

N/REF: 0017/2019

La consulta plantea la aplicabilidad de la normativa de protección de datos al sistema que pretende desarrollar la entidad consultante, consistente en el tratamiento de la señal recibida por los dispositivos de captación y análisis de señales Wi-Fi que se instalan en determinadas tiendas, al objeto de conocer los recorridos y tránsitos realizados por terminales electrónicos con emisión de dicha señal –“*WiFi tracking*”-. Este tratamiento de datos tendría por objeto la detección de los productos que generan mayor interés en los clientes para la posterior realización de acciones de mercadotecnia.

Antes de proceder a la emisión del presente informe, debe señalarse que el mismo solo puede analizar, atendiendo a los propios datos manifestados con la consultante, las cuestiones planteadas por la misma con carácter general, sin poder analizar, con carácter exhaustivo, las concretas medidas planteadas, no correspondiendo a esta Agencia validar, con carácter previo, ningún tipo de tratamiento, debiendo ser los responsables del tratamiento los que velen por su adecuación a la normativa de protección de datos personales, sin perjuicio de los supuestos excepcionales en que proceda formular consulta previa y de los poderes de investigación que corresponden a la misma.

I

La primera cuestión que debe analizarse consiste en determinar si el sistema descrito en la consulta implica o no un tratamiento de datos de carácter personal, en el sentido previsto por 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 por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos -**RGPD**-), y por tanto si debe o no aplicarse la normativa indicada.

En primer lugar, debe tenerse en cuenta que el artículo 4.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, define los datos personales como “: *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*”.

A su vez, de acuerdo con el contenido de la “Definición” del punto 2 del propio artículo 4 del RGPD, para que exista tratamiento de datos de carácter personal, se requiere la realización de *“cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”*. Por su parte, la definición de “fichero” se contiene en el apartado 6 del artículo 4, que refiere a *“todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica”*.

Los apartados 1 y 2 del artículo 2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales -**LOPDPGDD**-, “Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94”, establecen que:

“1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. (...)”

Según se expone en la consulta, se trata de desplegar un sistema de escáneres en el interior de instalaciones y establecimientos -ya sea aprovechando la infraestructura Wi-Fi del propietario o implementando una nueva-, que detecte todas las señales que emiten los dispositivos electrónicos cuando tienen el Wi-Fi encendido -*WiFi tracking*-. Así, el hecho de conocer qué zonas provocan más interés en los clientes, a través de la localización por Wi-Fi, puede permitir la creación de nuevas estrategias de marketing o promociones a los clientes con el fin de mejorar su participación en el mercado y posicionar las marcas a nivel más competitivo.

Pues bien, las cuestiones planteadas ya han sido resueltas en informes anteriores de esta Agencia - **0310/2010** y **0060/2011**, ambos de 3 de junio de 2011, **0149/2014**, de 30 de julio de 2014, y **0175/2015**, de 3 de marzo de 2016-, y en dictámenes del Grupo de Trabajo de Autoridades de Protección de Datos, creado por el artículo 29 de la Directiva 95/46/CE.

Reiterando que el tema ha sido tratado por el Grupo de Trabajo de Autoridades de Protección de Datos, creado por el artículo 29 de la Directiva 95/46/CE, ha de partirse del Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio (documento WP 136), que recuerda que es

posible hablar de la existencia de datos personales incluso en supuestos en los que **no se cuenta con una identificación singularizada** del interesado, dado que:

“(…) conviene señalar que, si bien la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así puede suceder cuando se utilizan otros «identificadores» para singularizar a alguien. Efectivamente, los ficheros informatizados de datos personales suelen asignar un identificador único a las personas registradas para evitar toda confusión entre dos personas incluidas en el fichero. También en Internet, las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto. En otras palabras, la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos. La definición de datos personales refleja este hecho. (...) Las autoridades nacionales de protección de datos se han enfrentado a casos en los que el responsable del tratamiento sostenía que sólo se habían tratado informaciones dispersas, sin referencias a nombres u otros identificadores directos, y abogaba por que los datos no se considerasen como personales y no estuvieran sujetos a las normas de protección de los datos. Y, sin embargo, el tratamiento de esa información sólo cobraba sentido si permitía la identificación de individuos concretos y su tratamiento de una manera determinada. En estos casos, en los que la finalidad del tratamiento implica la identificación de personas, puede asumirse que el responsable del tratamiento o cualquier otra persona implicada tiene o puede tener medios que «puedan ser razonablemente utilizados», para identificar al interesado. De hecho, sostener que las personas físicas no son identificables, cuando la finalidad del tratamiento es precisamente identificarlos, sería una contradicción flagrante. Por lo tanto, debe considerarse que la información se refiere a personas físicas identificables y el tratamiento debe estar sujeto a las normas de protección de datos.”

Y en cuanto a la posibilidad de identificación del interesado, el documento además recuerda lo siguiente: *“Por otra parte, se trata de una prueba dinámica, por lo que debe tenerse en cuenta el grado de avance tecnológico en el momento del tratamiento y su posible desarrollo en el período durante el cual se tratarán los datos. Puede que la identificación no sea factible hoy con el conjunto de los medios que puedan ser razonablemente utilizados en la actualidad. Si lo previsto es que los datos se conserven durante un mes, puede que no sea factible adelantar la identificación para que esté terminada dentro del «período de vida» de la información y, por lo tanto, esa información no debe considerarse como datos personales. Ahora bien, si el período de conservación previsto es de diez años, el responsable del tratamiento debe*

barajar la posibilidad de que la identificación pueda producirse al cabo de nueve años, con lo que adquiriría en ese momento la categoría de datos personales. Es preciso que el sistema sea capaz de adaptarse a los progresos tecnológicos a medida que éstos se produzcan y que introduzca las medidas técnicas y organizativas apropiadas a su debido tiempo.”

Por último, en lo que respecta al tratamiento de la dirección IP dinámica asignada por el operador por parte de otras entidades, el documento también considera posible entender que la misma tiene la condición de dato personal, al señalar que:

“El Grupo de trabajo considera las direcciones IP como datos sobre una persona identificable. En ese sentido ha declarado que «los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva».

Especialmente en aquellos casos en los que el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que los «medios que pueden ser razonablemente utilizados» para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto la información debe considerarse como datos personales.”

Y más específicamente en relación con el asunto que nos ocupa, esta opinión se singulariza **en relación con los dispositivos de telefonía móvil que permiten la localización** del interesado en su Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes (documento WP185).

En dicho documento, tras recordar las conclusiones ya alcanzadas en su anterior Dictamen 5/2005 (WP115), de las que se desprende que *“debido a que los datos de localización que se obtienen de las estaciones base se refieren a una persona física identificada o identificable, estos están sujetos a las disposiciones relativas a la protección de los datos de carácter personal que se establecen en la Directiva 95/46/CE del 24 de octubre de 1995”*, concluye, en lo que afecta a la aplicación de la citada Directiva, lo siguiente:

“Conforme a la Directiva sobre protección de datos, se entiende por datos personales toda información sobre una persona física identificada o identificable (el “interesado”); se considerará identificable toda persona cuya

identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social - artículo 2 (a) de la Directiva.

El considerando 26 de la Directiva presta especial atención al término "identificable" cuando señala: "considerando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona."

El considerando 27 de la Directiva expone el amplio alcance de la protección: "considerando que el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de elusión;"

En su Dictamen 4/2007 sobre el concepto de datos personales, el Grupo de Trabajo ha facilitado una amplia orientación sobre la definición de datos personales.

Dispositivos móviles inteligentes

Los dispositivos móviles inteligentes están inextricablemente ligados a las personas físicas. Normalmente existe una identificabilidad directa e indirecta.

En primer lugar, los operadores de telecomunicaciones que proporcionan acceso a Internet móvil y a través de la red GSM poseen normalmente un registro con el nombre, la dirección y los datos bancarios de cada cliente, junto con varios números únicos del dispositivo, como el IMEI y el IMSI.

En segundo lugar, la compra de software adicional para el dispositivo (de aplicaciones o apps) suele requerir un número de tarjeta de crédito y de ahí que enriquezca la combinación del o de los números únicos y los datos de localización con datos directamente identificativos.

La identificabilidad indirecta puede lograrse mediante la combinación del o de los números únicos del dispositivo, junto con una o más ubicaciones calculadas.

Cada dispositivo móvil inteligente posee al menos un identificador único, la dirección MAC. El dispositivo puede tener otros números de identificación únicos, que puede añadir el desarrollador del sistema operativo. Estos identificadores pueden transmitirse y tratarse posteriormente en el contexto de los servicios de geolocalización. Es cierto que la ubicación de un dispositivo concreto puede calcularse de forma muy precisa, especialmente cuando se combinan las distintas infraestructuras de geolocalización. Dicha ubicación puede apuntar a una casa o a un empleador. Es posible, especialmente a través de las observaciones repetidas, identificar al propietario del dispositivo.

A la hora de considerar los medios disponibles para la identificabilidad, los avances deben tenerse en cuenta ya que las personas tienden a divulgar cada

vez más datos de localización personal en Internet, por ejemplo, publicando la ubicación de su casa o su trabajo junto con otros datos identificables. Este tipo de divulgaciones también puede darse sin su conocimiento, cuando otras personas les geoetiquetan. Gracias a este avance resulta más fácil vincular una ubicación o un patrón de comportamiento con una persona específica.

Además, conforme al Dictamen 4/2007 sobre el concepto de datos de carácter personal, debe señalarse que un identificador único, en el contexto descrito anteriormente, permite realizar un seguimiento de un usuario de un dispositivo específico y, por tanto, permite "singularizar" al usuario incluso aunque se desconozca su verdadero nombre."

Por consiguiente, la dirección MAC es un dato de carácter personal, debiendo su tratamiento estar sujeto a esta normativa. Y específicamente en cuanto a los datos de localización, así lo ha reiterado posteriormente el mismo Grupo del Art. 29 de la Directiva 1995/46/CE en su Dictamen 2/2013 sobre las aplicaciones de los dispositivos inteligentes; tanto en la introducción como entre los datos personales tratados por las aplicaciones que pueden incidir significativamente en la vida privada de los usuarios y otras personas se incluye la localización.

II

En el mismo sentido que el Grupo de Trabajo del Art. 29 de la Directiva 1995/46/CE, esta Agencia ya trató la cuestión en los dos **informes de 3 de junio de 2011**, a los que se ha hecho mención anterior, estudiando un sistema también basado en la geolocalización de clientes, y señaló que:

*"De todo lo anteriormente indicado parece desprenderse que el tratamiento conjunto de los datos relacionados con un terminal móvil, consistentes en el TMSI (que podría asimilarse con la dirección IP dinámica), **la dirección MAC y el código IMSI (que podría equipararse a una suerte de dirección MAC de la tarjeta SIM del usuario)**, implican la recopilación de información suficiente para que pueda entenderse que dicho tratamiento se encuentra sometido a lo dispuesto en la Directiva 95/46/CE y, por ende, en la Ley Orgánica 15/1999.
(...)*

En resumen, de lo señalado en la consulta no se deriva que la consultante, en mayor medida cuanto mayor sea su ámbito de actuación, podrá conocer los tres datos identificativos del terminal y de la tarjeta SIM del usuario, así como sus hábitos de consumo, de forma que si resultase posible la asociación del titular con información adicional que permitiese una mayor identificación, el tratamiento podría perjudicar las garantías de su derechos fundamental a la protección de datos de carácter personal.

De este modo, sólo sería posible evitar la aplicación de la legislación de protección de datos en caso de que se produjese una disociación absoluta de los datos de TMS, IMSI y dirección MAC del terminal del usuario y que dicha información no pudiera en ningún caso ser objeto de

conservación por parte de la consultante; es decir, que se produjese un procedimiento de anonimización tal que resultase irreversible a la consultante conocer qué datos se ocultan bajo el número aleatorio asignado.

En consecuencia, la atribución de tal número debería derivarse de la aplicación de un algoritmo que combinase los tres datos señalados y cuya aplicación resultase completamente irreversible, no conservándose por la consultante dato alguno de los enumerados en la consulta, aplicándose el algoritmo de forma inmediata en el momento de la recepción de la señal emitida por el terminal móvil.

Ciertamente en ese caso la consultante podría seguir teniendo información referente a hábitos de conducta del portador del terminal móvil, pero la misma no iría referenciada a datos que pudiesen permitir la identificación de tal usuario, sino a un dato derivado de la aplicación de un algoritmo irreversible, lo que permitiría considerar que en el supuesto planteado se habría aplicado efectivamente un procedimiento de disociación en los términos establecidos en el artículo 3 f) de la Ley Orgánica 15/1999, que define como tal “Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Dicho lo anterior, deberían igualmente preverse normas de seguridad que impidiesen el acceso a la información por personal ajeno a la consultante, lo que parece derivarse de lo indicado en la consulta y el acceso a la información únicamente de forma agregada, tal como se señala en la misma.

Asimismo, se considera adecuada la exigencia por la consultante a las entidades clientes de establecer dispositivos de información, que deberán ser claros y visibles (...).

En todo caso, se ha partido en la emisión del presente informe de la consideración de que los únicos datos captados y que, según las indicaciones que se han incluido, deberán ser objeto de un procedimiento de disociación irreversible en el momento de su captación son los mencionados en la consulta, sin que el sistema recoja dato alguno relacionado con el tráfico generado o recibido por el terminal que tuviera activado su dispositivo WiFi.”

Como también dijimos en informe de 29 de abril de 2010, “habida cuenta de que los datos de localización se refieren siempre a una persona física identificada o identificable, constituyen datos personales, por lo que su tratamiento está sujeto a las disposiciones contenidas en la Ley Orgánica 15/1999 y su normativa de desarrollo”.

Dicha conclusión resulta claramente extrapolable al escenario normativo actual, al amparo de las definiciones anteriormente transcritas, contenidas en el Reglamento General de Protección de Datos -**RGPD**- y en la Ley Orgánica 3/2018, de 5 de diciembre -**LOPDGDD**-.

A mayor abundamiento, según se expone en la consulta, la técnica utilizada para el tratamiento de datos es la seudonimización y cifrado de los datos que, según manifiestan, permitiría que los interesados no sean directamente identificables. De tal modo, la información obtenida y tratada por la consultante no se encontrará previamente anonimizada, esto es, absolutamente dissociada en relación la información de carácter personal de los afectados.

Es por ello por lo que, siguiendo el relato del expositivo de la propia consultante -y, en concreto, lo señalado en el apartado 4) de su escrito-, por dicha consultante se ha decidido “adoptar más medidas técnicas y organizativas para disminuir los riesgos de intromisión ilegítima en la privacidad”.

Pues bien, siguiendo la definición de “tratamiento de datos” del artículo 4 del RGPD, se extrae que *únicamente* cuando la información con datos de carácter personal se encuentre sometida previamente a un procedimiento de disociación, no resultará aplicable lo dispuesto en dicho Reglamento, decayendo sus previsiones en relación con la información “anonimizada” objeto de tratamiento. En resumen, la normativa de protección de datos no resultará aplicable a los tratamientos sometidos a un previo procedimiento de disociación, pero sí en el supuesto de que dicha disociación no concurra.

Así, en el Considerando (26) del RGPD se contiene la interpretación de lo que ha de entenderse por *información anonimizada*, delimitando claramente dicho concepto del relativo a la “seudonimización” de datos, a saber:

“(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.”

Contrario sensu, el Considerando (28) del RGPD, interpreta la aplicación efectiva de la normativa de protección de datos a los tratamientos de datos seudonimizados, al disponer que “La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.”

Atendiendo a lo que acabamos de indicar, para que un procedimiento de anonimización pueda ser considerado suficiente a los efectos del Reglamento (UE) 2016/679, de 27 de abril de 2016, será necesario que de la aplicación de dicho procedimiento resulte imposible identificar un determinado dato con su sujeto determinado. En este sentido, las disposiciones internacionales reguladoras de la protección de datos de carácter personal vienen a considerar que el afectado no será determinable cuando su identificación exija un esfuerzo desproporcionado que haga imposible, en la práctica, identificar a la persona física titular de los datos personales previamente tratados por el responsable.

No obstante lo anterior, conviene insistir en la distinción entre ambas figuras. Así, mientras a través de la disociación se impide la identificación del sujeto afectado, y se sitúa la información objeto de tratamiento fuera del ámbito de aplicación de la normativa de protección de datos, la seudonimización requiere la adopción de medidas técnicas y organizativas necesarias para garantizar que se aplique el RGPD al tratamiento correspondiente si bien mantiene por separado la información adicional para la atribución de los datos personales a una persona concreta (*ex Considerando 29 RGPD*), quedando en estos casos los tratamientos de datos sometidos al régimen del RGPD.

Nótese que, incluso debido a su propia naturaleza y encaje normativo -*ex 25.1, 32.1 a) del RGPD*-, la seudonimización constituye en sí misma una medida de seguridad de carácter técnico y organizativo, que implicaría la sustitución de un identificador unívoco por otro identificar unívoco, entre los cuales hay una relación biunívoca, lo que podría permitir el perfilado de personas físicas identificadas o identificables, especialmente si se combinan con los datos obtenidos por otras fuentes. Así lo recuerda el Considerando 30 del RGPD: “Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas”.

En este sentido, el Dictamen 05/2014 del Grupo del 29 sobre técnicas de anonimización, señalaba que “La seudonimización consiste en la sustitución

de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo” y que “El resultado de la seudonimización puede ser independiente del valor inicial (tal sería el caso de un número aleatorio generado por el responsable del tratamiento o de un apellido escogido por el interesado) o bien derivarse de los valores originales de un atributo o conjunto de atributos, como por ejemplo en el caso de funciones hash o sistemas de cifrado”. En concreto, en relación con la función hash, indica lo siguiente:

□ **Función hash:** Se trata de una función que devuelve un resultado de tamaño fijo a partir de un valor de entrada de cualquier tamaño (esta entrada puede estar formada por un solo atributo o por un conjunto de atributos). Esta función no es reversible, es decir, no existe el riesgo de revertir el resultado, como en el caso del cifrado. Sin embargo, si se conoce el rango de los valores de entrada de la función hash, se pueden pasar estos valores por la función a fin de obtener el valor real de un registro determinado. Por ejemplo, si se aplica la función hash al número de identificación nacional para seudonimizar un conjunto de datos, dicho atributo se puede obtener simplemente ejecutando la función con todos los posibles valores de entrada y comparando los resultados con los valores del conjunto de datos. Habitualmente, las funciones hash se diseñan para poder ejecutarse de manera relativamente rápida, por lo que están sujetas a ataques de fuerza bruta. También se pueden crear tablas precalculadas para lograr una reversión masiva de un gran número de valores hash.

El uso de una función hash «con sal» (en la que se añade un valor aleatorio, conocido como «sal», al atributo al que se aplica la función hash) puede reducir la probabilidad de obtener el valor de entrada. No obstante, usando medios razonables, todavía existe la posibilidad de calcular el valor original del atributo que se oculta tras el resultado de una función hash con sal.

De lo indicado en la consulta se extrae que los datos tratados por la entidad consultante se someterán a un proceso de seudonimización, y, sobre ellos, se adoptarán otra serie de medidas técnicas y organizativas, precisamente en consideración al carácter personal de la información obtenida y tratada, y en aras de la disminución de los riesgos de intromisión ilegítima en la privacidad. En consecuencia, dado que los datos personales seguirán identificando de algún modo a los afectados, resultarán claramente aplicables las normas reguladoras de la protección de datos de carácter personal en relación con la información objeto de tratamiento.

En conclusión, como queda expuesto, el Reglamento (UE) 2016/679, de 27 de abril de 2016, instituye la “seudonimización” como una medida de *carácter técnico y organizativo* que se incardina en el marco de la seguridad del

tratamiento (*ex artículo 32 RGPD*), que requiere, asimismo, del acompañamiento de otra serie de medidas técnicas y organizativas coadyuvantes, implementadas en beneficio de la privacidad y de la protección de los datos personales de los afectados.

En el **Punto VIII** de nuestro informe número **195/2017**, de 24 de julio de 2017, se refieren las diversas consecuencias derivadas de los supuestos de anonimización de los datos, y de simple seudonimización de la información objeto de tratamiento, señalando lo siguiente:

““En quinto lugar, la consulta se refiere a “la “anonimización” de datos transaccionales, obtenidos a través de los productos y/o servicios de la entidad bancaria, para desarrollar nuevos productos y/o servicios basados en datos anonimizados y agregados”. Se trata según se indica de analizar patrones de uso de los servicios para el desarrollo de otros nuevos (...).

Como punto de partida, sería preciso que se clarificasen los términos de la consulta en este punto, toda vez que, si bien se hace referencia a la agregación y al uso de datos anonimizados, también pudiera derivarse de la misma la generación de patrones a partir de estudios de carácter longitudinal sobre el uso de los servicios, lo que implicaría la imposibilidad material de llevar a cabo una anonimización de los datos en los términos previstos en el Reglamento general de protección de datos.

En este sentido, debe recordarse que el considerando 26 del Reglamento general de protección de datos indica lo siguiente:

“Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.”

Por su parte, añade el considerando 29 que “Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un

análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas”.

En definitiva, de lo establecido en el Reglamento General de protección de datos se desprende que, en cuanto el mismo resulte de aplicación y al menos desde que éste entre en vigor, tanto la anonimización como la seudonimización de los datos personales llevarán aparejada la existencia de dos tratamientos sucesivos: el que supone la propia anonimización o seudonimización a partir de los datos personales de que dispone el responsable y el que se lleve a cabo posteriormente con los datos ya anonimizados o seudonimizados. La diferencia entre ambos supuestos estribará en el hecho de que mientras la normativa de protección de datos no será de aplicación a este segundo tratamiento si los datos han sido anonimizados, sí resultará aplicable en caso de que se haya producido únicamente una seudonimización.

Y esta diferencia también incidirá en la ponderación exigida por el artículo 6.1 f) respecto del primer tratamiento llevado a cabo, dado que en caso de que la anonimización sea completa, siendo imposible la vinculación de la información de forma directa o indirecta con un determinado afectado, la afección del tratamiento a la esfera de derechos e intereses de aquél será sustancialmente menor que en el supuesto en que los datos sigan pudiendo identificarle al revertirse el procedimiento de seudonimización.

Incluso esta incidencia será aún menor en caso de que la anonimización implique desde su origen una agregación de los datos de carácter personal de un determinado universo de afectados, dado que, a partir de ese momento, si los mecanismos de agregación son los adecuados, sería imposible disgregar del dato agregado la información referida a un sujeto concreto.

Quiere ello decir que en el supuesto planteado si el resultado del tratamiento fuera efectivamente la obtención de datos anónimos o, incluso en mayor medida, si los datos resultantes son agregados, de forma que no quepa en los términos mencionados en el considerando 26 del Reglamento volver a asociar la información con un afectado concreto, la incidencia mínima que pudiera existir en el derecho de los afectados como consecuencia de la aplicación sobre sus datos de un procedimiento de anonimización o agregación podría ceder ante el interés legítimo que pudiera justificar el que ese tratamiento se lleve a cabo, que en los términos de la consulta sería el desarrollo por la entidad de nuevos productos o servicios. Por ello, en estos casos no cabe duda de que sería posible la aplicación al proceso de anonimización y agregación de la legitimación fundada en el artículo 6.1 f) del reglamento general de protección de datos.

En el supuesto en que se lleve realmente a cabo un procedimiento de seudonimización y no de anonimización la ponderación dependerá de las garantías que se establezcan para garantizar la irreversibilidad del proceso, de forma que, siguiendo con lo establecido en el propio Reglamento, cuanto

mayores y más fiables sean dichas garantías mayor será el peso en la ponderación del interés legítimo del responsable sobre los derechos e intereses de los afectados.

De este modo, a diferencia de los procesos de anonimización no es posible en los de seudonimización dar una respuesta terminante a la cuestión planteada, por cuanto la aplicabilidad del artículo 6.1 f) del Reglamento dependerá de las garantías que se adopten para preservar la irreversibilidad del procedimiento de seudonimización.

En todo caso, como se ha indicado para los supuestos anteriormente indicados, será preciso informar a los interesados acerca de los tratamientos que van a tener lugar y garantizar el adecuado ejercicio por aquéllos de su derecho de oposición, al operar éste, según el artículo 21 del reglamento, en los supuestos en que el tratamiento se funde en la regla del equilibrio de derechos e intereses prevista en el artículo 6.1 f) del reglamento.””

De acuerdo con el relato de la consultante, en el supuesto objeto de consulta se procederá a la adopción de una serie de medidas técnicas y organizativas cuyo principal objetivo será la reducción de la posible injerencia en relación con la privacidad y la protección de los datos de carácter personal, minimizando el posible impacto que, en otro caso, podría producirse sobre dichos derechos.

No obstante, tal y como se señalará posteriormente, se trata de medidas que no pueden valorarse en abstracto, ya que las medidas a adoptar deberán ajustarse a un riguroso análisis de los riesgos que el tratamiento implica para los derechos y libertades de los afectados, a través de los instrumentos previstos en el RGPD.

En este punto, hay que tener en cuenta los especiales riesgos que supone el tratamiento de los datos de localización, y respecto de los que el Grupo del 29 vino insistiendo desde su Dictamen 5/2005 sobre el uso de los datos de geolocalización con vista a prestar servicios con valor añadido, en el que ya señalaba que en los últimos años se ha producido un aumento espectacular del uso de los datos de localización, debido al “aumento exponencial en el uso de los datos de localización vía satélite, que en la actualidad pueden ser muy precisos y valiosos, especialmente por lo que se refiere a la asistencia a personas en apuros” y a “la difusión sin precedentes de la telefonía móvil, merced a la cual cada usuario lleva siempre un dispositivo mediante el cual se le puede localizar”.

Asimismo, en el ya citado Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes, en el que se aclara el marco jurídico aplicable a los servicios de geolocalización disponibles en dispositivos móviles inteligentes (o que son generados por éstos) que se pueden conectar a Internet y están equipados con sensores de localización

tales como el GPS, el Grupo del 29 destacaba que “En general, el valor de la información aumenta cuando está ligada a una localización y toda localización puede ligarse a cualquier tipo de información: datos financieros, de salud o sobre el comportamiento de los consumidores. Con el rápido desarrollo tecnológico y la amplia difusión de dispositivos móviles inteligentes, se está desarrollando una nueva categoría de servicios basados en la localización”.

Y en el Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos advertía sobre sus múltiples riesgos:

“De hecho, una IO no sometida a controles podría evolucionar hacia el desarrollo de una forma de vigilancia de las personas que cabría considerar ilegal en el marco del Derecho de la UE. La IO suscita también grandes inquietudes, pues los fallos de seguridad pueden conllevar importantes riesgos para la intimidad de las personas cuyos datos son objeto de tratamiento en estos contextos.

Por ejemplo, los objetos corporales que se mantienen muy cercanos al interesado hacen posible la disponibilidad de otros identificadores, como las direcciones MAC u otros dispositivos que podrían ser útiles para generar una huella digital que permita rastrear la localización del interesado. La recogida de múltiples direcciones MAC de múltiples sensores ayudará a crear huellas digitales únicas e identificadores más estables que las partes interesadas en la IO podrán atribuir a determinadas personas. Estos identificadores y huellas digitales se podrían usar para diferentes fines, incluido el análisis de la localización o el análisis de las pautas de movimiento de grupos y de personas.

Esta tendencia se debe conjugar con la posibilidad de combinar esos datos más adelante con otros procedentes de otros sistemas (por ejemplo, televisión en circuito cerrado o registros de Internet).

En tales circunstancias, algunos de los datos obtenidos mediante sensores resultan especialmente vulnerables a los ataques de reidentificación.

A la luz de lo anterior, está claro que permanecer en el anonimato y proteger la intimidad en la IO será cada vez más difícil. El desarrollo de la IO suscita grandes preocupaciones relacionadas con la protección de datos y de la intimidad en este contexto.”

En nuestros anteriores informes -**0310/2010** y **0060/2011**, ambos de 3 de junio de 2011, **0149/2014**, de 30 de julio de 2014, y **0175/2015**, de 3 de marzo de 2016-, se recuerda que el derecho a la protección de datos constituye un derecho fundamental, por lo que antes de adoptar una medida restrictiva del mismo, como lo es el tratamiento de datos a que se refiere la consulta, debe analizarse la proporcionalidad de dicha medida.

Actualmente, el artículo **5.1.c) del RGPD**, consagra el “principio de **minimización**” de datos, por lo que sólo están amparados los tratamientos de datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que dichos datos son tratados.

Cabe, a este respecto, traer a colación lo señalado por el Tribunal Constitucional en su Sentencia 186/2000 en la que declaraba que ningún derecho fundamental es absoluto *“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, FJ 6, y 143/1994, FJ 6, por todas).

De ello se desprende la necesidad de que el tratamiento de un determinado dato de carácter personal, en el presente caso los **datos de localización**, deba ser proporcionado a la finalidad que lo motiva. De este modo, si dicha finalidad pudiera conseguirse por la realización de una actividad distinta al citado tratamiento, sin que dicha finalidad fuese alterada o perjudicada, debería optarse por esa última actividad, dado que el tratamiento de los datos de carácter personal supone, tal y como consagra nuestro Tribunal Constitucional, en Sentencia 292/2000, de 30 de noviembre, una limitación del derecho de la persona a disponer de la información referida a sí misma.

De los términos en los que la consulta ha sido formulada únicamente podemos concluir que el tratamiento del **MAC** -como identificador único y permanente de un dispositivo- supone el tratamiento de un dato de carácter personal, debiendo por tanto ajustarse a esta normativa. Y debe recordarse, una vez más, que **el RGPD ha supuesto un cambio sustancial en la forma de abordar la garantía del derecho fundamental a la protección de datos personales, que gira en torno al principio de responsabilidad proactiva o accountability de modo que es el responsable el que, a través de los instrumentos regulados en el propio RGPD como el análisis de riesgos o la evaluación de impacto en la protección de datos personales y asistido, en su caso, por el delegado de protección de datos, debe garantizar la protección de dicho derecho, documentando adecuadamente todas las decisiones que adopte.**

Debe, por tanto, ser el responsable el que, tras un análisis detallado de la situación, en los términos que posteriormente se expondrán, deberá valorar y

garantizar el cumplimiento de la normativa de protección de datos de carácter personal y de los principios que rigen la misma, debiendo hacerse especial referencia en el presente caso a los **principios de “licitud, lealtad y transparencia”** del artículo 5.1.a), el de “limitación de la finalidad” del artículo 5.1.b), el de “**minimización**” de los datos del **art. 5.1.c) del RGPD**, el de “**limitación del plazo de conservación**” del artículo 5.1.e), así como el ya citado de **responsabilidad proactiva del artículo 5.2.**, **teniendo especialmente en cuenta, en el presente caso, la protección de datos desde el diseño y por defecto a que se refiere el artículo 25.**

No obstante, al objeto de determinar la aplicación de dicha normativa y las responsabilidades de los distintos sujetos intervinientes en el tratamiento, sería preciso determinar, con carácter previo, el papel que desarrolla cada uno de ellos y quién es el que determina los fines y los medios del tratamiento. A este respecto, el RGPD considera en el artículo 4 como «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; y como «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Con la información facilitada, no puede determinarse, a priori, si la consultante tendrá la consideración de responsable o encargado, ya que dependerá de la intervención que tenga en el tratamiento y cómo se articule su relación con los titulares de los centros en los que se instale el sistema de Wifi Tracking, al objeto de determinar si contribuye a la determinación de los fines y los medios o si se limita a tratar los datos siguiendo las instrucciones del responsable, sin destinarlos a fines propios o, incluso, si no realiza dichas funciones y se limita a desarrollar la tecnología necesaria para el tratamiento. Asimismo, se desconoce a su vez si puede haber otros intervinientes, como encargados o subencargados, que participen en el análisis de los datos o en su almacenamiento.

Del texto de la consulta, parece inferirse que es la consultante la que decide la forma en la que se va a realizar el tratamiento, instalando sus receptores directamente o aprovechando la red Wifi del establecimiento, y que es la que define el proceso de seudonimización, las redes de transmisión y el modelo de almacenamiento, procediendo directamente al análisis de los datos según criterios previamente definidos por ella, por lo que parece que ostentaría la consideración de responsable y no de mero encargado.

En todo caso, independientemente de la situación que ocupe cada uno de los intervinientes en el tratamiento, todos deberán velar por que el mismo se ajuste a la normativa de protección de datos personales, tal y como señala el Considerando 78 del RGPD:

La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

IV

Comenzando con la legitimación del tratamiento, la normativa de protección de datos contempla diferentes supuestos que pueden dar lugar al tratamiento de datos de carácter personal. En concreto, de acuerdo con el **artículo 6** –“Licitud del tratamiento”-, del **RGPD**, entre otros, dicho tratamiento es lícito y legítimo cuando:

“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

- a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
- b) 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;
- c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
- d) el tratamiento es necesario para proteger intereses vitales del

interesado o de otra persona física;

e) 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;

f) 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 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 públicas en el ejercicio de sus funciones.”

Por consiguiente, el tratamiento de los datos de localización requerirá estar basado en alguna de las bases recogidas en el citado precepto, lo que implica que, en el caso de que el responsable no haya obtenido el consentimiento de los afectados, debería valorar si concurre el supuesto de interés legítimo recogido en la letra f).

Partiendo de lo anterior, esta Agencia considera que, con carácter general, el tratamiento de los datos de localización requiere el consentimiento del afectado. Este es el criterio que sigue la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), tal y como recuerda el Grupo del 29 en el ya citado Dictamen 5/2005 sobre el uso de los datos de geolocalización: “dado que el tratamiento de estos datos es un asunto especialmente sensible por referirse a la cuestión esencial de la libre circulación de las personas de forma anónima, el legislador europeo, teniendo en cuenta las consideraciones de las autoridades europeas de protección de datos, ha adoptado normas específicas que establecen la obligación de recabar el consentimiento de los usuarios o abonados antes de proceder al tratamiento de los datos de localización necesarios para prestar un servicio con valor añadido y de informar a los usuarios o abonados de las condiciones de dicho tratamiento (Artículo 9 de la Directiva 2002/58/CE de 12 de julio de 2002)”.

Dicha obligación se recoge en la normativa nacional de transposición de la Directiva, en concreto, por el artículo 48.2.c) de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que dispone que:

“Respecto a la protección de datos personales y la privacidad en relación con los datos de tráfico y los datos de localización distintos de los datos de

tráfico, los usuarios finales de los servicios de comunicaciones electrónicas tendrán los siguientes derechos: c) A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado. Los usuarios finales dispondrán del derecho de retirar su consentimiento en cualquier momento y con efecto inmediato para el tratamiento de los datos de localización distintos de tráfico.”

En el presente caso, dicha Directiva no resulta de aplicación al tratamiento propuesto por la consultante, ya que en un caso idéntico la entonces Comisión Nacional de las Telecomunicaciones informó a esta Agencia que no se trataba de un servicio de comunicaciones electrónicas, tal y como se recoge en el Informe 60/2011 ya citado. En este sentido, el Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes ya señalaba que “La Directiva sobre la protección de la intimidad y las comunicaciones electrónicas (2002/58/CE, modificada por la Directiva 2009/136/CE) solo se aplica al tratamiento de datos de las estaciones de base por servicios y redes públicos de comunicación electrónica (operadores de telecomunicaciones)”.

No obstante, dada la intromisión que la geolocalización supone en el derecho fundamental a la protección de datos, esta Agencia considera que el consentimiento resulta igualmente exigible, con carácter general, al amparo del RGPD, siempre que el tratamiento vaya dirigido a la identificación, directa o indirecta, de la persona. Este es el mismo criterio que el Grupo del 29 entendió aplicable a los prestadores de servicios de la sociedad de la información en el citado Dictamen 13/2011, “Dada la sensibilidad del procesamiento de los datos o pautas de datos de localización, el *consentimiento fundamentado previo* constituye también el principal factor aplicable para dar legitimidad al tratamiento de datos en lo que se refiere al procesamiento de las localizaciones de un dispositivo móvil inteligente en el contexto de servicios de la sociedad de la información”.

V

En relación con el “interés legítimo” y su aplicación como base legitimadora de los tratamientos de datos de carácter personal, en el **Considerando (47)** del RGPD, se señala que:

“El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, **siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los**

interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. **En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin.** En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.”

De acuerdo con estas previsiones, corresponderá **a cada uno de los responsables de los tratamientos** de la señal recibida por los dispositivos de captación y análisis de señales Wi-Fi el análisis de la concurrencia del referido interés. A dichos efectos, correrá de cuenta de dichos responsables la acreditación de la prueba de “sopesamiento”, exigida en relación con la concurrencia de la base legitimadora del *“interés legítimo”*, dentro del marco del juicio de proporcionalidad inherente a la aplicación de dicha base jurídica del tratamiento de datos de carácter personal.

Asimismo, los responsables de los tratamientos –esto es, aquellos que instalen los dispositivos de captación y análisis de señales Wi-Fi en sus establecimientos- deberán garantizar el pleno respeto de los derechos de los afectados por los tratamientos, e implementar a dichos efectos las garantías necesarias en orden al cumplimiento de sus obligaciones en materia de protección de datos de carácter personal.

Según se expone en la consulta, la empresa tiene interés en conocer los *recorridos o tránsitos* que hacen los dispositivos móviles dentro del establecimiento para contabilizarlos, determinando la frecuencia de visita y los itinerarios recorridos por los dispositivos, al objeto de la realización de actividades de mercadotecnia.

En el **Dictamen 6/2014**, de 9 de abril, sobre el concepto de *interés legítimo* del responsable del tratamiento, del grupo de trabajo creado por el

artículo 29 de la Directiva 95/46/CE -WP 217-, se incorporan diversas directrices y orientaciones en orden a la concurrencia del “interés legítimo”, así como los elementos de salvaguarda necesarios en atención al respeto y garantía de los derechos de los afectados por este tipo de tratamientos.

En el marco de dichas garantías, destaca la exigencia de la “*prueba de sopesamiento*” entre el interés legítimo del responsable del tratamiento o cualesquiera terceros a los que se comuniquen los datos y los intereses o los derechos fundamentales del interesado.

El análisis inherente a la “*prueba de sopesamiento*” requiere la consideración completa de una serie de factores, con el fin de garantizar que se tienen en cuenta debidamente los intereses y los derechos fundamentales de los afectados. Al mismo tiempo, se trata de una prueba modulable, que puede variar desde sencilla hasta compleja. Los factores que deben considerarse cuando se efectúe dicha prueba de sopesamiento comprenderán:

- **La naturaleza y la fuente del interés legítimo**, y si el tratamiento de datos es necesario para el ejercicio de un derecho fundamental, resulta de interés público o se beneficia del reconocimiento de la comunidad afectada;
- La **repercusión para el interesado** y sus expectativas razonables sobre qué sucederá con sus datos, así como la naturaleza de los datos y la manera en la que sean tramitados;
- Las **garantías** adicionales que podrían limitar un impacto indebido sobre el **interesado**, tales como la **minimización** de los datos, las tecnologías de protección de la intimidad, el aumento de la transparencia, el **derecho general e incondicional de exclusión voluntaria** y la portabilidad de los datos.

Por consiguiente, solo en los casos en que, como resultado de la prueba de sopesamiento, no prevalezcan los intereses y los derechos fundamentales de los afectados, podrá llevarse a cabo el tratamiento sobre la base jurídica del artículo 6.1.f) del RGPD.

Por otro lado, una evaluación adecuada del equilibrio en virtud de la “*prueba de sopesamiento*” -en ocasiones, facilitando la posibilidad de exclusión voluntaria del tratamiento-, puede originar otras alternativas, o aconsejar el recurso a otras bases jurídicas sustentadas en el “consentimiento” o en la ejecución de un “contrato”.

Como colofón, en relación con la garantía de los derechos de los afectados, **el Dictamen 6/2014, de 9 de abril, se refiere específicamente al derecho de oposición**, señalando lo siguiente:

“¿Qué sucede si el interesado ejerce su derecho de oposición?

- Cuando únicamente se establece un derecho condicionado de exclusión voluntaria como garantía: en caso de que el interesado se oponga al tratamiento, deberá garantizarse que existe un mecanismo adecuado y fácil de usar para evaluar de nuevo el equilibrio respecto de la persona afectada e interrumpir el tratamiento de sus datos si esta nueva evaluación demuestra que sus intereses prevalecen.
- Cuando se establece un derecho incondicional de exclusión voluntaria como garantía adicional: en caso de que el interesado se oponga al tratamiento, deberá garantizarse que se respeta su decisión, sin que se deba realizar otra evaluación o adoptar otra medida.”

En este mismo sentido, el Supervisor Europeo de Protección de Datos, en su Opinion 7/2015, Meeting the challenges of big data, considera como una buena práctica para acudir al interés legítimo el dar la opción de op-out a los interesados:

“Especially in borderline cases where the balance between the legitimate interests of the controller and the rights and interests of the data subjects are difficult to strike, a well designed and workable mechanism for opt-out, while not necessarily providing data subjects with all the elements that would satisfy a valid consent under European data protection law, could play an important role in safeguarding the rights and interests of the individuals”.

Por otro lado, en el **Dictamen 6/2014**, de 9 de abril, sobre el concepto de *interés legítimo* del responsable del tratamiento, del Grupo del Artículo 29, también se hace referencia a las actividades de mercado como uno de los supuestos en que procedería considerar la posible concurrencia de un interés legítimo. Así, en su apartado ¿Qué convierte a un interés en legítimo o ilegítimo? se menciona este tipo de actividad a título de ejemplo sometido a consideración, a saber:

“Sirva como ejemplo: los responsables del tratamiento pueden tener un interés legítimo en conocer las *preferencias de sus clientes* de manera que esto les permita *personalizar mejor sus ofertas* y, en último término, *ofrecer productos y servicios* que respondan mejor a las necesidades y los deseos de sus clientes. A la luz de esto, el artículo 7, letra f), puede constituir un fundamento jurídico apropiado en algunos tipos de *actividades de mercado*, en línea y fuera de línea, siempre que se prevean las garantías adecuadas (incluido, entre otros, un mecanismo viable que permita oponerse al tratamiento en virtud del artículo 14, letra b), (...).

Sin embargo, esto no quiere decir que los responsables del tratamiento puedan remitirse al artículo 7, letra f), como fundamento jurídico para supervisar de manera indebida las actividades en línea y fuera de línea de sus clientes, combinar enormes cantidades de datos sobre ellos, provenientes de diferentes fuentes, que fueran inicialmente recopilados en otros contextos y con fines diferentes, y crear —y, por ejemplo, con la intermediación de corredores de datos, también comerciar con ellos— perfiles complejos de las personalidades y preferencias de los clientes sin su conocimiento, sin un mecanismo viable de oposición, por no mencionar la ausencia de un consentimiento informado. Es probable que dicha actividad de elaboración de perfiles represente una intrusión importante en la privacidad del cliente y, cuando esto suceda, los intereses y derechos del interesado prevalecerán sobre el interés del responsable del tratamiento.”

Tal y como queda expuesto, corresponderá a cada uno de los **responsables** que procedan al tratamiento de la señal de los dispositivos de captación de señales Wi-Fi, la valoración de la concurrencia del “interés legítimo” en relación con la implantación del sistema en sus establecimientos y la realización de la correspondiente *prueba de sopesamiento*.

De tal suerte, corresponderá a cada uno de dichos responsables -titulares de la actividad y/o de los establecimientos abiertos al público- la referida valoración, toda vez que la invocación del “interés legítimo” afectará a las personas físicas que accedan a sus locales de negocio en calidad de clientes o de potenciales clientes.

En el contexto descrito, resultará ineludible que, por parte de dichos responsables se proceda a la adopción de las garantías necesarias en orden a la prevalencia del tan citado “interés legítimo” frente a los derechos de los afectados, ya que, en otro caso, dicho tratamiento no será lícito.

En consecuencia, la realización de las actividades de mercadotecnia a las que se refiere el presente informe sobre la base de lo dispuesto en el artículo 6.1 f) del RGPD -interés legítimo-, y que daría lugar al tratamiento de los datos de localización de los terminales electrónicos con emisión de señal “WiFi tracking”, únicamente podría reputarse lícita si se implementara acompañada de las salvaguardas, garantías y medidas técnicas y organizativas, incluyendo las relativas a la seguridad de la información, que resultaren necesarias, yendo precedida -en todo caso- de la necesaria ponderación inherente a la concurrencia del “interés legítimo” de los responsables de los tratamientos en los términos expuestos en este informe, no correspondiendo a esta Agencia pronunciarse, a priori, sobre la licitud de la misma, que estará supeditada a la existencia e intensidad de dichas garantías.

No obstante, sí se pueden adelantar algunos criterios de carácter general que deberán tenerse en cuenta por los responsables, sin perjuicio de

aquellas medidas que el responsable tendrá que implementar en función de la gestión del riesgo para los derechos y libertades de los afectados en virtud de los análisis a los que nos referiremos posteriormente:

- Deben adoptarse medidas que garanticen la anonimización temprana de los datos.
- Deberá valorarse el ámbito en el que se realiza el *wifi tracking*, atendiendo especialmente a la existencia de una relación comercial, de modo que se trate de clientes o potenciales clientes, evitándose, en todo caso, su empleo en la vía pública.
- Deberán limitarse y acotarse las zonas en las que se realiza, evitándose un control de los movimientos en zonas muy amplias, así como en aquellas que puedan suponer una injerencia excesiva en la privacidad de la persona, como pudiera ser, por ejemplo, en el caso de los aseos.
- No podrán utilizarse, sin el consentimiento de los afectados, en aquellas zonas en que puedan revelar categorías especiales de datos, como por ejemplo, las que tengan productos relacionados con la salud.
- En ningún caso se podrán cruzar los datos de geolocalización así obtenidos con otros datos procedentes de otras fuentes (como, por ejemplo, los pagos con tarjeta de crédito o las imágenes captadas por los sistemas de videovigilancia) que puedan permitir la identificación de la persona.
- Atendiendo al criterio de minimización de datos, si bien la recogida de los datos de posición ha de ser continua, el almacenaje y posteriores operaciones de tratamiento de la posición ha de limitarse a señalar las áreas indicadas como de interés de mercadotecnia por el responsable, impidiendo una recogida detallada y continua de los movimientos de los interesados.
- No se deberá utilizar en el servidor para los datos recogidos de un interesado en los locales de distintos responsables. Si el responsable dispone de varios locales, también deberán recogerse distintos identificadores.
- No se deberá asignar el mismo identificador a un mismo interesado en las distintas visitas que en el tiempo realice el interesado al mismo local.
- No se condicionará el acceso a la WiFi del responsable al consentimiento en el tratamiento de datos del interesado.

- Se ha de permitir a los interesados ejercer la opción de opt-out a la recogida de sus datos.
- Deberá garantizarse que los interesados tienen pleno conocimiento de que se está procediendo al tratamiento de sus datos personales, así como de su derecho a oponerse, en los términos que se analizan en el siguiente apartado.

VI

A su vez, en el marco de la actividad de mercadotecnia a la que se refiere la consulta, deberá darse el debido cumplimiento a lo dispuesto en el RGPD en relación con la obligación de informar, y, en concreto en sus artículos 12 y 13, referidos, respectivamente, a “Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado (artículo 12)”, y a la “Información que deberá facilitarse cuando los datos personales se obtengan del interesado (artículo 13)”, estableciendo además un procedimiento sencillo para el ejercicio del derecho de oposición.

En primer lugar, el artículo 12.1 del RGPD establece que la información a facilitar al interesado deberá serlo “en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo”.

Por su parte, el artículo 13 en sus dos primeros apartados especifica el contenido de la citada información en los supuestos en que los datos sean recabados del afectado al que los mismos se refiere. Dicha información deberá incorporar:

- la identidad y los datos de contacto del responsable y, en su caso, de su representante;
- los datos de contacto del delegado de protección de datos, en su caso;
- los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- cuando el tratamiento se base en el artículo 6, apartado 1, letra los intereses legítimos del responsable o de un tercero;
- los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

- el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
- cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
- el derecho a presentar una reclamación ante una autoridad de control;
- si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

En similar sentido, conforme a lo dispuesto en el artículo **11 de la LOPDGDD**:

“Artículo 11 LOPDGDD. Transparencia e información al afectado.

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el **artículo 13 del Reglamento (UE) 2016/679** facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

- a) La identidad del responsable del tratamiento y de su representante, en su caso.
- b) La finalidad del tratamiento.

c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.”

Según señala en su escrito, la entidad consultante pretende optar por la utilización de los sistemas informativos recogidos en las recomendaciones del GT29, y comprendidos en sus **Directrices -WP260-** sobre transparencia en el Reglamento (UE) 2016/679, revisadas el 11 de abril de 2018, en las que se establecen una serie de medidas adecuadas, entre las que se señalan las siguientes:

“Otros tipos de medidas adecuadas

(...)

Tecnología inteligente sin pantalla/entorno de internet de las cosas, como por ejemplo análisis de localización por wifi: iconos, códigos QR, alertas de voz, detalles por escrito incluidas en instrucciones de configuración por escrito, vídeos integrados en instrucciones digitales de configuración, información por escrito sobre dispositivos inteligentes, mensajes por SMS o correo electrónico, paneles visibles con información, señalización pública o campañas públicas de información.”

Pues bien, la opción de la consultante por facilitar la información a través de los citados medios, siempre que a ellos se incorpore la totalidad de la información prevista en los transcritos artículos 12 y 13 del RGPD, y 11 de la LOPDGDD, adecuándola al entorno en que debe ofrecerse, y siempre que se garantice el adecuado conocimiento por parte de los afectados de que están siendo geolocalizados, debe reputarse conforme con la normativa de protección de datos. A dichos efectos, por parte de la consultante, deberá garantizarse, en todo caso, el acceso a una capa informativa adicional en la que se contengan la totalidad de los extremos a los que dicha información deba referirse.

Por otro lado, tal y como se adelantaba anteriormente y así lo ha señalado reiteradamente esta Agencia y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”.

Directamente relacionado con el principio de responsabilidad proactiva recogido en el artículo 5.2. del RGPD se encuentra el principio de protección de datos desde el diseño y por defecto que se recoge en el artículo 25 del RGPD:

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Para el adecuado cumplimiento de dicho principio, el RGPD contempla una serie de instrumentos que permiten a responsables y encargados valorar el riesgo que pueda implicar el tratamiento y adoptar las medidas que procedan.

En primer lugar, resulta necesario realizar el **análisis de riesgos** al que se refiere el artículo 24 del RGPD:

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Cuando, en virtud de dicho análisis, “sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una **evaluación del impacto de las operaciones de tratamiento en la protección de datos personales**”, en los términos previstos en el artículo 35 del RGPD.

En los supuestos en que la Evaluación de Impacto relativa a la Protección de Datos muestre que el tratamiento sigue teniendo un alto riesgo para los derechos y libertades de los interesados aún tras aplicar las garantías, medidas de seguridad y mecanismos de protección razonables en cuanto a técnica disponible y costes de aplicación, el responsable del tratamiento deberá formular la **consulta previa** a la que se refiere el artículo 36 del RGPD:

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no haya identificado o

mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

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

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.
(...)"

En este contexto normativo se inscribe el artículo **28 de la LOPDGDD**, cuando -bajo el título "*Obligaciones generales del responsable y encargado del tratamiento*", prevé que:

"1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. **En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.**

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.”

Asimismo, deberán tenerse en cuenta las “Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos” y la “Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos” publicados por la Agencia Española de Protección de Datos al amparo de lo previsto en el artículo 35.5 del RGPD.

En este punto, hay que tener en cuenta que, en principio, la obligación de realizar una EIPD recaería sobre el responsable, circunstancia que, en principio ostentaría la consultante, si bien no puede determinarse con seguridad al desconocerse como se articula la relación con los titulares de los establecimientos en que se instala y la forma en que se realiza, tal y como se adelantaba en otro apartado de este informe.

No obstante, entiende esta Agencia que dicha EIPD debería realizarse por la consultante, dado que ello resultaría más acorde con los principios de protección de datos desde el diseño y por defecto, ya que como establece el considerando 78 RGPD anteriormente citado, al “desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos.” En definitiva, se considera que la evolución de impacto en materia de protección de datos, si bien corresponde al responsable del tratamiento, debería ser aquí proporcionada a éste por el desarrollador de la aplicación, el cual en el desarrollo y diseño de dichos productos debería haberse asegurado de cumplir los principios de protección desde el diseño y por defecto. Ello se ve además reforzado por lo establecido en el artículo 28.3, letra f), RGPD, en cuanto que establece la obligación para el encargado del tratamiento de ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 RGPD (y la evaluación de impacto se contiene en el artículo 35), teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado. En el presente caso se considera que la totalidad de la información en cuanto al desarrollo del sistema de *wifi tracking* reside en la consultante, independientemente de que la misma ostente la condición de responsable del tratamiento.

En el presente caso, a la vista de los referidos preceptos, a juicio de esta Agencia, por parte del órgano consultante **deberá procederse a la realización de la correspondiente EIPD**, al incardinarse los pretendidos tratamientos en el marco de lo dispuesto en el artículo 28.2 d) y f) de la LOPDGDD.

Por otro lado, un papel fundamental dentro de este nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeñará el delegado de protección de datos (DPD), que el Reglamento General regula en sus artículos 37 a 39, señalando este último precepto sus funciones:

Artículo 39 -Funciones del delegado de protección de datos-

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

En consecuencia, **la entidad consultante** deberá contar con los servicios de un Delegado de Protección de Datos que la informe, asesore y supervise en materia de cumplimiento de la normativa de protección de datos personales y sirva de interlocutor con las autoridades de protección de datos,

siendo obligatoria su designación conforme a lo establecido en el artículo 34.k) de la LOPDGDD:

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

VIII

Para determinar que las medidas y garantías adoptadas para garantizar que el tratamiento es conforme con la normativa de protección de datos personales, el responsable ha de tener en cuenta, como establece el artículo 24 del RGPD el ámbito, el **contexto** y los fines del tratamiento y los **riesgos para los derechos y libertades** de las personas físicas, y a partir del análisis de riesgos y la EIPD, deberá adoptar todas las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento, incluidas las correspondientes medidas de seguridad.

En cuanto a estas últimas, el artículo 32 del RGPD no establece una lista cerrada de medidas de seguridad que el responsable y el encargado hayan de adoptar, de manera que, adoptándolas, habrían cumplido con sus obligaciones en materia de seguridad, sino que en virtud del principio de responsabilidad proactiva, establece que *“teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”, que en su caso incluya, entre otras:*

- “a) la seudonimización y el cifrado de datos personales;
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento”.

En consecuencia, corresponde **al responsable** del tratamiento y, en su caso, al **encargado**, asesorados, en su caso, por el DPD, determinar, dentro del marco de gestión del riesgo para los derechos y libertades establecido en el artículo 24, todas las medidas y garantías, incluidas las medidas de seguridad,

necesarias para el tratamiento de datos personales que se pretende realizar, no correspondiendo a esta Agencia pronunciarse sobre las mismas, salvo en el supuesto excepcional de que resulte necesario formular una consulta previa cuando la EIPD muestre un riesgo alto para los derechos y libertades de las personas tras haber aplicado medidas para mitigarlo, y sin perjuicio de los poderes de investigación que corresponden a la misma.