N/REF: 025659/2018

Se solicita de la Agencia Española de Protección de Datos un informe sobre la conformidad a la normativa de protección de datos personales aplicable a los tratamientos de este carácter datos que pudieran efectuarse en el marco de las actividades de investigación del proyecto europeo MINDb4ACT, incluido en el ámbito del programa Horizonte 2020 de la Unión Europea.

El proyecto tiene como objetivo mejorar las políticas actuales contra la violencia extremista en los países representados en el consorcio que van a llevar a cabo el proyecto. Señala el proyecto que su objetivo principal es emitir recomendaciones sobre la política a seguir, extraídas de resultados validados obtenidos de cuatro tipos de intervenciones (acciones de investigación, intercambios entre fuerzas y cuerpos de seguridad, ejercicios de política estratégica, cursos de capacitación y varios proyectos piloto).

Según señala la consulta, en el proyecto participan diversas entidades públicas y privadas españolas y de países miembros de la Unión Europea. El proyecto comporta la realización de varios programas piloto en España.

I

De la información aportada se desprende la realización de diferentes tratamientos de datos personales durante la ejecución del proyecto, de una parte los relativos a las personas que voluntariamente participan en las diversas actividades del proyecto que, según se señala, se encuentra dirigido a los denominados profesionales de primera línea (trabajadores sociales, profesores, psicólogos, expertos, etc) y fuerzas y cuerpos de seguridad, si bien puede determinarse la participación de otras personas, entre ellas menores de edad, en alguno de los proyectos piloto. También parece desprenderse de la documentación aportada que algunos proyectos piloto pueden comportar el tratamiento de datos especialmente protegidos de personas que en ellos participen e incluso se hace referencia en uno de ellos al uso de datos recabados de internet y redes sociales. El presente informe examina como deben adecuarse los tratamientos de datos a la normativa reguladora de la materia con carácter general, haciéndose referencia al final del mismo a las especialidades que puede comportar el tratamiento de datos de los menores de edad y de datos especialmente protegidos.

II

La primera cuestión que resulta del proyecto sujeto a informe es la relativa a la aplicación en el tiempo de la normativa de protección de datos, teniendo en cuenta que a partir del 25 de mayo de 2018 resulta de aplicación, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), tal y como dispone su artículo 99.2.

Por consiguiente, en lo que al presente supuesto respecta en que la ejecución del proyecto se ha iniciado con anterioridad a 25 de mayo de 2018 continuándose su ejecución con posterioridad a dicha fecha, resultarán de aplicación hasta dicho momento las normas que hasta entonces venían rigiendo la materia, esto es, la Directiva 95/46 CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y la normativa que en cada país la desarrolla, normativa que en España viene constituida fundamentalmente por La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter Personal y su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre y, con posterioridad al 25 de mayo de 2018, el citado Reglamento General de Protección de datos.

En consecuencia en el presente informe se hará referencia a ambas normativas y a las obligaciones que siendo exigibles conforme a la normativa anterior se mantienen o modifican y a las nuevas exigencias que impone el Reglamento General de Protección de Datos.

III

En segundo lugar, debe examinarse la aplicabilidad de la normativa de protección de datos a los tratamientos de datos que puedan llevarse a cabo durante la ejecución del proyecto objeto de consulta.

A este respecto debe indicarse que los artículos 1 y 2 de la Ley Orgánica 15/1999, extendían su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento de sus datos de carácter personal, siendo definidos éstos en el artículo 3.a) de la citada Ley como "*cualquier información concerniente a personas físicas identificadas o identificables.*"

El artículo 5.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, precisaba que constituye un dato de carácter personal *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables."*

Dicha definición procede del artículo 2 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual se entenderán 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».*

El Grupo de trabajo del artículo 29, órgano consultivo independiente de la Unión Europea sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE, en su Dictamen 4/2007 sobre el concepto de datos personales, tras poner de manifiesto que la Directiva maneja un concepto lato de datos personales, analiza los elementos de dicha definición, señalando respecto a la expresión "toda información" lo siguiente:

"Desde el punto de vista de la naturaleza de la información, el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona. Por consiguiente, abarca información «objetiva» como, por ejemplo, la presencia de determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones «subjetivas». Esta última clase de afirmaciones constituye una parte considerable del caudal de datos personales tratados en sectores como el de la banca, para evaluar la fiabilidad de los prestatarios («Fulano es un prestatario fiable»), el asegurador («no se espera que Fulano muera pronto») o el laboral («Fulano es un buen trabajador y merece un ascenso»).

Para que esas informaciones se consideren «datos personales», no es necesario que sean verídicas o estén probadas. De hecho, las normas de protección de datos prevén la posibilidad de que la información sea incorrecta y confieren al interesado el derecho de acceder a esa información y de refutarla a través de los medios apropiados.

Desde el punto de vista del contenido de la información, el concepto de datos personales incluye todos aquellos datos que proporcionan información cualquiera que sea la clase de ésta. Por supuesto esto incluye la información personal considerada «datos sensibles» en el artículo 8 de la Directiva a causa de su naturaleza particularmente delicada, pero también otras categorías más generales de información. El término «datos personales» comprende la información relativa a la vida privada y familiar del individuo stricto sensu, pero también la información sobre cualquier tipo de activad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social. El concepto de «datos personales» abarca, por lo tanto,

información sobre las personas, con independencia de su posición o capacidad (como consumidor, paciente, trabajador por cuenta ajena, cliente, etc.).”

Como continuación de dicho análisis el Grupo de trabajo examina el término “sobre” indicando que “*ya se ocupó anteriormente de la cuestión de cuándo puede considerarse que una información versa «sobre» una persona. En el marco de sus debates sobre los problemas de protección de datos planteados por las etiquetas RFID, el Grupo de trabajo señaló que un «dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa».*

Debe, además resaltarse que tanto la voz como la imagen de las personas identificadas o identificables tienen la consideración de datos personales. En este sentido, el Dictamen 02/2012 del Grupo de Trabajo del artículo 29 sobre reconocimiento facial en los servicios en línea y Móviles al hacer referencia a las imágenes digitales como datos personales señala que **“***Si en una imagen digital se distingue tan claramente el rostro de una persona que es posible identificarla, dicha imagen se consideraría un dato personal. Ello dependerá de una serie de parámetros, como la calidad de la imagen o el encuadre concreto. En la mayoría de los casos no se considerarían datos personales las imágenes de escenas en las que se ve a personas en la distancia, o en las que los rostros están difuminados.”*

Por su parte, el Reglamento (UE) 2016/679, esto es, el Reglamento general de protección de datos, hace expresa mención a otros tipos de datos personales en la definición que de los mismos efectúa en su artículo 4.1, entendiendo por tales *“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.*

Dicha definición tiene en cuenta la aparición de nuevos datos identificativos de las personas, tal y como expresa su considerando 30 según el cual “*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.”*

De este modo, serán datos de carácter personal cualquier clase de

información, en los términos vistos, asociada a las personas físicas que en algún modo participan voluntariamente en el proyecto ya sea en el marco de las encuestas, entrevistas, talleres, etc. o los datos relativos a personas físicas que pudieran obtenerse de redes sociales o internet.

Asimismo, desde el punto de vista de los datos a tratar debe tenerse en cuenta que serán datos personales no solamente los identificativos y profesionales, sino también los relativos a imagen y voz de las personas, los datos relativos a ideas políticas o religiosas, las conclusiones que en su caso pudieran alcanzarse sobre ideología o personalidad, datos de localización, direcciones IP, etc.

En particular en lo que respecta a las direcciones IP, esta Agencia ha venido señalando su carácter de dato personal, ahora declarado expresamente en el artículo 4.1 del Reglamento (UE) 2016/679**,** así ya en informe de 12 de septiembre de 2003 se señalaba lo siguiente:

> *"El TCP/IP se trata de un protocolo básico de transmisión de datos en Internet, donde cada ordenador se identifica con una dirección IP numérica única. Las redes TCP/IP se basan en la transmisión de paquetes pequeños de información, cada una de los cuales contiene una dirección IP del emisor y del destinatario.*
>
> *Por otro lado, el DNS (sistema de nombre de dominio) es un mecanismo de asignación de nombres a ordenadores identificados con una dirección IP. Ciertas herramientas existentes en la red permiten encontrar el enlace entre el nombre de dominio y la empresa o el particular.*
>
> *A su vez, 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. Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha la hora y la duración de la asignación de dirección. Es mas, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación.*
>
> *En estos casos, ello significa que, con la asistencia de terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre dirección, número de teléfono, etc), por medios razonables, con lo que no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 3 de la Ley 15/1999.*

En otros casos, un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones estáticas.

Sin embargo, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como cookies con un identificador único o sistemas modernos de minería de datos unidos a bases de datos con información sobre usuarios de Internet que permite su identificación.

Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos."

Debe, asimismo, hacerse referencia al concepto de tratamiento de datos personales, toda vez que de lo expuesto en el proyecto se desprende la realización de diversos posibles tratamientos. A este respecto, constituye un tratamiento de datos, conforme a lo establecido en el artículo 3.c de la Ley Orgánica 15/1999, las *"operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."*

El artículo 4.2 del Reglamento (UE) 2016/679 define el tratamiento como *"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 consiguiente, la realización de alguna o varias de estas operaciones respecto de datos personales, esto es, de cualquier información asociada a una persona física identificada o identificable, dará lugar a un tratamiento de datos personales. Debe así tenerse en cuenta que la recogida de datos no constituye el único tratamiento posible, sino que otras operaciones (por ejemplo, conservación, elaboración, modificación o comunicaciones de datos)

constituyen también tratamientos de datos y son igualmente determinantes, de la aplicabilidad de la normativa de protección de datos.

IV

En la documentación aportada se hacen diversas referencias a la anonimización de los datos personales. Debe aquí recordarse la diferencia entre un proceso de seudonimización y un proceso de disociación o anonimización, ya que este último determina la inaplicación de la normativa de protección de datos. La Ley Orgánica 15/1999 describe los procesos de disociación en su artículo 3 f) como "*Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable"*

En lo que respecta a la seudonimización cabe recordar que el aludido Grupo de Trabajo del Artículo 29, en su Dictamen 5/2014 sobre técnicas de anonimización, define la seudonimización como "la sustitución de un atributo (normalmente un atributo único) por otro en un registro" señalando que "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. La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización."

En este sentido señalaba el Dictamen 4/2007 del Grupo de Trabajo del artículo 29 respecto de un mecanismo de seudonimización habitual como son los datos cifrados que "Los datos cifrados son un ejemplo clásico de «*seudonimización*». La información contenida en esos datos se refiere a un individuo al que se asigna un código cifrado, mientras que la clave para descifrarlos, es decir para establecer la correspondencia entre el código y los identificadores habituales de la persona (nombre, fecha de nacimiento, dirección, etc.) se guardan por separado."

Así, a título de ejemplo, indicaba el Dictamen 4/2007 que "Si a cada persona física se le ha asignado un único código, siempre existe un riesgo de identificación en caso de que sea posible acceder a la clave utilizada para el cifrado. Por lo tanto, los riesgos de un acceso ilegal desde el exterior, la probabilidad de que alguien de la organización remitente - a pesar de estar sujeto al secreto profesional -proporcione la clave *y por ende* la vía para una identificación indirecta, son factores que deben tenerse en cuenta para determinar si las personas pueden ser identificadas teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona y, por lo tanto, si la información debe considerarse como «datos personales».

El concepto de seudonimización aparece expresamente recogido en el artículo 4.5) del Reglamento europeo que define la «seudonimización» como "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"*

El considerando 26 de dicho Reglamento recuerda que "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos."

Y en el considerando 28, viene a poner de manifiesto la diferencia entre anonimización y seudonimización al señalar 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."*

De este modo, si la información relativa a las personas se encuentra asociada a un seudónimo, esta operación de seudonimización, por sí misma, no constituye un procedimiento de disociación puesto que a partir de la información de que se tiene conocimiento será posible realizar la operación inversa a la seudonimización, lo que da lugar a que la aplicación de la normativa de protección de datos no quede excluida.

En lo que respecta a la anonimización de los datos resulta de especial interés lo señalado por el Grupo de Trabajo del artículo 29 en sus dictámenes. Así ya en su Dictamen 6/2013 indicaba que "*La anonimización es cada vez más difícil de lograr con el avance de las modernas tecnologías informáticas y la disponibilidad de la información de forma ubicua. La reidentificación de las personas es cada vez más común y representa una amenaza en la actualidad. En la práctica, existe una importante zona gris, en la que el responsable del tratamiento de datos puede creer que un conjunto de datos está anonimizado,*

pero un tercero puede ser capaz de identificar al menos a algunas personas a partir de estos datos, por ejemplo, utilizando otros datos públicos o cualquier otra información de que disponga."

En particular en el Dictamen 5/2014, sobre técnicas de anonimización, el citado Grupo de Trabajo señalaba que "*A la luz de la Directiva 95/46/CE y de otros instrumentos jurídicos pertinentes de la UE, la anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación."*

Se recordaba en dicho Dictamen 5/2014 que *""El Grupo de Trabajo examinó el concepto de «datos personales» en el Dictamen 4/2007 sobre datos personales, en el que se centra en los elementos componentes de la definición del artículo 2, letra a), de la Directiva 95/46/CE, entre ellos la referencia a una persona física «identificada o identificable». En este contexto, el Grupo de Trabajo llegó a la conclusión de que «los datos anonimizados serían, por tanto, datos anónimos que antes hacían referencia a una persona identificable, pero que ahora ya no admiten identificación».*

Por consiguiente, el Grupo de Trabajo ya ha aclarado que la Directiva propone la razonabilidad de los medios usados («el conjunto de los medios que puedan ser razonablemente utilizados») como criterio para evaluar si el tratamiento de anonimización es suficientemente sólido, es decir, si la identificación es «razonablemente» imposible. Afectan directamente a la identificabilidad el contexto y las circunstancias particulares de cada caso.

(…) Una solución de anonimización eficaz impide a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos (o dos registros pertenecientes a conjuntos diferentes) e inferir cualquier tipo de información a partir de dicho conjunto. En definitiva, como norma general, no basta con eliminar los elementos que pueden servir para identificar directamente a una persona para garantizar que ya no se puede identificar al interesado. Con frecuencia habrá que tomar medidas adicionales para evitar dicha identificación, las cuales dependerán una vez más del contexto y de los fines del tratamiento de que van a ser objeto los datos."

En dicho Dictamen 5/2014 se ponía igualmente de manifiesto que *"Es importante dejar claro que el concepto de «identificación» no conlleva únicamente la posibilidad de recuperar el nombre o la dirección de una persona, sino que incluye también la identificabilidad potencial por singularización, vinculabilidad o inferencia. Es más, a efectos legales es irrelevante la intención del responsable del tratamiento o del destinatario. Mientras los datos sean identificables, se aplica la legislación sobre protección de datos."*

V

Debe aquí hacerse referencia a diferentes figuras reguladas en la normativa de protección de datos, ya que la posición que ocupan los miembros del consorcio desde el punto de vista de protección de datos determina las obligaciones y responsabilidades que les incumben y, con anterioridad a la aplicación del Reglamento (UE) 2016/679, determinaba la normativa nacional aplicable en cada caso.

Debe así examinarse en primer lugar la figura del responsable del tratamiento, debiendo diferenciarse al responsable del tratamiento del responsable del proyecto o de una fase del mismo ya que a dicha condición de responsable del tratamiento se anudarán determinadas consecuencias jurídicas distintas a las propias de quien está a cargo de un determinado trabajo.

Con carácter general, la condición de responsable del fichero o tratamiento es consecuencia del hecho de que una persona o entidad, debidamente legitimada, haya decidido tratar datos personales para sus propios fines, correspondiéndole por ello asumir las obligaciones impuestas por la normativa de protección de datos y las responsabilidades que de su incumplimiento pudieran derivarse. El artículo 2 de la Directiva 95/46 definía en su letra d) al responsable del tratamiento como *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales".* En el derecho español la Ley Orgánica 15/1999, definía al responsable del fichero o tratamiento como la *"persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".*

El Reglamento (UE) 2016/679 configura en la actualidad en su artículo 4.7 al responsable del tratamiento o responsable como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros."*

En lo que al presente supuesto respecta, la condición de responsable del tratamiento recaerá así en la entidad o entidades participantes en el consorcio que determinen, en cada caso, la finalidad, contenido o uso de cada tratamiento que se lleve a cabo durante la ejecución del proyecto.

Debe hacerse igualmente referencia a la figura del encargado del tratamiento, ya que si alguno de los miembros del proyecto actúa en tal condición, igualmente está sujeto a determinadas obligaciones y responsabilidades.

La figura del encargado del tratamiento obedece a la necesidad de dar respuesta a fenómenos como la externalización de servicios por parte de las empresas y otras entidades, de manera que en aquellos supuestos en que el responsable del tratamiento encomiende a un tercero la prestación de un servicio que requiera el acceso a datos de carácter personal por éste, dicho acceso no pueda considerarse como una cesión de datos por parte del responsable a quien le presta tal servicio, sino que el tratamiento de los datos se realiza por el encargado en nombre y por cuenta del responsable como si fuera este mismo quien lo lleva a cabo. El encargado del tratamiento venía definido en el artículo 2.e) de la Directiva como *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento."* De la misma manera el artículo 3 g) de la Ley Orgánica 15/1999, define así al encargado como "*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*". El Reglamento General de Protección de Datos, se refiere a esta figura en su artículo 4.8 como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento"*

Debe tenerse en cuenta respecto a las obligaciones que puedan incumbir a dicha figura que con anterioridad a la aplicación del Reglamento General de Protección de datos, en el caso de que alguna de las entidades participantes en el proyecto actuase como encargado del tratamiento le resultaba de aplicación la normativa de protección de datos que correspondiese al responsable por cuya cuenta actuaban, excepto en lo que respecta a la adopción de medidas de seguridad en que se aplicaba la normativa del Estado miembro en que tuviese su establecimiento el encargado del tratamiento.

Así resultaba de lo establecido en el artículo 17.3 de la citada Directiva, cuyo tercer epígrafe preceptuaba que *"las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.*" El apartado primero refiere a la obligación de adoptar las correspondientes medidas de seguridad, al prever que "*Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales."*

De este modo, los tratamientos de datos realizados por responsables cuyo establecimiento se encuentra en territorio español estaban sujetos a lo dispuesto en la Ley Orgánica 15/1999. Este sería el caso de las entidades

españolas participantes en el proyecto, si su participación comporta un tratamiento de datos personales y actúan en calidad de responsables, pero sería igualmente el caso de cualquier otra entidad participante si tuviera un establecimiento en España y efectuase un tratamiento de datos en el marco de las actividades del mismo. También quedaban sometidas a la normativa española de protección de datos las entidades que actuasen como encargadas de tratamiento de responsables sujetos a la normativa española, excepto en la aplicación de las medidas de seguridad que serían las del país en que tenga su establecimiento. No obstante, si alguna entidad española actuase como encargado del tratamiento de un responsable al que deba aplicarse la normativa de protección de datos de otro país de la Unión Europea, seguiría la ley nacional del responsable, salvo en lo que respecta a las medidas de seguridad que serán las establecidas en la normativa española.

A partir de 25 de mayo de 2018 tanto el responsable como el encargado del tratamiento deberán ajustar su actuación a lo previsto en el Reglamento UE 2016/679.

VI

Respecto a las obligaciones que incumben al responsable del tratamiento, tanto cuando estaba sujeto a la normativa nacional española como en la actualidad al Reglamento General de Protección de Datos debe hacerse referencia a las siguientes:

-Conforme a lo establecido en la Ley Orgánica 15/1999, el responsable debía notificar la creación del fichero a efectos de su inscripción en el Registro General de Protección de Datos de esta Agencia, obligación que dejó de ser exigible a partir de 25 de mayo de 2018. En la actualidad el artículo 31 del Reglamento (UE) 2016/679 a los responsables del tratamiento a mantener un registro de las actividades de tratamiento bajo su responsabilidad, y a los encargados a mantener registros de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable. Debe tenerse en cuenta que el número 5 de dicho artículo establece una excepción al cumplimiento de dichas obligaciones siempre y cuando se cumplan dos condiciones: la primera de ellas que se trate de una empresa u organización que emplee a menos de 250 personas y, la segunda, que el tratamiento que realice no entrañen un riesgo para los derechos y libertades de los interesados, no incluya categorías especiales de datos personales a los que se refiere el artículo 9 del Reglamento ni datos personales relativos a condenas o infracción penales a que se refiere el artículo 10 de la misma norma, ni dicho tratamiento sea ocasional. De este modo, aunque el consultante diera empleo a menos de 250 personas, el carácter habitual, aun cuando sea temporal, del tratamiento de datos personales precisos para llevar a cabo el proyecto, impide aplicar dicha excepción debiendo llevar a cabo dicho registro en los términos establecidos en el precepto transcrito.

- Requisito capital para que un tratamiento de datos personales sea conforme a lo establecido en la normativa de protección de datos es que el mismo se encontrase legitimado en lo previsto en el artículo 6 de la Ley Orgánica 15/1999 y, en la actualidad en lo dispuesto en el artículo 6 del Reglamento General de protección de datos. Ambas normas señalan el consentimiento como primera causa legitimadora del tratamiento.

De este modo, para tratar datos personales el responsable deberá recabar, de las personas físicas que participen en las actividades previstas en el proyecto, su consentimiento para el tratamiento de sus datos personales. La Ley Orgánica 15/1999, exigía expresamente en su artículo 3.h que el consentimiento reuniera las características de "*libre, inequívoco, específico e informado".*

Esta Agencia ha venido describiendo en sus informes dichas características de manera que se entiende por consentimiento libre aquel que ha sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por el Código Civil. El consentimiento específico viene referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento, tal y como impone el artículo 4.2 de la Ley Orgánica 15/1999. Para que pueda hablarse de consentimiento inequívoco se exige la realización de una acción u omisión que implique la existencia del consentimiento.

En cuanto al requisito de la información, supone que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que se efectúa. Dispone a este respecto el artículo 5 de la Ley Orgánica 15/1999 que *"los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".*

Por consiguiente, el modelo de consentimiento que debían firmar las personas cuyos datos se hayan recabado con anterioridad a 25 de mayo debía adecuarse a dichos requerimientos, identificando al responsable del tratamiento (que cómo se ha indicado no es el investigador, sin perjuicio de que se le señale como la persona ante la que puede ejercitar sus derechos) e indicándose la posibilidad de ejercer los derechos a que se refiere la letra d) de dicho precepto. Asimismo debía indicarse quienes son los posibles destinatarios de la información (en el presente supuesto, a título de ejemplo, otros socios del consorcio, en caso de que se les comunicasen datos

personales) recabando el consentimiento de los interesados para tal comunicación de datos.

A partir de 25 de mayo de 2018, la aplicación del Reglamento (UE) 2016/679 impone mayores exigencias respecto de la información que debe facilitarse a los interesados, lo que deberá tenerse en cuenta si se recaba el consentimiento de los interesados con posterioridad a dicha fecha, adaptando el formulario en que se recoja la información a tales exigencias.

El artículo 13 de dicho Reglamento regula la información que debe facilitarse cuando los datos personales se obtengan del interesado, disponiendo lo siguiente:

"1.Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) *la identidad y los datos de contacto del responsable y, en su caso, de su representante;*

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

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) 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.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) *el plazo durante el cual se conservarán los datos personales o, cuando*

no sea posible, los criterios utilizados para determinar este plazo;

b) 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;

c) 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;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) 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;

f) 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.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

Corresponde al responsable del tratamiento demostrar que se ha obtenido el consentimiento de los interesados para el tratamiento de sus datos. Dicha obligación figuraba tanto en el artículo 12 del Reglamento de desarrollo de la Ley Orgánica 15/1999 como en la actualidad en el artículo 7 del Reglamento (UE) 2016/679.

Debe además tenerse en cuenta que el consentimiento prestado es siempre revocable conforme a los artículos 6.3 y 11.4 de la Ley Orgánica 15/1999, pudiendo el interesado exigir el cese en el tratamiento de sus datos

mediante su pura y simple manifestación de voluntad. El Reglamento (UE) 2016/679 señala en la actualidad al respecto que *"3.El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo."*

- Dentro de las obligaciones del responsable debe destacarse, en tercer lugar, el deber de implantar en el fichero o ficheros creados las debidas medidas de seguridad. Esta obligación, como se ha señalado, incumbía igualmente a los encargados del tratamiento establecidos en España.

En este sentido cabe recordar que el artículo 9 de la Ley Orgánica 15/1999 dispone que *"El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural."*

El número 2 de dicho precepto prohíbe el registro de datos de carácter personal en ficheros "*que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas."*

Debe, además, recordarse que, como ha señalado reiteradamente la Audiencia Nacional en sus sentencias (por todas ellas SAN de 6-10-2011), la seguridad constituye una obligación de resultado consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros.

Tales medidas venían reguladas en el Reglamento de desarrollo de la Ley Orgánica 15/1999, cuyo artículo 80 clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, las previstas para el nivel correspondiente en función de la naturaleza de los datos a tratar, teniendo, además, en cuenta que tienen carácter acumulativo de forma que su establecimiento exige la adopción de las de nivel o niveles inferiores.

A partir de 25 de mayo debe tenerse en cuenta que la regulación del Reglamento General de protección de datos, adopta un enfoque diferente al establecido en la Ley Orgánica 15/1999 y su normativa de desarrollo en lo que respecta a las medidas de seguridad que el responsable o el encargado de un tratamiento de datos deben implementar.

Señala el considerando 83 de dicha norma que *" A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente*

Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales."

El artículo 32 del Reglamento General de Protección de datos, en sus números 1 y 2, dispone lo siguiente respecto de la seguridad del tratamiento:

"1.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 otros:

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.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

Asimismo, debe tenerse en cuenta que a partir de la aplicación del Reglamento general de protección de datos incumbe a todos los responsables la obligación de notificar, en su caso, las violaciones de seguridad de los datos a la autoridad de control (esto es, en el caso español a la Agencia Española de

protección de datos), disponiendo al respecto el artículo 33 de dicho Reglamento que:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

La notificación contemplada en el apartado 1 deberá, como mínimo:

a) *describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;*

b) *comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*

c) *describir las posibles consecuencias de la violación de la seguridad de los datos personales;*

d) *describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

VII

Conforme a lo previsto en la Ley Orgánica 15/1999, si alguna de las entidades sujetas a la normativa de protección de datos española efectuase una comunicación de los datos personales objeto de tratamiento en el proyecto a terceros, incluidas las demás entidades que participan en el mismo, o procediesen a su difusión o publicación por cualquier procedimiento, dicha comunicación o difusión constituía una cesión de datos personales definida en el artículo 3 i) de la Ley Orgánica 15/1999 como "*Toda revelación de datos realizada a una persona distinta del interesado".*

Tal cesión debía sujetarse al régimen general de comunicación de datos de carácter personal establecido en el artículo 11 de la Ley Orgánica 15/1999, donde se establece que la misma solo puede verificarse para el cumplimiento de fines directamente relacionados con las funciones legitimas del cedente y cesionario y exige, para que pueda tener lugar, el consentimiento del interesado (artículo 11.1), otorgado con carácter previo a la cesión y suficientemente informado de la finalidad a que se destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar (artículo 11.3), y que debe recabar el cedente como responsable del fichero que contiene los datos que se pretenden ceder.

De la misma manera en la actualidad tal comunicación de datos, constituye un tratamiento de datos conforme a la definición, antes transcrita, contenida en el artículo 4.2 del Reglamento General de Protección de datos. El Reglamento hace así referencia a la figura del destinatario, al que configura en el artículo 4.9 *como "la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero."* Dicha comunicación debe encontrarse legitimada en lo previsto en el artículo 6 de la misma norma, de modo que el consentimiento para comunicar tales datos puede operar igualmente como causa legitimadora de dicha comunicación.

No obstante, cabe recordar la posibilidad de que las demás entidades participantes en el proyecto puedan actuar en condición de encargados del tratamiento del responsable. En este sentido, el artículo 12 de la Ley Orgánica 15/1999 regula la figura del encargado del tratamiento, disponiendo que *"No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento*." A esta figura cabe acudir cuando se presta al responsable un servicio que comporta el tratamiento de datos personales (por ejemplo, el almacenamiento de los mismos). Para que quienes presten estos servicios al responsable tengan tal condición de encargado del tratamiento, si el responsable está sujeto a la normativa de protección de datos española, será preciso que se dé cumplimiento a los requisitos exigidos por el artículo 12 de la Ley Orgánica 15/1999 y su normativa de desarrollo, en otro caso, nos

encontraríamos ante una cesión de datos que requeriría el consentimiento del interesado. Dichos requisitos son los siguientes:

En primer lugar, es preciso que el acceso a los datos por el tercero se efectúe con la exclusiva finalidad de prestar un servicio al responsable del fichero, y que dicha relación de servicios se encuentre contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 de la Ley Orgánica 15/1999, impone que "*la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".*

En este sentido, debe además recordarse que uno de los requisitos determinantes de la condición de encargado de tratamiento es la inexistencia de una relación directa entre el afectado por el tratamiento de datos y el encargado, tal y como establece el último párrafo del número primero del artículo 20 del Reglamento de desarrollo de la Ley Orgánica 15/1999 según el cual "*se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado".* El encargado debe obrar en todo caso en nombre y por cuenta del responsable como si como si la relación fuese entre éste y el afectado. De este modo, si se establece dicha relación directa utilizando el encargado para sus propios fines los datos personales recabados por el responsable, carecería de tal condición deviniendo responsable y la comunicación de datos al mismo una cesión que requerirá el consentimiento de los interesados.

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la Ley Orgánica 15/1999, de forma que "*una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".*

El incumplimiento de esta previsión llevará aparejada la consecuencia, prevista en el artículo 12.4 de la citada Ley, de que *"En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".*

Esta Agencia Española de Protección de Datos ha venido indicando que el deber de devolución al que se refiere el artículo 12.3 de la aludida Ley Orgánica podrá verificarse mediante la entrega directa de los datos al propio responsable del tratamiento o mediante la realización de dicha entrega al encargado del tratamiento que este designase, toda vez que en este segundo caso el encargado actuaría como mero mandatario del responsable, siendo precisamente éste el que establece a quién han de entregarse los datos en su nombre y por su cuenta. Y así se recoge en el artículo 20.3 del Reglamento de desarrollo de dicha Ley al disponer "*no obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.*"

Por su parte, el artículo 22 del aludido Reglamento dispone respecto de la conservación de los datos lo siguiente:

"*1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento."

En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículo 9 y 12.2 de la Ley Orgánica 15/1999. Cabe recordar que antes de la aplicación del Reglamento UE 2016/679, las medidas de seguridad a adoptar por el encargado del tratamiento eran las establecidas por la normativa del Estado miembro en que tuviese su establecimiento.

El Reglamento (UE) 2016/679 impone al encargado del tratamiento mayores obligaciones que las establecidas en la Ley Orgánica 15/1999. Por otra parte, a efectos de determinar si los contratos existentes con anterioridad a dicha norma deben ajustarse a lo previsto en el Reglamento cuando el responsable o el encargado estuvieran sujetos a lo establecido en la Ley Orgánica 15/1999, habrá que estar a lo que se disponga en la normativa de desarrollo en España una vez se apruebe esta.

A esta figura del encargado del tratamiento cabe acudir cuando una entidad de las que participa en el proyecto lleve a cabo alguna actividad que comporte un tratamiento de datos en nombre y por cuenta de otra u otras que tengan la condición de responsables, siempre y cuando la entidad que actúe como encargado lleve a cabo dicha actividad conforme a las instrucciones del responsable y no establezca una relación directa con el afectado por el tratamiento, por ejemplo, cuando su actividad se limite a proporcionar un servidor para el alojamiento de los datos del responsable o responsables sin utilizar tales datos para ninguna otra finalidad distinta a tal alojamiento.

VIII

Debe tenerse en cuenta que todo tratamiento de datos debe ser respetuoso de los principios relativos a la calidad de los datos contenidos en la Directiva 95/46 CE. En este sentido, la Ley Orgánica 15/1999, recoge igualmente dichos principios, debiendo destacarse en particular el denominado principio de finalidad, recogido en el artículo 4.2 de dicha Ley y conforme al cual "*Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".* Debe aclararse aquí que la Audiencia Nacional partiendo de una interpretación sistemática de este precepto viene considerando la expresión "finalidades incompatibles" como sinónimo de "finalidades distintas".

De este modo no resultaría posible la utilización de los datos personales para una finalidad distinta a aquélla para la que se solicitó el consentimiento de los interesados, sin que nuevamente se recabe éste de manera informada o sin que dicho nuevo tratamiento encuentre su legitimación en alguno de los supuestos contenidos en el artículo 6 de la Ley Orgánica 15/1999. Debe así señalarse que en el caso de la aplicación a que hace referencia el proyecto la finalidad del tratamiento debe estar bien definida y ser comprensible para un usuario medio sin conocimientos jurídicos o técnicos especiales.

La limitación de la finalidad está vinculada al principio de proporcionalidad, consagrado en el artículo 4.1 de la Ley Orgánica 15/1999 conforme al cual *"Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."*

De este modo solamente deberán recabarse aquéllos datos que sean precisos para llevar a cabo las actividades objeto del proyecto.

Igualmente, dentro de los principios de calidad recogidos en la Ley Orgánica 15/1999, debe hacerse referencia al relativo a la conservación de los datos, disponiendo el número 5 del citado artículo 4 que "*Los datos de*

carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados."

En consecuencia, los datos personales recogidos no podrán mantenerse indefinidamente en los ficheros de los participantes en el proyecto, debiendo cancelarse una vez que dichos datos dejen de ser necesarios para la finalidad para la cual fueron obtenidos. En la información aportada sobre el proyecto objeto de consulta se estima que los datos deberán ser mantenidos durante 4 años tras la finalización del proyecto, momento a partir del cual deberán cancelarse.

Debe tenerse en cuenta, además, que cuando las entidades participantes en el proyecto actúan como encargados del tratamiento, como se ha señalado, deberán destruir o devolver los datos una vez cumplida la prestación contractual. En lo que respecta a la previsión contenida en el Reglamento de desarrollo de la Ley Orgánica 15/1999 sobre el mantenimiento por el encargado de tratamiento de los datos bloqueados debe tenerse en cuenta que tal norma viene referida al plazo de garantía contractual. Tales plazos deben reflejarse en el instrumento jurídico en que se plasme el encargo de tratamiento.

A tales principios se refiere también el artículo 5 del Reglamento UE 2016/679. Dicha norma refuerza el principio de proporcionalidad, al que denomina "minimización de datos" al ponerlo en relación con las exigencias de privacidad por defecto y desde el diseño.

IX

Por último debe hacerse referencia a otras cuestiones que en materia de protección de datos plantea dicho proyecto. Así se indica que como regla general las actividades del proyecto van dirigidas a los denominados profesionales de primera línea (trabajadores sociales, profesores, psicólogos, expertos, etc) y fuerzas y cuerpos de seguridad, no obstante, en el ámbito de alguna de las actividades, podría decidirse la participación de menores de edad.

En lo que a menores de edad respecta, y sin perjuicio de la protección que a éstos otorgan otras normas, el Reglamento de desarrollo de la Ley Orgánica 15/1999 contiene una previsión especial respecto a la solicitud de consentimiento para la protección de sus datos, dispone así su artículo 13 lo siguiente:

"1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija

para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales."

Por otra parte, en el marco de las actividades del proyecto pueden tratarse datos especialmente protegidos, tal y como éstos vienen regulados en el artículo 7 de la ley Orgánica 15/1999, que establece los supuestos en que es posible su tratamiento. Dispone dicho precepto en sus números 2 y 3 que:

"2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente."

Por consiguiente, deberá recabarse el consentimiento de los afectados para el tratamiento y cesión de tales datos, consentimiento que deberá ser expreso cuando se trate de los datos a que se refiere el número 3 de dicho precepto y expreso y por escrito cuando los datos a tratar o comunicar sean datos de los recogidos en su número 2.

El Reglamento (UE) 2016/697 considera en su artículo 9.1 como categorías especiales de datos personales los que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física." Dicho precepto prohíbe el tratamiento de tales datos salvo que concurra alguna de las causas que enumera, de las que interesa aquí la relativa al consentimiento explícito del interesado para el tratamiento de dichos datos personales, para uno o más fines especificados, que constituirá la legitimación para el tratamiento de los datos excepto cuando el Derecho de la Unión o de los Estados miembros establezca que tal prohibición no puede ser levantada por el interesado.

En cuanto a otras posibles obligaciones que pueda determinar el tratamiento de los datos de menores de edad o de categorías especiales de datos, debe tenerse en cuenta que el artículo 35.1 del Reglamento (UE) 2016/679 dispone que "*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."*

El número segundo de dicho precepto establece que "*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."*

Por consiguiente, debe examinarse por parte del responsable o responsables, si los tratamientos de datos a efectuar, requieren la previa realización de una evaluación de impacto. En este sentido y sin perjuicio de la existencia de diversas metodologías existentes que pueden ser utilizadas, cabe indicar que el Grupo de Trabajo del Artículo 29 ha adoptado recientemente

unas directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, que puede consultarse en el siguiente sitio web: (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083). Por su parte, esta Agencia ha publicado en su página web (www.agpd.es) una guía para las evaluaciones de impacto en la protección de datos sujetas al Reglamento General de Protección de Datos.

Por último, en cuanto a la posible actividad relativa al uso de datos recabados de redes sociales e internet, señala la consulta que tales datos serán completamente anonimizados. Debe aquí recordarse que la mera recogida de los datos constituye un tratamiento de datos que precisa encontrarse legitimado en lo previsto en la normativa de protección de datos. Debe igualmente recordarse lo señalado en el presente informe respecto de los procesos de anonimización y seudonimización, en tanto que los datos asociados a un identificador no pueden considerarse anonimizados, de modo que no quedaría excluida la aplicación de la normativa de protección de datos.