N/REF: 004813/2019

La consulta plantea la conformidad con la normativa de protección de datos del *proyecto* de investigación que se pretende desarrollar para proceder a la *anonimización* y posterior cifrado de datos procedentes de la captación pasiva de información de los parámetros de identificación móvil -*IMSI*-, en entorno de laboratorio.

Según se expone en la consulta, se trataría de conocer el número de transeúntes que recorren un determinado tramo de "El Camino de Santiago" en Navarra, mediante la captación de los códigos IMSI -*Identidad Internacional Abonado Móvil*- de sus terminales móviles. La consultante se serviría de sensores móviles de tecnología 2G para la captación de los *datos de tráfico* de usuarios de telefonía móvil, procesando dicha información y visualizando los datos inferidos. *El objeto principal* del proyecto es la implementación de un sistema de procesamiento de información que *garantice la inmediata "anonimización"* de los códigos IMSI tras la captura de estos.

La Universidad consultante acompaña a su escrito diversos textos, informes jurídicos, dictámenes, circulares y extractos de sentencias en relación con el asunto objeto del presente Informe, en los que se analiza el tratamiento del código *IMSI* y se obtienen las conclusiones que se incorporan a la consulta. Según se indica, la finalidad del proyecto sería la de la *"investigación científica"* regulada en el artículo 89 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 -**RGPD**-, concurriendo las circunstancias descritas en el artículo 35.3.c) de dicho Reglamento, al tratarse de un caso que conllevará la *"observación sistemática a gran escala de una zona de acceso público".*

I

Como cuestión previa, conviene referir que, si bien en su escrito de consulta la Universidad consultante se refiere a la captación de datos de *"tráfico"* de usuarios de telefonía móvil, de acuerdo con las definiciones de datos de tráfico y de localización, recogidas por el artículo 64 del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, debe entenderse que el tipo de datos sobre los que se interesa la emisión de Informe son los *"datos de localización",*

que indican la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público.

La cuestión fundamental planteada 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. (…)"

Por su parte, el artículo 64 b) del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, de 15 de abril, recoge la primitiva definición de datos de tráfico y de localización de la Directiva 2002/58/CE, señalando que son *"a) Datos de tráfico: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de su facturación. "b) Datos de localización: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público. (…)"*

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."

Es decir, con claridad meridiana resulta que 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 hábito 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**-.

III

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.

Según se expone en *la consulta*, la información obtenida y tratada por la consultante no se encontrará previamente anonimizada, esto es, no se encontrará absolutamente disociada en relación la información de carácter personal de los afectados.

Es por ello por lo que se implementará la completa disociación de la información con datos de carácter personal, y su posterior cifrado, poniendo en marcha *"pruebas de carga de laboratorio"* a dicho fin, mediante el uso de *scripts* que realicen tareas de captura de información, procesamiento, *anonimización, cifrado y posterior borrado* de manera secuencial y autónoma. En este sentido, la entidad consultante pretende disminuir los riesgos de intromisión ilegítima en la privacidad.

De acuerdo con el expositivo de la consulta y con el propio *"Título de proyecto",* este se dirige a la *"Investigación en un entorno de laboratorio para anonimizar y cifrar datos IMSI procedentes de sensores móviles pasivos";* así, el principal objeto del proyecto que se analiza lo *constituye -precisamente- la consecución de la inmediata anonimización* de los códigos IMSI captados, a cuyos efectos se desarrollaran experimentos en laboratorio destinados a demostrar la viabilidad de dicha opción.

De tal modo, el proyecto de investigación de que se trata tiene como objetivo la implementación de un sistema de procesamiento de información con *el fin de proceder a la anonimización y cifrado* posterior de los datos obtenidos de un sistema de captación pasiva de información -parámetro de identificación móvil IMSI-.

Según se señala en la consulta, el sistema propuesto considerará los siguientes aspectos:

- *"Tiene como variable de entrada un valor de IMSI captado en entorno de laboratorio, y con rango de cobertura limitado exclusivamente al laboratorio, que se procesará con el fin de convertirlo en un dato anonimizado. Para ello se empleará un generador de secuencia pseudo-aleatoria, con semilla basada en el dato de captura inicial de IMSI. A partir de dicho momento, dicho dato será descartado y borrado de la memoria.*

- *Una vez generada dicha secuencia pseudo-aleatoria, se cifrará empleando mecanismos testeados, como LINUX n-GPG, con el fin de poder ser transmitidos por la red de comunicaciones hacia un servidor remoto.*

- *Tras dicha transmisión del dato anonimizado y cifrado, se procederá al borrado secuencial de todos los datos en los nodos locales de manera inmediata."*

IV

En relación con la ***investigación científica***, los Considerandos (156) y (159) del RGPD disponen lo siguiente:

"(156) El tratamiento de datos personales con fines de archivo en interés público, *fines de investigación científica* o histórica o fines estadísticos debe estar supeditado a unas *garantías adecuadas para los derechos y libertades* del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican *medidas técnicas y organizativas* para que se observe, en particular, el *principio de minimización* de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que los Estados miembros establezcan, bajo *condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición*, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los *interesados ejerzan dichos derechos* si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos."

"(159) El presente Reglamento también debe aplicarse al tratamiento datos personales que se realice con *fines de investigación científica*. El tratamiento de datos personales con fines de investigación científica *debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada* y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben *aplicarse condiciones específicas*, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas."

Por su parte, bajo el título, *"Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos",* el artículo **89** del propio RGPD, establece que:

"1. El tratamiento con fines de archivo en interés público, *fines de investigación científica* o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de *medidas técnicas y organizativas*, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos

contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.
(…)"

A su vez, dentro de las ***excepciones y limitaciones*** derivadas de los tratamientos con fines de *investigación científica* o histórica, además de las correspondientes a los ejercicios de los derechos a los que se refiere el artículo 89, el Reglamento contiene otras relativas a los principios de limitación de la finalidad y limitación del plazo de conservación (artículo 5.1.b y e), al tratamiento de categorías especiales de datos (artículo 9.2.j), al deber de información (artículo 14.5.b), al derecho al olvido (artículo 17.3.d), al derecho de oposición (artículo 21.6).

En lo que se refiere al sentido que debe darse *al término "científico"*, finalidad en la que podría enmarcarse el proyecto objeto de la presente consulta, esta Agencia, en anteriores informes recordaba que la investigación científica y técnica, en el ámbito público, se encontraba regulada por la ahora ***derogada*** *Ley 13/1986*, de 14 de abril, de Fomento y Coordinación General de la Investigación, objetivo para el cual aquélla establecía el Plan Nacional de Investigación Científica y Desarrollo Tecnológico, pudiendo atribuirse la calificación de "científico" a aquellos proyectos insertos en el citado Plan.

Actualmente, la ***Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación***, desarrolla el título competencial contenido en el artículo 149. 1. 15ª de la Constitución Española e incorpora normas relativas a otros ámbitos de competencias de la Administración General del Estado. Se considera el *concepto de investigación científica y técnica* como equivalente al de investigación y desarrollo, entendido como el *trabajo creativo realizado de forma sistemática para incrementar el volumen de conocimientos, incluidos los relativos al ser humano, la cultura y la sociedad, el uso de esos conocimientos para crear nuevas aplicaciones, su transferencia y su divulgación*.

La ley tiene en cuenta la pluralidad de agentes que conforman hoy día el sistema. Junto a las *Universidades*, Organismos Públicos de Investigación, Centros Sanitarios y Empresas, responsables de la mayor parte de la actividad investigadora, en la actualidad tienen un papel muy destacado otros agentes como los centros de investigación adscritos a las Comunidades Autónomas, a la Administración General del Estado o a ambas, como son los Centros Tecnológicos, los Parques Científicos y Tecnológicos y las Instalaciones Científico-Técnicas Singulares.

Destacan entre los agentes las ***Universidades*** y los Organismos Públicos de Investigación; a todos ellos les es aplicable la gran mayoría de las normas contenidas en dicha ley.

El título II de dicha norma se centra en los recursos humanos dedicados a la investigación en Universidades públicas, Organismos Públicos de Investigación de la Administración General del Estado y Organismos de investigación de otras Administraciones Públicas. La sección 1ª -*Personal Investigador al servicio de las Universidades públicas, de los Organismos Públicos de Investigación y de los Organismos de investigación de otras Administraciones Públicas*- de su capítulo I, regula las disposiciones generales aplicables a todo el personal investigador de su ámbito de actuación, a saber:

> **"Artículo 12.** *Ámbito de aplicación.*
>
> Las disposiciones de esta sección serán de aplicación al personal investigador que preste sus servicios en las *Universidades públicas*, en los Organismos Públicos de Investigación de la Administración General del Estado y en los Organismos de investigación de otras Administraciones Públicas, salvadas las competencias que en dichos ámbitos tengan las Comunidades Autónomas y lo establecido por el resto de la legislación aplicable.
>
> **Artículo 13.** *Personal investigador.*
>
> 1. A los efectos de esta ley, se considera *personal investigador* el que, estando en posesión de la titulación exigida en cada caso, lleva a cabo una actividad investigadora, entendida como el trabajo creativo realizado de forma sistemática para incrementar el volumen de conocimientos, incluidos los relativos al ser humano, la cultura y la sociedad, el uso de esos conocimientos para crear nuevas aplicaciones, su transferencia y su divulgación. (el subrayado es nuestro)
>
> Será considerado personal investigador el personal docente e investigador definido en la ***Ley Orgánica 6/2001, de 21 de diciembre, de Universidades***, entre cuyas funciones se encuentre la de llevar a cabo actividades investigadoras. (la negrita es nuestra)
>
> 2. El personal investigador podrá estar vinculado con la Universidad pública u Organismo para el que preste servicios mediante una relación sujeta al derecho administrativo o al derecho laboral, y podrá ser funcionario de carrera, funcionario interino o personal laboral fijo o temporal, de acuerdo con el artículo 8 de la ***Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.*** (la negrita es nuestra)
>
> 3. El personal investigador funcionario se regirá por lo dispuesto en la Ley 7/2007, de 12 de abril, por lo dispuesto en esta ley, y

supletoriamente por la normativa de desarrollo de función pública que le sea de aplicación.

4. El personal investigador de carácter laboral se regirá por lo dispuesto en esta ley, en el Texto Refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 1/1995, de 24 de marzo, y sus normas de desarrollo, y en las normas convencionales. Asimismo, se regirá por los preceptos de la Ley 7/2007, de 12 de abril, que le sean de aplicación.

5. No obstante, el personal investigador al servicio de las Universidades públicas se regirá por lo dispuesto en la Ley Orgánica 6/2001, de 21 de diciembre, y su normativa de desarrollo, en el real decreto que apruebe el estatuto del personal docente e investigador universitario, en los estatutos de las Universidades, en las disposiciones que dicten las Comunidades Autónomas en virtud de sus competencias, en la Ley 7/2007, de 12 de abril, en el Real Decreto Legislativo 1/1995."

Por consiguiente, para considerar que el tratamiento de los datos a que la consulta se refiere pueda considerarse legitimado en una finalidad científica será preciso que a la investigación de que se trata pueda atribuírsele la *calificación de "científica",* respondiendo a la definición de *"actividad investigadora"* del artículo 13 de la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, y encontrándose *enmarcada en alguno de los planes de investigación científica y técnica* a que se refiere dicha norma.

En consecuencia, a los efectos de la consideración de la finalidad *"científica"* de la investigación, deberá procederse al análisis previo de si la misma responde a los referidos requisitos, encontrándose incluida en los planes de investigación científica o técnica a que se refiere la Ley 14/2011, de 1 de junio, y correspondiendo a una "actividad investigadora" a la que pueda atribuirse el cariz de científica.

Asimismo, para la determinación de los *fines "científicos"* a los que se refiere la consulta planteada desde el ámbito de actuación una ***Universidad pública***, habrá de estar a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la *Ley 14/2011*, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, y sus respectivas disposiciones de desarrollo, así como a la normativa específica sobre Universidades -*ex Ley Orgánica 6/2001, de 21 de diciembre, de Universidades*-, y a la normativa autonómica sobre estas materias.

En el artículo 32 de los **Estatutos** de la Universidad Pública de Navarra, aprobados mediante Decreto Foral 110/2003, de 12 de mayo, y modificados mediante Acuerdo del Gobierno de Navarra, de 21 de marzo de 2011, se dispone que son competencias del Consejo de Departamento, entre otras:

> "(…)
> b) Aprobar el informe anual de actividades docentes e investigadoras del Departamento, **establecer los planes de docencia e investigación**, y proponer los programas de doctorado. (la negrita es nuestra)
> c) Aprobar el Plan Estratégico del Departamento y sus modificaciones.
> d) Fomentar y favorecer la labor investigadora de los integrantes del Departamento.
> e) Aprobar el Plan de Ordenación Docente.
> (…)"

En el Capítulo III del TÍTULO III de dichos Estatutos -artículos 66 al 70-, bajo el título *"Investigación y Transferencia del conocimiento",* se concreta la regulación de la actividad investigadora en el marco de la Universidad consultante, disponiendo su **artículo 69** que son funciones de la Comisión de Investigación:

> "a) Proponer las directrices referidas a la política de investigación, transferencia de conocimiento y divulgación científica en el marco del plan estratégico.
> b) Proponer **programas propios de fomento de la investigación** que impulsen actividades investigadoras del personal. (la negrita es nuestra)
> c) Proponer la convocatoria y adjudicación subsiguientes de ayudas y becas de investigación.
> d) Realizar y encargar, a petición del Consejo de Gobierno o del Vicerrectorado de Investigación, actividades de seguimiento y evaluación de la actividad investigadora de grupos e investigadores de la Universidad.
> e) Proponer el establecimiento y concesión de premios y distinciones para reconocer la actividad investigadora.
> f) Proponer la normativa sobre reconocimiento de Grupos de Investigación.
> g) Informar sobre la creación de Centros o Institutos de Investigación.
> h) Asesorar al Consejo de Gobierno, Departamento, Centros e Institutos Universitarios en materia de planificación, coordinación, propuestas de estímulo y control del desarrollo de la investigación.
> i) Asesorar sobre publicaciones científicas propias de la Universidad y otros materiales de difusión y divulgación.
> j) Asesorar sobre la adquisición y utilización de la infraestructura universitaria de apoyo a la investigación.

k) Realizar el seguimiento y la evaluación de los efectos de los instrumentos de fomento a la investigación de la Universidad.
l) Elaborar su reglamento de régimen interno.
m) Cualquier otra que le atribuyan los Estatutos o el Consejo de Gobierno."

En este sentido, de la documentación acompañada a la consulta no se infiere con la certeza necesaria la concurrencia de los referidos requisitos que, en su caso, justificarían la consideración del proyecto de que se trata como proyecto de investigación científica, al no quedar debidamente acreditado que el estudio que se propone se encuentre enmarcado en alguno de los planes y/o programas de investigación científica y técnica a que se refieren los preceptos transcritos.

En consecuencia, deberá acreditarse la concurrencia de los requisitos que justifican la aplicación de lo dispuesto en el artículo 89 del RGPD, en relación con sus Considerandos (156) y (159).

V

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 identificación móvil -*IMSI*-, 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 como pilares básicos de la misma debemos destacar que, además de ajustarse en todo caso al principio de "minimización" de los datos del **art. 5.1.c) del RGPD**, todo tratamiento deberá **estar legitimado** en una de las causas del **art. 6** del propio RGPD.

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."

Según se expone en la consulta, la consultante tiene interés en conocer el número de transeúntes que recorren un determinado tramo de un área y/o recinto, mediante la captación de los códigos IMSI -*Identidad Internacional Abonado Móvil*- de los dispositivos móviles para contabilizarlos.

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-, también se hace referencia a la ***investigación científica*** como uno de los supuestos en que procedería considerar la posible concurrencia de un interés legítimo.

Así, en su apartado *"El concepto de interés",* señala:

"La naturaleza del interés puede variar. Algunos intereses pueden ser apremiantes y beneficiosos para la sociedad en general, tales como el interés de la prensa en publicar información sobre la corrupción gubernamental o el interés en llevar a cabo investigación científica (sujetos a las garantías adecuadas). Otros intereses pueden ser menos apremiantes para la sociedad en su conjunto o, en cualquier caso, el impacto de su búsqueda en la sociedad puede ser más dispar o controvertido. Esto puede, por ejemplo, aplicarse al interés económico de una empresa en aprender tanto como sea posible sobre sus potenciales clientes con el fin de orientar mejor la publicidad sobre sus productos y servicios."

En su apartado, *"Interés legítimo de terceros",* recoge que:

"Investigación histórica u otro tipo de investigación científica. Otro contexto importante en el que la revelación en el interés legítimo de terceros puede ser pertinente es la investigación histórica u otros tipos de investigación científica, especialmente cuando se requiere el acceso a determinadas bases de datos. La Directiva prevé el reconocimiento específico de dichas actividades, sujetas a las garantías y medidas adecuadas, pero no debe olvidarse que el fundamento

jurídico de estas actividades será con frecuencia un uso bien evaluado del artículo 7, letra f).”

A modo de supuestos práctico para ilustrar sobre la aplicación de la prueba de *sopesamiento,* exigida en relación con la concurrencia de la base legitimadora del *“interés legítimo*”, el mencionado Dictamen 6/2014, de 9 de abril, en sus ejemplos 19 -Investigación sobre los efectos del divorcio y el desempleo de los padres en el nivel educativo de los niños-, y 20 -Estudio de investigación sobre la obesidad-, se refiere con amplitud a la *“Investigación científica”.*

En este contexto, el desarrollo del proyecto al que se refiere el presente informe, que daría lugar a la captación y tratamiento de los datos de localización de los códigos IMSI -*Identidad Internacional Abonado Móvil*- de sus terminales móviles con los fines “científicos”, sobre la base de lo dispuesto en el artículo **6.1 f) del RGPD -interés legítimo-**, únicamente podría reputarse lícito y conforme con la normativa de protección de datos, si se implementara acompañado de las *salvaguardas, garantías y medidas de seguridad técnicas y organizativas* que resultaren necesarias.

Tal y como queda expuesto, en relación con dichas medidas a adoptar, el sistema propuesto por la consultante considera el empleo de “*un generador de secuencia pseudo-aleatoria, con semilla basada en el dato de captura inicial de IMSI”,* la generación de una *“secuencia pseudo-aleatoria, (que) se cifrará empleando mecanismos testeados, como LINUX n-GPG, con el fin de poder ser transmitidos por la red de comunicaciones hacia un servidor remoto”,* y el cifrado y anonimización del dato tras su transmisión, procediéndose *“al borrado secuencial de todos los datos en los nodos locales de manera inmediata.”*

Sin embargo, no consta la efectiva adopción de medidas cuyo principal objetivo sea la reducción de la ***injerencia en relación con la privacidad y la protección de los datos*** de carácter personal -minimizando el posible impacto que podría producirse sobre dichos derechos-, máxime considerando que los datos obtenidos no serán objeto de un previo procedimiento de disociación, y resultando las medidas anunciadas por la Universidad consultante claramente insuficientes.

La efectiva aplicación de las medidas de cumplimiento y salvaguarda del derecho a la protección de datos que prevé el RGPD para responsables y encargados, se hace depender directamente *del nivel y tipo de riesgo* que cada tratamiento implique para los derechos y libertades de los afectados *-ex artículo 24 RGPD-.* Por ello, el tratamiento de la información de carácter personal a la que se refiere el presente informe deberá ir precedida de dicho *“análisis de riesgos”,* directamente vinculado al debido cumplimiento de las disposiciones del propio RGPD. A saber:

“Artículo 24. Responsabilidad del responsable del tratamiento

> 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. (…)"

De tal modo, la finalidad principal del *"análisis de riesgos"* exigido por el RGPD, se concreta en la adopción por los responsables del tratamiento de medidas de control adecuadas para demostrar que se garantizan los derechos y libertades de las personas y la seguridad de los datos, teniendo en cuenta entre otros, los *"riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas"* y aplicando las medidas oportunas. Para ello, el responsable del tratamiento debe considerar las acciones preventivas suficientes para poder identificar, evaluar y tratar los riesgos asociados al tratamiento de datos personales, y así poder asegurar los principios de protección de los datos, garantizando los derechos y libertades de los interesados.

Según se señala en la consulta, el objetivo del proyecto es el diseño, despliegue, captura de datos y procesamiento de la información recogida mediante sensores móviles de tecnología 2G sobre los visitantes que recorren el Camino de Santiago, en una ruta que comprende 147 kilómetros. En dicha ruta, se escogerían cuatro ubicaciones en las que se instalarían los nodos de captura de datos, procesando el tiempo de estancia de los usuarios de móviles en la zona de cobertura, los patrones de flujos de usuarios y la correlación de patrones de nacionalidad, para su procesamiento en una plataforma. Asimismo, se prevé el procesamiento de datos relativos al comportamiento de los usuarios afectados.

A la vista del referido objetivo, resulta evidente que el tratamiento de información con datos de carácter personal se realizaría a *gran escala, de manera sistemática y masiva*, y generando un gran volumen de datos referidos a un ámbito espacial de gran amplitud, susceptible de *tránsito masivo de personas físicas*, que se verían afectadas por dicho tratamiento.

En conclusión -en aras de la reducción del impacto sobre la privacidad de los afectados por los tratamientos-, por parte de la Universidad consultante deberá realizarse el correspondiente análisis de riesgos para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que pretende desarrollar.

A su vez, en supuestos como el sometido a consulta, de las conclusiones del análisis de riesgos derivará la necesaria reflexión sobre la obligación de realizar una "Evaluación de Impacto relativa a la protección de

datos" *-ex artículo 35 RGPD-,* en los términos que se expondrán en el presente informe, y, en su caso, la formulación de una "consulta previa" a la autoridad de control *-ex 36 RGPD-.*

En definitiva, la superación del juicio de proporcionalidad exigible para la aplicación del artículo 6.1 f) del RGPD, se vincula a la adopción de medidas técnicas y organizativas suficientes para la garantía y protección de los datos personales de los afectados, que deberán ir precedidas -en todo caso- del correspondiente "análisis de riesgo" de los tratamientos de datos que pretenden realizarse.

VI

Por otra parte, también en el marco de la investigación científica a la que se refiere la consulta, debe 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 automatizas, 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 se ha señalado, el objetivo del proyecto es el diseño, despliegue, captura de datos y procesamiento de la información recogida mediante sensores móviles de tecnología 2G sobre los visitantes que recorren el Camino de Santiago, en una ruta que comprende 147 kilómetros. En dicha ruta, se escogerían cuatro ubicaciones en las que se instalarían los nodos de captura de datos, procesando el tiempo de estancia de los usuarios de móviles en la zona de cobertura, los patrones de flujos de usuarios y la correlación de patrones de nacionalidad, para su procesamiento en una plataforma. Asimismo, se prevé el procesamiento de datos relativos al comportamiento de los usuarios afectados.

A la vista del referido objetivo, resulta evidente que el tratamiento de información con datos de carácter personal se realizaría a *gran escala, de manera sistemática y masiva*, y generando un gran volumen de datos referidos a un ámbito espacial de gran amplitud, susceptible de *tránsito masivo de personas físicas*, que se verían afectadas por dicho tratamiento.

Sin embargo, en su escrito de consulta, por parte de la Universidad consultante no se indican los medios a través de los cuales se facilitará a los afectados la información relativa al tratamiento de sus datos, y que deberá incorporar 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-,

En conclusión, a la vista de la información ofrecida por la consultante en su escrito de consulta, y careciendo esta Agencia de otros elementos de juicio que el expositivo y fundamentación de la consulta, la realización de las actividades a las que se refiere el presente informe no puede reputarse legítima, al no garantizarse *la obligación de informar* a los afectados por los tratamientos en la forma prevista en los transcritos artículos 12 y 13 del RGPD, y 11 de la LOPDGDD.

Asimismo, en lo relativo al ejercicio del *derecho de oposición* se obtienen idénticas conclusiones, al no constar que por parte de la Universidad consultante se ofrezcan las adecuadas garantías para su consideración y ejercicio.

Baste recordar aquí que, de acuerdo con el artículo 21 RGPD, el interesado tiene derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que determinados datos personales que le conciernan sean objeto de un tratamiento basado en:

> "(…) 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".

En esta misma línea, el Considerando (59) del RGPD, señala que "*Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición."*

En conclusión, en el supuesto analizado, del examen de la documentación aportada no se infiere que se garantice el efectivo ejercicio por parte de los afectados de su derecho "oposición" al tratamiento de sus datos de carácter personal.

VII

Finalmente, debe recordarse que el **RGPD** incorpora entre sus principios el denominado principio de **responsabilidad proactiva**, debiendo ser los responsables de los tratamientos quienes adopten todas las medidas necesarias para dar cumplimiento a las obligaciones impuestas por la normativa de protección de datos, con algunas excepciones en que se prevé la intervención de las autoridades nacionales de control.

El principio de responsabilidad proactiva se establece en el **artículo 5** del RGPD, en el que se define el conjunto de principios que se ha de aplicar para la protección efectiva de los datos personales. Tal y como se ha adelantado anteriormente en este Informe, el apartado 2 se establece que la responsabilidad proactiva es una de las obligaciones del responsable del tratamiento en relación con los principios establecidos en el apartado 1 del mismo artículo. Por lo tanto, es una de las nuevas obligaciones que se establecen en el RGPD para asegurar el cumplimiento de dichos principios y

que consiste en la capacidad del responsable, de demostrar y proporcionar evidencias de dicho cumplimiento. A saber:

> "Artículo 5. Principios relativos al tratamiento
>
> 1. Los datos personales serán:
>
> a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);
> b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);
> c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);
> d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);
> e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);
> f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»). 2.El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).”

En cualquier caso, los arts. 32 y siguientes del RGPD -al determinar la seguridad del tratamiento de los datos personales-, no establecen una lista cerrada de medidas de seguridad que el responsable haya de adoptar, de manera que, adoptándolas, habría cumplido con sus obligaciones en materia de seguridad, sino que en virtud del principio de responsabilidad proactiva, establece que el responsable del tratamiento *“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 determinar las medidas de seguridad necesarias para el tratamiento de datos personales que ser pretende realizar, y ello ha de incluir una **reflexión sobre la necesidad de realizar una evaluación de impacto** relativa a la protección de datos, habida cuenta de lo dispuesto en art. 35 del RGPD.

“Artículo 35. Evaluación de impacto relativa a la protección de datos

1. Cuando 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. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el **asesoramiento del delegado** de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.”

En los Considerandos (84), (89), (90), (92), (92) y (94) del RGPD se contienen la interpretación auténtica y un conjunto de orientaciones sobre la necesidad de realizar evaluación de impacto en los supuestos referidos en el transcrito artículo 35.

Un informe de evaluación de impacto de protección de datos -**EIPD**- debe contener la identificación del responsable del tratamiento, de la unidad responsable en la organización, la descripción de las unidades gestoras de los

datos que intervienen en alguna de las fases del tratamiento, y la determinación -en su caso- de los encargados y subencargados del tratamiento. A su vez, debe incluir una breve descripción del tratamiento, su finalidad, las principales categorías de datos y la forma planeada para su implementación.

Asimismo, en dicho informe se deben destacar los factores de riesgo que motivan la realización de la EIPD y, en caso de no ser necesaria la EIPD, una exposición de los motivos por los que el responsable decide llevar a cabo la EIPD.

Finalmente, incluirá una breve descripción sobre el contexto de la EIPD como la metodología utilizada, la extensión y límites de la EIPD, los principales riesgos de privacidad identificados, los beneficios del tratamiento, las soluciones de gestión y técnicas planeadas, el análisis coste-beneficio y las conclusiones derivadas del riesgo residual y, en particular, la necesidad de realizar o no realizar una ***consulta previa*** a la AEPD.

En relación con la necesidad de realizar dicha ***consulta previa***, el artículo 36 del RGPD dispone:

> "Artículo 36 Consulta previa
>
> 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 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."

En conclusión, a la vista de los referidos preceptos, a juicio de esta Agencia, por parte de la 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) de la LOPDGDD.

Sin embargo, dicha Ley Orgánica 3/2018 de 5 de diciembre, que complementa en este punto lo previsto en el Reglamento (UE) 2016/679, de 27 de abril de 2016, no atribuye a la Agencia Española de Protección de Datos potestades de autorización previa de los tratamientos de datos con carácter general.

En consecuencia, solamente sería preciso el pronunciamiento de esta Agencia en los supuestos expresamente establecidos en dichas normas, tales como los previstos para transferencias internacionales de datos o los supuestos de **consulta previa** *-ex artículo 36 RGPD-* cuando una evaluación

de impacto *-ex artículo 35 RGPD-* relativa a la protección de datos muestre que el tratamiento entraña un alto nivel de riesgo si el responsable no toma medidas para mitigarlo.