de Datos 2020a):

- Revelación de pautas comportamentales de los interesados, asi como la realización de perfiles, puesto que los tratamientos de datos obtenidos en el seno de un entorno de IoT hacen posible la detección de rutinas diarias y comportamiento de los interesados que los utilizan, de forma muy detallada y completa. Se produce en este caso una vigilancia potencial que puede alcanzar la esfera más privada de la vida de las personas y generar situaciones donde la expectativa de privacidad no es más que una mera fachada.
- Falta de asimetría en la información, lo cual genera serias dificultades para los interesados a la hora de acceder, revisar, o consultar los datos que se recopilan, produciendo un efecto de falta de control sobre sus propios datos, siendo este fenómeno especialmente incidente en datos de caracter derivado o inferido.
- Falta de trasparencia en la información proporcionada a los interesados, previo su consentimiento, ya sea debido a posibles deficiencias en el servicio o debido a las

características restrictivas y limitadas del propio dispositivo, a la hora de proporcionar esta información.

- Problemas y conflictos de responsabilidad derivados de la multitudinariedad de los responsables presentes en los tratamientos realizados a través de redes de IoT, propiciando que el cumplimiento se difumine y obstaculice, en cuanto al nivel de responsabilidad de cada uno de los responsables.
- Existencia de tratamientos a terceras personas que en algún momento puedan encontrarse "próximas" al dispositivo mediante el que se realiza el tratamiento. Realizando el tratamiento accidental de sus datos sin unas prestaciones adecuadas de información, consentimiento, ect… Este riesgo se encuentra muy presente en los asistentes de voz, los cuales pueden captar ciertas conversaciones no destinadas directamente a su uso de forma automática.
- Evidentemente uno de los principales riesgos que se presentas es la falta de medidas adecuadas de seguridad, desde el diseño y por defecto, para dichos tratamientos. Bien debido a las limitaciones del dispositivo o aplicación, o deficiencias en usuarios y contraseñas, arquitecturas, programas…
- Y finalmente encontramos las dificultades que encuentran los usuarios para hacer uso de estos dispositivos de forma anónima. El argumento de muchos fabricantes en cuanto a la necesidad de identificación, basada en la finalidad del tratamiento, no constituye fundamentación suficiente para ignorar la inclusión de un modo de funcionamiento anónimo, tal vez prescindiendo de algunas características del servicio a cambio de este respeto más directo a la privacidad del usuario.

Como podemos apreciar, los riesgos que pueden afectar a estas tecnologías son variados, numerosos, y en ocasiones muy diferentes entre sí, haciendo aún más compleja si cabe la tarea de implementar soluciones eficaces y adaptadas a la realidad de cada dispositivo y tratamiento. Por si fuera poco, acorde a un estudio realizado por la entidad Kaspersky, el número de ataques a dispositivos de IoT se duplico durante los primeros seis meses de 2021, detectándose más de 1500 millones de de ataques contra dispositivos IoT (Kaspersky 2021).

Todos estos ataques a redes y dispositivos inteligentes pueden dar lugar a brechas de seguridad con consecuencias nefastas para la integridad de todo el sistema, como:

- Convertirse todos los dispositivos afectados en puertas de entrada desde las que realizar "ataques distribuidos de denegación de servicio", más conocidos como ataque DDOS, .
- Actuar ciertos dispositivos vulnerables con la finalidad de atacar otros sistemas o dispositivos que realmente sean el objetivo del ataque, debido a su importancia para el sistema o la de la información que contiene.
- Permitir la reconfiguración de aquellos dispositivos afectados, teniendo acceso potencial a aquellos datos tratados por el mismo, asi como manipular la configuración establecida originalmente por el usuario, afectado a su funcionamiento, accediendo por ejemplo a una cerradura inteligente programándola para abrirse a una determinada hora para acceder ilícitamente a una vivienda.

Algunas de estas consecuencias ya se han llegado a manifestar anteriormente, como fue el caso la vulneración de cientos de cámaras de seguridad localizada en los hogares de los interesados, pertenecientes al fabricante TrendNet, que tuvo como consecuencia el acceso no autorizado y la publicación en Internet de imágenes intimas; o la red de "bots" llamada "Carna" que infectó 420.000 dispositivos escaneando direcciones IP, o la red de "bots" descubierta por Proofpoint que lanzó 750.000 ataques de phishing y spam a través de dispositivos como frigoríficos y televisiones conectadas solo en 2013, siendo destacable que más del 25% del volumen de ataques se produjo a través de elementos convencionales como routers de hogares, centros multimedia, televisiones o incluso de un frigorífico (Alberta Jaquero 2014), poniendo de relieve el precio que conlleva desatender nuestros deberes como responsables el tratamiento en entornos de seguridad de la información.

4.2. Requisitos y medidas de seguridad para un uso responsable

A pesar del carácter eminentemente fragmentario de estas tecnologías, la amplia gama de posibilidades técnicas de acceso ilícito a los datos, y la falta de concienciación jurídica entre los desarrolladores y fabricantes de dispositivos, desde este estudio se pretende enfocar el tratamiento de datos mediante tecnologías de IoT desde un punto de vista proactivo, a través del planteamiento de posibles soluciones ofrecidas tanto por nuestras organizaciones nacionales e internacionales, como por estudios técnicos, junto a todas aquellas partes interesadas que pretendan hacer de este ambiente tecnológico un entorno más seguro para la privacidad y los datos de consumidores e interesados.

Por desgracia, muchos de los dispositivos pertenecientes al IoT no han sido diseñados teniendo en mente la seguridad de los datos de los interesados, por ello las organizaciones deben tomar medidas inmediatas para proteger sus sistemas y dispositivos de posibles brechas de seguridad (Robertson 2022). A continuación, procederemos a enumerar algunas de las propuestas y recomendaciones comunes a todas las partes interesadas, orientadas a proporcionar un nivel adecuado de seguridad en los entornos de IoT (Robertson 2022; Article 29 Data Protection Working Party 2014; Grupo de Trabajo sobre Protección de Datos del Artículo 29 2013; Sánchez-Alcón, JÓSE ANTONIO, López-Santidrián and Martínez 2015):

- Antes de lanzar una nueva aplicación con finalidades de tratamiento dentro de sistemas de IoT, se deben efectuar las correspondientes evaluaciones de impacto sobre la intimidad (PIA). Dichas evaluaciones pueden realizarse acorde a las pautas y recomendaciones contenidas en la guía de la AEPD sobre su elaboración (Agencia Española de Protección de Datos 2021a).
- Restringir el acceso de las partes interesadas, corresponsables del tratamiento, o encargados de tratamiento solo a los datos imprescindiblemente necesarios para el tratamiento pretendido, y no a todos los datos recabados de manera general por los dispositivos. Las partes interesadas deben eliminar todos aquellos datos innecesarios para la finalidad de su tratamiento apenas hayan extraído los datos que realmente necesitan.
- Todas las partes interesadas en tratamiento de IoT deben indistintamente implementar aquellos principios aplicables a su tratamiento en cuanto a la protección desde el diseño y por defecto regulados en el Art. 25 RGPD.
- Se debe asegurar a los interesados un ejercicio efectivo y accesible de sus derechos frente a los distintos responsables o partes involucradas en el tratamiento de sus datos, asegurando en todo momento el principio de autodeterminación de los datos.
- Las vías dispuestas para solicitar y revocar el consentimiento informado a los distintos interesados deben ser fácilmente comprensibles. Haciendo especial hincapié en las políticas de información y consentimiento a disposición de los usuarios.
- El consentimiento para el uso de un dispositivo, y sus consecuentes tratamientos, se debe dar libremente y tras haber sido plenamente informado. El acceso a las funciones generales de los dispositivos y servicios no deben degradarse para aquellos usuarios que hayan decidido no utilizar una característica concreta del dispositivo o servicio determinado.

- Además, los dispositivos y las aplicaciones se deben diseñar de manera que informen a los interesados, sean o no usuarios, de que el dispositivo está realizando en ese momento un tratamiento de datos. Los usuarios de los dispositivos de IoT deben informar de la presencia de estos dispositivos, y del tipo de los datos recogidos, a los terceros adyacentes cuyos datos se recogen pero que no son usuarios directos. También deben respetar las preferencias de aquellos terceros que no deseen ser objeto de tratamientos de datos por un determinado dispositivo.
- Los fabricantes de dispositivos deben informar a los usuarios del tipo de datos que se recogen y se someten a tratamiento por los dispositivos, asi como los tipos de datos que se reciben y de cómo se someterán a tratamiento.
- Los fabricantes de dispositivos deben ser capaces de comunicar inmediatamente al resto de las partes interesadas implicadas la retirada o la oposición del interesado a que sus datos se sometan a tratamiento.
- Para evitar el seguimiento y la localización, los fabricantes de dispositivos deben limitar las huellas digitales de los dispositivos, desactivando sus interfaces inalámbricas cuando no estén siendo directamente utilizados, a fin de impedir el uso de identificadores persistentes para el seguimiento o la localización.
- Los usuarios han de tener derecho de acceso a sus datos personales. Se les deben proporcionar herramientas sencillas y claras que les permitan exportar fácilmente sus datos con un formato estructurado y de uso habitual.
- Los fabricantes de dispositivos deben hacer posible que las entidades responsables y encargadas del tratamiento de datos proporcionen información clara a los usuarios de los datos recogidos por sus dispositivos y faciliten el almacenamiento y el tratamiento locales sin tener que transmitir los datos al fabricante del dispositivo
- Implementar un control de acceso a la red para obtener información precisa sobre los dispositivos que se pretenden conectar, verificando su postura de seguridad antes de proceder con la conexión.
- Se debe utilizar un sistema de protección contra intrusiones, detectando puntos débiles en las arquitecturas y sistemas disponibles, y proporcionando “parches virtuales” a los dispositivos a los que no se les pueden aplicar actualizaciones de software.

5. Un nuevo destino: Privacy of Things

5.1. Creación de ambientes seguros como vía de desarrollo de la interconexión digital

Han quedado constatados los múltiples retos a los que se enfrentarán estos tratamientos de datos si las estimaciones sobre su implementación en la sociedad alcanzan los niveles previstos. Pero, a pesar de haber abordado ciertas recomendaciones técnicas, secundadas por las principales autoridades nacionales e internacionales, aun se debe profundizar en aquellas soluciones reservadas para un ámbito de aplicación mucho más extenso. Estas metas, más bien definidas como filosofías, pretenden no solo aplicarse a determinados tratamientos concretos, cuando se apliquen en los mismos ciertas tecnologías del IoT especialmente perjudiciales para la privacidad de los interesados, sino que deben aspirar a extenderse a todos aquellos tratamientos en los que se plantee implementar cualquier mínima intervención de una red de dispositivos inteligentes en la consecución de los fines del tratamiento propuestos. Preservando un nivel adecuado de seguridad durante toda la vida útil de los dispositivos destinados al tratamiento de datos: desde su fase de diseño y fabricación, pasando por su mantenimiento o actualizaciones periódicas, y finalizando con su inevitable obsolescencia y retirada. Algunas de las medidas concretas recomendadas por expertos en la implantación a gran escala de estas tecnologías han sido (Shipley 2013):

- Disposición de un sistema de inicio seguro: en el momento de la primera ejecución del dispositivo este debe verificar la autenticidad, integridad y legitimidad del sistema operativo y programas instalados, diseñados y autorizados específicamente para ese modelo de dispositivo, implementando las medidas de seguridad previstas de base por el fabricante para la naturaleza del servicio contratado.
- Presencia de controles de acceso: deberán existir distintos controles de acceso a los sistemas del dispositivo, de tal forma que el propio sistema operativo instalado por defecto disponga de un mecanismo de limitación de privilegios a toda aplicación, entidad, o programa potencialmente inseguro o sospechoso. En consecuencia, las aplicaciones podrán acceder estrictamente a los mínimos recursos imprescindibles que necesiten para desarrollar su función. Esto implicará, que de verse comprometidas la confidencialidad, disponibilidad, o integridad de los datos personales debido a una brecha en la seguridad

del sistema, el intruso solo dispondrá de un acceso minimo correlativo a las credenciales previstas para el programa o aplicación comprometidos, reduciendo el posible impacto de la brecha de seguridad y simultáneamente preservando la integridad general del sistema.

- Instalación en los dispositivos de sistemas de autentificación: en el caso de que un dispositivo externo quiera acceder o conectarse a los recursos de la red de dispositivos IoT, este debe autentificarse previa cualquier extracción o intercambio de datos. Simultáneamente se recomienda que el proceso sea eminentemente automatizado entre los dispositivos intervinientes, simplificando la realización de estas conexiones para el consumidor medio, y limitando las posibles intromisiones fraudulentas de un posible usuario experimentado. Este tipo de medida sigue el mismo principio de funcionamiento que los sistemas de redes corporativas o internas, en las cuales se registra la actividad y credenciales de un determinado perfil de usuario ligadas a sus credenciales, de tal forma que el dispositivo IoT debería disponer de un conjunto similar de permisos asignados por perfiles de acceso almacenados en un área segura del sistema (Li, Xu and Zhao 2015).
- Disposición de Cortafuegos: es imperativo que todo dispositivo cuente con un cortafuegos que pueda monitorizar los accesos y el tráfico de datos, permitiendo las comunicaciones que hayan sido debidamente verificadas, y bloqueando las que no. Para asegurar su eficacia, esta función deberá actuar independientemente de todo software instalado en el dispositivo, y deberá implementarse en todo modelo comercializado para asegurar la integridad de las redes IoT, ya que solo haría falta una puerta de entrada a través de un dispositivo con un Cortafuegos defectuosos para comprometer a toda la red.
- Dependencia de un protocolo IPS: el sistema de trasmisión de información inalámbrica deberá contar con un protocolo IPS o sistema de prevención de intrusiones, el cual lleve a cabo un análisis en tiempo real de las conexiones y los protocolos involucrados para determinar si se está produciendo o se va a producir una brecha de seguridad, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red (Instituto Nacional de Ciberseguridad 2020).
- Comunicación e instalación remota de actualizaciones y parches: con el fin de proceder a un adecuado mantenimiento de las medidas de seguridad previstas a lo largo de la vida útil del dispositivo, este debe ser capar de recibir las actualizaciones y/o parches de seguridad, tanto para el sistema, como para las aplicaciones instaladas en el mismo; por ello, será preciso que el dispositivo sea capaz de verificar la fuente de la actualización, o

del parche de seguridad, como una fuente legitima. Tras lo cual se podrá proceder a su actualización e instalación sin comprometer la integridad del sistema.

Existen a su vez otras medidas de seguridad prometedoras que hoy se encuentran en distintas fases de investigación o implementación. Desde la instalación de VPNs (Virtual Private Networks) por defecto en los sistemas operativos de los dispositivos inteligentes, pasando por el empleo de funciones físicas no clonables o PUFs (Phisical unclonable funtions), basadas únicamente en hardware, con el fin de mejorar y permitir que las operaciones relacionadas con la seguridad se manejen a nivel de los sensores del dispositivo; y finalmente el empleo de tecnologías Blockchain a través de dispositivos de procesamiento de alto rendimiento, adicionalmente conectados a la red doméstica, para generar algoritmos de seguridad complejos e indescifrables (Butun, Osterberg and Song 2020). Todas ellas tienen como objetivo el propiciar un ambiente de innovación consecuente, donde los principios de seguridad desde el diseño y por defecto se extiendan no solo a todos los tratamientos de datos, sino a todos los componentes intervinientes en las redes de IoT.

Debido a esto, mediante la colaboración entre especialistas de las áreas empresarial, jurídica y tecnológica se tiene la oportunidad de ofrecer a los usuarios un entorno seguro donde se priorice tanto la seguridad, como la protección de sus datos personales. En el IoT, la limitación de recursos hace necesaria la implementación de medidas de seguridad que eviten obstruir el funcionamiento del sistema, o comprometer la calidad del servicio ofertado. En general, allí donde se localicen varios servicios o tecnologías cabe la posibilidad de integrar centros de operaciones de red, debidamente certificados, que se encarguen de funciones especializadas, como el análisis de inteligencia o la toma de decisiones sobre políticas de seguridad. Esto proporcionará gran capacidad de gestión y control para mantener y preservar remotamente la seguridad a medida diseñada para cada uno de los productos y servicios de internet de las cosas.(Sánchez-Alcón, José-Antonio, López-Santidrián and Martínez 2015).

5.2. Concienciación social, el arma definitiva para una protección efectiva

A pesar de todas las posibles medidas y contramedidas técnicas implementadas en estas redes, el mayor riesgo arraigado en la base de estos tratamientos mediante IoT es el grado de cautela, coherencia y precaución con el que se utilizan, tanto por los responsables del tratamiento como por los interesados afectado. Hoy en día, el avance de nuevos métodos de

tratamiento, su potencial rendimiento económico para los responsables, y su positivo impacto en el día a día del interesado ciega en muchos casos a todos los intervinientes ante los posibles riesgos que llevan aparejadas estas técnicas, consecuentemente poniendo en peligro los derechos de los consumidores finales.

Por tanto, debemos poner una especial atención en ofrecer, por un lado, la máxima trasparencia en los tratamientos a realizar, poniendo a disposición de los interesados información actualizada, simplificada, y veraz; y simultáneamente fomentar la formación social en materia de los riesgos que todas estas tecnologías conllevan para nuestros datos. La aceptación social de las nuevas tecnologías y servicios del IoT dependerá en gran medida de la fiabilidad de la información y el grado de protección de los datos tratados. Aunque se han desarrollado varios proyectos de seguridad y protección de la privacidad por distinguidas marcas en la industria tecnológica, todavía se necesita dar con un mecanismo fiable de protección eficaz para asegurar de manera efectiva la confidencialidad de los datos, la privacidad y la confianza total de los interesados. (Li, Xu and Zhao 2015)

Por todo ello, y como constata la propia AEPD en su análisis sobre la privacidad de grupo: “es la concienciación de las personas sobre la importancia de preservar la propia privacidad, que va más allá de las consecuencias que puede tener para su propia privacidad ya que también puede afectar a los derechos y libertades de la sociedad en su conjunto. Esto no es un impedimento para los innumerables potenciales de la tecnología, sino más bien una condición para que este potencial se lleve a cabo de una manera responsable” (Agencia Española de Protección de Datos 2020b)

6. Conclusiones

Las tecnologías y aplicaciones IoT han irrumpido en nuestra sociedad de manera extensa y repentina. Proclamándose como la solución a diversas necesidades presentes en nuestra sociedad, mejorando en consecuencia nuestra calidad de vida, y enraizándose profundamente en la intimidad de nuestros hogares.

Es justo, debido a la naturaleza de este fenómeno, que adquiere carácter imperativo el erigir una base firme y segura desde donde evolucionen estas aplicaciones tecnológicas IoT. Debiéndose acudir a estándares, buenas prácticas y medidas técnicas y organizativas adecuadas tan pronto como sea posible en su desarrollo, incluso desde los inicios del diseño de las mismas si se quiere proteger adecuadamente los datos de los usuarios sujetos a tratamiento. Sin embargo, si pretendemos alcanzar un verdadero entorno de seguridad tecnológica, del que se beneficien tanto responsables como interesados, debemos superar algunos obstáculos:

Primera.- Un marco normativo adaptado; actualmente y como hemos podido apreciar esta tecnología se ve inmersa en un marco juridico insuficiente para las necesidades y soluciones normativas que demanda en su aplicación. Debido en parte a caracteres específicos como: la escala de sus tratamientos, su potencial adaptabilidad y la relevante incidencia que presenta en la privacidad de sus usuarios, es prioritario reclamar un ordenamiento que exija unos niveles de seguridad adecuados. Encontrando el punto de equilibrio orgánico entre la seguridad de los datos y el fomento del desarrollo de estas nuevas tecnologías, dentro de un ambiente que proporcione un nivel adecuado de seguridad jurídica.

Por todo ello, debe atribuirse al poder legislativo y a la administración del estado, la ardua tarea de promover una normativa ajustada a las nuevas necesidades que van surgiendo en este sector, elaborando menciones especificas contenidas en un posible título de un potencial Reglamento de Desarrollo de la actual LOPDGDD. Fomentar y destinar ayudas públicas a entidades y organizaciones con fines pedagógicos o educativos como la Fundación de la Alianza para la Innovación del Internet de las Cosas, o la Asociación española de Domótica e Inmótica, coordinando posibles colaboraciones y programas de sensibilización junto con entidades o corporaciones locales. Y finalmente, sustituir poco a poco la predominante

potestad sancionadora de la AEPD como la vía hegemónica de concienciación entre responsables y agentes implicados.

Segunda.- Una estandarización del sector; debido en parte a la complejidad de la tecnología empleada, su versatilidad, y las diferencias intrínsecas entre los sistemas ofertados competitivamente por distintos fabricantes y distribuidores, el alcanzar una estandarización eficiente y eficaz para todo tipo de sistemas IoT parece más un ideal a largo plazo que un posible objetivo a plantear. Sin embargo, no se trata de una realidad tan ilusoria si tenemos en cuenta, tanto el avance exponencial de la tecnología, como el impacto generalizado que un sistema de estándares internacionales significaría; extendiendo sus beneficios a empresas responsables y a clientes interesados por igual. Este sistema estandarizado podría abarcar desde técnicas de fabricación, hasta procesos de calidad de producto, la implementación de medidas seguridad en los diferentes sistemas informáticos, o incluso un sistema de seguridad en el tratamiento de información personal en el seno de estas tecnologías.

Tercera.- Una formación y educación social adecuadas; solamente cuando se alcance un nivel de perspectiva del riesgo adecuados a nivel de usuario, podremos considerar a la sociedad preparada para los retos que se nos presentaran en el uso responsable de estas tecnologías. Ya que a pesar de que se alcance un nivel de seguridad jurídica adecuados en el ordenamiento, y los fabricantes se rijan por estándares de actuación delimitados, es en el uso responsable de estas tecnologías donde se determinará verdaderamente el mantenimiento de unos niveles de seguridad adecuados, y una prevención realmente eficaz de los incidentes o brechas sobre los datos personales. Para ello, una educación y formación social es esencial, no solamente centrada en la necesidad de una protección adecuada en los tratamientos de datos, el valor de los mismos y su potencial vulnerabilidad ante incidencias tecnológicas y físicas; sino en un uso responsable y el riesgo que conlleva el uso de todos aquellos dispositivos que, potencialmente sin darnos cuenta, jugarán un papel protagonista en multitud de tareas a lo largo de nuestro día a día, tratando y perfilado simultáneamente nuestros datos personales.

Es por todo ello que debemos aspirar a complementar la disciplina tecnológica de "*Internet of Things*" con una filosofía marcada por el "*Privacy of Things"*, entablando una relación simbiótica de la misma forma que el RGPD pretende vincular los conceptos de tratamiento de datos con la filosofía de la protección desde el diseño y por defecto. Imbuyendo todos los

procesos implementados con una atención suficiente en cuanto a la preservación de un nivel de seguridad de la intimidad y la protección de datos optimo.

Referencias bibliográficas

Bibliografía básica

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Guía de Privacidad desde el Diseño. . 2019. Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, IoT (I): Qué es IoT y cuáles son sus riesgos | AEPD. . 2020a. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-i-que-es-iot-y-cuales-son-sus-riesgos.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Privacidad de grupo | AEPD. . 2020b. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/privacidad-de-grupo.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Vehículos Conectados | AEPD. . 2020c. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/vehiculos-conectados.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. , 2021a. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, IoT (II): Del Internet de las Cosas al Internet de los Cuerpos | AEPD. . 2021b. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-ii-del-iot-al-iob.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, IoT (III) Domótica. Internet de las Cosas: riesgos y recomendaciones | AEPD. . 2021c. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/iot-iii-domotica.

ALBERTA JAQUERO, C., Internet of things (IoT). El lado “Inseguro” de las Cosas | INCIBE. . 2014. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/internet-of-things-ciberseguridad.

ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 8/2014 on the on Recent Developments on the Internet of Things. , 2014. Disponible en: http://ec.europa.eu/justice/data-protection/index_en.htm.

ASOCIACIÓN ESPAÑOLA DE DOMÓTICA, Estudio de mercado Sector de la Domótica e Inmótica. . 2020. Disponible en: https://static.casadomo.com/media/2018/02/estudio-mercado-domotica-inmotica-cedom-2016.pdf.

BARRIO ANDRÉS, M., Internet de las cosas (2a. ed.). , p. 164. 2020. DOI 10.30462/9788429022001. Disponible en: https://elibro.net/es/lc/uoc/titulos/185096.

BUTUN, I., OSTERBERG, P. and SONG, H., Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, p. 616–644. 2020. ISSN 1553-877X. DOI 10.1109/COMST.2019.2953364. Disponible en: https://ieeexplore.ieee.org/document/8897627/.

CAZURRO BARAHONA, V., Antecedentes y fundamentos del derecho a la protección de datos. *Antecedentes y fundamentos del derecho a la protección de datos*, 2020. DOI 10.2307/J.CTV14T46SM.

DIMITROV, W., GDPR entrapments. Proactive and reactive (re)design thinking. *XXV conference Telecom 2017* , 2017. Disponible en: http://ceec.fnts.bg/telecom/2017/documents/CD2017/Papers/26.pdf.

EUROPEAN COMMISION, Preliminary Report-Sector inquiry into Consumer Internet of Things. , 2021. Disponible en: https://ec.europa.eu/commission/presscorner/detail/el/qanda_21_2908.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» . . 2010. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 15/2011 sobre la definición del consentimiento adoptado el 13 de julio de 2011. , 2011. Disponible en: http://ec.europa.eu/justice/policies/privacy/index_es.htm01197/11/ES.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes Adoptado el 27 de febrero de 2013. , 2013. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp202_es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE . , 2014. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp217_es_interes_legitimo.pdf

GUO, B., YU, Z., ZHOU, X. and ZHANG, D., Opportunistic IoT: Exploring the social side of the internet of things. *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2012*, p. 925–929. 2012. DOI 10.1109/CSCWD.2012.6221932.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, ¿Qué son y para qué sirven los SIEM, IDS e IPS? . 2020. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips.

KASPERSKY, El número de ataques a dispositivos IoT se duplica en un año. . 2021. Disponible en: https://www.kaspersky.es/about/press-releases/2021_el-numero-de-ataques-a-dispositivos-iot-se-duplica-en-un-ano.

KASPERSKY, El 43% de las empresas no protege completamente su infraestructura IoT. . 2022. Disponible en: https://www.kaspersky.es/about/press-releases/2022_el-43-de-las-empresas-no-protege-completamente-su-infraestructura-iot.

LI, S., XU, L. da and ZHAO, S., The internet of things: a survey. *Information Systems Frontiers*, vol. 17, no. 2, p. 243–259. 2015. ISSN 15729419. DOI 10.1007/S10796-014-9492-7.

MCEWEN, A. and CASSIMALLY, H., Internet de las cosas : la tecnología revolucionaria que todo lo conecta. , 2014.

PALMA ORTIGOSA, A., Contexto normativo de la protección de datos personales. *Protección de datos, responsabilidad activa y técnicas de garantía*, p. 9–16. 2018.

PORTAL DE LA ADMINISTRACIÓN ELECTRÓNICA, La Unión Europea refuerza su ciberseguridad con la aprobación de la directiva NIS 2. . 2022. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Ani

o2022/Mayo/Noticia-2022-05-26-Union-Europea-refuerza-ciberseguridad-directiva-NIS-2.html.

PRETZ, K., The next evolution of the internet. *IEEE Magazine The institute*, vol. 50, no. 5. 2013.

REMOLINA ANGARITA, N., Neutralidad tecnológica y función administrativa electrónica. *Revista de derecho, comunicaciones y nuevas tecnologias*, no. 11. 2014. ISSN 1909-7786.

RIOS, M.D., Technological Neutrality and Conceptual Singularity. *SSRN Electronic Journal*, 2013. DOI 10.2139/ssrn.2198887.

ROBERTSON, J., Principales riesgos empresariales del Internet de las Cosas - Silicon. , 2022. Disponible en: https://www.silicon.es/experto-opinion/principales-riesgos-empresariales-del-internet-de-las-cosas.

SÁNCHEZ-ALCÓN, J.A., LÓPEZ-SANTIDRIÁN, L. and MARTÍNEZ, J.F., Solution to ensure privacy in the internet of things. *Profesional de la Informacion*, vol. 24, no. 1, p. 63–70. 2015. ISSN 16992407. DOI 10.3145/EPI.2015.ENE.08.

SEBASTIAN, J. de M., *Inteligencia en entornos inciertos y complejos*. 2022. S.l.: ISEN Centro Universitario. ISBN 978-84-124619-2-3.

SHIPLEY, A.J., Security in the Internet of Things: Lessons from the Past for the Connected Future The Intelligence in the Internet of Things. . 2013. Disponible en: https://www.researchgate.net/publication/308915644_The_Future_Internet_of_Things_and_Security_of_its_Control_Systems.

WHITMORE, A., AGARWAL, A. and DA XU, L., The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, vol. 17, no. 2. 2015. ISSN 15729419. DOI 10.1007/s10796-014-9489-2.

Bibliografía complementaria

SARMIENTO GONZÁLEZ, R. y VILCHES VIVANCOS, F. Lenguaje jurídico-administrativo. Una lengua de especialidad. 2ª ed. Madrid: Dyckinson, 2016.

Legislación citada

JEFATURA DEL ESTADO DE ESPAÑA, *Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.* 2018. 2018. S.l.: s.n.

NORMA ESTADO ESPAÑOL, Constitución Española de 1978. *BOE nº311, de 29 de diciembre de 1978*, 1978. ISSN 1098-6596.

UNIÓN EUROPEA, Reglamento General de Protección de Datos. *Diario Oficial de la Unión Europea*, vol. 2014, no. 119. 2016.

Listado de abreviaturas

Art./Arts.: Artículo/Artículos

AEPD: Agencia Española de Protección de Datos

BOE: Boletín Oficial del Estado

GT29: Grupo de Trabajo del Artículo 29

LOPDGDD: Ley Orgánica de Protección de Datos y Garantías de los Derechos Digitales

Núm.: Número

RGPD: Reglamento General de Protección de Datos

TC: Tribunal Constitucional