

La consulta plantea cuales son las condiciones y requisitos legales que han de cumplirse por el consultante en materia de protección de datos personales en el proyecto de investigación DANTE (Detecting and ANalysing TErrorist-related online contents and financing activities), cuyo objeto, según se expone es el desarrollo de nuevas herramientas TIC para la fuerzas y Cuerpos de Seguridad de los distintos Estados de la Unión Europea. El proyecto se centra en tres ámbitos distintos: la detección de la financiación de distintos grupos terroristas, la identificación de labores de propaganda y la detección de labores de reclutamiento y desinformación llevada a cabo por estos grupos. Para ello será preciso obtener información gráfica, video gráfica y sonora por lo que se analizarán tanto material multimedia (audio, video e imágenes) como información textual, accesible desde la web.

Según señala la consulta se analizarán datos públicamente disponibles en internet incluido el acceso a la dark net; datos facilitados por las Fuerzas y Cuerpos de Seguridad que participan en el consorcio, únicamente después de firmar un acuerdo que regule el uso de tales datos y su ciclo de vida, y conjuntos de datos disponibles en línea dentro de grupos privados, a los que los beneficiarios del proyecto tengan acceso, tras el registro, autorización, permiso y consentimiento de su propietario. Asimismo, el proyecto comporta la realización de pruebas piloto en las que se harán demostraciones del funcionamiento del sistema en entornos operacionales con datos reales.

Por otra parte, se tratarán datos de expertos que participan en la definición de los requerimientos y en los talleres que se organicen.

En el proyecto participan diversas entidades privadas, todas ellas de la UE, que se encargan de llevar a cabo los aspectos más técnicos del proyecto, universidades y centros de investigación y por Fuerzas y Cuerpos de seguridad de distintos estados miembros de la UE en calidad de usuarios finales.



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.

Debe así tenerse en cuenta que en el momento en que se inició la ejecución del proyecto, la normativa en materia de protección de datos estaba formada por 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.

No obstante, este marco normativo ha sido objeto de modificación, tras la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Por consiguiente es preciso examinar, en primer lugar, si resultaba aplicable a los tratamientos de datos efectuados durante la ejecución del proyecto al que se refiere la consulta lo establecido en la Directiva 95/46/CE, y en consecuencia, la normativa nacional que en cada caso la desarrollaba. En este sentido cabe recordar que la misma excluía de su ámbito de aplicación, en su artículo 3.2, el tratamiento de datos personales *“efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal”*

En este sentido el considerando 13 de dicha Directiva señalaba que *“Considerando que las actividades a que se refieren los títulos V y VI del Tratado de la Unión Europea relativos a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en el ámbito penal no están comprendidas en el ámbito de aplicación del Derecho comunitario, sin perjuicio de las obligaciones que incumben a los Estados miembros con arreglo al apartado 2 del artículo 56 y a los artículos 57 y 100 A del Tratado; que el tratamiento de los datos de carácter personal que sea necesario para la salvaguardia del bienestar económico del Estado no está comprendido en el*



ámbito de aplicación de la presente Directiva en los casos en que dicho tratamiento esté relacionado con la seguridad del Estado”

Ahora bien, entiende esta Agencia que el tratamiento de datos personales con fines de investigación científica de los datos que pudieran haberse recabado con tal finalidad de seguridad del Estado, sí se encuentran sujetos a lo dispuesto en la Directiva 95/46 CE toda vez que la exclusión contenida en dicha norma viene limitada a los tratamientos de datos que tengan por objeto “la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal”, pero no a otros posibles tratamientos que pudieran efectuarse lícitamente de tales datos como la investigación científica o técnica.

En lo que respecta a la normativa española de desarrollo de la Directiva 95/46 CE, el artículo 2 de la Ley Orgánica 15/1999 dispone que “*El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.*”

Debe aquí igualmente concluirse que dicha exclusión no determina la inaplicación de la Ley Orgánica 15/1999 al tratamiento que, con fines de investigación científica, pudiera legítimamente realizarse de datos recabados con la finalidad de investigación del terrorismo y otras formas graves de delincuencia organizada, sino que por el contrario tal tratamiento debe estar plenamente sujeto a dicha norma. Asimismo, en el proyecto se tratan otro tipo de datos personales, tales como los de las personas que voluntariamente participan en el proyecto como expertos, cuyo tratamiento también debía sujetarse a lo previsto en la Ley Orgánica 15/1999.

En segundo lugar, debe tenerse en cuenta que a partir de 25 de mayo de 2018, comenzó la aplicación del Reglamento (UE) 2016/679 tal y como establece su artículo 99.2 y que el artículo 63 de la Directiva (UE) 2016/680, relativo a la transposición de la misma prevé que “*Los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva. Comunicarán inmediatamente a la Comisión el texto de dichas disposiciones. Aplicarán dichas disposiciones a partir del 6 de mayo de 2018.*”

Dicha dualidad normativa exige examinar por cual de ambas normas debe regirse los tratamientos de datos que se inicien o continúen su ejecución desde la fecha de aplicación del Reglamento UE 2016/679, pudiendo suceder



que algunos tratamientos estén sometidos a dicho Reglamento y otros a la Directiva (UE) 2016/680 y a la normativa que la desarrolle.

Debe así tenerse en cuenta que el artículo 1, apartado 1 de la Directiva (UE) 2016/680 declara que su objeto consiste en establecer *“las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.”*

La citada Directiva (UE) 2016/680 en su artículo 8.1 establece respecto de la licitud del tratamiento con los fines señalados en su artículo 1 que *“los Estados miembros dispondrán que el tratamiento solo sea lícito en la medida en que sea necesario para la ejecución de una tarea realizada por una autoridad competente, para los fines establecidos en el artículo 1, apartado 1, y esté basado en el Derecho de la Unión o del Estado miembro.”* Su artículo 9 prohíbe el uso de tales datos recogidos por las autoridades competentes con fines distintos a los enumerados en su artículo 1 apartado 1, esto es, la prevención, investigación detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluida la protección y la prevención frente a las amenazas contra la seguridad pública, salvo que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. No obstante, su artículo 4 habilita un uso científico de los datos cuando su finalidad sea igualmente la establecida en el artículo 1, apartado 1 de la Directiva. Dispone el artículo 4 de dicha norma lo siguiente:

“2. Se permitirá el tratamiento de los datos personales, por el mismo responsable o por otro, para fines establecidos en el artículo 1, apartado 1, distintos de aquel para el que se recojan en la medida en que:

a) el responsable del tratamiento esté autorizado a tratar dichos datos personales para dicho fin de conformidad con el Derecho de la Unión o del Estado miembro, y

b) el tratamiento sea necesario y proporcionado para ese otro fin de conformidad con el Derecho de la Unión o del Estado miembro.

3. El tratamiento por el mismo responsable o por otro podrá incluir el archivo en el interés público, el uso científico, estadístico o histórico para los fines establecidos en el artículo 1, apartado 1, con sujeción a las salvaguardias adecuadas para los derechos y libertades de los interesados.”

De este modo, el tratamiento para uso de investigación científica de los datos personales recabados o que solamente pudieran ser recabados legítimamente con fines de investigación, prevención, detección o enjuiciamiento de infracciones penales por las autoridades competentes se encuadra así en lo previsto en el número 3 de tal precepto, toda vez que su



finalidad es facilitar las investigaciones policiales en materia de terrorismo desarrollando nuevas herramientas TIC para las fuerzas y Cuerpos de Seguridad. Sin embargo, otros tratamientos de datos personales, por ejemplo, los datos personales de aquellos participantes en el proyecto, sean éstos miembros de Fuerzas y Cuerpos de Seguridad o expertos que voluntariamente participen en el proyecto a fin de delimitar los requerimientos de las herramientas que el proyecto pretende crear, quedarían a partir de 25 de mayo de 2018, sujetos a lo previsto en el Reglamento (UE) 2016/679 (Reglamento Europeo de Protección de datos).

En lo que respecta a los tratamientos que deban quedar sujetos a la Directiva (UE) 2016/680, teniendo en cuenta que en España no se ha procedido todavía a su trasposición, seguirá resultando de aplicación a tales tratamientos lo previsto en la Ley Orgánica 15/1999, sin perjuicio de que dicha Directiva pueda resultar directamente aplicable en su caso. En este sentido cabe tener en cuenta que el proyecto de Ley Orgánica 15/1999, actualmente en tramitación en el Congreso de los Diputados prevé en su disposición transitoria cuarta que *“Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.”*

II

Teniendo en cuenta que en el proyecto participan entidades españolas y de otros Estados miembros de la Unión Europea, debe examinarse qué normativa nacional resultaba aplicable durante la vigencia de la Directiva 95/46 UE y la que en la actualidad resulta de aplicación cuando los tratamientos deban sujetarse a la ley nacional que desarrolle la Directiva (UE) 2016/680.

El artículo 4 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 dispone al respecto:

- 1 *Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:*



- a *el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable”*

Para determinar la legislación aplicable resulta necesario hacer referencia a las figuras de responsable y encargado del tratamiento (data controller y data processor respectivamente). El artículo 2 de la Directiva 95/46 define 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; (...)”*

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. (...)” Debe así diferenciarse el responsable del fichero o tratamiento del responsable del proyecto o de una fase del mismo ya que a dicha condición de responsable del fichero o tratamiento se anudan determinadas consecuencias jurídicas distintas a las propias de quien está a cargo de un determinado trabajo.

Por su parte, el encargado del tratamiento viene 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.”*

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.

Debe tenerse en cuenta que, para que pueda hablarse de encargado del tratamiento la Directiva 95/46/CE, venía a exigir los siguientes requisitos en su artículo 17, números 3 y 4:



“3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- 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.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente.”

En cuanto a las obligaciones que pudieran incumbir a dicha figura durante la vigencia de la Directiva 95/46, 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, con anterioridad a la aplicación del Reglamento UE 2016/679 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 tuviese 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, seguirá la ley nacional del responsable, salvo en lo que respecta a las medidas de seguridad que serán las establecidas en la normativa española.

En la actualidad, tanto el responsable como el encargado del tratamiento, en aquellos tratamientos de datos que no estén sujetos a la Directiva UE 2016/680, deberán ajustar su actuación a lo previsto en el Reglamento UE 2016/679.

Respecto de los tratamientos sujetos a la Directiva UE 2016/680, la legitimación para el tratamiento de datos con fines de investigación se encuentra vinculada, como anteriormente se ha señalado, a la legitimación para el tratamiento de tales datos con el objeto de dicha norma descrito en su número 1.1, toda vez que, conforme a su artículo 8, solamente estará habilitada la autoridad competente en cada caso para el tratamiento de datos personales con los fines establecidos en la misma, estando prohibida en su artículo 9 la utilización de los datos recabados para tales fines para otros diferentes salvo autorización del Derecho de la Unión o del Estado miembro, si bien la Directiva permite su uso con fines de uso científico por el propio responsable.

De este modo, en el marco del derecho español, los datos que recaben o que solamente puedan ser recabados por las Fuerzas y Cuerpos de Seguridad del Estado en el ejercicio de sus competencias con las finalidades previstas en el artículo 1 de la Directiva UE 2016/680, podrán ser utilizadas con fines científicos por las mismas, que tendrán la condición de responsables en todo caso, sin perjuicio de que otras entidades puedan actuar como encargadas del tratamiento respecto de tales datos.

III

Respecto a las obligaciones que incumben al responsable del tratamiento sujeto a la normativa española durante la vigencia de la Directiva 95/46 debe hacerse referencia a las establecidas por la Ley Orgánica 15/1999 y a las exigibles a partir de 25 de mayo de 2018, fecha en que entró en vigor el Reglamento UE 2016/679 para aquellos tratamientos sujetos al mismo y en su caso las que pudieran derivar de la Directiva (UE) 2016/680 en lo que sea directamente aplicable.

-En primer lugar, 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 (Reglamento general de protección de datos) obliga 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 responsable o responsables dieran 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. De la misma manera, el artículo 24 de la Directiva (UE) 2016/680 prevé la existencia de un registro de actividades de tratamiento llevadas a cabo bajo su responsabilidad.

Igualmente la Directiva (UE) 2016/680 establece la obligación de responsables de conservar un registro de todas las categorías de datos personales efectuadas bajo su responsabilidad y la obligación de los encargados de tratamiento de llevar un registro de todas las categorías de actividades de tratamiento de datos personales efectuadas en nombre del responsable.

-En segundo lugar, debe recordarse que el 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 encuentre debidamente legitimado. Debe así examinarse la legitimación de dicho tratamiento en el marco de la Ley Orgánica 15/1999, distinguiendo los supuestos en que es preciso el consentimiento del interesado de aquellos en que la legitimación puede ser otra de las previstas en dicha norma



El artículo 6 de la Ley Orgánica 15/1999 prevé al respecto que *“El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.”* Por otra parte, conforme al principio de finalidad, establecido en el artículo 4.2 de la misma norma *“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 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 para una finalidad distinta a aquella para la que se obtuvo el consentimiento de los interesados o la prevista legalmente, sin obtener nuevamente el consentimiento del interesado o sin que dicho tratamiento se encontrase legitimado en alguno de los supuestos contenidos en el artículo 6 de la Ley Orgánica 15/1999. No obstante, el propio artículo 4.2 de la Ley Orgánica 15/1999 dispone en su último inciso que *“No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.”*

Ahora bien, como tiene declarado esta Agencia en sus informes, no todo proyecto que se intitule como histórico, estadístico o científico tiene tal consideración, debiendo analizarse detenidamente y de forma individualizada si efectivamente a la vista del ente que desarrolla el estudio o investigación, el fin del mismo y la proporcionalidad de la intromisión o limitación del derecho a la protección de datos que el estudio conlleve, el tratamiento de datos resultante se encuentra amparado por lo previsto en los preceptos transcritos.

Dichas consideraciones toman como punto de partida que un tratamiento o cesión de datos personales constituye una limitación del derecho fundamental a la protección de datos de carácter personal, derecho que persigue garantizar a las personas, como ha declarado el Tribunal Constitucional en su Sentencia 292/2000, *“el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado”*. Debe así recordarse que conforme al artículo 53.1 la Constitución Española cualquier restricción de un derecho fundamental está sometida al principio de reserva de Ley y debe cumplir los principios de justificación y proporcionalidad

De este modo, 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 sus 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.

Dicha conclusión se plasmó en el Reglamento de desarrollo de la Ley Orgánica 15/1999, que concreta en el segundo párrafo del artículo 9.1 el criterio que debe adoptarse para calificar la finalidad de un tratamiento como histórica, estadística o científica estableciendo que *“Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.”*

Por consiguiente, para considerar que el tratamiento ulterior de los datos a que la consulta se refiere pudiera considerarse legitimado en una finalidad estadística o científica sería preciso que el estudio objeto de consulta estuviese considerado como estadística de cumplimentación obligatoria a los efectos previstos en la Ley 12/1989 o en la correspondiente Ley de estadística autonómica. Similar criterio debe adoptarse respecto al sentido que debe darse al término científico que podría amparar una investigación realizada con tales datos, dicha materia 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. De modo equivalente cabría considerar como científico a los efectos del artículo 9 del Reglamento a una investigación enmarcada en alguno de los planes de investigación científica y técnica a que se refiere la vigente Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación o, en su caso, la correspondiente norma autonómica.

En cuanto a la legislación aplicable al presente caso, en que el consultante señala que el tratamiento de datos se lleva a cabo en el marco de un proyecto del programa Horizonte 2020, vendría constituida por el Reglamento UE (nº 1291/2013 del Parlamento Europeo y del Consejo de 11 de

diciembre de 2013 por el que se establece Horizonte 2020, Programa Marco de Investigación e Innovación (2014-2020 y por el que se deroga la Decisión n o 1982/2006/CE. Por consiguiente, tratándose de un proyecto de I+D financiado por la Comisión Europea a través del aludido Programa Marco de Investigación e Innovación, cabe considerar que el tratamiento de los datos personales con el objetivo de desarrollar nuevas herramientas TIC para uso de las Fuerzas y Cuerpos de Seguridad, en particular para detectar actividades online de financiación de grupos terroristas, la identificación de labores de propaganda y la detección de labores de reclutamiento y desinformación llevada cabo por estos grupos, puede ser calificado como uso de investigación científica a los efectos de encontrarse legitimado en lo previsto en la Ley Orgánica 15/1999.

Esta interpretación que permitiría el uso científico de los datos recogidos o que solamente puedan ser recogidos en el ejercicio de sus competencias por la autoridad competente (en el presente supuesto las fuerzas y cuerpos de seguridad en el marco de las investigaciones de terrorismo) por la misma, viene expresamente prevista, como se ha señalado anteriormente, en el artículo 4 de la Directiva (UE) 2016/680, cuando tal investigación venga referida a los fines establecidos en el artículo 1.1 de la dicha norma.

En aquellos supuestos de otros tratamientos efectuados en el proyecto en que la legitimación se encuentra en el consentimiento del interesado, por ejemplo el tratamiento de los datos personales de los expertos que voluntariamente intervienen en el proyecto, corresponde al responsable recabar el mismo. Conforme a lo establecido en el artículo 3.h) de la Ley Orgánica, el consentimiento debe reunir 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) y se le indique la posibilidad de ejercer los derechos a que se refiere la letra d) de dicho precepto. Asimismo debe indicarse quienes son los posibles destinatarios de la información (en el presente supuesto, a título de ejemplo, otros socios del proyecto, 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 automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

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.

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.”*

Tales medidas se regulan 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. En lo que respecta a los datos especialmente protegidos, esto es, aquellos a los que se refiere el artículo 7 de la Ley Orgánica 15/1999 debe tenerse en cuenta que el artículo 81.3 de su Reglamento de desarrollo dispone que *“Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:*

- a) *Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. “*

Tales medidas continúan resultando de aplicación a los tratamientos de datos que deban sujetarse a la Directiva (UE) 2016/680, si bien debe tenerse en cuenta que dicha norma contempla en su artículo 29 un conjunto de medidas de seguridad de los tratamientos que deberán ser tenidas en cuenta por los responsables de los ficheros. Debe recordarse en este sentido 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.

En lo que respecta a los tratamientos a los que a partir de 25 de mayo de 2018 se aplique el Reglamento (UE) 2016/679, debe tenerse en cuenta que éste 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 (UE) 2016/679, 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 (UE) 2016/679 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.”

IV

El artículo 3.i) de la Ley Orgánica 15/1999 define en su artículo 3.i) la cesión de datos como *“toda Toda revelación de datos realizada a una persona distinta del interesado”*. De este modo si alguna de las entidades participantes en el proyecto sujeta a dicha norma efectúa una comunicación de los datos personales objeto de tratamiento en el proyecto a terceros, incluidas cualquiera las demás entidades que participan en el mismo o procediesen a su difusión por cualquier procedimiento, dicha comunicación o difusión constituirá una cesión de datos personales.

Tal cesión debe 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 legítimas 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.

No obstante, los datos especialmente protegidos se encuentran sujetos al régimen especial establecido en el artículo 7, números 2 y 3 de la citada Ley Orgánica, según la cual

“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.”

En lo que respecta a los tratamientos de datos que a partir de 25 de mayo de 2018 deban regirse por el Reglamento UE 2016/679, debe tenerse en cuenta que tal comunicación debe igualmente encontrarse legitimada en alguno de los supuestos contemplados en su artículo 6.1 cuya letra a) contempla igualmente el consentimiento del interesado para el tratamiento de sus datos con uno o varios fines específicos.

No obstante, en lo que respecta a posibles comunicaciones a otras entidades participantes en el proyecto, cabe recordar la posibilidad de que puedan actuar en condición de encargados del tratamiento del responsable, en tal caso no será preciso el consentimiento del interesado, en tanto no se produce una cesión de datos. 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.”*

En el marco del derecho español, para que la relación entre responsable y encargado del tratamiento pueda darse y se ajuste a la Ley, es preciso que se cumplan los requisitos expresados en el artículo 12 de la Ley Orgánica 15/1999, considerando los siguientes aspectos:

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 artículos 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.

En el caso de los tratamientos que a partir de 25 de mayo de 2018 estén sujetos a lo previsto en el Reglamento UE 2016/679, si el responsable establecido en España tuviese uno o varios encargados del tratamiento, debe tenerse en cuenta que dicho Reglamento impone mayores obligaciones al encargado del tratamiento que las establecidas en la Ley Orgánica 15/1999. A efectos de determinar si los contratos existentes con anterioridad a dicha norma deben ajustarse a lo previsto en el Reglamento, habrá que estar a lo que se disponga en la normativa de desarrollo del mismo una vez se apruebe esta.

V

Debe tenerse en cuenta que todo tratamiento de datos debe ser respetuoso de los principios propios de materia de protección de datos. La Ley Orgánica 15/1999 regula tales principios en su artículo 4, bajo el título de calidad de datos. A tales principios se refiere también el artículo 4 de la Directiva 2016/680 y el artículo 5 del Reglamento UE 2016/679.

De tales principios, debe destacarse el relativo a la proporcionalidad que se encuentra vinculado al de finalidad, establece a este respecto el artículo 4.1 de la Ley Orgánica 15/1999 que *“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 podrán tratarse aquéllos datos que sean precisos para llevar a cabo las actividades objeto del proyecto. Este principio se refuerza tanto en La Directiva (UE) 2016/680 como en el Reglamento UE 2016/679 al ponerse tal principio, denominado en esta última norma “minimización de datos” en directa relación con las exigencias de privacidad por defecto y desde el diseño.

Debe igualmente hacerse referencia al principio de exactitud que conforme al artículo 4 de la 3 de la Ley Orgánica determina que los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. En el diseño de las herramientas TIC objeto del proyecto que se consulta, dicho principio cobra especial relevancia ya que el tratamiento genera especiales riesgos para aquellas personas que queden o puedan quedar incluidas en las categorías de sospechosos.

Igualmente, dentro de los principios de calidad debe hacerse referencia al principio de conservación de los datos. El artículo 4.5 de la Ley Orgánica 15/1999 dispone 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.”

Por consiguiente, los datos personales objeto de tratamiento 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 las finalidades del proyecto objeto de consulta.

Debe tenerse en cuenta, respecto de los tratamientos sujetos a lo previsto en la Ley Orgánica 15/1999 que la cancelación de los datos no supone la eliminación automática del dato, sino su bloqueo tal y como determina el artículo 16.3 de dicha Ley al establecer que *“La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.”*



El Reglamento de desarrollo de la Ley Orgánica 15/1999, define en su artículo 5.1. b) la cancelación como *“Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.”*

En definitiva, el bloqueo consiste en que se impida el acceso a los datos por las personas que, en el marco de un tratamiento legítimo venían llevando éste a cabo, puesto que en el momento en que deba procederse a la cancelación de los mismos, sólo resultará lícita su utilización para su puesta a disposición de las Administraciones Públicas, Jueces y Tribunales y con la única finalidad de atender a responsabilidades surgidas del tratamiento de datos. Así, esta Agencia entiende que para ello resulta preciso restringir el acceso a dichos datos, por cualquier procedimiento apto para conseguir ese resultado, a una persona con responsabilidad dentro de la organización del responsable.

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.

Cuestión distinta es el mantenimiento de los datos que hayan sido aportados por el responsable, esto es las Fuerzas y Cuerpos de Seguridad en el caso de los datos recabados con fines de prevención o investigación de actividades terroristas, en sus propios ficheros destinados a tales finalidades, conservación que estará sujeta a las normas reguladoras de la materia.

VI

Por último debe hacerse referencia a las nuevas exigencias que comporta la Directiva (UE) 2016/680, en particular a los principios de protección de datos desde el diseño y por defecto, y a la realización de evaluaciones de impacto relativas a la protección de datos.

Tales exigencias tienen especial relevancia en el marco de los tratamientos que se pretenden llevar a cabo teniendo en cuenta que objeto del proyecto es diseñar herramientas TIC de uso para las fuerzas y cuerpos de seguridad, que se basan en obtener datos de diversas fuentes, en particular datos obtenidos de internet, se van a utilizar técnicas de minería de datos y perfilado y se van a tratar categorías especiales de datos (así entre otros ideología o creencias, origen racial o étnico, opiniones políticas o datos biométricos). Tales tratamientos generan riesgos y amenazas para la protección de datos personales como la posible estigmatización de personas pertenecientes a ciertos grupos, el riesgo de inexactitudes que den lugar a falsos negativos o falsos positivos, el tratamiento de datos personales de personas no sospechosas etc, que exigen que la concepción de las herramientas a utilizar respondan a los principios de protección de datos desde el diseño y por defecto.

En este sentido, el artículo 20 de la Directiva (UE) 2016/680 relativo a la protección de datos desde el diseño y por defecto establece lo siguiente.

“1.Los Estados miembros dispondrán que el responsable del tratamiento, teniendo en cuenta el estado de la técnica y el coste de la aplicación, y 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 planteados por el tratamiento, aplique, tanto en el momento de determinar los medios para el tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas, como por ejemplo la seudonimización, concebidas para aplicar los principios de protección de datos, como por ejemplo la minimización de datos, de forma efectiva y para integrar las garantías necesarias en el tratamiento, de tal manera que este cumpla los requisitos de la presente Directiva y se protejan los derechos de los interesados.

2 .Los Estados miembros dispondrán que el responsable del tratamiento aplique las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad. En concreto, tales medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin intervención de la persona, a un número indeterminado de personas físicas.”

De este modo, tal y como señala dicho artículo debe tenerse en cuenta la necesidad de incorporar las medidas de seguridad a adoptar, teniendo en cuenta las exigidas en la Directiva 2016/680, y las relativas entre ellas y en la medida de lo posible a la seudonimización de los datos. Muy en particular debe tenerse en cuenta el principio de minimización de datos, recogido en la letra c) del artículo 4 de la misma, exigiendo que los datos tratados sean *“adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados”*



La evaluación de impacto relativa a la protección de datos viene regulada en el artículo 27 de la citada Directiva (UE) 2016/680, según el cual *“1.Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, los Estados miembros dispondrán que el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.*

2.La evaluación mencionada en el apartado 1 incluirá, como mínimo, una descripción general de las operaciones de tratamiento previstas, una evaluación de los riesgos para los derechos y libertades de los interesados, las medidas contempladas para hacer frente a estos riesgos, y las garantías, medidas de seguridad y mecanismos destinados a garantizar la protección de los datos personales y a demostrar la conformidad con la presente Directiva, teniendo en cuenta los derechos e intereses legítimos de los interesados y las demás personas afectadas.”

En lo que al presente supuesto respecta, en la documentación aportada se señala que se tienen en cuenta los principios relativos a la protección de datos desde el diseño y por defecto y se va a llevar a cabo una evaluación de impacto. Por otra parte, debe valorarse positivamente que se establezcan mecanismos para evitar o limitar las posibilidades de que se produzcan falsos positivos.