N/REF: 005033/2017

Se consulta si resulta conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la utilización de imágenes captadas en grabaciones de videovigilancia durante simulacros de emergencia para la realización de un estudio de seguridad en caso de incendios y cómo debe actuarse para adecuar los tratamientos a lo previsto en dicha norma.

Según señala el estudio tiene dos fases, una primera en la que se quiere disponer de imágenes para comprobar la validez de un modelo de toma de datos biométrico que permita ubicar personas en distintos momentos y posiciones en el edificio para evaluar los tiempos de evacuación de cada uno de ellos, precisando para ello modelos reales para probar las bondades de la herramienta. En una segunda fase se evaluarían diferentes variables de sujetos voluntarios. Se consulta si es posible la cesión de imágenes captadas con cámaras de videovigilancia durante simulacros de emergencia para la investigación académica a efectuar y si es suficiente para ello la autorización del propietario del edificio. En la segunda fase se solicitará la autorización de los sujetos para recoger datos físicos y hábitos para definir a través de las imágenes de un simulacro una correlación entre sus características y los resultados obtenidos. El resultado global será anónimo y se transformará en un gráfico en función de la pirámide de población.

I

Los artículos 1 y 2 de la Ley Orgánica 15/1999 extienden su protección a los derechos de los ciudadanos en lo que se refiere al tratamiento automatizado 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, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa 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 tiene su origen en la contenida en la Directiva 95/46/CE de 24 de octubre de 1995 del Parlamento Europeo y del Consejo 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, cuyo artículo 2.a) define los

datos personales como "*toda información sobre una persona física identificada o identificable (en "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.*"

Conforme a tales definiciones, la imagen de una persona identificada o identificable constituye un dato personal, cuyo tratamiento se encuentra sujeto a las previsiones de la Ley Orgánica 15/1999. En este sentido se pronuncia 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 02/2012 sobre reconocimiento facial en los servicios en línea y Móviles al hacer referencia a las imágenes digitales como datos personales señalando 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."*

Esta circunstancia reviste especial interés en el presente supuesto, toda vez que si se aplica un proceso de disociación a las imágenes de modo que no pueda identificarse a las personas, ya sea mediante el pixelado de las fotos o cualquier otro sistema que impida irreversiblemente su identificación no resultaría de aplicación la normativa de protección de datos. De este modo, si se efectúa un proceso que impida distinguir el rostro de las personas con carácter previo a su comunicación por parte del responsable no nos encontraríamos ante una cesión de datos ni ante un tratamiento ulterior de los mismos, quedando excluida la aplicación de la normativa de protección de datos.

Por otra parte, debe aquí hacerse una referencia al concepto de responsable del fichero o tratamiento, la Ley Orgánica 15/1999 define 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 de desarrollo de dicha Ley, aprobado por Real Decreto 1720/2007, de 21 de diciembre, precisa en su artículo 5.1.q) dicha definición, estableciendo que será responsable del

fichero o tratamiento la *"Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente."*

Cabe así señalar, con carácter general, que la condición de responsable del fichero es consecuencia del hecho de que un ente o, en su caso, una persona física, debidamente legitimada conforme a lo previsto en el artículo 6 de la Ley Orgánica 15/1999, haya decidido tratar datos personales para sus propios fines, correspondiéndole por ello asumir la responsabilidad del cumplimiento de las normas sobre protección de datos. En el presente supuesto tendrán la condición de responsables de los ficheros de videovigilancia, quienes hayan determinado la instalación de un sistema de tal carácter en el edificio, ya sea un único propietario del mismo o una comunidad de propietarios.

Asimismo, debe tenerse en cuenta que el artículo 11.5 de la Ley Orgánica 15/1999 dispone que "*Aquel a quien se comuniquen los datos de carácter personal se obliga por el solo hecho de la comunicación a la observancia de las disposiciones de la presente Ley."* Ello determina que quien recibe los datos deviene responsable del fichero o del tratamiento de datos que efectúe y estará sujeto a los deberes que impone la normativa de protección de datos y a las responsabilidades que de la misma deriven.

En el caso presente no resulta claro si el cesionario de los datos será el propio consultante o la Universidad que colabora en el proyecto. Si el cesionario fuese el propio consultante, este resultaría responsable de los datos que le han sido comunicados y el acceso a tales datos por parte de la Universidad vendría a constituir igualmente una cesión de datos, efectuada esta vez por el consultante, cesión que debe encontrarse legitimada en lo previsto en la normativa de protección de datos y que convertiría a la Universidad en responsable respecto de los datos que le han sido comunicados.

De la misma manera si los datos se ceden por el responsable del fichero de videovigilancia a la Universidad, el acceso a éstos por el consultante (que parece no formar parte del personal de la Universidad, sino simplemente colaborar con ella para la realización del estudio objeto de consulta) sería igualmente una cesión de datos que aquélla efectúa al consultante y que

requiere también la correspondiente legitimación conforme a lo dispuesto en la normativa de protección de datos. Igualmente, el consultante devendría responsable del fichero o tratamiento de los datos personales que le han sido cedidos.

II

En el presente supuesto, se pretende, en la primera fase del estudio, la utilización de las imágenes captadas con fines de videovigilancia en diversos edificios durante simulacros de emergencia para validar un modelo de toma de datos biométricos que permita ubicar a las personas en distintos momentos y posiciones en el recinto para evaluar los tiempos de evacuación de cada uno de ellos, consultándose si es suficiente la autorización del propietario del edificio para la utilización de las imágenes.

Debe en primer lugar tenerse en cuenta que la entrega de las grabaciones de videovigilancia, si a tales imágenes no se les ha aplicado un proceso de disociación que impida la identificación de las personas, constituye una cesión de datos, definida por el artículo 3 i) de dicha Ley como "*Toda revelación de datos realizada a una persona distinta del interesado".*

El artículo 11 de la Ley Orgánica 15/1999 determina el régimen general de comunicación de datos de carácter personal, estableciendo 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. No obstante, la propia Ley Orgánica 15/1999 contempla diversas excepciones a la necesidad de obtener el consentimiento, señaladamente las contenidas en su artículo 11.2.

Así pues solamente sería conforme a lo establecido en la Ley Orgánica 15/1999 la comunicación de los datos contenidos en los ficheros de videovigilancia si se obtuviese previamente el consentimiento de todas y cada una de las personas que aparecen en las imágenes grabadas con las cámaras o resulta de aplicación alguna de las causas habilitadoras de dicha comunicación recogidas en la Ley Orgánica 15/1999, sin que pueda suplir el

consentimiento de los afectados la autorización del propietario del edificio o de cualquier otra persona o entidad que resulte responsable del fichero de videovigilancia, por el contrario, en su calidad de responsable debe velar porque tales datos no se comuniquen a terceros si no es con las garantías exigidas por la citada Ley Orgánica 15/1999, produciéndose en otro caso una infracción de lo previsto en dicha norma.

Dada la dificultad de recabar el consentimiento de los afectados en el presente caso debe analizarse si dicha comunicación de datos puede encontrarse legitimada en alguno de los supuestos habilitadores de tal cesión previstos en la Ley Orgánica 15/1999.

Debe así partirse de que el artículo 4 de la Ley Orgánica 15/1999 consagra el principio de finalidad en el tratamiento de los datos disponiendo que "*Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos."* 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*."

En este mismo sentido dispone el Reglamento de desarrollo de la Ley Orgánica 15/1999 en su artículo 8.3 que *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos*", mientras que el artículo 9.1 prevé que "*No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos*."

Ahora bien, el Reglamento de desarrollo de la Ley Orgánica 15/1999, concreta en el segundo párrafo de su 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 el presente supuesto, la consulta no hace referencia alguna a la inclusión del estudio que se pretende llevar a cabo en alguno de los planes a que anteriormente se ha hecho referencia y que podrían legitimar el tratamiento de datos en una finalidad estadística o científica en los términos del artículo 9 del Reglamento de desarrollo de la Ley Orgánica 15/1999.

No obstante, teniendo en cuenta la finalidad del estudio cabe analizar si la comunicación de datos por parte de los diferentes responsables y el tratamiento ulterior de los mismos por el consultante y la Universidad con la que colabora podrían venir legitimados en lo previsto en el artículo 7.f de la Directiva 95/46/CE, según el cual *"los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si (…) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva"*. En este sentido, es preciso recordar que la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 ha venido a reconocer el efecto directo de la mencionada disposición de la Directiva, lo que, en caso de resultar aplicable al caso,

permitiría la cesión y el ulterior tratamiento de los datos sin contar con el consentimiento de los afectados.

Tal y como recuerda la Sentencia del Tribunal de Justicia de la Unión Europea en su apartado 38, el artículo 7 f) de la *Directiva "establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado"* y, en relación con la citada ponderación, el apartado 40 recuerda que la misma *"dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado".*

Por este motivo, la sentencia señala en su apartado 46 que los Estados miembros, a la hora de adaptar su ordenamiento jurídico a la Directiva 95/46, deberán *"procurar basarse en una interpretación de ésta que les permita garantizar un justo equilibrio entre los distintos derechos y libertades fundamentales protegidos por el ordenamiento jurídico de la Unión*", por lo que, conforme a su apartado 47 "*nada se opone a que, en ejercicio del margen de apreciación que les confiere el artículo 5 de la Directiva 95/46, los Estados miembros establezcan los principios que deben regir dicha ponderación".*

Por tanto, para determinar si procedería la aplicación del citado precepto habrá de aplicarse la regla de ponderación prevista en el mismo; es decir, será necesario valorar si en el supuesto concreto objeto de análisis existirá un interés legítimo perseguido por el responsable del tratamiento que prevalezca sobre el interés o los derechos y libertades fundamentales de los interesado que requieran protección conforme a lo dispuesto en el artículo 1 de la Ley Orgánica 15/1999, según el cual "*la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*" o si, por el contrario, dichos derechos fundamentales o intereses de los afectados por el tratamiento de los datos de carácter personal han de prevalecer sobre el interés legítimo en que el responsable pretende fundamentar dicho tratamiento.

Para determinar si existe un interés legítimo, debe acudirse en primer lugar a la finalidad del tratamiento, que en el presente supuesto, según señala la consulta es desarrollar un sistema que permita realizar una toma de datos a través de imágenes grabadas y comprobar la validez del modelo de toma de datos biométrico que permita ubicar personas en distintos momentos y posiciones en el recinto para evaluar la evacuación de cada uno de ellos en el marco de un estudio con fines de seguridad en caso de incendio, finalidad ésta que a juicio de esta Agencia constituye un interés legítimo, cuyos resultados pueden además redundar en una mayor seguridad de los usuarios de los edificios objeto del estudio.

Ahora bien, debe tenerse en cuenta que el artículo 7.f de la Directiva exige una ponderación entre el interés legítimo del responsable y los derechos fundamentales afectados, no es suficiente con apreciar la concurrencia de un interés legítimo en el responsable del tratamiento, sino que, además, la intromisión en los derechos de los afectados debe resulte proporcional, prevaleciendo, en otro caso, dichos derechos fundamentales sobre el interés legítimo que pudiera tener el responsable.

A efectos de considerar dicha proporcionalidad, cabe tener en cuenta que aunque la consulta no lo indique expresamente, parece desprenderse de ella que las imágenes serían utilizadas únicamente para los fines mencionados y que con ellos no se pretende identificar a las personas que aparecen en las grabaciones, ni efectuar seguimiento alguno de las mismas.. No obstante, esta Agencia considera necesario que se introduzcan garantías reforzadas del cumplimiento de los principios contenidos en la legislación de protección de datos que permitan entender que el perjuicio de los derechos de los interesados se verá disminuido como consecuencia de la comunicación y tratamiento de los datos objeto de consulta, para poder entender prevalente el interés legítimo del consultante sobre los derechos de los afectados por la cesión y tratamiento ulterior de los datos.

El consultante no hace referencia alguna a cuales podrían ser dichas garantías, no obstante, cabe señalar, a título orientativo y sin perjuicio de que por el consultante se añadan otras, las siguientes:

La información a los posibles afectados, por parte del cedente con carácter previo a la cesión, de que los datos grabados con motivo del simulacro

van a ser cedidos a un tercero con la finalidad de llevar a cabo un estudio de seguridad, permitiendo a los afectados oponerse a dicha comunicación.

El compromiso por parte del cesionario o cesionarios de utilizar los datos cedidos exclusivamente para los fines precisos para el estudio que se pretende llevar a cabo, sin que se utilicen ulteriormente para ninguna otra finalidad, ni se comuniquen a terceros distintos de los que participan en el estudio (consultante y universidad) ni siquiera para su conservación.

El establecimiento de un plazo máximo de conservación de las imágenes por el cesionario que resulte adecuado a la finalidad del estudio, de modo que una vez transcurrido dicho plazo se proceda a la cancelación de las imágenes.

El compromiso de los cesionarios de destruir datos una vez haya transcurrido el período durante el cual los datos deben mantenerse bloqueados, o proceder a su disociación de modo que no pueda identificarse a las personas, aportando en su caso el correspondiente certificado de destrucción de los datos o garantía suficiente de que se ha llevado a cabo un proceso de disociación de los datos.

Por último, aunque las medidas de seguridad a aplicar en el presente supuesto son las de nivel básico, cabe reforzar las mismas aplicando otras distintas a las que con carácter obligatorio vienen recogidas en el Reglamento de desarrollo de la Ley Orgánica 15/1999.

De este modo, en la medida en que se ofrezcan estas garantías, que pueden documentarse en un acuerdo entre cedente y cesionarios, cabría considerar en el presente caso que prevalecería el interés legítimo del responsable del tratamiento en llevar a cabo la actividad objeto de consulta frente al derecho a la protección de datos de los posibles afectados por el tratamiento.

III

En lo que respecta a la segunda fase del estudio, se señala que se utilizarán datos de sujetos que voluntariamente participen en el mismo, de este modo el responsable del estudio deberá recabar de las personas físicas que vayan a participar en el mismo, su consentimiento para el tratamiento de sus datos personales, consentimiento que deberá reunir las características de

"libre, inequívoco, específico e informado" conforme a lo previsto en el artículo 3.h) de la Ley Orgánica 15/1999.

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".*

Debe, además, tenerse en cuenta que tanto la prestación del consentimiento como el cumplimiento del deber de información deberán poder ser acreditados por el responsable del fichero. Dispone a estos efectos el artículo 12.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, que "*corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.*" De la misma manera, corresponde al responsable del fichero acreditar que ha dado cumplimiento al deber de información, si bien tras la anulación de lo previsto en el artículo 18 del Reglamento de desarrollo de la Ley Orgánica 15/1999 por Sentencia de 15 de julio de 2010 del Tribunal Supremo, debe entenderse que rige la libertad de forma para acreditar el cumplimiento de la misma, de modo que el responsable podrá demostrar por cualquier medio de prueba admisible en derecho el cumplimiento del deber de informar exigido por el artículo 5 de la Ley Orgánica 15/1999.

Por último, debe recordarse que el consentimiento prestado siempre es 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.

IV

El responsable o responsables del fichero deben además dar cumplimiento a las restantes obligaciones establecidas en la Ley Orgánica 15/1999 de las que cabe destacar las siguientes.

-Deberá notificarse la creación del fichero a efectos de su inscripción en el Registro General de Protección de Datos de esta Agencia. Debe así tenerse en cuenta que, en cumplimiento de lo previsto en el artículo 26 de la Ley orgánica 15/1999 y 55 de su Reglamento de desarrollo, los ficheros que contienen datos de carácter personal deben ser notificados a la Agencia Española de Protección de datos, con carácter previo a su creación, para su inscripción en el Registro General de Protección de Datos. Dicha notificación deberá contener los requisitos indicados en el citado artículo 55 del Reglamento, pudiendo llevarse a cabo a través del sistema de notificaciones automáticas de la Agencia Española de Protección de Datos (NOTA), disponible en su página web (www.agpd.es).

-En segundo lugar será preciso implantar en los ficheros creados las medidas de seguridad establecidas en el Reglamento de desarrollo de la Ley Orgánica 15/1999.

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.

Debe igualmente hacerse una referencia a la regulación que en materia de medidas de seguridad será aplicable a partir del 25 de mayo de 2018, fecha en la que resultará aplicable 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 y por el que se deroga la Directiva 95/46/CE

(Reglamento general de protección de datos), norma que sustituirá a la actualmente vigente en la materia, en tanto que dicho Reglamento (UE) 2016/679 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 de un fichero debe implementar.

Señala el considerando 83 del Reglamento General de Protección de datos 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."*

Y en su artículo 32, 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, una vez resulte de aplicación el Reglamento (UE) 2016/679, incumbirá 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."

- Debe además recordarse que todo tratamiento de datos debe ser respetuoso de los principios relativos a la calidad de los datos consagrados en el artículo 4 de la Ley Orgánica 15/1999, debiendo destacarse en particular el denominado principio de finalidad, al que ya se ha hecho referencia anteriormente, 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.

La limitación de la finalidad está vinculada al principio de proporcionalidad, contenido en el número primero del citado artículo 4 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 estudio.

- 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 que hayan sido cedidos al responsable del fichero, en la forma vista anteriormente en el presente informe o éstos hayan recabado con el consentimiento de los interesados no podrán mantenerse indefinidamente en los ficheros del responsable, debiendo cancelarse una vez que dichos datos dejen de ser necesarios para la finalidad para la cual fueron obtenidos. No obstante la cancelación no determina la destrucción de los datos, el artículo 16.3 de la Ley Orgánica 15/1999 dispone 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."*

Por su parte el Reglamento de desarrollo de la Ley Orgánica 15/1999 determina cómo debe llevarse a cabo el bloqueo en su artículo 5.1. b) al definir la cancelación como el "*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 cuanto a cuáles son los plazos de prescripción de responsabilidades, esta Agencia se ha pronunciado en diversas ocasiones señalando en informe de 1 de agosto de 2005 que "En lo atinente a la determinación de los períodos

en que el dato habrá de permanecer bloqueado, en relación con lo dispuesto en el artículo 16.3, resulta imposible establecer una enumeración taxativa de los mismos, debiendo, fundamentalmente, tenerse en cuenta, como ya se ha indicado con anterioridad, los plazos de prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al consultante con su cliente, así como los derivados de la normativa tributaria o el plazo de prescripción de tres años, previsto en el artículo 47.1 de la propia Ley Orgánica 15/1999 en relación con las conductas constitutivas de infracción muy grave."

En cuanto a la forma de llevar a cabo el bloqueo, este consiste, en definitiva, en que se impida el acceso a los datos al personal que habitualmente estuviera autorizado a tal acceso para el desempeño de sus funciones, 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 que se limite el acceso a los datos de modo que solamente pueda ser efectuado por alguna persona con responsabilidad dentro de la organización del responsable cuando ello sea necesario para dar respuesta a requerimientos judiciales o administrativos.

- Debe asimismo tenerse en cuenta que el responsable se encuentra sujeto a un deber de secreto respecto de los datos que trate conforme a lo establecido en el artículo 10 de la Ley Orgánica 15/1999, según el cual "*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*" y que entre sus obligaciones se encuentra también la de dar adecuada respuesta en la forma prevista en los artículos 15 y siguientes de la Ley Orgánica 15/1999 y concordantes de su Reglamento de desarrollo, a los supuestos de ejercicio de los derechos de acceso, rectificación y cancelación y oposición.