FACULTAD DE DERECHO

LEGALIDAD DE LA RECOPILACIÓN, USO Y CESIÓN DE DATOS QUE LLEVAN A CABO LOS AUTOMÓVILES INTELIGENTES

Autor: José Manuel García-Alfonso González

5º de E-3 B

Derecho Constitucional

Tutor: Dr. Francisco Valiente

Madrid

Abril de 2020

RESUMEN

El mundo se encuentra en un proceso de digitalización imparable, lo que ha desembocado en una serie de nuevos retos para el Derecho. Esto, a su vez, ha obligado a los legisladores a adaptar la legislación a las necesidades cambiantes de la sociedad. En este sentido, se publicó en 2016 el Reglamento Europeo 679/2016 de Protección de Datos (RGPD), el cual entró en vigor en 2018. Junto con esta norma europea, a finales de ese mismo año se promulgó en España, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (en adelante LOPDyGDD), que adapta la legislación nacional al nuevo Reglamento comunitario, con la intención de dar una mejor respuesta a las necesidades de una sociedad digitalizada.

Este trabajo se va a centrar en estudiar uno de los problemas jurídicos más recientes que existen en la actualidad, como es el tratamiento (en especial, la obtención, el uso y la comunicación o cesión de datos) por parte de los automóviles inteligentes. Un desafío para el derecho que va a ir en aumento, pues cada vez más vehículos son capaces de recopilar una gran cantidad de datos personales.

Palabras clave: digitalización, vehículo, inteligente, protección de datos, cesión.

ABSTRACT

The world is in a process of unstoppable digitalization, which has led to a series of new challenges for the law. This has forced legislators to adapt legislation to the changing needs of society. In this respect, the European Data Protection Regulation 679/2016 was published in 2016 and entered into force in 2018. Together with this European regulation, at the end of that same year, the Law on Data Protection and Guarantee of Digital Rights was enacted in Spain, which adapts national legislation to the new Community regulation, with the intention of providing a better response to the needs of a digitalized society.

This paper will focus on studying one of the most recent legal problems that currently exist, namely the processing (in particular, the collection, use and communication or transfer of data) by intelligent cars. This is a challenge for the law that is going to increase, as more and more vehicles are capable of collecting a large amount of personal data.

Keywords: digitization, vehicle, smart, data protection, transfer

ÍNDICE

INTRODUCCIÓN

Nos encontramos en una sociedad cambiante en la que las nuevas tecnologías han pasado a formar parte de nuestra vida diaria. En este proceso de disrupción tecnológica, los datos personales obtenidos mediante dispositivos inteligentes, han pasado a tener cada vez mayor importancia. En este contexto de disrupción tecnológica, los datos personales que se obtienen por parte de las empresas son un activo de enorme valor, que generan un escenario en el que es preciso regular la forma en la que dichos datos personales son tratados como mercancía por quienes los recopilan, procesan y comercializan, pues no dejan de contener información personal sensible que afecta a un derecho fundamental, constitucionalmente protegido, como es el derecho a la intimidad personal (artículo 18 de la Constitución Española). Como bien es sabido, el derecho va siempre por detrás de la sociedad y es deber de éste, garantizar el ejercicio de los derechos y libertades de los ciudadanos, cuando dichos derechos, debido a los cambios sociales, se ven amenazados o perjudicados, como es el caso que aquí va a estudiarse.

Con el objetivo de proteger los derechos de sus ciudadanos, en España se promulgó la LOPDyGDD en diciembre de 2018, ley que supone la adaptación de la normativa española al Reglamento de la Unión Europea 2016/679 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. Ambos documentos han supuesto un gran cambio en la forma en la que los distintos operadores (públicos y, sobre todo, privados) gestionaba la obtención y el procesamiento o tratamiento de los datos personales, aquellos referentes a una persona física identificada o identificable.

Este trabajo va a centrarse en el caso particular de aquellos datos personales que son recogidos por parte de vehículos inteligentes (fundamentalmente automóviles), así como el tratamiento y la comunicación o cesión que se realiza de dichos datos por parte de las compañías que los obtienen. El de los automóviles inteligentes es uno de los campos más novedosos y con más recorrido futuro, tanto tecnológico como jurídico, por lo que va a tratar de analizarse la legalidad del tratamiento de los datos recogidos por estos vehículos, como consecuencia de su uso por parte de personas físicas que son propietarias de dichos vehículos o que ostentan sobre el mismo un derecho de uso privado y personal.

CAPÍTULO I: NUEVAS TECNOLOGÍAS Y OBTENCIÓN DE DATOS PERSONALES

1. Digitalización de la Sociedad

Actualmente, nos encontramos en la conocida como "Sociedad de la Información", una sociedad en la que la materia prima de las empresas con mayor capitalización bursátil del mundo no son sus activos materiales, como podría parecer en un primer momento, sino que el producto que les da poder y les hace ser tan valiosas son los datos personales que recopilan y tratan. Un claro ejemplo de ello son empresas como Google, Apple, Facebook, Amazon o Microsoft, las 5 empresas con mayor capitalización bursátil en este momento (para referirse a ellas, existe un acrónimo de nueva creación: "GAFA" o "GAFAM", Moulier-Boutang, (2016)[1]).

Todas ellas obtienen datos personales a través de los dispositivos que venden o de los servicios que prestan. Mediante estos datos, consiguen establecer perfiles de sus usuarios o clientes, perfiles que poseen un elevado valor económico, sobre todo a gran escala, pues permiten conocer las tendencias del mercado, los posibles intereses de los consumidores y su identificación plena, por lo que quienes posean un gran número de datos (en calidad y cantidad) pueden influir de forma muy significativa en la venta de servicios propios o de terceros. De este modo, se pasa de un modelo de negocio en el que se recomienda un producto al cliente, a un modelo de negocio en el que se le prescribe un determinado producto según los intereses de dicho cliente y de los millones de consumidores que tienen perfiles similares al suyo, cometiéndose en muchas ocasiones, verdaderos abusos por la falta de equilibrio entre lo que el cliente percibe (cree facilitar) y la verdadera realidad de lo obtenido por estas grandes compañías y otras muchas no mencionadas.

Debido a esta revolución de la información que está sufriendo el mundo, y que comenzó alrededor del año 2007, con la expansión del número de teléfonos inteligentes, la creación y recopilación de información que se está produciendo es cada vez mayor. Los datos no

[1] Moulier-Boutang, Y. (22 de julio de 2016). Ahora ya todos trabajamos para las GAFA sin cobrar. (L. Amiguet, Entrevistador)

sólo se recogen por ordenadores personales y por los llamados *smartphones*[2], sino que cada vez más aparatos del día a día recogen los datos de uso que hacemos de ellos. Ejemplo de esto son los relojes y pulseras inteligentes, que recopilan no sólo la distancia que recorremos o la geolocalización, sino también la frecuencia cardiaca de una persona. Es fácil imaginar la importante afectación del derecho a la intimidad de quien está siendo permanentemente geolocalizado si no es consciente de ello, o de quien cree conservar seguros y para uno mismo, datos médicos como la frecuencia cardiaca, cuando ello puede estar siendo utilizado por aplicaciones diversas que, además, ceden dichos datos a otros terceros: las posibles consecuencias que de esto pueden derivarse para la intimidad y los derechos individuales, son enormes. Las neveras, bombillas, enchufes o televisiones son sólo algunos de los electrodomésticos presentes en los hogares y que cada día recopilan millones de datos acerca de la población sin que sus propietarios lleguen a ser conscientes de ello.

En definitiva, el problema que se plantea no es tanto la generación de una enorme cantidad de información por parte de los ciudadanos, que puede ser aprovechada. El problema es que dicha información se utilice para obtener un enorme beneficio por parte de empresas que ocultan o dificultan, de las más variadas formas, tanto la cantidad de datos que se generan, como las finalidades para las que pretenden usar dicha información. Ejemplo de ello es el ya conocido escándalo Cambridge Analytics y Facebook, por el cual, la compañía estadounidense fue condenada a paga una multa de 87 millones de dólares, debido a la forma en la cual trataron y vendieron los datos de millones de personas, BBC News Mundo (2019)[3].

2. Nuevos Modos de Recopilación de Datos

Tal y como se ha mencionado con anterioridad, el modo en que se recogen datos por parte de las empresas y de los gobiernos, ha cambiado de forma considerable desde la llegada

[2] Se trata, según la Real Academia Española (2020), de un terminal móvil que ofrece servicios avanzados de comunicaciones (acceso a internet y correo electrónico), así como servicios de agenda y organizador personal con un mayor grado de conectividad que un terminal móvil convencional.
[3] BBC News Mundo. (24 de julio de 2019). BBC. Obtenido de Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios: https://www.bbc.com/mundo/noticias-49093124

de las nuevas tecnologías a la vida de las personas. Couper (2005)[4] estudió la forma en la que la llegada de internet ha alterado el modo en el que se recopilan datos. Habla de una diferencia fundamental: la falta de un intermediario que los recopile o haga preguntas. Antes de la llegada de ordenadores y algoritmos era necesaria la figura del entrevistador, mientras que en la actualidad, ésta prácticamente ha desaparecido, dando paso a una recolección automática de datos por parte de las plataformas con las que interactúa el usuario. Dicha automatización permite un aumento muy considerable de la cantidad de datos recopilados, pues se multiplican no sólo el número de dispsitivos de los que se extrae información, sino también el tiempo, al ser capaces de recopilar datos 24 horas al día.

En este entorno surgió el conocido como *Big Data*, concepto que parece necesario definir con claridad, pues resulta de enorme importancia en este trabajo. Para ello, el artículo de Maté Jiménez (2014)[5], en el que expresaba que aún no existiendo una definición exacta para este concepto, la que más se aproxima es la que da el diccionario inglés de Oxford: "*datos de tamaño muy grande, típicamente hasta el extremo de que su gestión presenta retos logísticos significativos*". Asimismo, establece que esta definición debe completarse con la que nos otorga la consultora americana McKinsey: "*conjuntos de datos cuyo tamaño va más allá de la capacidad de captura, almacenado, gestión y análisis de las herramientas de base de datos*".[6]

El *Big Data*, por tanto, es consecuencia directa de las nuevas teconologías, y de la llamada sociedad de la Información en la que vivimos. El Big Data se encuentra íntimamente relacionado con las llamadas *cookies*, cuyo concepto se explica en el Informe del Despacho de Abogados Cuatrecasas, Gonçalves Pereira, (2014) donde definen las *cookies* de acuerdo a la jurisprudencia y a las resoluciones de la Agencia Española de Protección de Datos: "*las cookies sirven para intercambiar información entre el equipo del usuario y el servidor de origen. Esta información puede servir a propósitos muy diferentes, desde la mera operatividad del sistema (optimizando la conexión y los contenidos que se descargan, evitando la necesidad de reiteración de tareas o incrementando la seguridad de la conexión), hasta la personalización de la apariencia y funcionalidad de la*

[4] Couper, M. P. (2005). Technology Trends in Survey Data Collection. Social Science Computer Review, 486-501.
[5] Maté Jiménez, C. (2014). Big data. Un nuevo paradigma de análisis de datos. Anales de Mecánica y Electricidad, página 10
[6] Ibid, página 11.

información que se envía al equipo del usuario mediante la observación de sus hábitos de navegación."[7]

Mediante las *cookies* se consiguen realizar distintos perfiles de los usuarios que acceden a diferentes páginas web y van comprando, leyendo, o adquiriendo diferentes servicios de distintas empresas, de modo que se terminan creando perfiles de distintos tipos de consumidores. Estos perfiles se realizan con millones de datos obtenidos de infinidad de páginas web, proporcionando a las compañías unos modelos predictivos de un valor muy elevado.

Esta constante recopilación de datos cada vez que cualquier persona accede a internet, plantea una problemática legal que va a tratarse en este trabajo. Las empresas más interesadas en las *cookies* son empresas como Google, Amazon o Facebook, ya que se trata de compañías con una capacidad de recolección muy abundante, así como con una elevada capacidad de computación. Esto se debe a que son necesarios numerosos medios informáticos para ser capaz de procesar millones de datos de forma correcta y utilizarlos para obtener conclusiones y perfiles que más tarde puedan ser vendidos a compañías de marketing o utilizados para uso propio. De este modo, Google puede ofrecer servicios consistentes en anuncios que sólo van a llegar a clientes que han sido previamente analizados, y de cuyos perfiles de comportamiento es lógico deducir que van a estar interesados en el producto que se les ofrezca, siendo de especial utilidad a aquellas empresas que buscan optimizar su publicidad (toda clase de periódicos, revistas, generadores de contenidos, webs transaccionales, …). Se pasa así, de una publicidad predictiva a una proactiva, lo que genera un enorme valor para quien trata los datos, de modo que en lugar de recomendar el producto o servicio al potencial cliente, ofrece lo que el algoritmo ya sabe que el cliente quiere, ya que conoce el perfil del mismo. El poder que supone el tratamiento y generación de perfiles de datos personales es tan grande, que ha supuesto una disrupción brutal en las inversiones en publicidad que efectúan las empresas. Ahora, esas inversiones son cada vez más on line (internet), cuando hasta hace poco, la gran mayoría era off line. Decrecen las inversiones en publicidad en los medios tradicionales y se centran en internet, donde se conoce al individuo a través de múltiples facetas, al efectuar el seguimiento de su navegación e intereseses a través de las cookies.

[7] Cuatrecasas, Gonçalves Pereira. (2014). El Régimen Jurídico de las Cookies y su aplicación por la Agencia Española de Protección de Datos. Aranzadi Doctrinal, página 5.

Según Castellano (2019)[8], directiva de KANTAR, multinacional americana de referencia en el mundo en Investigación de Mercados, en 2020 se espera que la inversión publicitaria en medios digitales aumente. Así, el 84 % de los profesionales planea incrementar su inversión publicitaria en vídeos online en los próximos 12 meses mientras que el 70 % planea aumentar el gasto publicitario en redes sociales y el 63 % planea hacerlo en podcasts. Esto contrasta en gran medida con los medios impresos, donde el 70 % de los profesionales del marketing dice que reducirá su inversión en revistas y el 66 % la disminuirá en periódicos.

[8] Castellano, S. (13 de noviembre de 2019). Kantar España Insights. Obtenido de La publicidad en 2020: Dominarán las redes sociales y el vídeo online pese a las dificultades de medición: https://es.kantar.com/empresas/marcas/2019/noviembre-2019-getting-media-right/

CAPÍTULO II: LA PROTECCIÓN DE DATOS Y SU REGULACIÓN EN ESPAÑA

1. El Derecho a la Protección de Datos como Derecho Constitucional

El Derecho a la Protección de Datos en España se encuentra recogido en el Artículo 18[9] de la Constitución Española de 1978, el cual recoge, entre otros derechos fundamentales, el derecho a la intimidad, al honor, a la propia imagen o a la inviolabilidad de domicilio.

Llama poderosamente la atención el apartado 4, y cómo el legislador constitucional supo anticiparse al futuro, y a pesar tratarse de un texto de 1978, incluyó, dentro de los derechos fundamentales, un párrafo que se dedicaba explícitamente a proteger el derecho a la intimidad, personal y familiar en la informática. Por ello, resulta de justicia reconocer que, desde la transición española, se ha prestado una especial atención a los derechos relacionados con la informática y las telecomunicaciones, tratando de proteger la intimidad de los ciudadanos.

En este sentido, y debido a su repercusión y reciente publicación, destaca la Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo, la cual atiende a un Recurso de Inconstitucionalidad interpuesto por el Defensor del Pueblo respecto del apartado primero del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales. El artículo 58 bis apartado primero de la LO 5/1985 establecía lo siguiente:

> *"1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades*

[9] Constitución Española de 1978, Cortes Generales, BOE nº311 de 29 de diciembre de 1978: El artículo 18 establece:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas."

Tras examinar el contenido del artículo, parece claro que el mencionado primer apartado vulnera el Derecho a la Protección de Datos Personales, por lo que se presentó un Recurso de Inconstitucionalidad específicamente contra apartado 1. El Tribunal Constitucional, como era de esperar, lo declaró inconstitucional amparándose en los siguientes fundamentos de derecho:

"Ello implica aludir al contenido tanto del Reglamento (UE) 2016/679 RGPD como de la LOPDyGDD, pues en la actualidad ambas fuentes configuran conjuntamente, de forma directa o supletoria, el desarrollo del derecho fundamental a la protección de datos de carácter personal que exigen los artículos 18.4 y 81.1 CE (...) La declaración de inconstitucionalidad y nulidad se basa, como se ha dicho en el fundamento jurídico anterior, en que la Ley Orgánica 3/2018 no ha fijado por sí misma, como le impone el artículo 53.1 CE, las garantías adecuadas por lo que respecta específicamente a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales. Ello constituye una injerencia en el derecho fundamental a la protección de datos personales de gravedad similar a la que causaría una intromisión directa en su contenido nuclear."[10]

En primer lugar, debe destacarse como el Tribunal se ampara en dos textos que van a ser el eje de este trabajo y que van a analizarse en detalle más adelante, el Reglamento Europeo de Protección de Datos 2016/679 y la Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales, pues son los textos encargados de desarrollar en profundidad la regulación de la protección de datos. Se les concede la potestad de regular esta materia en los artículos 53.1[11] y el 81.1[12] de nuestra Carta Magna, tal y como se establece en la sentencia. Por tanto, en base a los anteriores preceptos, el citado artículo 58 bis apartado 1 de la Ley orgánica del Régimen Electoral General, no cumple con las garantías requeridas por el RGPD, ya que se trata de una injerencia en un Derecho

[10] Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo de 2019. Página 10.
[11] Artículo 53.1 de la Constitución Española: Los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a).
[12] Artículo 81.1 de la Constitución Española: Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución.

Fundamental reconocido en el artículo 18.4 de la Constitución Española, como es el derecho a la intimidad. Puesto que se trata de un derecho fundamental, cualquier tipo de intromisión en el mismo ha de estar perfectamente justificada. En aquellos casos en los que entren en colisión dos derechos, se habrá de adoptar, tal y como establece la doctrina del Tribunal Constitucional, el principio de proporcionalidad (a este respecto, resulta interesante el tratamiento efectuado por Roca Trías & Ahumada Ruiz (2013)[13] que indican lo que aquí se señala). Todo ello con la intención de que ninguno de los dos derechos se vea totalmente mermado, sino que se reduzcan de forma proporcional.

Así se hace en esta sentencia, donde se habla de una injerencia en el contenido nuclear del derecho a la protección de datos. El contenido nuclear o esencial de un derecho se encuentra recogido en el mencionado artículo 53.1 de la Constitución, siendo dicho contenido esencial, según Parejo, (1981)[14] "*aquel reducto último que compone la sustancia del derecho, disuelto el cual, el derecho deja de ser aquello a lo que la norma fundamental se refiere*." De modo que basado en el principio de proporcionalidad, así como en el contenido esencial del derecho a la protección de datos, y en la LOPDyGDD y el RGPD, el Tribunal Constitucional termina por declarar inconstitucional el artículo 58 bis de la Ley Orgánica del Régimen Electoral General.

DERECHO DE AUTODETERMINACIÓN INFORMATIVA. Parece especialmente oportuno, llegados a este punto, abordar el denominado Derecho de autodeterminación informativa, que se configura como un derecho fundamental, de construcción jurisprudencial, como lógico desarrollo del Artículo 18 de la Constitución.

Para delimitar el Derecho a la autodeterminación informativa, nos referiremos a dos importantes Sentencias del Tribunal Constitucional español:

- La STC 254/1993 del 20 de julio.
- La STC 11/1998 del 13 de enero.

Empezaremos diciendo que ambas se dictan bajo la vigencia de la LOPD 5/92, del tratamiento automatizado de datos de carácter personal (a la que nos referimos en el

[13] Roca Trías, E., & Ahumada Ruiz, M. (2013). Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española. REUNIÓN DE TRIBUNALES CONSTITUCIONALES DE ITALIA, PORTUGAL Y ESPAÑA ROMA - OCTUBRE 2013. Roma.
[14] Parejo, L. A. (1981). El contenido esencial de los derechos fundamentales en la jurisprudencia constitucional, a propósito de la Sentencia del TC del 8 de abril de 1981. Revista Española de Derecho Constitucional, 169-190.

siguiente apartado), y que la doctrina entiende que existen antecedentes históricos en una Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983. En ella, se reconoce al ciudadano un doble derecho a decidir y disponer libremente sobre sus datos personales, y a decidir qué es lo que otros pueden saber de él.

La STC 254/1993 del 20 de julio es la primera que introduce el concepto de "derecho a la autodeterminación informativa" como parte del derecho a la intimidad. Se trata de una de las sentencias más importantes en este ámbito, tal y como asegura el catedrático de Derecho Civil Vallejo (1994:325)[15], en esta sentencia se establece: *"Una nueva forma de entender el derecho a la intimidad"*. Así, su Fundamento Jurídico SEXTO establece:

"... nuestra CE ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso ***estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama "la informática"****.*

El FJ 7º, señala: *"A partir de aquí se plantea el problema de cuál deba ser ese contenido mínimo, provisional, en relación con este derecho o libertad que el ciudadano debe encontrar garantizado, aun en ausencia de desarrollo legislativo del mismo. (se refiere a la ausencia de desarrollo del A. 18 CE).*

Un primer elemento, el más "elemental", de ese contenido es, sin duda, negativo, respondiendo al enunciado literal del derecho: el uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, ***la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona.***

[15] Orti Vallejo, A. (1994). El nuevo derecho fundamental (y de la personalidad) a la libertad informática (A propósito de la STC 254/1993, de 20 de julio). Derecho Privado y Constitución, página 325.

La llamada "libertad informática", es así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)."

En definitiva, el Tribunal Constitucional se refiere a un nuevo derecho, al que denomina **libertad informática**, que es garantía de otros derechos: el honor y la intimidad.

Lo relevante ahora es comparar cómo se compadece el hecho de que los datos personales de los ciudadanos se recaben, gestionen y cedan sin que ellos puedan ejercer sus legítimos derechos al control de sus propios datos, de información únicamente relativa a su persona, a través de dispositivos que impiden o limitan gravemente la capacidad de la persona de conocer que se están recabando datos, qué datos en concreto se están obteniendo y para qué finalidades (que deben ser legítimas) se usarán esos datos.

En este sentido, procede citar la sentencia **Riley v. California**, 573 U.S. 373 (2014), en la que David Riley, un joven estadounidense fue obligado a detenerse, en un primer momento, por una violación de una norma de tráfico. Los agentes, al darle el alto, procedieron a inspeccionar el vehículo. Al hacerlo, se percataron de que Riley llevaba dos armas en el coche sin estar autorizado para ello, por lo que le detuvieron. Asimismo, se accedió al contenido del teléfono móvil de Riley, descubriendo que contenía fotografías y vídeos que le relacionaban con una banda callejera. Fue llevado a juicio en base al contenido de su teléfono y a un informe de balística de las armas confiscadas, pruebas ambas que le vinculaban a un tiroteo entre bandas rivales que había sucedido en los días previos.

El joven alegó que se había violado su derecho a la intimidad, ya que la policía no tenía derecho a acceder al contenido de su teléfono móvil. El veredicto fue unánime por parte de los 9 jueces que componen la Corte, concluyendo que si bien los policías tenían derecho a registrar el vehículo, así como a Riley, amparados en la seguridad que este acto les confiere, el acceso al contenido del teléfono móvil no suponía ninguna amenaza para la integridad física de los agentes, y, por tanto, nunca se debió acceder a dicho dispositivo. Distinguieron el *Smartphone* de la cartera de un detenido, pues, según alegaban los magistrados, los *smartphones*, son "microordenadores llenos de una masiva cantidad de información privada, *(...) se podrá acceder a dicha información mediante orden judicial o en aquellos casos en que los intereses del gobierno sean tales, que el acceso esté justificado"*[16]. De este modo, el Tribunal Supremo de los Estados Unidos estableció que

[16] Riley v. California, 573 U.S. 373 (2014).

la información que almacenan los dispositivos móviles debe estar protegida de un modo especial, ya que contienen información protegida por derechos fundamentales tales como la intimidad, y por ende, la privacidad, que estarían en peligro de no otorgar esa protección.

2. Regulación Histórica de la Protección de Datos

2.1 Ley Orgánica 5/1992 de 29 de octubre, relativa a la regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).

En cuanto a la Ley que desarrolla el contenido del artículo 18.4 de la Constitución, encontramos, en primer lugar, la Ley Orgánica 5/1992 de 29 de octubre, relativa a la regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), cuya exposición de motivos, resulta de particular relevancia debido al modo en el cual explica la importancia de la regulación en el ámbito de la protección de datos. Dicha exposición de motivos comienza por establecer una importante diferencia entre el Derecho a la Intimidad y el Derecho a la Privacidad:

"El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, ***la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado****. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo."*[17]

[17] Ley Orgánica 5/1992 de 29 de octubre, relativa a la regulación del tratamiento automatizado de los datos de carácter personal. Exposición de motivos, página 1.

Esta distinción, reflejada ya en el año 1992, es uno de los pilares de la regulación de la protección de datos, pues como se especifica en el párrafo anterior, no se trata simplemente de la intimidad, siendo la privacidad un concepto más amplio, que abarca una serie de facetas que de forma individual pueden carecer de importancia, pero que de darse todas juntas conforman un derecho que ha de ser protegido por la ley. Una vez realizada la distinción entre intimidad y privacidad, y teniendo claro que el objeto a tratar en la regulación de la protección de datos es la segunda, y, por tanto, este trabajo va a centrarse en el derecho a la privacidad.

En este sentido, destaca la definición de privacidad que escribe uno de los juristas españoles más importantes en el campo de la protección de datos, Davara Rodríguez: *"término al que podemos hacer referencia bajo la óptica de la pertenencia de los datos a una persona, su titular, y que en ellos se pueden analizar aspectos que individualmente no tienen mayor trascendencia, pero que al unirlos a otros pueden configurar un perfil determinado sobre una o varias características del individuo que éste tiene derecho a exigir que permanezcan en su esfera interna, en su ámbito de privacidad"*[18].

Se trata de una definición que se asemeja a la citada Ley Orgánica 5/1992, en el sentido de que en ambos casos se habla de unos datos que tomados por separado pueden llegar a carecer de valor o de protección jurídica, pero que, al tomarse de forma conjunta, pasan a tener una importancia significativa, apareciendo así la necesidad de protección jurídica que otorga el derecho a la privacidad. En este sentido, Davara argumenta que el tratamiento, la captura y el almacenamiento de datos abren grandes posibilidades para que se lleven acabo actividades ilícitas con esos datos. Ya en 1992, con una capacidad de recolección y computación de datos muy menor, comparada con la actual, establecía: "*Hoy día los grandes almacenes, las empresas gestoras de tarjetas de crédito, los hospitales, la propia Administración disponen de tal cantidad de datos de nosotros que fácilmente pueden lograr un perfil muy completo de nuestra persona. Este perfil, en algunos casos, puede ser determinante a la hora de solicitar un trabajo o al tratar de contratar un seguro; por ello su protección es cada día más importante*."[19] Siendo precisamente esa problemática la que va a abordarse en este trabajo, y es que los datos que recogen los automóviles inteligentes pueden ser compartidos con las aseguradoras,

[18] Davara Rodríguez, M. (1992). La Ley española de protección de datos; ¿una limitación al uso de la información para garantizar la intimidad? Actualidad Jurídica Aranzadi. Página 76.
[19] Ibid, página 77.

entre otras empresas, algo que puede terminar provocando serios perjuicios para el conductor del vehículo.

Esta fue la primera ley orgánica que desarrolló en España la protección de datos personales, y estaba centrada, tal y como establecía su artículo 2, en los ficheros de datos de carácter personal susceptibles de tratamiento automatizado. De modo que se trataba de una ley que aún no contemplaba, de forma alguna, la recolección y el procesamiento de datos que ha conllevado la disrupción tecnológica a la que se ha visto expuesta la sociedad durante el Siglo XXI.

2.2 DIRECTIVA 95/46/CE. del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Podemos considerarla como la primera gran norma moderna emitida por la Unión Europea, y supuso un gran paso adelante en la protección de la privacidad y los derechos relativos a la intimidad de los ciudadanos.

Hasta esa fecha, no existía una interpretación homogénea por parte de los socios comunitarios de cuál debía ser el posicionamiento de la UE a este respecto. Algunas legislaciones internas apostaban mucho más que otras por ser restrictivos ante las amenazas provocadas por el uso masivo de datos en entornos tecnológicos e informáticos. Entre quienes se decantaron desde un principio por este posicionamiento, estaba claramente España (también Alemania y Holanda), cuyos juristas influyeron en este campo a la hora de redactar la Directiva.

2.3 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Tras la anterior ley de 1992 y la Directiva de 1995, España promulga en 1999 la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Se trata de una Norma mucho más enfocada a una sociedad en la que la llegada de los ordenadores y de internet comenzaba a ser una realidad y que incorporaba al ordenamiento jurídico español la Directiva 95/46. El *boom* de internet se produjo alrededor del año 1996, y las empresas comenzaban a informatizarse; el popular Windows

95 llevaba 4 años en el mercado, de modo que el ordenador en el puesto de trabajo estaba cada vez más a la orden del día.

La Directiva crea el llamado Grupo de Trabajo del Artículo 29, un órgano consultivo asesor que ha tenido una extraordinaria importancia en el desarrollo de la normativa de privacidad y que ha colocado a Europa como el referente mundial en esta materia. Su composición incluía a representantes y expertos de todos los estados miembros, además de a representantes de la Autoridad Europea de Protección de Datos y a un representante de la Comisión.

Es, entre otras cosas, gracias a la gran importancia y alta cualificación técnica de este Grupo por lo que la propia UE decide en 2016 (once años después) unificar y fortalecer esta normativa mediante la promulgación de un Reglamento comunitario, con eficacia directa: el Reglamento de la Unión Europea 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de éstos (en adelante RGPD)

Si bien la Ley 15/99 carece de exposición de motivos, su contenido desprende una clara vocación de ser más restrictiva que su predecesora. Se trata de una ley orgánica bastante más extensa, que otorga una mayor importancia a la Agencia Española de Protección de Datos (es la Autoridad Española en la materia, con amplias facultades de interpretación, supervisión, inspección y sanción) y que presta más atención a una cuestión que se considera entonces crítica: el movimiento internacional de datos. Tanto es así que esta ley estuvo vigente hasta ser derogada por la actual LOPDyGDD del año 2018 y, en parte, por el RGPD.

3. Legislación Actual

Debido a la disrupción tecnológica vivida durante el Siglo XXI, ha sido necesaria una renovación completa de las leyes dedicadas a regular el derecho a la privacidad. Esto se debe, en gran parte, a la llegada de los *smartphones* a manos de la mayoría de la población. Así lo refleja el dato de que en 2018 se estimaba que alrededor del 97,4% de la población española poseía un teléfono móvil, de los que el 83,4% contaba con acceso a internet[20]. Este aumento del número de usuarios no sólo en España, sino en todo el

[20] Instituto Nacional de Estadística. (2018). España en cifras 2018. Madrid: INE, página 24.

mundo, con el consiguiente impacto en la recolección y uso de datos personales por parte de los mencionados dispositivos inteligentes, llevaron a la Unión Europea a dar un paso más en la legislación relacionada con la protección de datos. En este sentido, se promulgó el Reglamento de la Unión Europea 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. Este reglamento, aunque se prueba en 2016, entró en vigor en mayo de 2018, de modo que se concedió una *vacatio legis* de dos años a los Estados miembros, debido al gran cambio que suponía en el ámbito de protección de datos.

Se trata de un Reglamento, por lo que no necesita transposición. Dicho texto enuncia una serie de principios de obligado cumplimiento, como el de calidad, proporcionalidad, finalidad o minimización (y que no son, por tanto, recomendaciones, sino verdaderas obligaciones). Junto con el Reglamento, y como ya se ha dicho, España promulgó la LOPDyGDD. A este respecto, Ramón y Cajal Abogados (2019)[21] señala que la LOPD actúa de manera conjunta con el RGPD, de modo que no lo sustituye, sino que se encuentra más bien subordinada al mismo, y trata de desarrollar algunos aspectos que pueden no haberse visto estipulados en el texto de la Unión Europea. Entre estos aspectos, que se analizan en mayor profundidad en los apartados venideros, el ya citado Miguel Ángel Davara Rodríguez (2018)[22] establecía que los más importantes eran: "*(...) el tratamiento de datos de personas fallecidas; el whistleblowing, esto es, el tratamiento de datos en el sistema interno de denuncias en una empresa; las medidas de responsabilidad activa –más conocido como accountability-; el tratamiento con fines de videovigilancia; el derecho de supresión y el derecho a la portabilidad de los datos y la figura del delegado de protección de datos, más conocido por sus siglas en inglés: DPO"(Data Protection Officer).* Argumentaba, en esta entrevista concedida antes de la entrada en vigor del Reglamento o la LOPDyGDD, que dicha Ley pretendía ir un paso más allá del Reglamento, tratando de cubrir aquellos problemas no cubiertos por éste.

Es importante destacar que, en el apartado de Sanciones, el RGPD establece importantes multas de hasta 20 millones de Euros o hasta el 4% de la facturación mundial del infractor, debiendo escogerse entre la mayor de ambas cantidades.

[21] Ramón y Cajal Abogados. (2019). Novedades Ley Protección de datos. Madrid: Ramón y Cajal Abogados.
[22] Davara Rodriguez, M. (28 de enero de 2018). Entrevista a Miguel Ángel Davara: El legislador europeo quiere evitar que resulte "rentable" vulnerar el derecho a la protección de datos de las personas. (N. Jurídicas, Entrevistador).

Sin embargo, no ha habido sanciones especialmente destacables (con alguna honrosa excepción) desde que entrase en vigor el RGPD. En este sentido, señalar la sanción a Google de 50 millones de Euros, impuesta por la Autoridad de Protección de Datos francesa, la "Comisión Nacional de la Informática y las Libertades CNIL", Ayuso (2019)[23].

Es más, ha habido recientemente (finales de 2019 y principios de 2020) sanciones mucho más importantes (150 Millones € a Google, y 1100 Millones € a Apple), basadas en incumplir normas de competencia, que parece resultar más sensible que la defensa de un derecho fundamental como el de la privacidad.

[23]Ayuso, S. (21 de enero de 2019). Francia multa a Google con 50 millones de euros por falta de transparencia. El País.

CAPÍTULO III: EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS LA LEY ORGÁNICA 3/2018, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

1. Introducción

La forma en la cual deben obtenerse y tratarse los datos personales se regula en las disposiciones contenidas en la LOPDyGDD y el RGPD. Como se ha especificado con anterioridad, es importante aclarar que ambas normas actúan de forma conjunta, teniendo en cuenta que en caso de entrar en conflicto prevalecería, en todo caso, el Reglamento, al tratarse de una norma con eficacia directa, de nivel europeo.

En primer lugar, es necesario realizar una serie de aclaraciones acerca del Reglamento, en primera instancia y de la LOPDyGDD, más adelante, para comprender el modo en el que se está atajando el problema de la invasión de la privacidad en Europa y más concretamente en España.

El RGPD se fundamenta en una serie de principios (a los que la propia Agencia Española de Protección de Datos otorga una especial relevancia en su Guía para el Ciudadano (2019)[24]), que se encuentran recogidosen el Artículo 5.1 del RGPD[25]. Dichos principios

[24] Agencia Española de Protección de Datos. (2019). Protección de Datos: Guía para el Ciudadano. Madrid: Guías AEPED. Páginas 8 y 9.

[25] RGPD. "Artículo 5: Los datos personales serán:
a) tratados de manera lícita, leal y transparente en relación con el interesado (**«licitud, lealtad y transparencia»**);
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales (**«limitación de la finalidad»**);
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (**«minimización de datos»**);
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan (**«exactitud»**);
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado (**«limitación del plazo de conservación»**);

han de observarse, necesariamente, por parte de todas y cada una de las personas jurídicas privadas o instituciones públicas que se dispongan a realizar cualquier tipo de tratamiento de datos de carácter personal.

a) Dichos principios son el de **licitud, lealtad y transparencia**, esto es, el tratamiento de los datos debe estar amparado por cualquiera de las causas contenidas en el artículo 6[26] del citado texto, y que serán desarrolladas más adelante.

b) El segundo de los principios que han de cumplirse a la hora de tratar datos de carácter personal, es el de **limitación de la finalidad**, de modo que el fin por el que los datos de una persona física son recabados deben ser lícitos, explícitos y legítimos. Además, para que los datos sean tratados lícitamente deben contar con una base jurídica legítima, de las contenidas en el Artículo 6 del Reglamento:

1. Consentimiento del interesado: "*el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;"*
2. *Ejecución de un contrato: "el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;"*
3. *Cumplimiento de una obligación legal: "el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento"*
4. *Protección de intereses vitales: "el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;"*
5. *Interés Público: "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;"*
6. *Interés Legítimo: "el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y*

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas **(«integridad y confidencialidad»**).

libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño."

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades publicas en el ejercicio de sus funciones."

c) El tercero de los principios que han de respetarse es el de **minimización de datos**, de modo que los datos que se recaben por parte de los Responsables de datos han de adecuarse y ser proporcionales a los fines para los que son tratados, ello implica que que no es lícito recabar o mantener datos simplemente porque pudieran llegar a ser útiles en determinadas circunstancias, o en un futuro.

d) El siguiente principio enunciado en el Reglamento es el de **exactitud**, entendiendo por el mismo, el deber que tienen los Responsables de los datos de actualizar, rectificar o suprimir los datos para garantizar que el tratamiento efectuado está basado en datos exactos, puestos al día y mantenidos debidamente actualizados, lo que es de enorme importancia para asegurar que la información sobre una persona concreta es la que debe ser, y no la que fue hace años.

e) En consonancia con lo anterior, se ha de respetar el principio de limitación del **plazo de conservación,** de tal modo que los datos sólo sean mantenidos en las bases o ficheros durante el tiempo estrictamente necesario, que estará basado en razones legales (prescripción o caducidad de derechos), teniendo en cuenta, asimismo, la vigencia -por ejemplo- del contrato que obligue a prestar el servicio para el que los datos fueron recogidos.

En este sentido, como antecedente del plazo de conservación, resulta oportuno citar la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 21 de diciembre de 2016 (asuntos TELE2 SVERIGE AB y otros; C- 203/15 y C 698/15), en la que la Gran Sala vino a poner en cuestión la adecuación al Derecho de la Unión Europea de la previsión, en los Ordenamientos internos, de una conservación generalizada de datos con fines preventivos. En la citada Sentencia se analizó si Tele2 Sverige, proveedor de servicios de comunicaciones electrónicas establecido en Suecia, podía negarse a conservar los mismos durante seis meses tal y como exigía la ley sueca. El TJUE entró a valorar si la conservación generalizada e indiferenciada de datos de comunicaciones electrónicas era incompatible con los artículos 7, 8 y 52, apartado 1, de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE) y concluyó que una Normativa

Estatal que establezca una conservación indiscriminada de datos, aunque fuera amparada en la lucha contra la delincuencia, vulneraba los derechos fundamentales y libertades reconocidos en la CDFUE, precisando que ello sólo sería admisible si la Ley establece límites según categorías de datos a conservar, personas afectadas y períodos concretos, debiendo, además, indicar las circunstancias y los requisitos en los que se efectuaría dicha conservación. Las conclusiones de la aludida Sentencia son plenamente extrapolables a nuestro país, por lo que la conservación preventiva de datos, con el fin de investigar delitos, requiere que nuestra normativa se encuentre ajustada a los parámetros fijados por el TJUE.

f) El sexto principio es el de **integridad y confidencialidad**, entendido como aquel principio por virtud del cual los datos personales habrán de ser tratados de forma que se garantice una adecuada seguridad de los mismos, evitando el tratamiento no autorizado o ilícito y tomando las medidas necesarias en función de la cantidad de datos y la calidad de los mismos (grado de afectación a la intimidad de los afectos que dichos datos pueden generar).

Finalmente, el principio más importante de todos es el conocido como **Principio de *Accountability* o de responsabilidad proactiva**. Podría decirse que se trata de un principio que en cierto modo engloba todos los demás. La implantación de este principio como preceptivo, tiene la intención de hacer responsables a las empresas no sólo de tomar todas las medidas y respetar todos los principios mencionados en el Reglamento, sino también de ser capaces de demostrar que han puesto todos los medios para cumplirlos. Se abandona la anterior regulación (antigua LOPD 15/99), por la cual se establecían listados de obligaciones a cumplir, y sanciones por su incumplimiento. El nuevo principio de responsabilidad activa se enfoca totalmente a la evitación de un resultado lesivo para el ciudadano, o de un resultado ilícito o prohibido por la ley y deja en manos de las empresas la obligación de acreditar que se han diseñado adecuadamente los procesos ("privacy by design", "privacy by default[27]" o privacidad desde el diseño, privacidad por

[27] Se trata de un principio jurídico por virtud del cual, una organización se asegura de que sólo aquellos datos personales estrictamente necesarios para cada propósito específico, son procesados por defecto, sin la intervención de ningún usuario.

defecto) y se ha cumplido con todos los principios y con la diligencia debida si se diese cualquier incidencia, European Data Protection Supervisor (2019)[28].

En lo relativo a la LOPD 3/2018, destacan una serie de novedades, que han de resaltarse en este trabajo (para lo que se ha tenido en cuenta el Informe de Uría & Menéndez (2018) citado)[29]. La primera de ellas es su función como norma de desarrollo del citado RGPD. Si bien es cierto que al ser un Reglamento UE no resulta necesario ningún tipo de transposición de dicha norma, la LOPDGDD trata de arrojar luz sobre algunos aspectos que puedan dar lugar a algún tipo de ambigüedad a la hora de ser interpretados, de modo que efectúa un desarrollo del Reglamento de carácter restrictivo, incorporando aspectos como la edad mínima para prestar consentimiento por parte de los menores de edad o el establecimiento de categorías especiales según la tipología de los datos.

La segunda de las novedades es la regulación de determinados tratamientos específicos de datos que no se encuentran expresamente recogidos en el RGPD, como el tratamiento de datos con fines de video vigilancia o los ficheros de solvencia patrimonial, de modo que la LOPDGDD incluye una regulación expresa para estas cuestiones.

La siguiente es probablemente la novedad más importante que incluye esta ley, que es la creación de los conocidos como Derechos Digitales, los cuales se encuentran regulados en el Artículo 79 y siguientes de la ley. En total son diecisiete nuevos derechos digitales que, según Uría Menéndez (2018) "*Nacen con la intención de proteger los intereses de los españoles ante las cuestiones derivadas de la incorporación de las nuevas tecnologías en el día a día de los ciudadanos*[30]."

Llama la atención la última frase del artículo 79 de la LOPDGDD, pues expresa lo siguiente: "*Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación".* De este modo se incluye en estos llamados Derechos Digitales, el Principio de *Accountability* mencionado en el RGPD, de tal modo que hace responsables a las empresas prestadoras de servicios, del efectivo ejercicio de los derechos por parte de los ciudadanos.

[28] European Data Protection Supervisor. (2019). European Data Protection. Obtenido de Accountability Principle; European Data Protection: https://edps.europa.eu/data-protection/our-work/subjects/accountability_en
[29] Op. Cit. Uría Menéndez. (2018). Principales novedades de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. Madrid.
[30] Ibid. Página 8.

Otra de las novedades que presenta la LOPD respecto al RGPD es el nuevo estatuto de actuación de la Agencia Española de Protección de datos, así como las Guías de actuación para las autoridades autonómicas competentes en esta materia (que se limitan a competencias respecto a ficheros de carácter público, pero ficheros de titularidad privada), con el objetivo de unificar criterios y ser más eficientes. Finalmente, la última novedad de esta Ley frente al Reglamento, es el Régimen Sancionador aplicable en nuestro país según el tipo de infracción que se cometa; de nuevo vuelve a realizar una extensión del RGPD, categorizando las conductas en leves, graves y muy graves. Asimismo, y tal y como señala Uría Menéndez (2018): "*Un elemento novedoso respecto a las disposiciones del RGPD es la expresa incorporación de la responsabilidad solidaria del representante de los responsables o encargados situados fuera de la Unión Europea*[31]". De modo que la responsabilidad pasa a ser solidaria por parte de la empresa matriz, con el fin de desincentivar este tipo de conductas. Como se viene diciendo a lo largo de este trabajo, todos estos principios, disposiciones y derechos habrán de ser respetados en la recopilación, uso y cesión que hacen los automóviles inteligentes por parte de todos los datos que recopilan, siendo esta problemática parte del objeto de estudio de este trabajo.

2. El Derecho a la Privacidad en el uso de Dispositivos Inteligentes

Se va a comenzar por estudiar el derecho a la privacidad en todos los dispositivos inteligentes para pasar, en el siguiente apartado, a analizar este derecho en el dispositivo inteligente que constituyen los propios automóviles inteligentes. En este sentido, destaca el artículo de Mato (2019)[32], quién argumenta que aún existiendo una legislación cada vez más completa en el ámbito de la protección de datos, constan multitud de aplicaciones que tratan de instalar algún tipo de programa maligno junto con la función principal de la misma. En primer lugar, critica las interminables condiciones de uso que se plantean al usuario al comenzar a utilizar una aplicación o incluso cualquier dispotitivo inteligente. Mato argumenta que en numerosas ocasiones, las leyes no tienen nada que hacer debido

[31] Op. Cit. Uría Menéndez. (2018). Principales novedades de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales. Madrid. Página 10.
[32] Mato, O. (2019). Cefa Digital. Obtenido de http://www.cefadigital.edu.ar, Página 1.

a que el usuario acepta en las condiciones de uso, una utilización de sus datos de la que no es consciente, pero para la cual está prestando un consentimiento, en teoría, expreso.

En esta línea, y tal como se mencionaba en el RGPD, se ha de atender, por parte de quién trata los datos, a los principios recogidos en dicha disposición legal, sin embargo, como se aprecia en la realidad, esto no termina de ser así. El artículo 7.2 de dicho reglamento especifica lo siguiente:

"Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento."

Si se atiende a este precepto, parece obvio que resulta ilícito incluir finalidades adicionales en las condiciones de uso de una aplicación sin que estas se encuentren claramente definidas y separadas de aquellas que sí resultan estrictamente necesarias para el correcto funcionamiento de la misma.

En este sentido, llama la atención la política de privacidad de un dispositivo tan común en los hogares españoles como es el llamado televisor inteligente o *Smart TV*, es decir, cualquier televisor con capacidad para conectarse a internet y poder disfrutar de servicios de *streaming* [33]como "Netflix", "Youtube", "Amazon Prime Video" o similares. Los televisores inteligentes son un claro ejemplo de un dispositivo que se ha convertido en un ordenador (están dotados de procesadores avanzados), y que es capaz de recopilar una cantidad muy importante de datos sin que el usuario llegue a ser consciente de ello en ningún momento (algo muy similar a lo que está ocurriendo con los automóviles inteligentes).

Al revisar la política de privacidad de Samsung Electronics Co. Ltd (2020)[34] para el uso de cualquiera de sus televisores inteligentes, se observa que no se respeta el mencionado artículo 7.2 del Reglamento Europeo de Protección de datos, ni se atiende a la mayor parte de los principios que se incluyen en el mismo y se han mencionado con anterioridad.

[33] Real Academia Española (2020), establece que *streaming* es el equivalente español a visualización/transmisión en directo o en continuo.
[34] Samsung Electronics Co. Ltd. (2020). Samsung. Obtenido de Política de Privacidad de Samsung: https://www.samsung.com/es/info/privacy_legal/

Se ha de aclarar que se escoge Samsung debido al número de ventas de televisiones que vende en España, alrededor de un 31% de las ventas totales de nuestro país según Urranca (2019)[35] y a que se trata de una política de privacidad muy similar y representativa del resto de telivsores inteligentes que se venden en España.

La política de privacidad de Samsung es un documento que aparece por primera y última vez en la pantalla del televisor al sacarlo de la caja y encenderlo. Se trata de una pantalla en la que aparecen los epígrafes "*Servicio Samsung: Términos y Condiciones*", "*Elementos destacados de la política de privacidad de Samsung*", "*Servicios de información de visualización*" y "*Política de privacidad de los anuncios individualizados*" junto a un botón en el que aparece escrito "*Ver detalles*". De modo que si bien es posible leer una a una las diferentes políticas de privacidad que aparecen, es importante resaltar que todas ellas vienen ocultas y vienen por defecto aceptadas, incitando al usuario a su aceptación mediante la colocación de un botón con la frase "Aceptar todas".

De este modo, el consumidor puede aceptar tres políticas de privacidad distintas sin abrir ninguno de los documentos, ya que le supone más tiempo y esfuerzo ir abriendo uno a uno los documentos que pulsar el botón de "*Aceptar todas*". Algo que va en contra de la buena fe y del espíritu y la letra del mencionado artículo 7.2 del RGPD, pues si bien aparecen como apartados distintos, todas ellas vienen aceptadas por defecto, sin que el consumidor llegue a ser realmente consciente de que está aceptando unos términos y condiciones que van más allá de lo necesario para ver una televisión.

Al leer dicha política de privacidad, encontramos algunos de los datos concretos que Samsung recolecta. Entre ellos se encuentra la "*Información del calendario*", el "*Historial de navegación en Internet*", "Información acerca de música y fotos del usuario", "Datos de ubicación", "*Información de otros dispositivos conectados*" o "*Información del dispositivo, entre la que se incluye las aplicación que instala, los contenidos que visualiza o cómo y cuándo utiliza el dispositivo*".

Todos los datos mencionados previamente sirven para que la marca coreana genere un perfil muy ajustado de la persona que está viendo cada uno de los televisores de Samsung. Puede saber en qué manzana vive, debido a la localización, puede saber aproximadamente el número de personas que ven la televisión, ya que puede acceder al número de

[35] Urranca, J. M. (2019). Mercado de TV en España en 2019. Revista ON OFF. Página 1.

dispositivos conectados al mismo router que la televisión o al número de usuarios de Netflix que se ven ese dispositivo, algo que -en mi opinión- atenta contra el principio de minimización de datos. Que Samsung recopile estos datos no parece suficientemente justificado desde ningún punto de vista; esto es, cuando un consumidor adquiere un televisor, está pagando por un dispositivo con el que pretende conseguir acceder a contenidos audiovisuales, pero en el momento en el que se efectúa la adquisición del dispositivo **en ningún caso se le informa, por parte de ningún vendedor, independientemente del canal utilizado** (ya sea en la tienda física o ya sea a través de una web) de que ese televisor le va a obligar a que se recopilen una serie de datos personales suyos y de su familia, con los que el fabricante del aparato va a poder acceder a un perfil muy completo que, sin ninguna duda y en mi opinión, puede suponer una forma grave de antentar contra su derecho a la privacidad.

Debemos pensar que, al comprar el televisor, se oculta deliberadamente que ese aparato va a tener un doble coste: por una parte, será necesario pagar el precio del dispositivo. Por otra, el fabricante genera un contexto de acceso a las prestaciones del televisor, en el que indirectamente obliga al usuario a "aceptar" (si es que puede considerarse una aceptación ese comportamiento) un uso de sus datos que supone un importantísimo ingreso para dicho fabricante. De manera que el consumidor paga dos veces, sin que nadie le advierta de tal extremo: paga el precio y vuelve a pagar, al aportar importantísimos y muy valioso datos que serán convenientemente monetizados por parte del fabricante, para comercializar con ellos.

Parece lógico preguntarse si este comportamiento del fabricante (Samsung, en el caso analizado) no debería dar lugar a una actuación inmediata de la Autoridad Española o Europea de Protección de Datos, que deje completamente claro que hay derechos (como el que nos ocupa) que deberían resultar indisponibles. En nuestra opinión, recabar datos personales y generar perfiles a través del uso de los televisores (lo que puede incluso permitir que el fabricante deduzca datos sobre ideas políticas, sexuales, religiosas o morales), cuando el consumidor ya ha abonado el precio del dispositivo debería generar importantes sanciones que eviten esta clara intromisión en la privacidad de los ciudadanos.

Sin embargo, no se trata de una excepción, sino tan sólo de un ejemplo, pues la cantidad de datos recopilados por teléfonos inteligentes es muy superior (número de pasos,

palabras escritas, contactos, llamadas o geolocalización permanente son algunas de ellas), así como los recopilados por los llamados asistentes personales como Google Home, Siri o Alexa, los cuales analizan las conversaciones que escuchan con el supuesto fin de mejorar su reconocimiento de voz, pero sin el más mínimo recato acerca de la capacidad real de escuchar conversaciones privadas a cuyo acceso inconsentido el ordenamiento jurídico reserva castigos importantes.

Es más, incluso el Código Penal español (al igual que el de los países de nuestro entorno) tienen tipificadas importantes penas, incluso privativas de libertad, lleve a cabo actos de descubrimiento y la vulneración de la intimidad de otro (A. 197 CP).

Tal y como establecía Mato (2019)[36]: "*Cualquier usuario de estos dispositivos que lea este artículo puede pensar ¿quién lo va a espiar a él, quién estaría interesado en sus datos o en husmear en su privacidad, pues entre tantos millones de dispositivos que se venden, justo a el lo van a espiar? Pero lo que todos debemos tomar conciencia es que en la actualidad esa información va a repositorios que a través de técnicas de minería de datos (data mining) y de Big Data, junto a plataformas muy potentes, se gestiona y analiza la misma en tiempo real, y el resultado es obtener información acerca de la privacidad de cualquier persona (o de un grupo) sin que esta (o estos) lo sepan*."

Por ello resulta tan importante para los consumidores ser conscientes de que su derecho a la privacidad se está viendo afectado cada vez que aceptan unas condiciones de uso que en muchas ocasiones contienen cláusulas que no respetan la legislación vigente, sino que van más allá de los límites y recaban información personal sin tener ningún tipo de potestad para hacerlo.

Debe tenerse en cuenta, además, cuál es la expectativa razonable de privacidad que puede albergar un consumidor que adquiere un televisor (extremo que fue específicamente alegado como defensa, por el reclamante en el Caso Barbulescu al que me refiero a continuación). En mi opinión, si la expectativa razonable de privacidad puede eliminarse cuando se facilita una información adecuada que debe evitar que nazca esa expectativa razonable, muy difícilmente quedaría limitada en el supuesto del comprador de un "Smart TV".

[36] Mato, O. (2019). Cefa Digital. Obtenido de http://www.cefadigital.edu.ar, Página 4.

En este sentido, como decimos, resulta particularmente significativa la sentencia del Tribunal Europeo de Derechos Humanos 2017/61 del 5 de septiembre de 2017, Barbulescu contra Rumanía. El demandante, un ciudadano rumano lleva a juicio a la compañía para la que trabajaba al considerar que su despido se basaba en la vulneración de su derecho a la vida privada y correspondencia, que se encontraban amparados por el artículo 8[37] del Convenio[38] (RCL 1999, 1190, 1572), y de que los tribunales nacionales no protegieron ese derecho cuando avalaron el despido al que fue sometido este trabajador por parte de su empresa. El despido se basaba en el reglamento interno de la empresa, cuyo artículo 50 establecía lo siguiente: *"Está estrictamente prohibido perturbar el orden y la disciplina en el recinto de la empresa y particularmente: (...) usar los ordenadores, fotocopiadoras, teléfonos, el télex y la máquina de fax con fines personales."*

Sin llegar a especificar nada acerca de la posibilidad de la empresa de vigilar dichos dispositivos con la intención de comprobarlo. Sin embargo, se demostró por parte de ésta que el demandante estaba utilizando su cuenta personal de correo electrónico con el ordenador y el internet de la empresa, durante el horario de trabajo, por lo que procedieron al despido del empleado alegando que éste había faltado al citado artículo 50 del reglamento interno de la compañía. El Tribunal da la razón al demandante, alegando que en efecto se violó el citado artículo 8 y estipula: "*(...) no parecía que el demandante hubiera sido informado con antelación del alcance y de la naturaleza del control efectuado por la empresa o de la posibilidad de que la empresa tuviera acceso al contenido de sus comunicaciones (...) Asimismo, no parece que los órganos jurisdiccionales nacionales hayan comprobado suficientemente la existencia de razones legítimas que justificaran el establecimiento de un control de las comunicaciones del demandante. (...) Por otra parte, ni el Tribunal del Condado ni el Tribunal de Apelación examinaron suficientemente si el objetivo perseguido por el empleador podía haberse*

[37] 1.Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

[38] Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983.

logrado mediante métodos menos intrusivos que el acceso al contenido mismo de las comunicaciones del demandante.”.

Destacan varios aspectos de esta sentencia, en primer lugar, que resulta necesario avisar de forma clara a los trabajadores de una compañía de que se va a vigilar sus comunicaciones. De modo que se desprende que éstas pueden llegar a ser vigiladas si se llevan a cabo con el material proporcionado por la compañía. En esta línea, el Tribunal aclara otro aspecto relevante, y es que la empresa debe buscar previamente, otro modo menos intrusivo de probar que el trabajador está llevando a cabo actividades personales en su tiempo de trabajo, sin que pueda accederse a las comunicaciones del trabajador como primera medida. Finalmente, esta sentencia habla de las razones legítimas que ha de tener una compañía para intervenir las comunicaciones de uno de sus empleados, sin que en este caso hayan sido capaces de probar razón legítima alguna. Por todo ello, se condena a la empresa, dando así la razón al trabajador.

Parece oportuno traer a colación la Sentencia Barbulescu, por el extraordinario agravio comparativo que considero se produce, entre lo que se exige a una empresa para que pueda defender sus derechos frente a comportamientos laborales discutibles, y la grave (en mi opinión) laxitud con la que son tratadas las grandes corporaciones con cláusulas y comportamientos manifiestamente abusivos respecto al derecho fundamental de privacidad de los ciudadanos.

Incluso aun en el caso de que el controvertido caso Barbulescu pueda defenderse, resulta descorazonador comparar el distinto rasero con el que se trata un comportamiento laboral discutible respecto al comportamiento de las grandes corporaciones que trafican con los datos de sus clientes.

3. El Derecho a la Privacidad en el uso de Vehículos Inteligentes

Por todo lo dispuesto con anterioridad, este trabajo va a centrarse en analizar la legalidad del tratamiento (recopilación, uso y cesión) de datos por parte de los automóviles inteligentes, ya que un automóvil inteligente es un dispositivo en auge que puede llegar a recopilar una gran cantidad de datos y producir, por tanto, una importante cantidad de repercusiones no sólo jurídicas en las vidas de los ciudadanos.

Parece conveniente empezar por aclarar qué se entiende por automóvil inteligente, a fin de diferenciarlo de una confusión común, pues en multitud de ocasiones se confunde con el vehículo autónomo. Se entiende por automóvil inteligente, aquel automóvil con conectividad integrada, es decir, capaz de ofrecer servicios avanzados de comunicaciones, como el acceso a internet o a la geolocalización y con un mayor grado de procesamiento y conectividad que un automóvil convencional.

El mejor ejemplo de automóviles inteligentes son todos los automóviles pertenecientes a las empresas de *Carsharing*[39] como pueden ser Emov, Car2Go o Wible, empresas que basan su modelo de negocio en la economía colaborativa. De este modo, los usuarios que utilicen dichas empresas pueden, mediante una aplicación, conocer la localización de los automóviles disponibles para alquilar y hacer uso de los mismos por minutos, pagando según el tiempo que dure dicho alquiler.

El problema jurídico del modelo de negocio reside en la cantidad de información recopilada por parte de los vehículos de la compañía. Ejemplo de ello es la política de privacidad de Wible[40], la cual establece lo siguiente:

"DriveSmart recaba exclusivamente datos que sean necesarios para monitorizar la conducción del usuario como la velocidad o geolocalización […] Respecto de estos datos de monitorización que son necesarios para la elaboración del perfil de conducción, DriveSmart es Encargado del tratamiento y Wible el responsable, por lo que mediante el correspondiente contrato han regulado de modo transparente sus responsabilidades y obligaciones. Podrás ejercitar los derechos indicados en el apartado 8 dirigiéndote a Wible por medio de las vías señaladas. Una vez más te informamos que Drive Smart nunca puede llegar a identificarte. Puedes acceder a su política de privacidad en el siguiente enlace: […] "[41]

De modo que, en la propia política de privacidad de Wible, remiten al usuario a otra política de privacidad distinta, de otra compañía que, como especifican, establece un perfil de cada usuario que conduce el automóvil. En este sentido se repite el problema que se daba con los televisores inteligentes, pues a la hora de registrarse, simplemente aparece un pequeño recuadro que debe ser pulsado y con el que se acepta la política de

[39] Se conoce con este nombre una nueva modalidad de alquiler de coches en la que el usuario solo paga por el tiempo de uso del mismo, así lo define Iati Seguros, (2019).
[40] WIB ADVANCE MOBILITY S.L. (2019). Política de Privacidad de Wible. Madrid, España.
[41] WIB ADVANCE MOBILITY S.L. (2019). Política de Privacidad de Wible. Madrid, España.

privacidad y los términos y condiciones generales de uso, sin que se especifique, en ningún momento, que sus datos van a ser utilizados para elaborar un perfil de su conducción por parte de una empresa distinta a Wible, como es Drive Smart.

En su política de privacidad, Drive Smart[42] establece que analiza "*Los resultados de velocidad, frenada, aceleración, giros y anticipación al tráfico",* de modo que una empresa que no es con la que el cliente cree estar contratando, al conocer la ubicación del vehículo accede también a datos tales como si se está superando la velocidad permitida en carretera, si se está haciendo un uso adecuado de los frenos o si los giros que se están haciendo por parte del conductor son adecuados o erráticos. Esto, unido a que la ya citada política de privacidad de Wible permite la cesión de los datos entre otros a las aseguradoras: "*Destinatarios de los datos: […] A entidades aseguradoras, para la gestión de siniestros y/o accidentes"*. Hacen que, en caso de accidente, se pueda determinar la velocidad a la que iba el conductor en el momento del siniestro, si estaba utilizando el móvil, si hizo uso del volante o los frenos… Pudiendo ser muy beneficioso para la compañía de *carsharing* y muy perjudicial para el usuario.

Todo ello puede ser más o menos aceptable en la medida en que se cumplan los principios del RGPD, y se informe al usuario de forma correcta de lo que se va a hacer con sus datos, ya que, al fin y al cabo, se trata de un automóvil que no es propiedad de quién lo conduce, sino del arrendador, en este caso, Wible o cualquier otra compañía de *carsharing* (es, por tanto, un supuesto criticable pero de menor gravedad que el de los televisores, más atrás analizado).

El verdadero problema, sin embargo, aparece cuando toda esta información es recopilada por parte de automóviles que son de nuestra propiedad o forman parte de un contrato de *Renting* o "Leasing"[43], así como aquellos vehículos que forman parte de la retribución en especie o son utilizados para trabajar y son propiedad de la empresa, pues se están recabando una serie de datos que pueden llegar a ser perjudiciales para el propio cliente de la marca.

[42] DRIVESMART TECHNOLOGIES S.L. (2019). Política de privacidad de DriveSmart. Madrid, España.

[43] Contrato de Leasing Financiero: Contrato que permite al usuario disfrutar del bien por un precio y duración variables, no dándose en este caso la intermediación de la sociedad de leasing, sino que el propio fabricante ofrece la posibilidad de financiación. El Leasing Operativo se da en aquellos casos en los que la entidad arrendadora afronta el riesgo técnico, prestando los servicios de mantenimiento y asistencia. (STS, 1ª, 10-IV-1981)

En este sentido, destaca la Sentencia del Tribunal Superior de Justicia de Galicia 3031/2014 del 6 de junio de 2014, en la que un trabajador demanda a la empresa de la que ha sido despedido. Considera que el despide es improcedente, ya que la empresa para la que trabajaba como vigilante de seguridad, instaló un GPS en los vehículos utilizados para realizar las rondas de vigilancia. La empresa tenía sospechas de la falta de rigor al realizar las rondas de vigilancia, por lo que, ayudados por el GPS instalado en vehículo, decidieron seguir al demandante. Comprobaron que efectivamente, el demandante se dedicaba a dormir o a descansar durante parte de su ronda de vigilancia, algo que venía repitiéndose durante las últimas semanas. Al ser conductas que violaban las normas de comportamiento de la empresa, fue despedido. Sin embargo, el trabajador despedido demandó a la empresa alegando que se habían violado los derechos que el artículo 18 de la Constitución le confería. Sin embargo, el Tribunal Superior de Justicia de Galicia, apoyado en la doctrina del Tribunal Constitucional estableció: "*Como ha puesto de relieve la sentencia del TC de 10-Jul-2000 , el derecho a la intimidad personal, consagrado en el artículo 18.1 CE , se configura como un derecho fundamental estrictamente vinculado a la propia personalidad y que deriva, sin ningún género de dudas, de la dignidad de la persona que el artículo 10.1 CE reconoce e implica "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" y que el derecho a la intimidad es aplicable al ámbito de las relaciones laborales (STC 98/2000).*

Igualmente es doctrina reiterada del Tribunal Constitucional que "el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho" (SSTC 57/1994 143/1994 , por todas). En este sentido debe tenerse en cuenta que el poder de dirección del empresario, imprescindible para la buena marcha de la organización productiva".

De modo que, una vez más, se recurre, por parte de los tribunales españoles, a lo que parece ser una de las claves para que el tratamiento de datos esté amparado, y es la justificación del mismo.

La localización vía GPS del empleado lesiona los derechos contenidos en el A. 18 CE, y así se recoge en la sentencia. Sin embargo, esta lesión se encuentra justificada por diversas razones. La ya mencionada justificación de la propiedad del vehículo, ya que se trata de un vehículo propiedad de la empresa, unida a las sospechas que tenía la misma acerca de la falta de rigor por parte del empleado de llevar a cabo de forma adecuada la tarea encomendada.

Y la segunda es que se trata de un vehículo afecto a la actividad laboral, que no puede utilizarse para otra tarea que no sea la vigilancia. Esta falta del elemento privativo a la hora de utilizar el vehículo, que se considera una herramienta de trabajo proporcionada por la empresa y que ha de quedarse en el puesto de trabajo una vez los empleados finalicen su jornada, permite a la empresa la localización del mismo, pues, tal y como puede apreciarse en la sentencia siguiente, si esos vehículos fuesen utilizados fuera del horario laboral, esto presentaría una nueva problemática en el uso del GPS por parte de la empresa.

Ejemplo de ello es la Sentencia del Tribunal Superior de Justicia de Asturias, Sala Social, Sentencia 3058/2017 de 27 Dic. 2017, en la que el Sindicato Comisiones Obreras, demanda a una empresa de telecomunicaciones por incorporar a los vehículos de la compañía un GPS con diversas funcionalidades. La compañía envía una circular a todos sus empleados e informa de aquellos vehículos en los que va a ser instalado, así como las funciones que posee el dispositivo que va a integrarse, entre dichas funciones se encuentran: "*localización en tiempo real, visualización de trayectos con posición segundo -a segundo, visualización de tramos conducidos con exceso de velocidad, detección de vehículo más cercano a un punto / calle, cuentakilómetros basado en GPS y creación de alertas, datos que a su vez permitirán elaborar informes de distancia por día o por periodos, ralentí, recorridos".*

Por tanto, se trata de un dispositivo que permite convertir cualquier vehículo convencional en un vehículo inteligente. Asimismo, se informa a sus trabajadores acerca de sus derechos en materia de protección de datos mediante una circular. La Empresa que implanta esta medida se ampara en el artículo 20.3[44] del Estatuto de los Trabajadores,

[44] Artículo 20.3: "El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad". Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.

alegando su derecho a controlar las obligaciones de los trabajadores, así como su productividad en horas de trabajo, pues los vehículos son propiedad de la empresa y son para uso exclusivo para la actividad empresarial, de modo que en ningún caso constituyen salario en especie ni pueden ser utilizados para nada más. CC.OO solicita: que la empresa "*garantice de forma fehaciente a los representantes de los trabajadores que el dispositivo de geolocalización no estará operativo a partir del momento en que finalice la jornada laboral y con cuanto más proceda en derecho*". Ya que alega que el dispositivo instalado en los vehículos puede utilizarse de forma abusiva por parte de quien lo instala, afectando a los derechos de los trabajadores. Asimismo, el sindicato alega: "*que la sentencia sacrifica injustificadamente el derecho de intimidad de los trabajadores al derecho de la empresa al control de sus trabajadores durante la prestación de servicios laborales. La instalación y uso de los dispositivos GPS es una medida restrictiva de aquel derecho fundamental que no es idónea, necesaria ni proporcionada por lo cual incumple las exigencias mínimas para su licitud.*". Como puede apreciarse, se cita, por parte de CC.OO., aquellos principios que se veían reflejados en la Sentencia BARBULESCU del TEDH como son la proporcionalidad de la medida, así como que ésta sea lo menos invasiva posible.

Destaca otro aspecto muy relevante, y es que el sindicato alega que los datos obtenidos por parte de la empresa no son datos anonimizados: "*el sistema instalado por la empresa ZENER afecta a personas identificables pues cada vehículo es utilizado por trabajadores previamente determinados. Su función, revelada en las comunicaciones remitidas al Comité de Empresa y a los trabajadores, es la obtención y el tratamiento automatizado de datos sobre el uso de los vehículos, que encajan en el concepto visto de datos personales. El propio comportamiento de la demandada inscribiendo los ficheros en la Agencia de Protección de Datos y sometiendo su régimen a las prescripciones de la LOPD y al reglamento que lo desarrolla pone de manifiesto el conocimiento por la demandada de tales circunstancias."* De este modo, se pone de manifiesto, que al tratarse de datos personales (por ser identificables los trabajadores), deben tener mayor protección. Sin embargo, el Tribunal asegura que: "*La empresa ZENER antes de comenzar el seguimiento con dispositivos GPS procedió a comunicar al Comité de Empresa y a los trabajadores la medida en unos términos que cumplen el mandato legal (…). Por consiguiente, la desestimación de la pretensión principal en la sentencia de instancia no incurre en las infracciones denunciadas."*

Por tanto, la empresa, aún tratándose de datos personales (permiten identificar al interesado), cumplió con todos los mandatos que impone la ley (destruyó la expectativa razonable de privacidad del trabajador en el uso del vehículo, al que se refiere la Sentencia Barbulescu), por lo que se desestima que se esté faltando a la LOPD 1999[45]. Finalmente, y llegando así a la parte más importante de la sentencia, se establece: *"Uno de los pilares fundamentales para la licitud del control de los desplazamientos por medio de dispositivos GPS y del tratamiento de los datos personales obtenidos por su medio es que la existencia de relación laboral faculta a la empresa ZENER para, en el ejercicio de sus facultades directivas y supervisoras, establecer algunos límites a derechos fundamentales de los trabajadores.*

Cuando finaliza la jornada laboral o acaba el tiempo de trabajo, dichas facultades empresariales desaparecen y el contrato de trabajo deja de constituir el vínculo entre las partes que ampara el poder de la demandada para imponer las medidas implantadas de captación y tratamiento de datos. A partir de ese momento, es imprescindible el consentimiento de los trabajadores para mantener en funcionamiento los dispositivos GPS y para el análisis automatizado de los datos personales conseguidos por ese medio pues el supuesto deja de estar comprendido en la excepción prevista en el art. 6.2 LOPD y se rige por la regla general del art. 6.1 LOPD . (...) La protección por la empresa de sus bienes y el control del uso que de ellos se haga una vez terminada la jornada de trabajo no constituye una excepción a la vigencia de la indicada regla general."

De modo que si bien la empresa tiene derecho a monitorizar todos los aspectos que pueden llevarse a cabo mediante el uso del chip, este uso sólo puede llevarse a cabo **durante la jornada laboral** de los trabajadores, ya que, a partir del momento en el cual dicha jornada laboral termina, los trabajadores no han sido debidamente informados de que se les va a realizar dicho seguimiento, pues la circular hablaba de seguimiento durante la misma. Igualmente, el artículo 20.3 ET deja de amparar el seguimiento y el desempeño laboral una vez la jornada ha terminado, por lo que, si la empresa desea seguir monitorizando sus vehículos, deberá basarse en otros argumentos jurídicos para poder hacerlo, más allá del fin de la jornada laboral, debiendo, asimismo, informar con una nueva circular a sus empleados.

[45] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Una vez analizada la citada jurisprudencia, resulta conveniente centrarse en analizar la política de privacidad esgrimida por los fabricantes de vehículos inteligentes, que han de aceptar los ciudadanos cuando adquieren uno de estos vehículos. En este sentido, parece útil analizar la **política de privacidad de Tesla**, pues se trata de la marca con más ventas en automóviles inteligentes, especialista además en este tipo de vehículos (nos referimos siempre en el presente trabajo a vehículos inteligentes a los que resulta de aplicación la normativa comunitaria).

Se ha de puntualizar que los vehículos que Tesla fabrica son vehículos inteligentes con un "modo autónomo" que puede activarse y que requiere la atención plena del conductor, pues debe mantener las manos en el volante para que el modo autónomo continúe activo, recayendo la responsabilidad de la conducción sobre el conductor en todo momento. La Política de Privacidad, Tesla Legal (2020)[46], debe ser aceptada por el adquirente y no sólo puede recopilar información mediante los múltiples sensores del vehículo, sino también:

- *"Mediante nuestros Servicios Digitales*
- *A través de aplicaciones de crédito u otros medios*
- *A través de la cuenta Tesla creada por el usuario*
- *Sin conexión*
- *A través del navegador o dispositivo"*

Lo primero que llama la atención es la cantidad de diferentes canales a través de los que Tesla recaba información tanto de clientes, como de potenciales clientes. Respecto a la segunda, recaba información "a través de aplicaciones de crédito u otros medios". La información recabada a través de aplicaciones de crédito, de acuerdo con la normativa Europea, sólo puede destinarse a conocer la solvencia del potencial comprador. La mención a "Otros medios" que no se especifican, no sería acorde al derecho comunitario. En todo caso, habría que permitir al potencial cliente que se niegue a que se use cualquier medio no expresamente autorizado por él.

[46] Tesla Legal. (2020). Política de privacidad de Tesla Inc. . Fremont, California, Estados Unidos: Tesla Inc.

Sin embargo, este trabajo se va a centrar en el segundo apartado de la política de Privacidad de Tesla, la cual establece los distintos métodos en los que los vehículos de la marca estadounidense recopilan datos:

"Podemos recopilar distinta información sobre su vehículo Tesla. El tipo de información que recopilamos y procesamos varía según el año, la configuración y el modelo de su vehículo. Entre los ejemplos de información recopilada se incluyen los siguientes:

- ***Datos de registro telemáticos**: para mejorar nuestros vehículos y servicios, recopilamos ciertos datos telemáticos relativos al rendimiento, uso, funcionamiento y estado de su vehículo Tesla como, por ejemplo: número de identificación del vehículo; información sobre la velocidad; lecturas del odómetro; información sobre la gestión del uso de la batería; historial de carga de la batería; funciones del sistema eléctrico; información sobre la versión de software; datos del sistema de información y entretenimiento; datos relacionados con la seguridad e imágenes de las cámaras (incluida la información relativa a los sistemas SRS del vehículo, el frenado y la aceleración, la seguridad, el freno electrónico y los accidentes); vídeos breves sobre accidentes;(...) Podríamos recopilar dicha información en persona o mediante acceso remoto.*
- ***Datos de análisis remoto**: podemos realizar una conexión dinámica con su vehículo Tesla para diagnosticar y resolver los problemas que presente, y para ello podría ser necesario acceder a la configuración personal del vehículo (por ejemplo, los contactos, el historial de consultas y el historial de navegación). Esta conexión dinámica también nos permite ver la ubicación actual de su vehículo, pero dicho acceso está restringido a un número limitado de empleados de Tesla.*
- ***Datos de análisis de seguridad**: a fin de mejorar nuestros productos y servicios, podemos recopilar y almacenar otros datos relativos al vehículo como, por ejemplo: información sobre los accidentes en los que se haya visto implicado su vehículo Tesla (p. ej., las veces que ha saltado el airbag, imágenes y datos del sensor de la cámara y otros datos recientes de los sensores); datos sobre los servicios remotos (cierre y apertura*

remotos, inicio/detención de la carga, mandos para tocar el claxon); un informe de datos para confirmar que su vehículo está en línea, junto con información relativa a la versión actual de software y ciertos datos telemáticos; información sobre la conectividad del vehículo; datos sobre cualquier problema que pueda afectar negativamente al funcionamiento de su vehículo; datos sobre cualquier problema relacionado con la seguridad; y datos relativos a cada actualización de software y firmware. Podríamos recopilar dicha información en persona (p. ej., al realizar una inspección técnica del vehículo) o mediante acceso remoto. (...)

- ***Historial del servicio técnico**: a fin de facilitar el mantenimiento de su vehículo, recopilamos y tratamos datos sobre el historial del servicio técnico de cada vehículo Tesla. Por ejemplo: nombre del cliente, número de identificación del vehículo, historial de reparaciones, avisos pendientes del vehículo por problemas técnicos, facturas pendientes, reclamaciones de los clientes y cualquier otro tipo de información relacionada con el historial del servicio técnico. (...)*
- ***Desactivación del uso compartido de datos**: si no desea que recopilemos datos de registro telemáticos o cualquier otro dato de su vehículo Tesla, póngase en contacto con nosotros según se indica en la sección "Cómo ponerse en contacto con nosotros" que aparece a continuación. Tenga en cuenta que, si decide desactivar la opción de recopilación de datos de registro telemáticos o cualquier otro dato de su vehículo Tesla (con excepción de los ajustes para compartir datos descritos anteriormente), no podremos informarle de asuntos relacionados con su vehículo en tiempo real. Esto podría suponer una reducción de las funcionalidades de su vehículo, que sufra daños graves o que tenga un mal funcionamiento, y también podría inhabilitar muchas funciones de su vehículo como, por ejemplo, actualizaciones periódicas de software y firmware, servicios remotos e interacciones con aplicaciones para móviles y funcionalidades del interior del automóvil como la búsqueda de ubicación, la radio a través de Internet, los comandos de voz y la funcionalidad del navegador web."*

Lo primero que llama la atención al leer este apartado de la política de privacidad, es que Tesla recabe de forma remota, es decir, desde cualquier lugar del mundo y sin necesidad de que el propietario preste consentimiento, datos de velocidad, cámaras o localización del vehículo. Sorprende porque no parece existir ningún tipo de fundamento jurídico mínimamente equilibrado que ampare esta masiva e intrusiva recopilación de datos. Como se ha mencionado anteriormente, se deben cumplir en Europa los principios de minimización de datos y limitación de la finalidad: deben recabarse el menor número de datos posibles para prestar el servicio o vender el producto y los fines para los que se usen los datos deben ser lícitos, explícitos y legítimos.

Surge la pregunta, por tanto, de cuál es el fin que justifica la recopilación de datos tan intrusivos y potencialmente agresivos para el ciudadano como vídeos de accidentes, velocidad exacta del vehículo o la geolocalización permanente. Se especifica, textualmente: "*para mejorar nuestros vehículos*", algo que, tal y como se establecía en las sentencias previamente analizadas, no se trata de un fin legítimo para llevar a cabo una recopilación de datos tan extensa. La pregunta lógica es si, todos esos datos se dirigen únicamente a mejorar el proceso de fabricación y mantenimiento de los vehículos (lo que resulta, simplemente poco creíble) o si, también se usan para generar perfiles del cliente y comercializar dichos datos entre otras empresas para quienes esa información puede resultar valiosísima: aseguradoras, empresas de investigación de mercados, incluso agencias de detectives, Policía o Agencias gubernamentales encargadas de gestionar multas, sanciones o de recaudar determinados impuestos.

Y es que, como estipulaba Sentencia del Tribunal Europeo de Derechos Humanos 2017/61 del 5 de septiembre de 2017, Barbulescu contra Rumanía, deben usarse los métodos menos intrusivos para obtener la información que resulte necesaria, así como existir una justificación lo suficientemente relevante como para que pueda verse afectado el derecho a la privacidad. Tomando en consideración que el vehículo es propiedad del cliente que efectúa la operación de compraventa con Tesla Motors Inc., parece que el interés de la compañía estadounidense pierde peso, pues si su única intención es la de mejorar el producto que ofrecen, esto podría llevarse a cabo únicamente en coches que acuden a reparación o mediante un programa en el que Tesla dispusiese de sus propios vehículos y empleados para recabar datos, no de clientes. O, incluso, podría pactarse una retribución del cliente que permitiese que sus datos fueran utilizados para este fin, lo que aseguraría que el consentimiento existe.

Podría tener sentido, y estar justificado que se guardasen esos datos en el disco duro del ordenador del vehículo, sin que la compañía pudiera acceder a ellos de forma remota, previo consentimiento expreso y suficientemente informado del cliente. Esto podría ser beneficioso para el dueño del Tesla en caso de accidente, actuando el disco duro a modo de caja negra, como si se tratase de un avión. Asimismo, podría usarse en caso de avería, siempre previo consentimiento del cliente, para asesorar mejor el posible arreglo del vehículo. Finalmente, en caso de multa, podría demostrarse que la velocidad captada por el radar o que la multa de aparcamiento han sido interpuestas de manera errónea si los datos de geolocalización y velocidad estipulan datos distintos a los que establecen las autoridades en la multa (aunque la ausencia de alegaciones en este sentido, en este tipo de vehículos supondría una presunción a favor de que la sanción se interpuso correctamente).

De este modo, el dueño del vehículo podría usar los datos que éste capta según sus intereses, y no al revés. Al fin y al cabo, parece lógico suponer que si el vehículo es propiedad del comprador y no de Tesla y, sobre todo, si los datos los genera el ciudadano y son datos relativos a su persona, los datos que Tesla recaba pertenecen a su dueño, y no al fabricante (Principio de autodeterminación informativa).

Se llega así, al último párrafo de la Política de Privacidad, en el que se asegura que el cliente puede desactivar la función de compartir datos con Tesla. Se trata de un proceso complejo, pues no consiste en desactivar un ajuste determinado, como en el caso del piloto automático o de las funciones avanzadas, sino que el propietario del vehículo deberá leer primero un texto titulado: "*Cómo ponerse en contacto con nosotros*", más tarde deberá llamar, o mandar un correo electrónico, y esperar la respuesta de los empleados de Tesla. Surge la duda de por qué son necesarios todos estos pasos cuando otras recopilaciones de datos se pueden desactivar de forma manual y sencilla desde el propio vehículo. Asimismo, uno se pregunta si estas dificultades y esta definición de procesos sobre tratamiento de datos personales, objetivamente complejos y engorrosos, son acordes a los principios de privacidad por defecto y privacidad por diseño. Incluso si el comportamiento de Tesla puede considerarse como una actitud de buena fe por parte de la compañía y si no esconde un evidente ánimo de que el consumidor, ante estas trabas, no desactive la recopilación de datos que supone grandes beneficios para Tesla.

Y es que Tesla establece que si no se comparten los datos de forma remota el vehículo puede perder funcionalidades, sufrir daños graves o tener un mal funcionamiento. Una vez más, se infiere el recelo de Tesla a que cualquier consumidor deje de compartir con ellos los datos recopilados por sus automóviles, pues estos datos tienen un enorme valor. Pueden no sólo utilizarse para predecir cuáles son las velocidades medias de las carreteras mundiales, sino también para establecer la forma en la que conduce una persona media, si se está respetando una forma adecuada de conducción, y por tanto se tiene derecho a una reparación en garantía o, por el contrario, si se ha llevado una conducción agresiva (cuestión que sólo determinará Tesla) y el desgaste del vehículo nada tiene que ver con el desgaste que consideren medio de un automóvil. Asimismo, pueden conocer cuáles son las rutas más transitadas por sus vehículos y, por ende, dónde puede ser más conveniente ubicar talleres, cargadores, comercios o vallas publicitarias.

Por todo ello, mi conclusión es que la recopilación de datos que llevan a cabo los automóviles inteligentes, así como la llevada a cabo por la mayoría de dispositivos inteligentes, como las mencionadas *Smart TVs*, no se ajustan a la legalidad vigente. Si bien es cierto que en teoría consiguen un consentimiento expreso por parte de los usuarios para llevar a cabo la recopilación de información, el consentimiento prestado no es -en mi opinión- suficientemente informado, y dicha recopilación excede con creces el principio de minimización de datos, sin que tampoco cumpla ninguno de los presupuestos del ya citado artículo 6 RGPD, en especial el de limitación de la finalidad de uso de los datos, en función de la expectativa de privacidad razonable del cliente, por lo que no existe ningún fundamento jurídico que lo ampare más allá del dudoso "*para mejorar nuestros productos*" que exponen estas compañías, y que enmascaran un flagrante ataque a la privacidad de los usuarios.

4. Cesión de datos

Una vez se ha establecido la dudosa legalidad de la recopilación de ciertos datos por parte de los fabricantes de vehículos inteligentes al no respetar principios como el de minimización de datos o proporcionalidad, o el de recabar consentimientos suficientemente sólidos e informados, se ha de estudiar otro aspecto crítico: la comunicación o cesión de los mismos. En este sentido, existe un apartado en la política

de privacidad de Tesla que se dedica exclusivamente a tratar el "*Uso compartido de su información*". Esclarecen que pueden compartir información con:

1. *"Nuestros proveedores de servicios y socios comerciales cuando sea necesario para prestar servicios en nuestro nombre o en su nombre.*
2. *Terceras partes autorizadas por usted.*
3. *Otras terceras partes según lo exige la ley.*

Podemos compartir su información para fines como el procesamiento de pagos, la tramitación de pedidos, la instalación de productos, el servicio al cliente, el marketing, la financiación, el servicio o la reparación y otros servicios similares."

Los puntos dos y tres parecen entrar dentro la legalidad y no merecen más comentarios, pues, al fin y al cabo, si son terceras partes autorizadas por el cliente de Tesla (siempre que el consentimiento sea expreso y se encuentre correctamente recabado e informado) o si se trata de terceras partes exigidas por la ley, parecen cumplir la legalidad vigente.

El principal problema reside en el primero de los puntos pues, tal y como se infiere del inciso final del párrafo, se trata de terceras partes no autorizadas explícitamente por el usuario de Tesla, sino de empresas colaboradoras de Tesla. De este apartado destacan negativamente, la cesión de datos a las aseguradoras:

"*Con proveedores de presupuestos de reparación y cualquier compañía de seguros para permitir que Tesla o un centro de servicios o proveedores externos ofrezcan servicios de reparación o mantenimiento en su vehículo (...) con otros socios comerciales externos, en la medida en que estén relacionados con la compra, el alquiler o el servicio técnico de sus productos Tesla. Compartimos una cantidad limitada de información personal o sobre sus productos Tesla con empresas asociadas como, por ejemplo, instituciones financieras y de arrendamiento, empresas de registros, de título y de seguro (...)"*

De modo que, sin que ni siquiera concreten a qué clase de datos se refieren (lo que impide al cliente saber quién accede a cuáles de sus datos), Tesla comparte información con las aseguradoras, ya que las considera socios comerciales.

En caso de concertar cualquier tipo de contrato de financiación con la compañía estadounidense, y contratar por tanto cualquier seguro, comparte con la aseguradora una serie de datos, pues como establece Tesla se trata de una actividad "necesaria para prestar servicios", algo que puede resultar altamente perjudicial para cualquier propietario de un

vehículo Tesla. Y es que el precio del seguro se revisa de forma anual, y Tesla -como decimos- no especifica los datos que comparte con las aseguradoras, de modo que si ha quedado patente en el apartado anterior que conoce velocidad, uso de frenos, geolocalización y forma en la que un usuario carga y descarga la batería de un coche, parece lógico pensar que toda esa información puede ser cedida a la compañía de seguros colaboradora de Tesla, y así determinar el precio del seguro que ha de pagar el propietario del vehículo; esto es, los datos del cliente podrían usarse en contra de sus intereses, mediante procesos que impiden reconocer al ciudadano (o, como mínimo, limitan) quién accede a sus datos, a qué datos accede y con qué finalidades podrán tratarse sus datos.

Algo que puede terminar condicionando no sólo el precio del seguro de este vehículo concreto, sino el seguro del hogar o de vida (mayor riesgo) o incluso el conjunto de los seguros que contrate esta persona en un futuro, pues los comportamientos que una persona tiene al conducir podrían ser extrapolables por parte de una aseguradora, a otros seguros.

En segundo lugar, destaca la enunciación que hace Tesla acerca de un apartado final que no está contenido en ninguno de los tres anteriores y que establece lo siguiente:

"También podemos compartir información en algunos otros casos. Por ejemplo:

Con su empleador u otro operador de flota o con el propietario del vehículo/producto Tesla, en caso que Usted no sea directamente el propietario y según fuere autorizado por la ley aplicable."

Se trata de un precepto que va en contra de la sentencia TSJ Asturias, Sala Social, nº 3058/2017 de 27 Dic. 2017, citada con anterioridad, en la que no se permitía que estos datos fuesen compartidos más allá de la jornada laboral. Asimismo, los datos entonces recogidos y compartidos eran muy reducidos en comparación con todos los que recoge un vehículo Tesla.

También surge la pregunta de si el empleado -de acuerdo con la normativa europea- debería ser avisado no sólo mediante la política de privacidad de Tesla, sino también mediante una circular específica del empleador en la que advierta de que puede acceder a los datos, ya que no parece suficiente con un párrafo, sino que se debería hacer consciente al empleado de que se están recogiendo sus datos por parte del empleador.

En este sentido, y para conocer la legalidad de la cesión de datos, más allá de los posibles perjuicios que pueda causar a los propietarios de los vehículos Tesla, destaca el Informe

Jurídico 2016-0278, elaborado por la Agencia Española de Protección de Datos (2016)[47]. Se plantea, por parte de un particular, una consulta a la Agencia Española de Protección de Datos (en adelante AEPD), relativa a la cesión de datos de carácter personal. La AEPD, basándose en el ya publicado RGPD (si bien no había entrado en vigor en 2016), establece los criterios necesarios para cumplir con la legalidad a la hora de ceder datos personales a terceros.

En primer lugar, establecen lo que es un Dato Personal, basándose en el artículo 4 del citado Reglamento. Una vez se ha establecido lo que es un dato personal, procede a establecer quiénes están legitimados para tratarlos. Se invoca, por la AEPD, el ya citado Artículo 6.1 RGPD, de modo que la cesión de datos se encuentra representada en el apartado f), ya que habla de "*Un tercero"* legitimado para el tratamiento de los mismos. Aquí se podría plantear si la cesión por parte de Tesla a una aseguradora estaría contenida dentro de este apartado pues se habla de un interés legítimo por parte del tercero. De este modo, la AEPD continúa explicando un concepto fundamental en la actual normativa, pero que puede resultar un tanto ambiguo, como es el de interés legítimo como base jurídica justificativa del tratamiento de datos personales.

"*Una segunda posibilidad que excepciona la necesidad del consentimiento del interesado la constituye la existencia de un interés legítimo,* ***siempre que en un ejercicio de ponderación entre dicho interés legítimo y los derechos fundamentales de los afectados prevaleciera el primero sobre el segundo.***

Así, la Sentencia del Tribunal de Justicia declaró expresamente el efecto directo del artículo 7 f) de la Directiva 95/46/CE, según el cual:

"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (...) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

Además, la nueva norma europea, el RGPD, contempla como causa legitimadora para el tratamiento de datos el interés legítimo, según su artículo 6.1.f)

[47] Agencia Española de Protección de Datos. (2016). *Informe Jurídico 2016-0278.* Madrid

Por tanto, para determinar si procedería la aplicación del citado precepto habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis existirá un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos que prevalezca sobre el interés o los derechos y libertades fundamentales del interesado que requieran protección conforme a lo dispuesto en el artículo 1 del RGPD, o si, por el contrario, los derechos fundamentales o intereses de los interesados a los que se refiera el tratamiento de los datos han de prevalecer sobre el interés legítimo en que el responsable o el tercero pretende fundamentar el tratamiento o la cesión de los datos de carácter personal.

De este modo, a efectos de efectuar la necesaria ponderación exigida, ***deberá plantearse si, atendiendo a las circunstancias concretas que se producen en el presente supuesto, el interés del tercero en acceder a los datos solicitados debe prevalecer sobre el derecho a la protección de datos de los afectados cuyos datos sean objeto de comunicación***."

En línea con el citado informe de la AEPD, en el marco de la cesión de datos, destaca la Sentencia del TJUE del 1 de octubre de 2019, C_673/17, la cual versa sobre la legalidad de instalar cookies de terceros al acceder a una página web. La demanda se interpuso debido a que al aceptar las *cookies*, no se especificaba de forma clara que así como se aceptaban las del sitio web al que accedía el usuario, también se aceptaban las cookies de terceros. En este sentido, el TJUE se pronunció estableciendo que era necesario informar al cliente acerca de quiénes van a ser los terceros a los que sus datos puedan ser cedidos: *"(...) estas indicaciones incluyen, en particular, además de la identidad del responsable del tratamiento y de los fines del tratamiento de que van a ser objeto los datos, cualquier otra información tal como los destinatarios o las categorías de destinatarios de los datos, en la medida en que, habida cuenta de las circunstancias específicas en que se hayan obtenido los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado."*

Algo que, cómo ha podido observarse con anterioridad no se cumple en la política de privacidad de Tesla, pues se habla de la cesión de datos a terceros, sin esclarecer, en ningún momento, la identidad de los mismos, incumpliendo así, la jurisprudencia del TJUE.

Por todo ello, al atender a la jurisprudencia del TJUE, así como al resto del RGPD, no existe una definición exacta de interés legítimo que pueda aplicarse en todos los casos de forma indistinta, sino que habrá de atenderse al caso particular, ponderando las circunstancias concretas y la importancia y legitimidad del fin perseguido y el derecho que va a verse afectado por ese fin. En todo caso, como principio general, no es sencillo imaginar circunstancias en las que un derecho fundamental como el de la privacidad, deba decaer ante un pretendido "interés legítimo" de la empresa que recaba datos o del beneficiario a quien se comunican, si dichas empresas no cumplen de forma cabal con los principios de lealtad, transparencia, minimización y resto de principios incluidos en el RGPD.

En el caso concreto que aquí se estudia, teniendo en cuenta el derecho a la intimidad, junto con el artículo 7 f), parece que la intromisión en los derechos fundamentales por parte de Tesla, así como la cesión de datos a una aseguradora, no justifica la cesión de datos a la misma.

La primera razón y probablemente la más obvia es que la mayoría de vehículos y sus correspondientes seguros no necesitan de ningún tipo de recopilación de datos por parte del vehículo para su correcto funcionamiento. En segundo lugar, parece lógico que a cambio de que el usuario aceptase a ceder sus datos, tanto Tesla como la aseguradora le concediesen algún tipo de compensación, ya que la información que ellos recopilan posee un enorme valor. Finalmente, no parece existir ningún tipo de proporcionalidad entre la potencial agresión del derecho a la privacidad evidenciada en la cesión de datos por parte de las empresas fabricantes de automóviles inteligentes, y la "necesidad" de cesión de esos datos por parte de las mismas.

CONCLUSIONES

1. La disrupción tecnológica se ha convertido en uno de los grandes retos a los que se enfrenta el Derecho contemporáneo. El Derecho español primero y, el comunitario después, han efectuado un considerable esfuerzo de anticipación y adaptación a una realidad tan compleja y multidisciplinar como es la adaptación a las nuevas tecnologías. El ordenamiento jurídico debe continuar evolucionando para adaptarse a los nuevos hábitos y asegurar una adecuada defensa de los derechos de los ciudadanos, haciéndolos compatibles con los efectos reales de la digitalización de la sociedad.
2. La citada digitalización de la sociedad está permitiendo una recopilación automatizada de datos personales sin precedentes en la historia, en la que los afectados son todos los ciudadanos, lo que supone un peligro para el Derecho a la privacidad de los ciudadanos.
3. En este contexto, cobra especial sentido la defensa de un derecho fundamental, como es el de la intimidad / privacidad. A pesar de la importante cuantía de las sanciones que establece el RGPD (hasta el 4% de la facturación global mundial del infractor), y a que la UE parece contar con instrumentos legislativos adecuados para defender al ciudadano, y pese a la antigüedad de la normativa comunitaria (mayo-2016, con entrada en vigor en mayo 2018), apenas ha habido actuaciones de las Autoridades de Privacidad Europeas realmente disuasorias frente a los grandes tratadores de datos.

   Así, continúan dándose comportamientos agresivos hacia los consumidores (mundiales, no solo europeos), basados en implementar fórmulas de recabar todo tipo de datos personales, sin respetar los principios de minimización de datos y de licitud y transparencia, cuando dichos consumidores adquieren productos tales como –entre otros- televisores o vehículos inteligentes, respecto de los que, en principio, cabe razonablemente esperar una alta expectativa de privacidad.
4. Parece difícil de entender la altísima exigencia que el TEDH ha adoptado a la hora de determinar cómo puede defenderse una empresa, en el marco de una relación laboral (Sentencia Barbulescu analizada) frente a comportamientos laborables cuando menos, discutibles, si esa exigencia se compara con la laxitud que, de hecho, se permite a los grandes tratadores de datos, en contextos jurídicos distintos (garantías jurídicas de los ciudadanos como consumidores cuando adquieren productos o servicios en los que se gestionan sus datos personales).

5. Samsung, a través de sus televisores (Smart TV) o Tesla a través de sus vehículos eléctricos inteligentes, son algunos ejemplos significativos de la distancia existente entre las obligaciones europeas y españolas en materia de protección de datos y lo que las grandes corporaciones establecen como métodos de obtención y tratamiento de datos personales, en suelo europeo respecto de ciudadanos europeos.
6. La AEPD y la Autoridad Europea de Protección de datos deberían contar con medios significativamente más relevantes, en especial de personal técnico cualificado, para poder aplicar la normativa comunitaria a todos por igual.
7. Pese a todo, Europa es hoy un claro referente en materia de protección de datos y es donde acuden el resto de países avanzados (excepto algunas corporaciones norteamericanas) a la hora de establecer mecanismos que permitan proteger con efectividad los derechos fundamentales de sus ciudadanos en materia de privacidad.

BIBLIOGRAFÍA

Agencia Española de Protección de Datos. (2016). *Informe Jurídico 2016-0278.* Madrid.

Agencia Española de Protección de Datos. (2019). *Protección de Datos: Guía para el Ciudadano.* Madrid: Guías AEPED.

Ayuso, S. (21 de enerp de 2019). Francia multa a Google con 50 millones de euros por falta de transparencia. *El País*.

BBC News Mundo. (24 de julio de 2019). *BBC*. Obtenido de Cambridge Analytica: la multa récord que deberá pagar Facebook por la forma en que manejó los datos de 87 millones de usuarios: https://www.bbc.com/mundo/noticias-49093124

Castellano, S. (13 de noviembre de 2019). *Kantar España Insights*. Obtenido de La publicidad en 2020: Dominarán las redes sociales y el vídeo online pese a las dificultades de medición: https://es.kantar.com/empresas/marcas/2019/noviembre-2019-getting-media-right/

Couper, M. P. (2005). Technology Trends in Survey Data Collection. *Social Science Computer Review*, 486-501.

Cuatrecasas, Gonçalves Pereira. (2014). El Régimen Jurídico de las Cookies y su aplicación por la Agencia Española de Protección de Datos. *Aranzadi Doctrinal*, 1-21.

Davara Rodríguez, M. (1992). La Ley española de protección de datos; ¿una limitación al uso de la información para garantizar la intimidad? *Actualidad Jurídica Aranzadi*.

Davara Rodriguez, M. (28 de enero de 2018). Entrevista a Miguel Ángel Davara: El legislador europeo quiere evitar que resulte "rentable" vulnerar el derecho a la protección de datos de las personas. (N. Jurídicas, Entrevistador)

DRIVESMART TECHNOLOGIES S.L. (2019). Política de privacidad de DriveSmart. Madrid, España.

European Data Protection Supervisor. (2019). *European Data Protection*. Obtenido de Accountability Principle; European Data Protection: https://edps.europa.eu/data-protection/our-work/subjects/accountability_en

Iati Seguros. (2019). Carsharing ¿Qué es y por qué está tan de moda? *Iati Blog*.

Instituto Nacional de Estadística. (2018). *España en cifras 2018.* Madrid: INE.

Maté Jiménez, C. (2014). Big data. Un nuevo paradigma de análisis de datos. *Anales de Mecánica y Electricidad*, 10-16.

Mato, O. (2019). *Cefa Digital.* Obtenido de http://www.cefadigital.edu.ar

Moulier-Boutang, Y. (22 de julio de 2016). Ahora ya todos trabajamos para las GAFA sin cobrar. (L. Amiguet, Entrevistador)

Orti Vallejo, A. (1994). El nuevo derecho fundamental (y de la personalidad) a la libertad informática (A propósito de la STC 254/1993, de 20 de julio). *Derecho Privado y Constitución*, 305-332.

Parejo, L. A. (1981). El contenido esencial de los derechos fundamentales en la jurisprudencia constitucional, a propósito de la Sentencia del TC del 8 de abril de 1981. *Revista Española de Derecho Constitucional*, 169-190.

Ramón y Cajal Abogados. (2019). *Novedades Ley Protección de datos.* Madrid: Ramón y Cajal Abogados.

Real Academia Española . (2020). *Diccionario Español Jurídico.* Obtenido de https://dej.rae.es/lema/smartphone

Real Academia Española. (2020). Equivalencia de straming. Madrid, España.

Roca Trías, E., & Ahumada Ruiz, M. (2013). Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española. *REUNIÓN DE TRIBUNALES CONSTITUCIONALES DE ITALIA, PORTUGAL Y ESPAÑA ROMA - OCTUBRE 2013.* Roma.

Samsung Electronics Co. Ltd. (2020). *Samsung.* Obtenido de Política de Privacidad de Samsung: https://www.samsung.com/es/info/privacy_legal/

Tesla Legal. (2020). Política de privacidad de Tesla Inc. . Fremont, California, Estados Unidos: Tesla Inc.

Uría Menéndez. (2018). *Principales novedades de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.* Madrid.

Urranca, J. M. (2019). Mercado de TV en España en 2019. *Revista ON OFF*.

WIB ADVANCE MOBILITY S.L. (2019). Política de Privacidad de Wible. Madrid, España.

JURISPRUDENCIA CITADA

- Sentencia del Tribunal Supremo, Sala 1ª, del 10 de abril de 1981.
- Sentencia del Tribunal Constitucional 254/1993 del 20 de julio.
- Sentencia del Tribunal Constitucional 57/1994 del 28 de febrero.
- Sentencia del Tribunal Constitucional 143/1994 del 23 de junio.
- Sentencia del Tribunal Constitucional 11/1998 del 13 de enero.
- Sentencia del Tribunal Constitucional 84/2000 del 27 de marzo.
- Sentencia del Tribunal Superior de Justicia de Galicia 3031/2014 del 6 de junio de 2014.
- Sentencia del Tribunal Europeo de Derechos Humanos 2017/61 del 5 de septiembre de 2017, Barbulescu contra Rumanía.
- Sentencia del Tribunal Superior de Justicia del Principado de Asturias, Sala de lo Social, Sentencia 3058/2017 de 27 Dic. 2017, Rec. 2241/2017.
- Sentencia del Tribunal Constitucional 76/2019, de 22 de mayo de 2019.
- Sentencia del Tribunal de Justicia de la Unión Europea de 21 de diciembre de 2016 (asuntos TELE2 SVERIGE AB y otros; C- 203/15 y C 698/15).
- Sentencia del Tribunal de Justicia de la Unión Europea, del 1 de octubre de 2019, C_673/17.
- Riley v. California, 573 U.S. 373 (2014), sentencia del Tribunal Supremo de Estados Unidos.

LEGISLACIÓN CITADA

- Constitución Española de 1978, Cortes Generales, BOE nº311 de 29 de diciembre de 1978.
- Convenio para la protección de los derechos y de las libertades fundamentales, hecho en Roma el 4 de noviembre de 1950; el protocolo adicional al Convenio, hecho en París el 20 de marzo de 1952, y el protocolo número 6, relativo a la abolición de la pena de muerte, hecho en Estrasburgo el 28 de abril de 1983.
- Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.
- Ley Orgánica 5/1992 de 29 de octubre, relativa a la regulación del tratamiento automatizado de los datos de carácter personal.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
- 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-RGPD).
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.