Universidad Internacional de La Rioja
Máster en Protección de Datos

El Internet of Things en el sector de la automoción. Análisis desde la protección de datos.

Trabajo fin de máster presentado por: J. Salvador Esteban Rivero
Titulación:
Master Universitario en Protección de Datos
Área jurídica: Derecho
Director: D. Victor Cazurro Barahona

Murcia 3 de diciembre de 2018

Resumen

Este trabajo fin de máster (TFM) que se presentará a su defensa en relación con el Máster Universitario en Protección de Datos de la Universidad Internacional de la Rioja, gravita sobre la hipótesis de que cualquier esfuerzo del legislador a la hora de tutelar los derechos y libertades de las personas físicas en relación con el uso de este tipo de dispositivos que conforman el Internet de las Cosas (*Internet of Things*, por sus siglas en inglés IoT) y la forma en que los mismos tratan sus datos personales y su intimidad, será fútil mientras no exista una actitud proactiva del usuario en relación con su conocimiento y educación en relación, por un lado, con el contenido de sus derechos y deberes en materia de protección de datos y, por otro, con el alcance, sistemas, tecnologías, etc, de los dispositivos IoT.

Al final de este TFM se analizará el caso del SEAT CRISTÓBAL, concept car de SEAT presentado en ***Smart City Expo World Congress*** de 2018, y cómo afectan las novedades tecnológicas propuestas en el mismo a la protección de datos.

Keywords:

IoT, SEAT CRISTÓBAL, proactividad, GDPR, IoE, riesgos de seguridad, PIA, Privacidad, Educación, Formación, protección de datos, datos biométricos, datos de salud, automoción, geolocalización, *Privacy by design*, *Privacy by default*

1. LISTADO DE ABREVIATURAS Y SIGLAS

AEPD: Agencia Española de Protección de Datos

BOE: Boletín Oficial del Estado.

CNIL: Comisión Nacional de Informática y de las Libertades

DDOSS: *Denial of Service*. (Denegación de servicio).

GDPR: *General Data Protection Regulation* (Reglamento General Protección de Datos 2016/679 de 27 de abril).

IoE: *Internet of Everything* (Internet de Todo)

IoT: *Internet of Things* (Internet de las Cosas).

LOPD: Ley Orgánica de Protección de Datos 15/1999, de 13 de diciembre.

NNTT: Nuevas Tecnologías.

PLOPDyGDD: Proyecto de Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.

RLOPD: Reglamento de desarrollo de la Ley Orgánica de Protección de Datos, RD 1720/2007 de 21 de diciembre.

TFM: Trabajo Fin de Máster.

WP: *Working Paper* (Dictamen)

2FA: Doble factor de autenticación.

2. ÍNDICE DEL ANÁLISIS

3. INTRODUCCIÓN AL TFM

EL IoT implica extender la conectividad de Internet más allá de los dispositivos tradicionales, como ordenadores, *smartphones* y *tablets*, a cualquier rango de dispositivos físicos y objetos cotidianos que tradicionalmente no han contado con acceso a Internet. Esta nueva categoría de dispositivos no sólo se pueden comunicar e interactuar a través de Internet con otros dispositivos sino que además, se pueden monitorear y controlar remotamente. Los dispositivos conectados forman parte de un escenario en el que cada dispositivo habla con otros dispositivos relacionados en un entorno para automatizar las tareas del hogar y de la industria, y para comunicar datos de sensores útiles a usuarios, empresas y otras partes interesadas.

Este tipo de dispositivos se pueden categorizar en tres grupos principales: aquellos cuyo target de destinario son los consumidores, las empresas o las industrias. Los dispositivos conectados al consumidor incluyen desde televisores inteligentes, juguetes, hasta frigoríficos, sistemas de calefacción e incluso vehículos automóviles. Los contadores inteligentes, los sistemas de seguridad comercial y las tecnologías de ciudades inteligentes (*Smart cities*), como los que se utilizan para supervisar el tráfico y las condiciones climáticas, son ejemplos de dispositivos de IoT industriales y empresariales. En una casa inteligente, por ejemplo, el usuario llegará al domicilio, y su automóvil se comunicará con el garaje para abrir la puerta.; a la vez, el termostato ya está ajustando el interior de la vivienda a la temperatura seleccionada, y la iluminación se establecerá en la intensidad –e incluso en el color- seleccionado. En la empresa, los sensores inteligentes ubicados en una sala de conferencias pueden ayudar a los empleados a ubicar y programar una sala disponible para una reunión, asegurando que el tipo de habitación, el tamaño y las características adecuadas estén disponibles. Al conocer a los asistentes al ingresar a la sala, la temperatura se ajustará de acuerdo con la ocupación, y las luces se atenuarán a medida que se cargue el PowerPoint apropiado en la pantalla, y el orador comience su presentación.

Llegaremos al final, al análisis de cómo el IoT está siendo, no ya valorado, sino como se va incorporando por los fabricantes de automóviles como valor añadido a sus vehículos más vanguardistas, con el objeto de hacerlos más seguros, más eficientes y, sobretodo, más atractivos, ante una demanda cada vez más exigente con las nuevas tecnologías.

Es indudable que el IoT crea un nuevo escenario de oportunidades tanto para las empresas como para los usuarios, pero también podemos afirmar que ésta es sólo una de las caras de la moneda.

La otra viene determinada sin duda, en la forma en que esta nueva tecnología –o si se prefiere, este nuevo concepto- y los objetos o dispositivos que cuentan, o contarán con ella, afecta a la privacidad y/o intimidad de los usuarios; en consecuencia deberán arbitrarse, tal y como veremos a lo largo del desarrollo de este TFM, aquellas medidas que desde los principios de la privacidad por defecto y desde el diseño, permitan al usuario disponer a su propia voluntad cuáles de sus datos personales compartir, y/o hasta qué punto permitir la intromisión en su intimidad por este tipo de dispositivos; y es precisamente la introducción de estos dos nuevos principios una de las novedades más importantes introducidas por el GDPR, y así veremos como el principio de la privacidad desde el diseño es un término mucho más amplio que el expuesto hasta el momento e implica la creación de nuevos subprincipios (quizás con igual que importancia que el principio matriz) como son el carácter preventivo y no correctivos, así como el proactivo y no reactivos; igualmente, con el hecho de ser exigida la privacidad que venga incrustada desde el diseño, así como la privacidad por defecto que podríamos traducir como que los más altos stándares de privacidad deben venir activados como configuración predeterminada en los objetos IoT.
Ambos principios han sido recogidos en el, de momento, Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, considerándose infracciones graves su inobservancia (Vid Artículo 73. Infracciones consideradas graves).

Terminaremos este TFM analizando el caso concreto del concept car fabricado por Seat, denominado “Cristóbal”, y que fue presentado durante la ***Smart City Expo World Congress*** de 2018, al encontrarnos ante la presencia de dispositivos que tratarán datos biométricos y de salud, por un lado, así como datos identificativos tanto de usuarios como de terceros, por otro, que van más allá de la utilidad final de un vehículo (el transporte) pero que aportan un valor añadido que deberá ser puesto en una balanza con respecto a los derechos en la protección de los datos de sus usuarios.

4 .- ANÁLISIS

1. Introducción al *Internet of Things* (Internet de las cosas)

El internet de las cosas (desde ahora y durante todo el TFM: **IoT**) lejos de ser un concepto novedoso y disruptivo podría ser considerado la evolución de los trabajos realizados por Nikola Tesla[1] en el año 1927 en relación con las comunicaciones inalámbricas y de radio

Fue en el año 1969 con la red ARPANET, creada por el departamento de Defensa de Estados Unidos, cuando tuvo lugar la primera conexión entre ordenadores y, aunque la palabra Internet no estaba todavía en el vocabulario, supuso la semilla de lo que World Wide Web es ahora. Según aquella red iba creciendo y poniendo en conexión más y más computadores, empezaron a surgir otras redes tales como Aloha o Ethernet, cuyo denominador común es que ya se producía la conexión entre dos elementos: los ordenadores.

Sin embargo, es cierto que en esta temprana etapa, el factor humano seguía siendo imprescindible: hacía falta quien enviara los datos o información y se necesitaba a alguien en el otro lado que la reciba, analice y, en su caso, envíe una respuesta.

Mark Weiser, en el año 1990 anunciaba que "ordenadores invisibles" incorporados en objetos de uso cotidiano sustituirían a los ordenadores (llamémosles ordinarios). En su exposición afirmaba que "La computadora es un punto de conexión demasiado enredado, su manejo requiere mucha atención exclusiva, quitando la atención al usuario de la tarea que debe hacer"[2].

Sobre esta idea del citado investigador, es sobre la que gravita la idea del IoT, esto es, permitir al ser humano centrar toda su atención en otras actividades que no sea la de suministrar información y/o instrucciones a los aparatos electrónicos de uso cotidiano, quedando esta tarea autogestionada por ellos mismos.

Aunque Mark Weiser fue el autor que marcó el camino de lo que después se configuraría como el IoT, no fue hasta el 1999 que Kevin Ashton en una conferencia impartida en Procter

[1] TESLA, N.: A Life From Beginning to End., Hourly History
[2] 09-91 SCI AMER WEISER M.: Scientific American Ubicomp Paper after Sci Am editing

and Gamble en el año 1999 afirmara acerca de la necesidad de disponer de un estándar , un internet de las cosas, que permitan a los equipos entender el mundo real.

La afirmación de que existe una evidente relación entre el crecimiento de la World Wide Web y la incorporación de objetos cotidianos con diversas funcionalidades a la misma, pertenece a la obra "Cuando las cosas empiezan a pensar" publicada en el año 1999 por Neil Gershelfeld y, desde entonces, el término IoT ha ido adquiriendo mayor importancia y significación y que, para acabar con esta introducción al IoT, podríamos definir como la interconexión entre ellos de objetos ordinarios o cotidianos a través de internet o la interconexión de los citados objetos cotidianos con sus usuarios.

2. *Internet of Things* (Internet de las cosas) y la protección de datos desde el plano del nuevo GDPR

2.1. Hipótesis

2.2. Estado de la cuestión

2.2.1. Riesgos legales

2.2.2. Vacíos legales

2.3. IoT en el futuro

2.1 Hipótesis

Por medio de este Trabajo Fin de Máster se pretende probar que, gracias a la nueva regulación (GDPR y PLOPDyGDD) se consigue de alguna forma proteger los derechos a la intimidad y protección de datos de las personas físicas, en su condición de consumidor, aunque sin embargo seguirá siendo la educación y formación de estos últimos en la materia la única vía para conseguir su protección frente a las potenciales intromisiones (nos referimos por supuesto a las legítimas) diseñadas por los diseñadores, fabricantes y comercializadores de objetos IoT.

2.2 Estado de la cuestión.

Si bien la publicación del nuevo Reglamento de protección de datos viene de alguna manera a crear un nuevo escenario en el que se dota a los usuarios, como titulares de los datos de carácter personal que podrán ser tratados, de unas mayores garantías y de un conjunto de derechos que conlleva, lógicamente, el paralelo incremento de obligaciones y responsabilidades para aquelos operadores que traten dichos datos, tal y como veremos posteriormente[3], se tiene sin embargo que seguir hablando de riesgos para la privacidad de los usuarios utilizando las nuevas tecnologías de IoT, entre otras razones por la existencia tradicional de una seria de vacíos legales -lógicos por otro lado- si tenemos en cuenta que la tecnología y los legisladores suelen llevar de manera habitual diferenctes velocidades.

[3] Véase así la pág. 13

Si nos centramos, por ejemplo, en una tecnología wearable tan común hoy en día e impensable 6 o 7 años atrás, como son las "SmartBand" que registran un abanico enorme de información sobre los hábitos y estilo de vida de la persona que la porta e incluso permite conocer su ubicación por geolocalización e incluso el historial de los lugares y caminos por los que ha transitado. Esta tecnología y la información a la que permite acceder suministra a las empresas fabricantes o a terceros interesados, una ingente cantidad de datos de los usuarios que, convenientemente analizada, les permite conocer multitud de datos, información y al final –que es de lo que se trata- conocimiento sobre los mismos; pudiendo, tras el tratamiento oportuno de dicha información, crear un perfil sobre el usuario que puede ser muy atractivos para otras empresas o incluso para el propio fabricante del wereable[4].

2.2.1 Riesgos legales

Según Cisco, el número de dispositivos conectados a Internet en 2020 será de 50 billones[5] frente a 7,6 billones de personas en el mundo. Este incremento en el número de dispositivos que estarán a disposición del público exigirá –y exige- que los intervinientes en la comercialización de dichos dipositivos, incluyendo diseñadores, fabricantes, comercializadores, etc, dispongan de metodologías y procedimientos encaminados a garantizar, no sólo la funcionalidad del producto puesto en el mercado para su consumo, sino también, sinio también la privacidad, intimidad o seguridad de sus usuarios.

Dispositivos tan cotidianos como routers wifi, impresoras, electrodomésticos, sistemas de calefacción y alumbrado, coches inteligentes, smartphones, wereables, sistemas de planchado, etc, -esto es, elementos de uso cotidiano que se pueden encontrar en cualquier hogar -, son objetos que, con una dirección IP o URI, son capaces de recoger información, procesarla y compartirla en las redes de comunicación.

A lo largo del año 2013[6] se han conocido varios ataques relacionados con IoT. Entre éstos cabe destacar la vulneración de cientos de cámaras de seguridad para el hogar, del fabricante TrendNet, que tuvo como consecuencia el acceso no autorizado y la publicación en Internet

[4] Wereable: dícese de las tecnologías que se llevan cerca del cuerpo, en el cuerpo e incluso dentro del cuerpo. Disponible en https://www.wearable-technologies.com

[5] 50 billions: 1 billion equivale a 1.000 millones, lo que en España sería 1 millardo.

[6] Fuente: ALBERTA JAQUERO, C. INCIBE. Internet of Things (IoT). El lado inseguro de las cosas. Disponible en https://www.incibe.es/protege-tu-empresa/blog/internet-of-things-ciberseguridad. Referencia: 9 de noviembre

de imágenes de personas en sus vidas cotidianas; la red de bots llamada "Carna" que infectó 420.000 dispositivos embebidos no seguros escaneando direcciones IPv4 o la botnet descubierta por Proofpoint que lanzó 750.000 ataques de phising y spam a través de dispositivos como frigoríficos y televisiones conectadas. De este último ataque, se desprende un dato muy inquietante: 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.

Los principales riesgos, tanto regulatorios como legales, que se derivan del IoT, y que podrían suponer pérdidas económicas ya sean directas –por reclamaciones de los titulares de los datos- como indirectas –si se puede considerar así las que se podrían derivar de los daños reputacionales-, podrían resumirse en los siguientes:

1. **Intromisión en la intimidad**, que tendría lugar en los casos es que los objetos IoT recogen, almacenan y tratan todo tipo de información acerca de nuestros gustos, preferencias y actividades para ser procesada y usada no acorde con la finalidad explícita con la que en un principio se recaba.
2. **Recogida, almacenamiento y tratamiento de datos no autorizada.** Desde que los datos de usuarios y clientes han pasado de ser un elemento más necesario para la gestión del negocio, a ser considerados el negocio mismo –o al menos una importante fuente de ingresos paralela a la actividad principal- el "Big Data" se incorpora a la escena como un nuevo reto desde el punto de vista legal. La masiva recolección de datos que permiten los dispositivos IoT, puede ser legítima y llevarse a cabo de manera leal y transparente con los usuarios y clientes, pero es indudable que supone una fuente generadora de potenciales riesgos en cuanto a la vulneración de los derechos de los titulares de los datos de carácter personal en cuanto a la pérdida de capacidad de disposición sobre qué datos desea compartir o que sean tratados, ya sean los mismos necesarios para las finalidades legítimas, expresas e informadas de la empresa que los recoge, almacena y trata o, punto más delicado, no sean necesarios para conseguir aquéllos objetivos y, además, se oculte a los titulares de los datos.

Lo anterior deriva, entre otras razones que no son objeto de este TFM, por la carencia de tecnologías y estándares internacionales sectorizados, y así:

1. **La inexistencia de una tecnología o sector estandarizado** que permita prever la coexistencia de dispositivos con tecnologías incompatibles, y en consecuencia, la

pérdida de utilidad hacia el usuario de dispositivos IoT podrían derivar en pérdidas económicas ya sea, por daño reputacional o por ejercicio de acciones judiciales contra los fabricantes de dichos dispositivos.

2. **La ausencia de un estándar internacional** que garantice a los usuarios y, en paralelo, obligue a los fabricantes, a cumplir y ser respetuosos con la con la normativa de protección de datos de carácter personal, en especial y como veremos más adelante, con la privacidad desde el diseño (*privacy by design*) y la privacidad por defecto (*privacy by default*) como cimientos sobre los que desarrollar y comercializar sus dispositivos.

2.2 Vacíos legales

Emilio Aced Felez[7] respecto de lo que podríamos denominar tratamiento de datos derivados del consumo, ya afirmaba que el mismo gravita sobre los términos precisos y concretos que el consumidor finalmente ha de aceptar si es su deseo disfrutar de la tecnología IoT, y así afirmaba que *Es importante destacar que quien acepta los términos es quien se pone el sensor*.

En definitiva, de las conclusiones de Aced se infiere que ni nadie está obligado a comprar el dispositivo IoT (por ejemplo el smartwatch) ni a permitir que se recopile determinada información del usuario y sea remitido a un tercero; esto es, la tecnología que se ponga en el mercado respecto de dispositivos de la naturaleza sobre la que trata este TFM también va a exigir que aumente, igualmente de modo exponencial, el conocimiento que el usuario potencial o real tiene respecto de sus derechos –en lo que aquí importa en cuanto a sus datos de carácter personal, así como del contenido de los términos y condiciones del dispositivo adquirido para, de esa forma, poder tomar la decisión correcta respecto de la adquisición o no del mismo, a lo que aquí añade Aced "*otra cosa es que te los leas o no; aquí entraríamos ya en el terreno de si la información proporcionada es suficiente o no*[8]".

Si se permite que se traten unos datos de salud se tiene que saber en qué condiciones se está aceptando ese tratamiento de datos, para qué se van a utilizar, y luego ya se decidirá si se quiere o no compartirlos; pero también se tiene que saber si el gestor de todo esto va a hacer

[7] Fuente: ACED FÉLEZ E. jefe de Área. Unidad de apoyo al Director de la Agencia Española de Protección de Datos. Disponible en: http:// www.aepd.es. Referencia: 6 de noviembre de 2018.

[8] Fuente: ACED FÉLEZ E. jefe de Área. Unidad de apoyo al Director de la Agencia Española de Protección de Datos. Disponible en : http:// www.aepd.es. Referencia: 6 de noviembre de 2018.

algo más con esos datos, como por ejemplo establecer perfiles para venderlos a compañías de seguros para estudios de tarificación y análisis de riesgos -evidentemente datos anónimos, algo que ya está pasando; o ceder esos datos para investigaciones científicas con nombres y apellidos. "Todo eso lo tengo que saber claramente, de manera entendible, de modo que yo pueda aceptar esas condiciones de forma informada"[9].

Las Autoridades europeas de protección de datos (Grupo de Trabajo del Artículo 29[10]) aprobaron en el año 2014 el primer Dictamen conjunto sobre internet de las cosas. El documento, cuya elaboración fue liderada por la Agencia Española de Protección de Datos junto con la Autoridad francesa (CNIL), no sólo se limitó a identificar que riesgos pueden derivarse de estos dispositivos hacia la privacidad de las personas, sino que además, definió un esquema de responsabilidades. A los sólos efectos de este epígrafe, es necesario aclarar que los dictámenes del Grupo de Trabajo del artículo 29 no son fuente legislativa, pues tal y como se dice en el artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos[11], el meritado y prestigioso Grupo de Trabajo tiene carácter consultivo e independiente; ello no es obstáculo para entender el gran peso que sus dictámenes y opiniones tienen en materia de protección de datos y, como se ha configurado como un organismo generador de doctrina que las distintas Autoridades de Control siguen.

En este dictamen, se enfatiza las obligaciones en cuanto a protección de datos de los diversos actores que participan en el IoT enumerando los derechos que amparan a los ciudadanos, en cuanto usuarios de este tipo de dispositivos. La base sobre la que gravita este dictamen, es que los dispositivos que conforman el IoT recogen piezas o fragmentos aislados de información, que por sí sólo no supondría –a priori- un riesgo para los usuarios, pero que si se considera el conjunto de datos recogidos de diferentes fuentes y analizados de otra forma o en conjunción con otros pueden revelar auténticos patrones de la vida de las personas que podría incluso condicionar la forma en la que las personas se comportan en la vida real.

---

[9] Fuente: ACED FÉLEZ E. jefe de Área. Unidad de apoyo al Director de la Agencia Española de Protección de Datos. Disponible en: http:// www.aepd.es. Referencia: 6 de noviembre de 2018.

[10] Working Paper 223, año 2014 article 29 Working Group. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. Referencia 9 de octubre.

[11] Derogada con efectos de 25 de mayo de 2018, por Reglamento 2016/679, de 27 de abril (Ref. DOUE-L-2016-80807)

El Dictamen plantea tres escenarios: la conocida como tecnología para llevar puesta (wearable computing), los dispositivos capaces de registrar información relacionada con la actividad física de las personas y la domótica.

El Dictamen advierte de que, de hecho, si esta vigilancia potencial llegara a producirse, el usuario puede perder el control sobre la difusión de sus datos en función de si la recogida y el tratamiento de los mismos se realiza de manera transparente o no. Al aumento de la cantidad de datos generados hay que sumar las posibilidades que existen para combinarlos y analizarlos de forma cruzada, obtener nuevos datos sobre los originalmente solicitados y utilizarlos para usos secundarios, afines o no al tratamiento inicial. Un ejemplo destacado en el Dictamen es la información recogida por el acelerómetro y el giroscopio de un teléfono inteligente, que podría ser utilizada para deducir información con un significado muy diferente al inicial, como los hábitos de conducción del individuo.

El Grupo de Trabajo del art. 29 recuerda que el marco jurídico aplicable a cualquier sistema dirigido a usuarios europeos es la Directiva de Protección de Datos 95/46/CE, en combinación con la Directiva 2002/58/CE de Privacidad y Comunicaciones Electrónicas, y que los beneficios de esta protección no dependen de que las organizaciones estén establecidas en territorio europeo.

Así, las entidades que participan en el IoT, deben asegurarse de que la persona haya dado su consentimiento para lo cual, no sobra decir, es necesario que se solicite, de manera efectiva después de haberle proporcionado información clara y completa sobre, entre otros aspectos, qué datos se recogen, cómo se recopilan y con qué fin se van a tratar, además de cómo pueden ejercer los derechos que les asisten. Esos datos personales deben ser recogidos de manera leal y lícita, por lo que no deben ser recogidos y tratados sin que la persona sea consciente de ello. Este requisito es especialmente importante en un sector en el que los sensores son diseñados para ser tan invisibles como sea posible.

El Dictamen insiste en que la información personal sólo puede ser recogida para unos fines determinados, explícitos y legítimos. Este principio permite a los usuarios conocer cómo y con qué fines se están utilizando sus datos y decidir en consecuencia. Además, los datos recogidos deben limitarse a los estrictamente necesarios para la finalidad definida previamente. El Dictamen puntualiza que “los datos que son innecesarios para tal fin no deben ser recogidos y almacenados por si acaso o porque podrían ser útiles más adelante”.

Por último, los datos personales recogidos y tratados en el marco del IoT no deben mantenerse durante un período superior al necesario para los fines para los que fueron recogidos. El documento del GT29 especifica que, por ejemplo, los datos facilitados por un usuario cuando se suscribe a un servicio se deben eliminar tan pronto como el usuario pone fin a su suscripción. Del mismo modo, la información borrada por el usuario en su cuenta no debe mantenerse y, cuando un usuario no utiliza un servicio o aplicación, el perfil debe establecerse como inactivo hasta que pasado un tiempo se eliminen esos datos, proporcionando una información clara en todos los casos.

Como es conocido, el principio de calidad de datos es uno de los principios que inspira la legislación sobre tratamiento de datos personales, que ya venía recogido en el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Este principio implica, entre otras cuestiones, que los datos deben ser necesarios y pertinentes para la finalidad para la cual hubieran sido recabados o registrados, así como exactos y completos; podemos traducirlo, por tanto, en la afirmación de que una empresa no ha de obtener, y siempre bajo el filtro del desarrollo de su legítima actividad, más datos personales que los estrictamente necesarios.

Consecuencia de esto es que una vez que los datos personales dejen ser necesarios para los fines que se obtuvieron, se debe proceder a su cancelación, sin necesidad de esperar a la intimación a tal efecto vía solicitud del titular de los datos. Así lo establecía explícitamente este mismo artículo en su punto 5 al establecer que los datos personales deben ser *cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados*. Por tanto, el principio de calidad de datos impone a cualquier entidad, cuando proceda, cancelar los datos en su debido momento.

Pero, es quizás el quid de la cuestión poder definir de manera razonable cuándo un dato personal deja de ser necesario para la finalidad para la que se obtuvo, pues si bien no es posible hacer una generalización, si se acude a criterios de prudencia y razonabilidad y, partiendo siempre de la finalidad para la que se recabaron los datos sí será posible que se aproximen a ese momento. Por ejemplo, si una entidad solicita a través de medios de comunicación currículums para un puesto de trabajo, una vez otorgado éste a alguno de los candidatos, el resto de currículum ya no son necesarios, pues su finalidad era la de acceder a ese puesto de trabajo.

Cancelar un dato no significa su eliminación, más bien todo lo contrario, implica la obligación de conservarlo bloqueado durante un cierto tiempo. Así, cancelar un dato implica inicialmente su bloqueo, y posteriormente su eliminación física del soporte en el que esté almacenado. Por tanto, inicialmente la cancelación da lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Tan solo cumplido este plazo debe procederse a la supresión de los datos.

Para la determinación del período de bloqueo de los datos debe tenerse en cuenta el principio de reserva de ley en cuanto a las limitaciones al derecho fundamental de protección de datos de carácter personal, de forma que cualquier limitación a ese derecho deberá constar en una disposición con rango de Ley para que el bloqueo de los datos pueda considerarse lícitamente efectuado. Resulta imposible establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, los plazos de prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula a la entidad con los afectados, así como los derivados de cualquier legislación que resulte de aplicación, como el plazo de cuatro años de prescripción de las deudas tributarias, si los datos tuvieran trascendencia desde el punto de vista tributario.

El nuevo GDPR no altera los conceptos y ejemplos que se acaban de exponer, sino que haciendo gala de un "más a más" en el mismo se recogen varias de las afirmaciones vertidas en el Dictamen que acabamos de ver, ahora sí, con naturaleza legal.

Tenemos que tener en cuenta que el IoT forma parte de un "mundo en otra dimensión" más amplio y que por ahora no está dividido por países ni continentes, el mundo tecnológico, un problema añadido ya que entran en juego las diferentes normativas de cada país –la protección de datos está regulada actualmente de manera diferente en Estados Unidos y en Europa, por ejemplo, y la normativa puede llegar a variar en función de la industria de la que hablemos-.

2.3 *Internet of things* en el futuro

Gartner[12], incluyó el Internet de Todo o *Internet of Everything* (IoE) entre el top de tendencias tecnológicas estratégicas pasándose a considerar como la evolución natural del IoT.

El concepto del IoE fue acuñado en Cisco[13], que lo considera como "**reunir personas, procesos, datos y cosas para conseguir que las conexiones de red sean más pertinentes y valiosas que nunca,** convirtiendo la información en acciones que creen nuevas capacidades, experiencias más ricas y oportunidades económicas sin precedentes para las empresas, las personas y los países[14]".

El IoE tiene el objetivo de mejorar empresas, industrias y la vida de las personas al añadir progreso al Internet de las Cosas, y **se sostiene sobre los 4 pilares que constan en su definición:**

- **Personas**: conectar a las personas de una forma más valiosa.

- **Datos**: convertirlos en lo suficientemente inteligentes como para tomar mejores decisiones.

- **Procesos**: dar la información correcta a la persona o máquina correcta en el momento correcto.

- **Cosas**: dispositivos y objetos físicos conectados a Internet y entre ellos para la toma inteligente de decisiones (IoT).

Como se puede apreciar, el Internet de las Cosas es sólo uno de estos cuatro pilares[15]. Si nos remitimos a la definición más extendida de IoT, este se refiere a cualquier tipo de objeto (físico o virtual) o entidad al que puede darse la habilidad de transmitir datos sin la

---

[12] Gartner, Inc. (NYSE: IT), es una compañía de investigación y asesoramiento de referencia mundial, miembro del S&P 500.

[13] Fuente: Cisco Systemas. Disponible en https://internetofthingsagenda.techtarget.com/definition/Internet-of-Everything-IoE

[14] Fuente: Cisco Systems (año 2013). Disponible en https://gblogs.cisco.com/la/la-manera-en-la-el-internet-de-todo-mejorara-el-mundo/

[15]Fuente Cisco Systemas. Disponible en https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf

interacción hombre-máquina. Además, también incluiría las comunicaciones generadas por el usuario y las interacciones asociadas a toda la red global de dispositivos.

Podemos diferenciar ambos conceptos en el que IoE va más alla que el IoT al que engloba de forma tal que, por ejemplo traspasa el concepto de la comunicación máquina-máquina (M2M) situándose en un escenario en donde entran en juego nuevos actores: personas y procesos; es decir, en el IoT las comunicaciones se entienden como M2M, pero en el IoE se amplía incluyendo, además, las comunicaciones máquina-persona (M2P) y persona-persona tecnológicamente asistidas (P2P).

En términos sencillos, mientras el IoT conecta vía internet personas, datos, procesos y cosas, el IoE presenta un mundo en el que los dispositivos (contados por miles de millones) y a través de protocolos estandarizados, miden, valoran y detectan, no sólo su estado, sino el de otros dispositivos, otros procesos y también como no, a las personas.

Tal y como se ha afirmado anteriormente, son cuatro los pilares -personas, procesos, datos y cosas- sobre los que se sustenta el IoE, que es la evolución o está basado en el IoT que a su vez está basado en un solo pilar: las cosas.

¿Se puede afirmar entonces que el IoE es el futuro del IoT?, a día de hoy sí, pero teniendo en cuenta la velocidad a la que evolucionan tanto conceptos como tecnologías, sería temerario afirmar que el IoE es la estación de destino. Lo que sí es indudable es que este nuevo concepto rediseñará no sólo los modelos de negocio, también los procesos empresariales y, por último el denominado momento empresarial, cuyo significado veremos a continuación.

Tal y como afirma Hung Le Hong, Vicepresidente de Investigación y Socio de Gartner "En el primer nivel, la tecnología digital está mejorando nuestros productos, servicios y procesos, la experiencia de nuestros clientes y la manera en que trabajamos en nuestras organizaciones y en nuestras colaboraciones. Hacemos lo que hacemos normalmente, pero la digitalización nos permite hacerlo mejor o desarrollar productos mejores en nuestro sector[16]."

La exigencia de implementar procesos de diseño, fabricación y comercialización a una velocidad cada vez mayor implica la necesidad de que tenga lugar la reinvención digital, lo que Gartner denomina el "momento empresarial."

[16] Fuente: https://www.bbvaopenmind.com/en/the-internet-of-everything-ioe

IoE creará decenas de millones de nuevos objetos y sensores que recopilen datos en tiempo real. Según Nick Jones, Vicepresidente de Investigación y analista de Gartner "Los datos son dinero y por ello las empresas necesitarán del big data y tecnologías de almacenamiento para recopilar, analizar y almacenar el enorme volumen de información. Asimismo, para convertir los datos en dinero, los responsables de empresas e informáticos tendrán que tomar decisiones. Puesto que no dispondrán del tiempo ni la capacidad para tomar las decisiones por sí mismos, necesitarán potencia de procesamiento.[17]"

Para Dave Aron, Vicepresidente de Investigación y Socio de Gartner. "Lo digital no es una opción, no es un complemento, y no es una ocurrencia tardía, es la nueva realidad que exige un liderazgo digital integral.[18]"

Es indudable, que todos estos avances, y aquí me refiero respecto de la captura, almacenaje y posterior procesamiento de los datos recopilados implicará, irremediablemente una carrera de velocidad entre los diseñadores, fabricantes, comercializadores y terceras partes implicadas en la puesta en el mercado de estos dispositivos, con la finalidad de que recopilen más y más datos, para lo cual, será necesario a su vez, que aquellos, interconecten e intercambien también información. No es necesario añadir, que en paralelo aumentarán (o al menos debería) los recelos que el consumidor final pueda tener respecto a la protección de su privacidad y seguridad, lo que me lleva a volver a afirmar (aún a riesgo de caer en la reiteración) que el consumidor, destinatario de este tipo de dispositivos que en realidad se podría identificar como el producto en sí mismo, realice un ejercicio de autocrítica respecto del conocimiento real de sus dispositivos en cuanto a qué hacen, para qué lo hacen y para quién lo hacen.

Quien consiga ganar la confianza del consumidor, cada vez más consciente de los riesgos que para su privacidad conlleva el uso de este tipo de dispositivos, equilibrando en su justa medida la privacidad, por un lado, y la recolección de datos, por otro, será quién se convierta en el ganador de esta carrera hacia la captura del dato personal, tratable, gestionable, procesable y, por tanto, monetizable.

[17] Fuente: https://www.gartner.com/newsroom/id/2621015

[18] Fuente: Are you ready for The Internet of Things? Artículo publicado en advantage technology, 12 Febrero 2014.

Sin embargo sí podemos a día de hoy atisbar una serie de pautas que permitan o permitirán a los usuarios procurar alcanzar unos umbrales razonables de privacidad:

1. "Todo dispositivo que esté conectado a Internet es susceptible de ser accedido, y por tanto, deberá ser protegido.
2. Deberían desarrollarse estándares de seguridad de fabricación de dispositivos con conexión a internet para que todos los fabricantes puedan seguirlos.
3. Cualquier dispositivo que venga configurado con una password por defecto deberá ser cambiada siguiendo unas reglas de complejidad mínimas.
4. El fabricante puede diseñar un dispositivo para ser seguro, pero en última instancia dependerá del usuario protegerlo y asegurarse de que es inaccesible; por ejemplo, accediendo a la web del fabricante para descargarse las actualizaciones del dispositivo que cubran vulnerabilidades detectadas.
5. Conocer nuestros derechos y obligaciones en relación a la privacidad y protección de nuestros datos personales[19]".

3. Protección de Datos y privacidad en el IoT desde el GDPR.

Desde la entrada en escena del nuevo GDPR, todas las empresas y organizaciones que tratan datos de ciudadanos que se encuentren en la Unión Europea[20], sean locales o internacionales, deberán seguir una única legislación, acabando por tanto con la práctica del denominado "forum shopping[21]". Esta nueva normativa va a fortalecer los derechos de las personas físicas en cuanto a usuarios del IoT y titulares de sus datos personales, y seguramente arrastrará a las legislaciones de otros países, con el objetivo de homogeneizar estos derechos y ello con independencia de las legítimas razones por motivos comerciales que pudieran servir de detonante para adoptar decisiones de tal calado. Muestra de esta última afirmación la encontramos en España, al encontrarnos en el momento de redacción de este TFM a la espera de la publicación en el BOE de la nueva LOPDyGDD en el que se recoge la edad mínima a

[19] Fuente: *ALBERCA JAQUERO, C. "El lado inseguro de las cosas". INCIBE, marzo de 2012. https://www.incibe.es/protege-tu-empresa/blog/internet-of-things-ciberseguridad*

[20] Véase corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), de 19 de abril de 2018. https://www.boe.es/doue/2018/127/L00003-00007.pdf

[21] Forum shopping: Foro de conveniencia. Cuando se permite al sujeto elegir entre varias legislaciones la que le resulta más rentable y propicia, ya sea en términos fiscales, económicos o legales.

partir de la cual los menores son hábiles para otorgar por sí su consentimiento en el mínimo de 14 años, y en cuya decisión quizás nuestro legislador ha tenido en cuenta la opinión de los diseñadores, fabricantes y distribuidores de videojuegos,- cuya razón de ser es la publicación del nuevo GDPR-, al no ser necesario su remisión por parte del Senado a las Cortes Generales y, por tanto, ser suficiente su publicación directa en el BOE.

Con el GDPR, la protección de los datos personales pasa conceptualmente de ser un mero cumplimiento formal de un conjunto de obligaciones que, salvo raras excepciones, es percibida por el sector empresarial como un obstáculo frente a sus objetivos a entenderse como una oportunidad más de negocio y de consolidación de la fidelidad de los clientes a través de la incorporación en sus procesos de una verdadera cultura de la privacidad al estilo de lo que venía sucediendo, ya desde hace algún tiempo, con el cumplimiento normativo o Compliance, en donde lo que se persigue es que toda la estructura organizativa y las actuaciones de los distintos operadores económicos disfruten de una verdadera cultura de cumplimiento, embebida en sus procedimientos y sistemas, y no se limiten a cumplir con el ojo puesto en las posibles sanciones o repercusiones reputacionales que el incumplimiento de normas o estándares sectoriales les podrían acarrear.

De entre los mecanismos que incorpora el nuevo GDPR para proteger los derechos de los ciudadanos, deberíamos destacar dos: el análisis de riesgos y la evaluación de impacto para la privacidad (PIA en ingles, *Privacy Impact Assessment*).

Nos detendremos en esta última.

Entre los beneficios de la realización de una PIA, conforme al GDPR, se encuentran los siguientes:

• Establecer y mantener el cumplimiento de las leyes y reglamentos de privacidad y protección de datos.

• Analizar, evaluar y gestionar los potenciales riesgos que para los usuarios de este tipo de dispositivos o aplicaciones pueden suponer para con la privacidad de los usuarios.

• Obtener beneficio de las aplicaciones mientras se evalúa el cumplimiento de la seguridad y privacidad desde las primeras etapas de diseño y desarrollo.

La PIA, gravita sobre la gestión de riesgos en relación con la protección de datos y la privacidad teniendo como objetivo último, ayudar a aquellos que traten datos de carácter personal respetar tanto la privacidad como la intimidad de las personas, de una forma coherente con la realidad social en la que nos encontramos.

El proceso PIA (*Privacy Impact Assessment*) forma parte inseparable del concepto de "*accountability*" ayudando a identificar, analizar y gestionar los riesgos generados contra la privacidad de sus clientes que deriven de sus productos; de forma tal que permita, desde el inicio realizar una trazabilidad de la implicación que el agente (se trate de quien se trate) tiene en cuanto al respeto y cumplimiento de las obligaciones que pesan sobre el mismo en materia de garantizar los derechos que sobre sus datos de carácter personal tienen los ciudadanos.

El proceso consta de las siguientes fases:

1. Descripción del producto, así como de sus funcionalidades.
2. Identificación de riesgos para la privacidad que podría conllevar el uso del producto. Estimar la probabilidad de ocurrencia de dichos riesgos y la magnitud del impacto.
3. Documentación de los controles existentes y propuestos para mitigar los riesgos identificados previamente.
4. Documentación de los resultados del análisis.
5. Implementar los controles y medidas propuestas para minimizar los riesgos que se hayan identificado y,
6. Documentar los resultados de la mencionada implementación.

La planificación de la prevención de la intromisión excesiva en los datos de los usuarios y clientes no sólo deberá estar integrada en todas las actividades de la empresa sino que también deberá implicar a todos los niveles jerárquicos.

Las medidas técnicas para eliminar o reducir los riesgos en el origen (siguiendo el principio de *Privacy by design*), serán prioritarias respecto a las medidas de protección cuyo objetivo es minimizar sus consecuencias, siendo de carácter vital las acciones de información y formación para lograr comportamientos seguros y fiables de los usuarios y clientes respecto a los riesgos a los que potencialmente puedan estar expuestos por mor de la adquisición y uso de estos dispositivos IoT.

Los procedimientos para el control de los riesgos a fin de mantenerlos en niveles tolerables a

lo largo del tiempo constituyen un conjunto de actividades, que deberán ser reguladas por escrito, y que recogerán las medidas que, además de la empresa, debe adoptar el usuario priorizándolas en función de la gravedad de los riesgos existentes.

Se deberá entender por medidas de prevención todas aquellas que eliminan o disminuyen el riesgo en su origen minimizando la probabilidad de que el acontecimiento no deseado se materialice. En cambio, las medidas de protección, control y reducción de riesgos actúan fundamentalmente evitando o disminuyendo las consecuencias de los sucesos previstos.

Entre las medidas de control y reducción de riesgos que no deberían faltar en cualquier objeto o producto que encaje en el concepto de IoT, podríamos mencionar las siguientes:

1. Debe suministrar información suficiente sobre los fines del tratamiento de la información que va a recopilar así como qué categoría de datos de carácter personal van a estar afectados.
2. Mostrar, de manera transparente y accesible el procedimiento para la rectificación o eliminación de datos de carácter personal por la mera voluntad del usuario.
3. Implementar controles de acceso según la categoría de datos de carácter personal sometidos a tratamiento así como a las funcionalidades del dispositivo IoT.
4. El dispositivo IoT debería salir de fábrica con el principio "*Privacy by design*" incrustado, de tal forma que se evite que el usuario del mismo ceda, comparta o de cualquier modo "ponga en el mercado" de manera inconsciente datos de carácter personal, ya sean suyos o de su entorno.
5. Poner a disposición del usuario IoT de manera transparente, tanto las políticas como los procedimientos aplicables tanto respecto del almacenamiento como para la eliminación de los datos de carácter personal suministrados.
6. Establecimiento de controles sencillos y que a su vez sean de fácil uso, comprensión y utilización tanto respecto de la información como respecto de las diferentes funcionalidades de la aplicación o dispositivo IoT.
7. Implementación en el dispositivo IoT de las medidas de seguridad de la información necesarias que impidan o al menos dificulten -según se encuentre el estado de la técnica-, tanto cualquier intento de acceso no autorizado que implique el acceso a la información recopilada legítimamente por el dispositivo IoT como cualquier intento de acceso cuyo único objetivo sea dejar inservible el mismo.
8. Igualmente, sería deseable que el dispositivo IoT disponga de mecanismos, como

pudiera ser el cifrado de datos, cuyo objetivo sea garantizar la confidencialidad e integridad de la información manejada.

9. El dispositivo IoT deberá llevar consigo un procedimiento de actualización de software que permita al usuario diligente, tener la seguridad de que sus datos se encuentran protegidos y salvaguardados en los términos de las políticas de privacidad aplicables, llegando al extremo de que el fabricante, deje sin funcionalidad al dispositivo hasta que las nuevas políticas sean aceptadas, implementando, si ello fuera necesario, al estilo del 2FA un 2FC (doble factor de consentimiento).
10. Impregnar el producto o servicio del IoT del principio de *Privacy by Default*, de manera que el usuario tenga la relativa tranquilidad de saber que, sin perjuicio de que se le pueda exigir un nivel de diligencia mínimo, el tratamiento de los datos que recojan los dispositivos será el mínimo para que los mismos sean funcionales, quedando su privacidad e intimidad salvaguardadas.

Estas medidas, que deben derivar de la realización de una evaluación de riesgos en protección de datos y, en función de los resultados obtenidos, deberán aflorar una serie de acciones preventivas para implantar las medidas pertinentes. Dicha planificación se programará para un período de tiempo determinado y se le dará prioridad en su desarrollo en función de la magnitud de los riesgos detectados y del número o tipo de derechos que se puedan ver afectados. Se pueden distinguir así tres tipos de actuaciones preventivas, las cuales deberán quedar debidamente registradas:

1. Las medidas materiales para eliminar o reducir los riesgos en el origen, considerando siempre que las medidas materiales de prevención que eliminan o disminuyen la probabilidad de materialización de los riesgos en la protección de datos serán prioritarias respecto a las medidas de protección cuyo objetivo es minimizar sus consecuencias.
2. Las acciones de información y formación para lograr comportamientos seguros y fiables de los usuarios respecto a los riesgos a los que potencialmente puedan estar expuestos y de los que deben ser cumplidamente informados.
3. Los procedimientos para el control de los riesgos a fin de mantenerlos en niveles tolerables a lo largo del tiempo.

4. Seguridad en dispositivos del *Internet of Things*

4.1. Construyendo un entorno seguro en dispositivos del *Internet of Things*.

4.2. Requisitos de seguridad en el *Internet of Things* desde el punto de vista de la protección de datos.

4.3. Riesgos de seguridad en el *Internet of Things*.

4.1 Construyendo un entorno seguro para la protección de datos en dispositivos del *Internet of Things*.

La seguridad en los dispositivos IoT debe abordarse durante todo el ciclo de vida de los mismos, desde el diseño inicial hasta su comercialización (lo que se denomina el entorno operativo[22]). Para que un dispositivo IoT se encuentre impregnado del principio de *Privacy by design* y/o *Privacy by default* será preciso:

Que disponga de un sistema de arranque seguro Cuando el dispositivo se ejecuta por primera vez, la autenticidad e integridad del programa debe verificarse y debe hacerse por vía telemática de tal forma que sólo se cargará el programa diseñado y autorizado para ese dispositivo, según las especificaciones del fabricante y según las características o niveles de servicios comprados por el consumidor y suministradas por el fabricante[23].

Que exista un control de acceso Pueden existir distintos recursos al alcance del consumidor o del fabricante (léase también comercializador) que utilicen como vehículo el mismo dispositivo IoT. Se deberá contar con distintos controles de acceso de tal forma que el sistema operativo del dispositivo disponga de un mecanismo de limitación de privilegios y, en consecuencia, las aplicaciones sólo puedan tener acceso a los recursos que necesitan para desarrollar su función. De esta manera, por ejemplo, en el supuesto de que la integridad, confidencialidad o seguridad del dispositivo se vea comprometida el intruso tendrá sólo un acceso mínimo de tal forma que la integridad de la información recogida en el dispositivo IoT permanezca lo más a salvo posible al estilo de los mecanismos de seguridad establecidos basados en redes, donde se persigue que no quede comprometida la integridad del sistema.

[22] SHIPLEY, A., "Security in the internet of things, lessons from the past for the connected future," Security Solutions, Wind River, White Paper, 2013.

[23] ATZORI, L., IERA, A., MORABITO, G., and NITTI, M. “The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, pp. 3594- 3608, 2012.

Que se implemente un sistema de autenticación del dispositivo Cuando el dispositivo está conectado a la red, debe autenticarse antes de recibir o enviar datos. Esta afirmación, que parece inherente y casi consecuencia natural de este tipo de dispositivos, sin embargo, ha de ser diseñado de forma que no se cuente con la colaboración del usuario, pues obligar a estos a tener que ingresar las credenciales necesarias para obtener acceso a la red, supondría el fracaso comercial más absoluto. ¿Cómo, entonces, puede garantizarse que estos dispositivos se identifiquen correctamente? un buen sistema sería al estilo de la autenticación de usuario permite al usuario acceder a la red corporativa y a los recursos o permisos concedidos en su favor en función de la contraseña y el nombre de usuario, de tal forma que el dispositivo IoT debería disponer de un conjunto similar de credenciales almacenadas en un área de almacenamiento segura[24], incluso llegando al sistema de 2FA si fuera necesario pero autogestionado por el mismo dispositivo.

Que disponga de Firewall e IPS El dispositivo necesita disponer de un sistema firewall diseñado que monitorice el tráfico de datos, admitiendo las comunicaciones autorizadas y bloqueando las que no, y ello, con independencia de su implementación directa en el hardware o software del dispositivo IoT o, por qué no, en ambos. Igualmente sería deseable que el dispositivo disponga de un sistema de transporte de información que se ejecute por redes IP estándar, pero bajo la protección del protocolo IPS.

Aquí nos encontramos con uno de los problemas comentados anteriormente, el riesgo de que los diferentes dispositivos IoT dispongan de protocolos únicos e incompatibles entre sí. Por ejemplo, la red eléctrica inteligente tiene su propio conjunto de protocolos que rigen la forma en que los dispositivos se comunican entre sí. Esta es la razón por la cual existe la necesidad de un protocolo específico para la industria que disponga de unas capacidades de inspección profundas para identificar cargas maliciosas ocultas en protocolos de IoT no estandarizados y aparentemente inocuos. El dispositivo no debe estar diseñado para generar un mayor nivel de filtrado del tráfico en Internet, para eso deberían estar los dispositivos de red comunes sin embargo sí debe estar concebido para proteger la información cuando la misma sea

[24] ATZORI, L., IERA, A. and MORABITO, G., "The internet of things: A survey," Computer Networks, vol. 54, pp. 2787-2805, 2010.

recolectada (y por tanto transferida), momento más delicado en el proceso de garantizar la confidencialidad e integridad de la información[25].

Disponibilidad de actualizaciones y parches Cuando el dispositivo IoT arranque, debería comenzar a recibir las actualizaciones y/o parches de seguridad de las aplicaciones instaladas en el mismo (al estilo de lo que sucede con nuestros actuales smartphones); por lo tanto, será preciso en primer lugar que el dispositivo sea capaz de autenticar la fuente de la actualización o del parche de seguridad, procurando no consumir mucho ancho de banda o afectar a la su seguridad. Una vez autenticado el origen se podrá proceder a su actualización o instalación.

4.2. Requisitos de seguridad en el *Internet of Things*, desde el punto de vista de la protección de datos.

Desde el punto de vista del usuario en general los objetos del IoT utilizan diversos modelos de comunicación entre sí y para con el usuario, que sirven para ilustrar la capacidad de agregar valor que tienen los dispositivos conectados en red. Al permitir que el usuario logre un mejor acceso a un dispositivo de la IoT y a sus datos, el valor global del dispositivo aumenta. Por ejemplo, al crear procesos que permitan comunicar datos a la nube, los usuarios y los proveedores de servicios pueden agregar, analizar y visualizar datos más fácilmente; además, las tecnologías de análisis predictivo obtienen más valor de los datos de la IoT del que pueden obtener las aplicaciones de silos de datos tradicionales. En otras palabras, las arquitecturas de comunicación eficaces son un importante generador de valor para el usuario final, ya que abren la posibilidad de utilizar la información de formas nuevas. Sin embargo, cabe señalar que estos beneficios no vienen sin desventajas. Al considerar una arquitectura determinada, es necesario considerar cuidadosamente el coste en que deben incurrir los usuarios para conectarse a recursos en la nube, especialmente en las regiones donde los costos de conectividad del usuario son elevados.

Los modelos de comunicación efectivos benefician al usuario final, pero también cabe mencionar que los modelos eficaces de comunicación de la IoT también mejoran la innovación técnica y las oportunidades para el crecimiento comercial. Se pueden diseñar nuevos productos y servicios que aprovechen los flujos de datos de la IoT que antes no existían, y estos podrían ser el germen que catalice la innovación.

[25] JARA, A. J., ZAMORA, M.A., and SKARMETA, A.F. "An internet of things---based personal device for diabetes therapy management in ambient assisted living (AAL)," Personal and Ubiquitous Computing, vol. 15, pp. 431- 440, 2011.

Todos estos flujos de comunicación, en los que tiene lugar una transmisión de datos de carácter personal deberán ser previstos, analizados, organizados y expuestos por el fabricante al usuario al fin de que este sea capaz de saber en qué momento se está produciendo la captación y posterior transmisión y/o procesamiento, etc. de sus datos de carácter personal, lo que debería tener lugar mediante el uso de un lenguaje sencillo y altamente comprensible.

Si observamos una infraestructura diseñada para dar servicio a dispositivos IoT, es indiscutible que la capa de red es la que tiene que hacer frente a los mayores desafíos si de seguridad hablamos. A continuación se describen algunos requisitos de seguridad de una infraestructura IoT[26]:

1. Tolerancia frente a fallos de comunicación: el sistema debe ser capaz de encontrar un nodo alternativo, cuando ocurre una interrupción en el trafico en uno de los nodos, para evitar que el servicio se interrumpa.
2. Autenticación: debe autentificar el objeto y la fuente de información.
3. Control de acceso: los proveedores de información, que en este caso serían los usuarios de los dispositivos IoT deben poder ser capaces de disponer de un control de acceso en relación con los datos proporcionados.
4. Privacidad: No entendida en exclusiva como la privacidad respecto del fabricante o comercializador del dispositivo IoT en relación con el tipo de información que recopila el mismo, sino también ampliada a otros aspectos como: identificación del usuario, almacenamiento seguro, administración de identidades, comunicación segura de datos, disponibilidad, acceso seguro a la red, contenido seguro, entorno de ejecución segura, manipulación indebida resistencia. La arquitectura de seguridad de IoT se divide en cuatro niveles:

1. Capa física
2. Capa de red
3. Capa de soporte
4. Capa de aplicación

[26] BABAR, P., MAHALLE, A., STANGO, PRASAD, N., and PRASAD, R., "Proposed security model and threat taxonomy for the internet of things (IoT)," in Recent Trends in Network Security and Applications, ed: Springer, 2010, pp. 420-429. Disponible en https://link.springer.com/chapter/10.1007/978-3-642-14478-3_42

1. Capa física

En esta capa, es a través de dispositivos periféricos, es decir, equipos físicos, como se recopila los datos y la información y como se identifica el mundo físico, incluyendo, las propiedades del objeto, condiciones ambientales etc. El elemento principal de esta capa son los sensores para capturar y representar el mundo material que existe alrededor del dispositivo IoT en el mundo digital. Debido a que los nodos de almacenamiento son muy cortos y la capacidad de potencia también, es muy complicado técnicamente hablando aplicar algoritmos de cifrado y por tanto es muy difícil establecer un sistema de protección de seguridad. Son, por tanto, vulnerables a los ataques de la red externa, como la denegación de servicio, lo que a su vez también puede generar nuevos problemas de seguridad.

2. Capa de red

Esta capa es responsable de la transferencia de información desde el procesamiento de la información preliminar de la capa conceptual. En esta capa, la transferencia de información depende de varias redes de Internet, como por ejemplo: una red de comunicaciones móviles y redes de televisión por satélite y una infraestructura de red inalámbrica, siendo por tanto precisos protocolos de comunicación que permitan intercambiar información entre los distintos dispositivos. A pesar de que, al menos en teoría, proteger la seguridad en la capa de red sería la parte más sencilla, todavía existen los denominados ataques Man-In-the-Middle-Attack, así como la existencia de virus informáticos diseñados para "infectar" de manera específica este tipo de dispositivos. Por lo tanto, la seguridad en este nivel es muy importante para garantizar la integridad, confidencialidad y autenticidad de la información en los dispositivos IoT, teniendo también, a día de hoy, el mismo problema que en la capa física, esto es, la implementación de mecanismos de seguridad es difícil.

3. Capa de soporte

La capa de soporte desempeña el papel de la aplicación combinada de la capa superior y la capa de red en la parte inferior. Tal y como señala Hyassinni Margarita Lizárraga Álvarez "La capa de soporte de datos aísla de manera efectiva los procesos de comunicación en las capas superiores desde las transiciones de medios que pueden producirse de extremo a extremo. Un paquete se recibe de un protocolo de capa superior y se dirige a éste, en este caso IPv4 o IPv6, que no necesita saber qué medios de comunicación utilizará.

Sin la capa de enlace de datos, un protocolo de capa de red, tal como IP, tendría que tomar medidas para conectarse con todos los tipos de medios que pudieran existir a lo largo de la ruta de envío. Más aún, IP debería adaptarse cada vez que se desarrolle una nueva tecnología de red o medio. Este proceso dificultaría la innovación y desarrollo de protocolos y medios de red. Éste es un motivo clave para usar un método en capas en interconexión de redes.

El rango de los servicios de la capa de enlace de datos tiene que incluir todos los tipos de medios actualmente utilizados y los métodos para acceder a ellos. Debido a la cantidad de servicios de comunicación provistos por la capa de enlace de datos, es difícil generalizar su papel y proporcionar ejemplos de un conjunto de servicios genéricos. Por ese motivo, tenga en cuenta que cualquier protocolo dado puede o no admitir todos estos servicios de la capa de enlace de datos"[27].

4. Capa de aplicación

Esta capa proporciona servicios personales de acuerdo a las necesidades del usuario. Los usuarios pueden iniciar sesión en Internet a través de la capa de interfaz de la aplicación ya se trate de un PC, un Smartphone, un móvil, una TV, y así sucesivamente. Los requisitos de seguridad varían según el entorno, el nivel de diferentes aplicaciones que entran en juego en esta capa, así como el alcance y contenido del intercambio de datos entre el dispositivo y el usuario o, entre los mismos dispositivos. En esta capa se necesitan resolver dos problemas: por un lado el de la autenticación a través de una red pública y, el segundo, es la privacidad del usuario.

4.3. Riesgos de seguridad para la privacidad desde el IoT

Al ser dispositivos conectados a internet, por definición, y al no disponer de manera habitual con los mismos estándares de seguridad que otro tipo de dispositivos que precisa de la red para su funcionamiento, el riesgo de que sean accedidos por terceros y se vea comprometida su seguridad, en términos de información claro está, es relevante.

Las deficiencias de seguridad más habituales en los dispositivos IoT, suelen ser:

---

[27] Fuente: LIZÁRRAGA ÁLVAREZ, M., curso de CCNA1 de Cisco Systems. Disponible en https://sites.google.com/site/cursoenlineaccna1

1. "Usuarios y contraseñas de acceso por defecto y sin mecanismos que obliguen al usuario a cambiarlas por otras más seguras;
2. Páginas web de control y configuración inseguras o accesibles en remoto;
3. Inexistencia de cifrado en las comunicaciones;
4. Falta de personalización en la configuración de la seguridad;
5. Falta de soporte y actualizaciones de los fallos de seguridad detectados tanto en el software de control como en el firmware de los dispositivos"[28].

Es precisamente, la virtud de los dipositivos IoT lo que les puede hacer más atractivos a la hora de recibir ataques; y esto tiene lugar por la sencilla razón de que en realidad, el acceso no autorizado no tiene por destinatario el dispositivo IoT específicamente (que bien es cierto que sí podría tener lugar), sino que lo se busca es un punto de entrada –una puerta- a la que acceder de manera más sencillas al encontrarse menos protegidos que otros puntos de acceso a la información a la que ilegítimamente se pretende acceder, o a la información que maliciosamente se pretende dañar.

El ataque y compromiso de estos dispositivos puede dar lugar a consecuencias graves para la seguridad como:

1. Ser convertidos en dispositivos Zombie que puedan realizar ataques DDoS;
2. Ser utilizados, tal y como hemos afirmado anteriormente, como punto de acceso para atacar a otros equipos que formen parte de la misma red, verdadero objetivo, ya sea para robar, bloquear, manipular todo tipo de información o comprometer los servidores;
3. Reconfigurar los dispositivos y, por tanto, manipular las instrucciones del usuario afectando de esta forma las condiciones de utilización. (por ejemplo, manipulación de los termostatos de un CPD con el objetivo de dañarlos físicamente a través del aumento de la temperatura de la sala).

Entre las medidas que el Instituto Nacional de Ciberseguridad (INCIBE) propone con carácter general, se encuentran:

[28] Fuente: INCIBE. Riesgos del internet de los trastos. Disponible en https://www.incibe.es/protege-tu-empresa/blog/iot-riesgos-del-internet-los-trastos

1. Cambiar las contraseñas de fábrica por defecto;
2. Adquirir los dispositivos que resulten más seguros y que permitan actualizaciones de seguridad;
3. Habilitar su acceso a la red solo cuando sea necesario;
4. Evitar configurar el acceso a la red wifi de la empresa o domicilio;
5. Deshabilitar el acceso remoto a los mismos desde fuera de la red interna corporativa o doméstica;
6. Restringir el acceso únicamente a personas autorizadas;
7. Desactivar la interfaz web si es posible y el dispositivo lo permite;
8. Establecer un canal cifrado de comunicación.

A las que se pueden añadir:

1. Cambiar las credenciales predeterminadas de nuestros dispositivos IoT.
2. Utilizar contraseñas robustas.
3. Actualizar su firmware a su última versión.
4. Instalar las actualizaciones de las aplicaciones de nuestros dispositivos IoT tan pronto como estén disponibles.
5. Deshabilitar las características y funcionalidades que no deseemos utilizar.
6. Si no utilizamos la conectividad de red de nuestro dispositivo, apagarla. Si la usamos, o si es necesaria para el funcionamiento del dispositivo, verificar que el panel de administración no está accesible desde internet.
7. Aplicar una sólida segmentación de red para los dispositivos IoT conectados. Debemos preguntarnos: ¿El dispositivo necesita conectarse a internet? ¿Necesita acceder a la misma red a la que se conectan nuestros otros dispositivos corporativos?
8. Deshabilitar o proteger el acceso remoto a nuestros dispositivos IoT mientras que éste no sea necesario. El acceso remoto es la funcionalidad que permite controlarlos a distancia.
9. Investigar y aprovechar las medidas de seguridad que ofrece nuestro dispositivo IoT en concreto.

Consecuencia de lo anterior es que los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los

medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identi ficable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación. El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización en los dispositivos IoT, ya sea como opción única de funcionamiento ya sea como opción a considerar por el usuario, permitiendo al mismo tiempo que la funcionalidad publicitada del dispositivo no vea perdida totalmente su utilidad, pues entonces aquellos usuarios más formados en materia de protección de datos o aquellos otros más celosos de su intimidad dejarán de ser destinatarios y potenciales clientes de los meritados dispositivos. **No es la primera vez que una tecnología puntera se abandona por falta de rendimiento económico.**

El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe

darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

El establecimiento principal de un responsable del tratamiento en la Unión debe ser el lugar de su administración central en la Unión, salvo que las decisiones relativas a los fines y medios del tratamiento de los datos personales se tomen en otro establecimiento del responsable en la Unión, en cuyo caso, ese otro establecimiento debe considerarse el establecimiento principal. El establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables. Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza en dicho lugar. La presencia y utilización

de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determi nantes de un establecimiento principal. El establecimiento principal del encargado del tratamiento debe ser el lugar de su administración central en la Unión o, si careciese de administración central en la Unión, el lugar en el que se llevan a cabo las principales actividades de tratamiento en la Unión. En los casos que impliquen tanto al responsable como al encargado, la autoridad de control principal competente debe seguir siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, pero la autoridad de control del encargado debe considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el presente Reglamento. En cualquier caso, las autoridades de control del Estado miembro o los Estados miembros en los que el encargado tenga uno o varios establecimientos no deben considerarse autoridades de control interesadas cuando el proyecto de decisión afecte únicamente al responsable. Cuando el tratamiento lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

5. *Internet of Things*: Sector de la Automoción. ¿Autopista hacia la desprotección de los datos de carácter personal?

Un coche fabricado por la empresa Tesla tuvo un accidente cuando estaba en piloto automático. El coche se metió debajo del remolque de un camión produciendo la muerte inmediata del conductor que iba en el vehículo.

Joshua Brown, había delegado la responsabilidad de la conducción en su vehículo, que a través de inteligencia artificial va aprendiendo de la conducción manual del conductor[29]. Según los informes oficiales, el coche de Brown iba a mucha velocidad y no frenó cuando debería de haber frenado.

A pesar de la cantidad de sensores que lleva el vehículo, no detectó el camión, ya que era blanco y la luz que había ese día pudo haber contribuido a la no detección del camión.

[29] Fuente: The NewYork Times. https://www.nytimes.com/2016/07/02/business/joshua-brown-technology-enthusiast-tested-the-limits-of-his-tesla.html

Al ser el primer accidente de este tipo, existe un vacío legal y no está claro de quién es la responsabilidad del accidente. Desde la compañía explican que en el momento que el piloto automático es puesto en marcha, es una condición imprescindible mantener las manos en el volante, y si el coche no detecta esto, se detiene inmediatamente. Así pues, ¿es culpa del conductor o de la empresa que ha fabricado el coche y el accidente es producido por la "inteligencia artificial" Tesla?

Existe un concepto en filosofía que se denomina "Moral utilitaria". Es una doctrina que se basa en que el resultado final es lo que importa. Podemos aplicar este concepto al ejemplo de los automóviles autónomos. Si estos automóviles se programan según esta moral, en caso de accidente siempre se buscaría producir el menor número de muertos posibles, pudiendo darse el caso de que el coche decidiera matar a sus ocupantes si fuera menor que el número de muertos resultantes que produciría si no lo hiciera.

Este tipo de comportamiento del vehículo produce una serie de dilemas morales y legales que son difíciles de abordar.

Un estudio de la revista Science (Jean-François Bonnefon, Azim Shariff, Iyad Rahwan ,2016), realizó una encuesta en la que planteaba si un vehículo autónomo debería comportarse según esta situación30. La gran mayoría de personas creía conveniente que estos vehículos deberían de comportarse así, incluso si sus propios hijos fueran a bordo del vehículo.

Las aplicaciones en la industria de la automoción incluyen el uso de "cosas inteligentes" para poder monitorizar las variables y eventos que tienen lugar en un automóvil y así poder controlar desde la presión en los neumáticos a la proximidad de otros vehículos.

En la industria del automóvil, los sensores y los sistemas embebidos ya desempeñan un papel importante. Sin embargo, estos se vuelven aún más importantes cuando se trata de integrarlos en un futuro "Internet de los vehículos" dónde se pueda establecer comunicación entre ellos y entre los vehículos y las infraestructuras que los rodean. Esto se ha convertido en un área de investigación muy importante en los últimos años. Existen distintos casos de uso que han sido propuestos y analizados, que van desde sistemas de advertencia relacionados con la seguridad hasta aplicaciones de información y entretenimiento. Los vehículos que se activan de forma inalámbrica pueden disponer de aplicaciones para la detección de las condiciones de la

[30]The social dilemma of autonomous vehicles. **http://science.sciencemag.org/content/352/6293/1573**

carretera a través de sensores y de un módulo de comunicaciones que además permitiría a cada vehículo de forma autónoma conectarse con el resto e intercambiar información.

Al detectar posibles riesgos en la carretera, estos vehículos pueden generar mensajes que contienen una descripción de la incidencia y su posición geográfica. Estos mensajes pueden ser transmitidos inmediatamente a todos los vehículos que se encuentren dentro de los límites de comunicación, y estos a su vez pueden almacenarlos, evaluarlos y reenviarlos.

Los sistemas de comunicación de corto alcance o DSRC (Dedicated Short Range Communication) también ofrecen la posibilidad de emplear mayores tasas de bits y reducir la posibilidad de interferencia con otros equipos.

Las comunicaciones vehículo a vehículo o V2V (vehicle to vehicle) y vehículo a infraestructura o V2I (vehicle to infrastructure) impulsarán significativamente las aplicaciones basadas en sistemas de transporte inteligente o ITS (Intelligent Transportation Systems), tales como los servicios de seguridad de los vehículos o los de gestión del tráfico, integrándolas totalmente en la infraestructura del Internet de las Cosas31.

El propio vehículo también se considera como una "cosa", lo que le permitiría realizar por ejemplo llamadas automáticas de emergencia en caso de accidente o avería, mediante la recopilación de todos los datos posibles del vehículo así como del entorno en el que se encuentra, para dar parte de ellos y poder asistir a la persona accidentada.32

Además, mediante el uso de estas tecnologías también se puede llevar un mejor control de las emisiones del vehículo de forma que se contribuye a una mejora en la calidad del aire.

Existe una amplia gama de tecnologías complementarias de captura de datos e identificación automática o AIDC (Automatic Identification and Data Capture) que pueden ser utilizadas en

---

[31] Fuente: Sistemas inteligentes de transporte. Departamento de ingeniería de la información y las comunicaciones. Universidad de Murcia. https://www.um.es/gsit/research_lines/its/?l=es

[32] Este sistema, denominado e-call es obligatorio en todos los coches y vehículos comerciales nuevos que vayan a ser comercializados en la Unión Europea a partir del 31 de marzo de 2018, en virtud de la entrada en vigor del Reglamento (UE) 2015/758 del Parlamento Europeo y del Consejo, de 29 de abril de 2015, relativo a los requisitos de homologación de tipo para el despliegue del sistema eCall basado en el número 112 integrado en los vehículos y por el que se modifica la Directiva 2007/46/CE, si bien está enfocado a los accidentes y no a las averías. Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015R0758

numerosas aplicaciones de este tipo. En la actualidad también se están considerando otras técnicas, tales como el uso de pequeños microprocesadores con algún tipo de capacidad de comunicación.

Por otro lado, la tecnología RFID se utiliza para optimizar la cadena de producción de vehículos, mejorar la logística y los mecanismos de control de calidad así como para mejorar el servicio al cliente. Los dispositivos que se incorporan en las diferentes piezas o productos contienen información relacionada con el nombre del fabricante, lugar y fecha de fabricación, número de serie, código de producto, y en algunas aplicaciones pueden contener hasta la ubicación concreta de la pieza en la instalación en ese momento. La tecnología RFID ofrece datos en tiempo real sobre el proceso de fabricación o las operaciones de mantenimiento. De esta forma proporciona una forma de gestión nueva y más eficaz.

El uso de dispositivos de identificación inalámbrica acelera los procesos de montaje y facilita la localización de vehículos o componentes en apenas unos segundos. Las tecnologías inalámbricas son ideales para los sistemas de localización en tiempo real o RTLS (Real Time Location System) y para la conexión con otras subredes del Internet de las Cosas.

Toyota junto con Microsoft y la compañía de software Salesforce.com han desarrollado una aplicación, Toyota Friend, basada en una red social que permite establecer comunicación entre vehículos, así como entre los automóviles y sus conductores. Esta nueva plataforma se pondrá en marcha durante este año en Japón.

Gracias a esta nueva aplicación los usuarios podrán comunicase entre sí además de recibir en forma de alertas en el móvil o tweets notificaciones sobre el estado de su vehículo o su situación geográfica (informando por ejemplo de la distancia a la que se encuentra del hogar del usuario) o avisos por ejemplo de su nivel de batería o combustible, la presión de las ruedas o incluso del estado del tráfico. Este sistema también proporcionará información acerca del tiempo o avisos de que el vehículo debe pasar la revisión correspondiente. Además los usuarios podrán publicar estas notificaciones en su perfil de Facebook o Twitter.

Gracias a toda esta información el usuario puede también decidir qué camino elegir para dirigirse a su destino o incluso si sería conveniente utilizar el transporte público en lugar de su propio vehículo en función del estado de su automóvil, las condiciones del tiempo o el tráfico en ese momento.

Otra de las aplicaciones del Internet de las Cosas relacionadas con el mundo del automóvil se basa en el uso de sensores para determinar a los conductores la localización de las plazas de aparcamiento gratuitas. Esta aplicación también se utiliza en aparcamientos públicos para indicar a los conductores mediante sensores inalámbricos dónde se encuentran las plazas libres. Los datos recogidos sobre el estado del aparcamiento se envían periódicamente a una base de datos mediante una red inalámbrica de sensores, para posteriormente remitírselos a los vehículos que van accediendo al parking. Cuando los automóviles entran en el aparcamiento pueden obtener un plano general de todo el parking en el que se indican las plazas libres de aparcamiento.

Riesgos para la privacidad

Uno de los mayores riesgos que puede presentar esta aplicación está relacionado con la capacidad del automóvil para actualizar en todo momento su ubicación y por lo tanto la del conductor. En estos casos se plantean cuestiones relativas a la privacidad como, ¿qué podría ocurrir si el conductor olvida modificar la configuración de privacidad de esta aplicación y su ubicación se revela de forma automática sin tener él conocimiento de ello? ¿o si su automóvil publica en su cuenta de Facebook o Twitter la fecha de su próxima revisión, revelando públicamente la fecha y hora de su localización y la del conductor en el futuro? Esto puede suponer una amenaza para los usuarios de este tipo de aplicaciones, ya que cualquier individuo podría tener acceso a información muy valiosa acerca de estos usuarios, pudiendo llegar a rastrear sus movimientos y hábitos en función de la localización de su automóvil.

6. El caso concreto del Seat Cristóbal

Según el propio fabricante, el prototipo desarrollado por SEAT dispone en una primera vesión

del concept car con al menos 6 asistentes de seguridad, entre ellos, una caja negra parecida a la de los aviones que le permitirá desarrollar 19 funciones que encajarían dentro del objeto de investigación de este TFM: el IoT en su versión vehículos.

De esta forma, y según la presentación que se hizo en la pasada Smart City Expo desarrollada en Barcelona, el Seat Cristóbal dispone de las siguientes funcionalidades inteligentes:

Asistente 'Mentor', por el que se puede limitar la zona geográfica por la que el coche puede circular así como la velocidad. Si el vehículo sobrepasa los límites señalados por el administrador del sistema, le llega un aviso al propietario y el conductor recibirá instrucciones para regresar, por el camino más corto, al área de circulación autorizada. Incluso Seat anuncia que se podrían pensar en activar medidas disuasorias tales como no poder usar la música mientras el vehículo permanezca fuera de los límites –lo que debe ser traumático para un adolescente en su fin de semana-.

Igualmente, a través del denominado asistente "Mentor" se puede programar el vehículo para que quede inutilizado –en el sentido de que no se pueda arrancar- en el caso de que tras usar el etilómetro incorporado al vehículo supere, no ya los límites legales marcados en el momento en que el usuario pretenda hacer uso del vehículo, sino del límite que la persona con permisos de administrador haya dejados señalados como límite para su uso.

Uso de cámaras. Se trata de dos cámaras, una frontal y otra dirigida hacia el interior del vehículo. La primera, que graba la carretera, hace las veces de caja negra de forma tal que en el caso de que los sensores del vehículo detecten un frenazo violento, dejará registrado los últimos 10 segundos de la conducción así como una serie de parámetros tales como: localización, usuario, velocidad, aceleraciones y frenazos; información que en forma de metadatos y en unión del video, se enviará directamente al smartphone del conductor o del administrador en el caso de que no coincidan. La segunda, está diseñada para hacer reconocimiento facial del conductor, es lo que se denomina una cámara de 'face tracking'. Si apartas los ojos de la carretera, recibes un aviso para que no lo hagas. Si detecta que te estás durmiendo, hace vibrar el asiento para espabilarte y te muestra un aviso en la pantalla de navegación para que pares y descanses, incluso desde Seat se anuncia que está bajo estudio detectar vía dilatación de pupilas detectar el uso de estupefacientes o medicamentos por parte de quien esté en ese momento al volante así como también impedir que el vehículo se pueda poner en marcha si el rostro del conductor no es reconocido. Igualmente, esta cámara interior detectará si el conductor –por la razón que sea- aparta la mirada de la calzada, de forma tal

que saltará un aviso o, en su caso, si la razón de la distracción es por haber dirigido su atención hacia el Smartphone o, incluso la consola de información del propio vehículo, este activará una voz que leerá los mensajes y que dispondrá de un sistema preconfigurado de respuestas activables por un simple gesto.

Funcionalidades tales como el 'Guardian Angel' gracias al cual, si se supera la distancia de seguridad o se detectan síntomas de fatiga o cansancio en el conductor o se superen en el porcentaje señalado por el administrador del sistema los límites de velocidad, el vehículo será capaz de lanzar avisos en forma de vibración del asiento o sonoros.

A través de lo que el diseñador del vehículo denomina sistema 'Display Mirror" el conductor, puede activar de una manera muy sencilla una cámara que permitirá ver, respecto de la parte posterior del vehículo que está sucediendo persiguiendo, en principio con esta funcionalidad eliminar los denominados ángulos muertos.

Si se cierra el vehículo dejando dentro pasajeros, niños o animales, el propio vehículo será capaz de regular la temperatura interior (llegando incluso si es necesario a abrir el techo del mismo) así como enviar un mensaje a la app del conductor. En el supuesto de que el conductor hiciera caso omiso podrá, incluso, activarse la alarma del vehículo.

El otro punto se encuentra en las puertas laterales pues si detecta que se acerca un objeto dentro del radio de apertura de la puerta, está previsto un sistema de alarmas vía vibración del asiento, iluminación del retrovisor o incluso avisos de voz para que no se abra dicha puerta.

Hasta ahora se ha tenido la oportunidad de ver las bondades del Cristóbal como concept car de Seat, pero todas estas bondades llevan aparejadas una ingente cantidad de tratamientos de datos de carácter personal que, sin las debidas medidas, podrían suponer una inmisión excesiva y desproporcionada en los derechos que los usuarios, en cuanto titulares de dichos datos de carácter personal tienen reconocidos legalmente, por lo que haremos un análisis de cómo el nuevo Reglamento UE 2016/679 de 27 abril (GDPR), regula aquellos aspectos más destacables de las funcionalidades del concept car de Seat sobre los que nos vamos a centrar: la geolocalización, el tratamiento de datos de salud y el tratamiento de datos biométricos.

No se puede proseguir en el desarrollo de este TFM sin estudiar, aunque sea brevemente, los nuevos principios que respecto de la forma de tratar los datos de carácter personal se incorporan, destacando en especial33:

Responsabilidad proactiva; mediante la implementación de mecanismos que nos faculten para acreditar de alguna forma que se han tomado todas, o al menos aquellas disponibles, las medidas necesarias para tratar los datos de carácter personal.

Protección de datos por defecto y desde el diseño; consistente básicamente en adoptar, todas aquellas medidas organizativas y técnicas que sean necesarias para que la obtención de los datos, y su mantenimiento tenga garantizada la seguridad y privacidad de los mismos, por una lado; y por otro, que el dispositivo (en este caso nuestro Seat Cristóbal) y sus funcionalidades salga de fábrica con los parámetros necesarios activados o desactivados, de tal forma que la privacidad del propietario del vehículo se encuentre bajo máximos en términos de garantía de su privacidad. La privacidad desde el diseño se extiende a una trilogía que comprende: 1) sistemas de TI; 2) prácticas comerciales responsables; y 3) infraestructuras de red.

Los principios de privacidad por diseño pueden aplicarse a todos los tipos de información personal, pero con especial vigor a los datos confidenciales, como la información médica y los datos financieros. La solidez de las medidas de privacidad implementadas tiende a ser proporcional a la sensibilidad de los datos. Los objetivos del *Privacy by Design* son garantizar una privacidad sólida y obtener un control personal sobre la información personal y, para las organizaciones, obtener una ventaja competitiva sostenible puede lograrse mediante la práctica de los Principios Fundamentales, que tienen la intención de servir como la base de uno. prácticas de privacidad. son garantizar una privacidad sólida y obtener un control personal sobre la información personal y, para las organizaciones, obtener una ventaja competitiva sostenible puede lograrse mediante la práctica de los 6 Principios Fundamentales, que tienen la intención de servir como la base de uno. prácticas de privacidad.

Las regulaciones de privacidad de los datos imponen pautas específicas sobre las clases de datos que deben protegerse, incluidos los datos personales, la información médica protegida y los datos financieros. Los datos obtenidos a través de sensores de IoT, los códigos de geolocalización, los números de identificación del vehículo (VIN) y las direcciones IP, junto

[33] DIMITROV, W. XXV conference Telecom 2017 26-27 October, NSTC, Sofia, Bulgaria. **GDPR entrapments. Proactive and reactive (re)design thinking.** University of Library Studies and Information Technologies (UNIBIT) Bulgaria. http://ceec.fnts.bg/telecom/2017/documents/CD2017/Papers/26.pdf

con muchos otros elementos de datos, son considerados datos de carácter general por el nuevo GDPR).

Principio de transparencia; haciendo que todos los avisos legales y políticas de privacidad sean exteriorizados y comunicados de manera sencilla e inteligible. Este principio es complemento directo del Principio de información y, por tanto, del consentimiento, tal y como podremos ver a continuación. La falta de información sobre cómo se han obtenido los datos, podría llevar a una responsabilidad financiera o legal, además de afectar la cuenta final de resultados de la empresa que trata los datos. Los datos obtenidos legítimamente, pero almacenados de manera inadecuada, pueden llevar igualmente a sanciones costosas para las organizaciones. Los datos mal categorizados también pueden suponer la vulneración de la normativa vigente. No saber qué contiene cada uno de sus conjuntos de datos crea confusión sobre quién puede acceder a esos datos; y si individuos no autorizados acceden a información confidencial, estarán poniendo, incluso sin su propio conocimiento, en riesgo a la empresa.

Además de los seis principios que, con carácter general, se han tener en cuenta en el uso, tratamiento y almacenamiento de datos de carácter personal, siendo los mismos:

Los datos personales deben ser tratados de forma lícita, leal y transparente.

Los datos personales deben ser recogidos con fines determinados explícitos y legítimos.

Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario en relación con el tratamiento.

Los datos personales deben ser exactos y estar siempre actualizados.

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

Los datos personales deben ser tratados de tal manera que se garantice su seguridad.

Es evidente, que a falta de mejor base legítima para el tratamiento de los datos de salud, biométricos y de geolocalización, considerados los dos primeros por el GDPR como categoría especial de datos28, y el último especialmente intrusivo en la intimidad de las personas, será el consentimiento del afectado la base legitimadora por excelencia que faculte al tratamiento de dichos datos para poder disfrutar de las funcionalidades del Seat Cristóbal.

Como sabemos, el consentimiento ha de ser:

Libre: esto es, obtenido sin vicio del consentimiento en los términos de nuestro Código Civil, lo que implica que no puede obtenerse cercenando la posibilidad de no aceptación de la cláusula que permita el tratamiento o recogida de los datos de carácter personal

Inequívoco: y ahora bajo el nuevo régimen del GDPR, además sólo expreso, se acabaron los consentimientos tácitos.

Específico: Se otorga el consentimiento para que los datos se utilicen con concretas finalidades, lo cual va a suponer que si la finalidad del tratamiento cambiara de forma sustancial, el responsable del tratamiento deberá conseguir que el consentimiento se renueve para cubrir esta nueva o distinta finalidad.

Informado: Seat deberá asegurarse de que los adquirentes de su vehículo se encuentren previa y adecuadamente informados sobre todos aquellos elementos clave del tratamiento de datos de carácter personal que las funcionalidades del vehículo necesitará captar, procesar y gestionar para funcionar correctamente.

Previo: Ya desde el Dictamen 13/2011 del Gt artículo 29 se insistió en la importancia del consentimiento fundamentado previo, cercenando de alguna manera que el consentimiento pueda ser válidamente prestado a posteriori.

SALUD

Como hemos visto anteriormente, entre las funcionalidades del Seat Cristóbal se encuentran el impedir conducir a personas que superen una tasa de alcohol –ya sea la legalmente admitida o la programada dentro de ese margen por el administrador del sistema-, así como detectar otro tipo de situaciones que afecten a la salud del conductor y, por tanto, a su capacidad para poder desarrollar una conducción responsable, como lo son la detección de consumo de estupefacientes o medicamentos así como situaciones de cansancio.

A estos efectos, podemos partir del informe de la AEPD del año 2005[34], en la que se analizó la delimitación de la naturaleza de los datos de salud (en cuanto a su naturaleza jurídica)

[34] Véase informe 0129/2005 AEPD. Disponible en http://www.aepd.es. La legislación española y la AEPD a través de sus infromes han matizado este concepto amplio de salud, entendiendo que los datos de fumador o no fumador o el consumo de alcohol no son datos de salud en sí mismos si no vienen unidos a otros datos que

partiendo de las normas, tanto nacionales como internacionales, que se encontraban vigentes en la fecha del meritado informe.

Del mismo resultaba que "tanto el artículo 8 de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, como el artículo 6 del Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, ratificado por España en fecha 27 de enero de 1984, hacen referencia a los datos de salud como sujetos a un régimen especial de protección, de tal forma que, como indica el citado Convenio, tales datos no

El apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa viene a definir la noción de datos de carácter personal relativos a la salud" considerando que su concepto abarca las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo" pudiendo tratarse de informaciones sobre un individuo de buena salud, enfermo o fallecido. Añade el citado apartado 45 que debe entenderse que estos datos comprenden igualmente las informaciones relativas al abuso del alcohol o al consumo de drogas.

En este mismo sentido, la Recomendación no R (97) 5, del Comité de Ministros del Consejo de Europa, referente a la protección de datos médicos afirma que la expresión datos médicos hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas.

El apartado 38 de la mencionada Recomendación considera igualmente, siguiendo lo señalado en el Convenio 108 que la expresión datos médicos debería incluir igualmente cualquier información que ofrezca una visión real sobre la situación médica del individuo, incluyendo datos como los referidos al abuso de las drogas, abuso de alcohol y nicotina o consumo de drogas.

A la vista de lo indicado en las anteriores normas, cabe apreciar que tanto el Convenio 108 como la Recomendación 97 establecen una diferenciación entre los datos referidos al

indiquen un hábito o un abuso, pero sí tendría la consideración de dato de salud, en todo caso, el consumo de drogas.

consumo de tabaco (nicotina, en la terminología de la Recomendación) o alcohol frente al consumo de drogas, en su terminología general.

De este modo, según las fuentes citadas, debería considerarse dato directamente vinculado con la salud aquel que reflejase, en relación con las sustancias estupefacientes en general, su mero consumo. Sin embargo, en el caso del consumo de alcohol o tabaco el dato referido al mero consumo, sin especificación de la cantidad consumida, no sería en principio un dato vinculado con la salud, revistiendo tal naturaleza el dato que reflejase la cantidad consumida, en caso de que el mismo significase un consumo abusivo, no siendo esta Agencia Española de Protección de Datos la competente para determinar en qué supuesto concurre tal circunstancia".

Pues bien, sentado lo anterior, podemos afirmar que el tratamiento de datos que realizaría la funcionalidad descrita en estos momentos del Seat Cristóbal, entraría de lleno en el nuevo concepto de "categoría especial de dato"

Otro tanto podemos decir respecto del tratamiento de datos biométricos que se llevará a cabo por el Seat Cristóbal a través de su sistema de cámaras.

Efectivamente, una de las novedades incorporadas por el nuevo GDPR, junto con el de los datos genéticos, es el cambio producido en la calificación de los datos biométricos, que pasan a ser considerados datos de categoría especial, tal y como dispone el artículo 9.1 del GDPR. El precepto hace referencia, en concreto, a los "datos biométricos dirigidos a identificar de manera unívoca a una persona física", impidiendo su tratamiento, salvo que concurra alguna de las excepciones contempladas en el apartado 2 del art. 9 GDPR.

Pero al igual que se ha realizado anteriormente respecto de la naturaleza del dato de embriaguez o consumo de drogas, medicamentos o cansancio, es preciso detenernos un momento para analizar qué son los datos biométricos.

Según el GDPR, los datos biométricos se definen como aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos"31. De este modo, se reconoce una cierta amplitud de procedimientos o sistemas basados en la obtención de esta categoría de datos personales de forma tal que cualquier sistema de identificación mediante

reconocimiento facial, quedaría sometido a las nuevas previsiones establecidas por el GDPR.

Si finalmente viera la luz la funcionalidad anunciada de impedir que el vehículo pueda circular si no identificar el rostro del conductor, también es indiscutible que nos encontraríamos, por definición, ante un tratamiento de datos de carácter personal de naturaleza biométrica.

Ambas categorías especial de datos, así como el especial régimen al que se encuentra sometido su tratamiento por los distintos agentes (ya sean responsables, corresponsables o encargados de tratamiento, autoridades u organismos públicos o privados que actúen en el cumplimiento de una misión de interés público) se encuentra específicamente tratado en los Considerandos 51, 52 y 54. En lo que afecta a este TFM, y contemplado en el Considerando 51 "Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito ....".

¿Qué consecuencias tiene que el concept car Seat Cristóbal lleve a cabo tal cantidad de tratamiento de datos de carácter personal?

Lo que en a priori puede parecer sencillo, sin embargo puede volverse técnicamente muy complejo. La parte sencilla es la de establecer la hoja de ruta a realizar; veamos:

1. Someter a examen los tipos de datos de carácter personal que se van a tratar, con el objeto de identificar aquellos que entren dentro de la categoría de dato sensible.
2. Una vez detectado un tratamiento sobre un dato de categoría especial, acudir al GDPR en la búsqueda de excepción a la general prohibición del tratamiento de este tipo de datos de carácter personal.
3. Recabar en todo caso el consentimiento explícito del afectado, auténtico cajón de sastre y gran soporte como generador de base legítima para someter a tratamiento los citados datos de categoría especial.
4. Informar, de manera clara, transparente y mediante un lenguaje sencillo y entendible, cada una de las finalidades de uso de dichos datos
5. Realizar una EIPD antes de iniciar el tratamiento
6. Llevar igualmente un Registro de las Actividades de Tratamiento

7. Aplicar las medidas de seguridad apropiadas que garanticen

Es indiscutible que el consumidor que esté interesado en adquirir un vehículo con las funcionalidades como las previstas para el futuro Seat Cristóbal, prestará su consentimiento para llevar a cabo los tratamientos de datos necesarios, ahora bien, esto no exime de tener que dar fiel cumplimiento a lo expresado no sólo anteriormente, sino también a lo largo de este TFM y, así, se deberá permitir que el usuario revoque su consentimiento en cualquier momento lo que realmente será mucho más sencillo de lo que en un principio se pudiera pensar: bastará con que el usuario desconecte la funcionalidad que no desea tener activa en un momento determinado, pudiendo volver a conectarla a voluntad.

De ahí que, es la información la clave del tratamiento de los datos que se llevará a cabo en este vehículo (y en cualquier otro que incorpore esta o parecida tecnología). "El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados.

Además de la información respecto del tratamiento de los datos de carácter personal en los términos ya expuestos, el nuevo GDPR incluye dentro de la información a facilitar, la siguiente: los datos de contacto del delegado de protección de datos; la base jurídica sobre la que se sostiene el tratamiento de datos de carácter personal; los intereses legítimos perseguidos en que se fundamente el tratamiento de esos datos, en su caso; la intención de transferir los datos a un tercer país o a una organización internacional y la base para hacerlo, en su caso; el plazo durante el cual se conservarán los datos; el derecho a solicitar la portabilidad; el derecho a retirar en cualquier momento el consentimiento que se haya prestado; si la comunicación de datos es un requisito legal o contractual o un requisito

necesario para suscribir un contrato; el derecho a presentar una reclamación ante una autoridad de control; la existencia de decisiones automatizadas, incluida la lógica aplicada y sus consecuencias.

Los responsables y encargados del tratamiento de los datos de carácter personal habrán de cumplir con todas estas previsiones, pues salvo en aquellas ocasiones que expresamente sean previstas en la normativa, no tienen la capacidad para elegir qué aplicar y qué no implementar en el diseño, fabricación y comercialización de productos y servicios IoT.

Antes de continuar, es interesante abordar dos cuestiones más: una el principio de finalidad y otra las consecuencias no previstas respecto del tratamiento de datos sobre personas que no sean los propietarios en los que además coincida la condición del conductor del vehículo; me refiero por ejemplo a situaciones en las que por ejemplo el propietario deja el uso del automóvil a terceras personas.

Al igual que estaba previsto en el artículo 4 de la LOPD, que establecía que los datos personales no pueden utilizarse para una finalidad distinta o incompatible con aquellas para las que los datos hubieran sido recogidos, el vigente GDPR34 en su art. 5 modifica sustancialmente el régimen establecido previamente en España, al hablar exclusivamente de "usos incompatibles".

Pues bien, si se imagina un siniestro en el que ha intervenido uno o varios vehículos que dispongan de dispositivos y funcionalidades iguales o similares a las previstas en el concept car de Seat; ¿Estarían legitimados los cuerpos y fuerzas de seguridad el Estado, policía autonómica o policía local, para acceder a la caja negra del vehículo y descargar toda la información recogida por el vehículo y sus sensores?

Pregunta complicada de contestar pues, si bien es cierto que en los accidentes de vehículos inteligentes con mayor repercusión mediática (nos referimos a los vehículos Tesla) se conocen los datos previos al momento de tener lugar el siniestro, también es cierto que son facilitados por el propio fabricante quizás, con el interés legítimo de intentar acreditar ante usuarios actuales y potenciales de sus vehículos que sigue siendo el factor humano el desencadenante de los accidentes y no, por supuesto, la tecnología implantada en aquellos; por cierto, tengo mis serias dudas de que bajo el paraguas del GDPR se permitiera, incluso previo consentimiento por aceptación de las cláusulas y políticas de privacidad del fabricante de los afamados vehículos autónomos, que por parte de Tesla se hicieran públicos los

metadatos correspondientes a los instantes previos a un accidente de circulación.

¿Qué sucederá con los tratamientos de datos de aquellos conductores u ocupantes que no hayan aceptado de manera expresa, inequívoca, libre e informada el tratamiento de datos que realizará el vehículo –o mejor dicho- el fabricante?.

Se defiende sobre esta cuestión que, indudablemente, se hace aquí más exigible si cabe la posibilidad de que estas funcionalidades sean desconectadas y conectadas a voluntad del usuario, siendo para ello suficiente conocer la contraseña o password (lo que por cierto, genera en sí mismo un riesgo de acceso inconsentido) e introducirla en el sistema. Ya queda para el ámbito "doméstico" las consecuencias de la desconexión, por ejemplo, de la zona de transito autorizada, o el registro y/o monitoreo de excesos de velocidad, etc, entre el propietario del vehículo y el usuario.

Entender lo contrario, supondría no sólo que el propietario se convierte en corresponsable del tratamiento de datos de carácter personal, sino que, de no advertir al conductor tercero respecto de cuáles son las funcionalidades de las que dispone el vehículo y su forma de activar o desactivarlas podría incluso llevarle a la comisión de un ilícito penal.

Por último, y previo a la conclusión de este TFM, se analiza la geolocalización como otro tratamiento de datos llevado a cabo por el Seat Cristóbal.

Podemos considerar a la geoinformación como aquel conjunto de datos y servicios que, de forma directa o indirecta, hacen referencia a una localización o zona geográfica específica respecto de un sujeto, animal u objeto.

Es tan espectacular el fenómeno de la geolocalización y su uso está creciendo de una forma exponencial que ya no es que se estén desarrollando nuevas herramientas para su uso, sino que se está germinando un sector destinado a prestar servicios basados en la localización.

Frente a los comienzos, en donde se utilizaban las conocidas "coordenadas X, Y, Z", ahora se utiliza otro tipo de herramientas para mejorar la precisión, (por ejemplo el código postal de la zona, la dirección IP de un terminal o el sistema GPS de nuestro teléfono móvil o vehículo). Los conocidos "metadatos" suelen tener mayor relevancia desde el punto de vista del tratamiento de datos de carácter personal, pues incluyen, además de toda la información que describe los conjuntos y servicios de datos geoespaciales, la posibilidad de localizarlos,

inventariarlos, tratarlos y tras convertirlos en conocimiento, utilizarlos.

Entre las numerosas bondades de esta tecnología, se precisa mencionar la ayuda que presta en labores de rescate y salvamento de personas (tal y como se vio anteriormente en este TFM en relación con el botón e-call, por ejemplo), supuestos en los que la privacidad quedaría desplazada o limitada ante la necesaria seguridad e integridad física.

La geolocalización en sí misma no es buena ni mala depende, como tantas cosas, del uso y destino al que vaya enfocada. Sin embargo es cierto que de por sí, el uso de esta tecnología genera una serie de riesgos (desde el prisma de la privacidad) pues genera una diaria "huella histórica" trazable, de los lugares, actividades y tiempos en los se ha encontrado el dispositivo o sensor, o el vehículo que lo incorpora. De ahí, que la geolocalización de personas y bienes afecta y puede afectar a diversas esferas de derechos como la intimidad, la privacidad, el libre desarrollo de la personalidad, la libertad de expresión, el derecho al honor, etc.

Sería muy amplio abordar cada una de esas dimensiones, y como botón de muestra se tratará desde la perspectiva de la privacidad a sus riesgos y como minimizarlos.

Cada vez hay menos duda entre el público en general, que los datos de geolocalización son realmente datos de carácter personal, que identifican o pueden hacer identificable a una persona de manera más o menos directa35, y así viene recogido en el vigente GDPR, pero ya disponíamos de otros antecedentes tales como la regulación contemplada de los mismos en la Directiva 2002/58/CE36, que en su artículo 2, definía los datos de localización como "cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal del usuario de un servicio de comunicaciones electrónicas disponible para el público", definición que se recogía igualmente en el artículo 64.b) del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Pero quizás no esté igualmente tan asumido que la geolocalización y las aplicaciones de mapas son empleados más comúnmente de lo que pensamos para cometer acciones delictivas. No es ciencia ficción la realidad de que los delincuentes utilizan estas herramientas para encontrar objetivos potenciales y aumentar los resultados criminales, por ejemplo, gracias a las publicaciones de los usuarios en redes sociales y a la información facilitada por mapas

virtuales compartidos en línea o a través de aplicaciones.

En otro orden de cosas, la geoinformación puede ser facilitada voluntaria e involuntariamente, incluso sin que el usuario o propietario del dispositivo sea consciente y a pesar de que haya podido desactivar ciertos servicios o sensores.

Habitualmente, la información geográfica personal se facilita de manera voluntaria, principalmente a través de aplicaciones y redes sociales o, como en nuestro caso, a través del vehículo. Estos datos suelen ser almacenados y analizados por los proveedores de servicios de Internet, generalmente para mostrar publicidad personalizada. Pero al mismo tiempo, la geoinformación personal puede difundirse de manera involuntaria. En unos casos, porque se facilite información personal sobre nuestra ubicación sin nosotros saberlo, como por ejemplo a través de los metadatos de imágenes y videos y en otras situaciones, son los videos y fotos que tomamos y publicamos en redes sociales (aquí podemos recordar que el Seat Cristóbal podrá tener acceso a twitter, Facebook y demás RRSS, además de la red social privada de Toyota, de la que se ha hablado en este TFM anteriormente) los que asocian metadatos con los que se puede identificar la ubicación exacta donde fueron tomados. Para ayudar a una utilización más segura de la geolocalización personal, se debería procurar:

Revisar los ajustes de privacidad de los dispositivos y asegurarse de que solo personas de confianza o, al menos, conocidas pueden ver las actualizaciones que contengan localización personal.

Desactivar las opciones para informar automáticamente sobre la localización personal. En caso de usar servicios específicos cuya función principal sea informar sobre la localización personal, revisar atentamente la política de privacidad y los datos que se suministran de manera pública aunque es indudable que, nuevamente, será el consentimiento la base legitimadora del tratamiento de datos de carácter personal que via geolocalización se va a llevar a cabo.

Al igual que sucedía con el tratamiento de datos biométricos y de salud que podrá llevar a cabo el concept car Seat Cristóbal, al encontrarnos ante una tecnología especialmente invasiva de la privacidad, el análisis de riesgos y el estudio de impacto en protección de datos (PIA por sus siglas en inglés) es de obligado cumplimiento.

Como expone el Grupo de Trabajo del Artículo 29 en su Dictamen 02/2013 sobre las

aplicaciones de los dispositivos inteligentes[35], "a fin de utilizar un servicio de geolocalización particular, puede ser necesario activar dichos servicios en el dispositivo o navegador. Si esta capacidad de geolocalización se activa, cualquier sitio Internet puede leer los detalles de localización del usuario del dispositivo móvil inteligente". Por tanto, a fin de evitar que se nos vigile secretamente, es importante que se advierta de forma permanente por el dispositivo que la geolocalización se encuentra activada, vía por ejemplo a través de un icono visible de forma permanente.

Un caso de consentimiento presunto, y por tanto inválido en este caso, sería el deducido de la falta de intervención por parte de los usuarios de un sistema operativo que establece por defecto la transmisión de datos de localización. Por defecto los servicios de geolocalización deben encontrarse desactivados y los usuarios deben poder consentir de forma gradual que se activen aplicaciones concretas. El Grupo de Trabajo del Artículo 29 en el dictamen 15/2011 sobre la definición del consentimiento ejemplificó que el hecho de no modificar los parámetros de privacidad establecidos por defecto de una red social, parámetros a los que no se accede necesariamente al utilizarla, no permite inferir al responsable del tratamiento para inferir que se aprueba el tratamiento.

[35] Dictamen 2/2013, grupo de trabajo del art. 29. Disponible en https://sontusdatos.org/wp-content/uploads/2013/04/ce-dictamen-02-2013-aplicaciones-dispositivos-inteligentes.pdf

5. CONCLUSIONES

Las soluciones IoT no sólo han venido para quedarse, sino que están llamadas a evolucionar.

Sin embargo, el germen de esa evolución hacia tecnologías que mejoren la calidad de vida del ser humano debe partir de unos pilares robustos en materia de seguridad y privacidad por lo que habrá que afrontarla desde la fase de diseño para llegar, a través de un sistema de privacidad by default hasta el verdadero propietario de los datos y de las intimidades: el usuario. Para ello será preciso enfrentar varias líneas de actuación:

Educación y comunicación. Que en este caso supone la participación de varios actores, desde los ingenieros y diseñadores que deben ser capaces de cuantificar, desde el punto de vista técnico, los riesgos a que expondrán a sus usuarios, pasando por las organizaciones empresariales, para terminar, en cuanto a la educación, por las entidades que dispongan de tales responsabilidades, ya sea a nivel de protección de datos, de protección del consumidor o de protección en términos de ciberseguridad.

Nos referimos, por tanto, a una auto protección que va más allá de lo señalado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprobó el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, llegando incluso a plantearse cuál es la razón por la que ya se habla de educación vial en las escuelas de primaria pero sin embargo, y teniendo en cuenta el impacto en la privacidad que supone el sector de los videojuegos y RRSS en la intimidad de los menores, y sin embargo no se plantea todavía el debate sobre la incorporación de la cultura de la protección de datos en tales estadíos de formación de la persona.

Adquisición. Será evolución natural que el resultado de la educación incorpore nuevas metodologías de decisión de compra y aceptación de este tipo de tecnología y, es previsible, que el impuslo instantáneo de compra compulsiva (tan valorado por algunos departamentos de marketing) de la última tecnología disponbile, forme parte de una balanza en donde el consumidor sitúe en un extremo lo que le aporta la tecnología basada en el IoT y o que él tiene que aportar para darle valor a dicha tecnología, o dicho de otro modo, para que dicha tecnología tenga sentido.

Si el responsable del diseño y comercialización de productos y servicios que puedan ser

considerados como del IoT llevara siempre al consumidor y/o usuario a la decisión salomónica de: privacidad o funcionalidad, fracasará estrepitosamente pues, a pesar de que en un corto plazo el consumidor seguirá arrastrado por la fiebre consumista, siempre ávida de las últimas novedades tecnológicas, llegará un momento en que llegará el pico de sierra, valorándose en mucha mayor medida aquellos productos respetuosos con la intimidad y la protección de datos de los usuarios que presten servicios o funcionalidades similares o que hayan sido descartadas por inútiles o carentes de valor añadido.

Regulación. Al legislador le toca la no tan fácil tarea de conciliar y velar por el interés general de los usuarios como titulares de los datos que serán parte esencial para que la tecnología IoT sea últil, con los legítimos intereses de la cadena productiva de estos insrumentos de tal forma que la normativa legal no sea el freno del desarrollo de este tipo de tecnología, pero que tampoco suponga carta blanca para los intereses empresariales.

De tal forma que corresponderá a la Administración del Estado promover y desarrollar la protección y defensa de los consumidores y usuarios, especialmente en los siguientes aspectos:

1. Elaborar y aprobar el Reglamento General de la LOPDyGDD, y las demás disposiciones de general aplicación en todo el territorio español.
2. Apoyar y, en su caso, subvencionar las asociaciones de consumidores y usuarios, que tengan por finalidad la educación de los mismos en materia de protección de datos.
3. Apoyar la actuación de las autoridades y Corporaciones Locales y de las Comunidades Autónomas.
4. Promover la actuación de las demás Administraciones públicas y, en caso de necesidad o urgencia, adoptar cuantas medidas sean convenientes para proteger y defender los derechos de los consumidores o usuarios, especialmente en lo que hace referencia a su salud, seguridad y protección frente a intromisiones ilegítimas.
5. Ejercer la potestad sancionadora con el alcance que se determine.
6. En general, adoptar en el ámbito de sus competencias cuantas medidas sean necesarias para el debido cumplimiento de lo establecido en la Ley pendiente de publicación en el BOE.

Pero también nos encontramos en España con las Competencias de las comunidades autónomas, de tal forma que corresponde a las mismas la protección y defensa de los consumidores o usuarios, de acuerdo con lo establecido en sus respectivos estatutos de

autonomía y, en su caso, en las correspondientes leyes orgánicas complementarias de transferencia de competencias.

Por lo general, la defensa del consumidor y usuario es una competencia recogida en los estatutos de autonomía, de acuerdo con la legislación básica estatal que regula la ordenación de la actividad económica general y la política monetaria del Estado, las bases y coordinación general de la Sanidad, en los términos de lo dispuesto en los artículos 38, 131 y en los números 11, 13 y 16 del apartado 1 del artículo 149 de la Constitución.

Por último, nos encontramos con las competencias de las corporaciones locales, a las que corresponde promover y desarrollar la protección y defensa de los consumidores y usuarios en el ámbito de sus competencias y de acuerdo con la legislación estatal y, en su caso, de las comunidades autónomas y, especialmente, en los siguientes aspectos:

La información y educación de los consumidores y usuarios, estableciendo las oficinas y servicios correspondientes, de acuerdo con las necesidades de cada municipio. La inspección de los productos y servicios para comprobar su adecuación a la normativa vigente, ya sea de origen europeo (como el GDPR) o nacional (como la nueva LOPDyGDD). La realización directa de las inspecciones técnicas y de los correspondientes controles y análisis, en la medida en que cuenten con medios para su realización, o promoviendo, colaborando o facilitando su realización por otras entidades y organismos. Adoptar las medidas urgentes y requerir las colaboraciones precisas en los supuestos de crisis o emergencias que afecten a la salud o seguridad graves de los consumidores o usuarios. Ejercer la potestad sancionadora con el alcance que se determine en sus normas reguladoras (ordenanzas municipales) en cuanto las intromisiones en los datos de carácter personal de usuarios y clientes de dispositivos IoT puedan afectar a los derechos que como consumidores tengan los mismos.

En definitiva, quién sea capaz de aportar al consumidor un valor superior a la experiencia creada por el uso del dispositivo IoT adquirido y por el que se ha pagado un precio, no sólo en términos estrictamente monetarios, sino también en términos de privacidad, será quién logre mantenerse en el mercado y por tanto por los consumidores. Pensar que esto puede tener lugar sin que exista una paralela educación de estos últimos en materia de privacidad, implica tener una venda de la que es preciso desprenderse cuanto antes.

6. BIBLIOGRAFÍA, BIBLIOGRAFÍA WEB, LEGISLACIÓN CITADA

BIBLIOGRAFÍA

TESLA, N.: A Life From Beginning to End., Hourly History

SCI AMER WEISER, M., Scientific American Ubicomp Paper after Sci Am editing

SHIPLEY, A., "Security in the internet of things, lessons from the past for the connected future," Security Solutions, Wind River, White Paper, 2013

ATZORI, L., IERA, A., MORABITO, G., and NITTI, M. "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol. 56, pp. 3594- 3608, 2012.

ATZORI, L., IERA, A., MORABITO, G., "The internet of things: A survey," Computer Networks, vol. 54, pp. 2787-2805, 2010.

JARA, A. J., ZAMORA, M.A., and SKARMETA, A.F., "An internet of things---based personal device for diabetes therapy management in ambient assisted living (AAL)," Personal and Ubiquitous Computing, vol. 15, pp. 431- 440, 2011.

BABAR, P., MAHALLE, A., STANGO, PRASAD, N., and PRASAD, R., "Proposed security model and threat taxonomy for the internet of things (IoT)," in Recent Trends in Network Security and Applications, ed: Springer, 2010, pp. 420-429.

DIMITROV, W., XXV conference Telecom 2017 26-27 October, NSTC, Sofia, Bulgaria. **GDPR entrapments. Proactive and reactive (re)design thinking.** University of Library Studies and Information Technologies (UNIBIT) Bulgaria. http://ceec.fnts.bg/telecom/2017/documents/CD2017/Papers/26.pdf

BIBLIOGRAFÍA WEB

Wereable: definición disponible en https://www.wearable-technologies.com

ALBERTA JAQUERO, C. INCIBE. Internet of Things (IoT). El lado inseguro de las cosas. Disponible en https://www.incibe.es/protege-tu-empresa/blog/internet-of-things-ciberseguridad
ACED FÉLEZ E. jefe de Área. Unidad de apoyo al Director de la Agencia Española de Protección de Datos. Disponible en: http:// www.aepd.es. Referencia: 6 de noviembre de 2018.

Gartner, Inc. (NYSE: IT), es una compañía de investigación y asesoramiento de referencia mundial, miembro del S&P 500.

Fuente: Cisco Systemas. Disponible en https://internetofthingsagenda.techtarget.com/definition/Internet-of-Everything-IoE

Fuente: Cisco Systems (año 2013). Disponible en https://gblogs.cisco.com/la/la-manera-en-la-el-internet-de-todo-mejorara-el-mundo/

Fuente Cisco Systemas. Disponible en https://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf

https://www.bbvaopenmind.com/en/the-internet-of-everything-ioe

https://www.gartner.com/newsroom/id/2621015

Fuente: Are you ready for The Internet of Things? Artículo publicado en advantage technology, 12 Febrero 2014.

Fuente: *ALBERCA JAQUERO, C., "El lado inseguro de las cosas". INCIBE, marzo de 2012. https://www.incibe.es/protege-tu-empresa/blog/internet-of-things-ciberseguridad*

Fuente: LIZÁRRAGA ÁLVAREZ, M., curso de CCNA1 de Cisco Systems. https://sites.google.com/site/cursoenlineaccna1

INCIBE. Riesgos del internet de los trastos. Disponible en https://www.incibe.es/protege-tu-empresa/blog/iot-riesgos-del-internet-los-trastos

The NewYork Times. https://www.nytimes.com/2016/07/02/business/joshua-brown-technology-enthusiast-tested-the-limits-of-his-tesla.html

The social dilemma of autonomous vehicles. **http://science.sciencemag.org/content/352/6293/1573**

Sistemas inteligentes de transporte. Departamento de ingeniería de la información y las comunicaciones. Universidad de Murcia. https://www.um.es/gsit/research_lines/its/?l=es

LEGISLACIÓN CITADA[36]

Working Paper 223, año 2014 article 29 Working Group. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

Reglamento 2016/679, de 27 de abril (Ref. DOUE-L-2016-80807)

Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), de 19 de abril de 2018. https://www.boe.es/doue/2018/127/L00003-00007.pdf

Reglamento (UE) 2015/758 del Parlamento Europeo y del Consejo, de 29 de abril de 2015, relativo a los requisitos de homologación de tipo para el despliegue del sistema eCall basado en el número 112 integrado en los vehículos y por el que se modifica la Directiva 2007/46/CE. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32015R0758

Informe 0129/2005 Agencia Española de Protección de Datos. Disponible en http://www.aepd.es..

Dictamen 2/2013, Grupo de trabajo del artículo 29. Disponible en https://sontusdatos.org/wp-content/uploads/2013/04/ce-dictamen-02-2013-aplicaciones-dispositivos-inteligentes.pdf

[36] Incluye los dictámenes de la AEPD, así como los dictámenes del grupo de trabajo del artículo 29.