



N/REF: 168980/2018

I

La consulta plantea la posibilidad de implementar, desde el punto de vista de la normativa de protección de datos personales, el ya mencionado "Proyecto de sistema inteligente de monitorización y gestión de los núcleos de radicalización violenta", que, de acuerdo con la descripción que se contiene en la memoria que acompaña la consulta, consistiría en esencia en el establecimiento de una estructura funcional por niveles, básicamente reiterada a nivel de cada municipio, cuyo objeto sería "aprehender el conocimiento sobre casos de radicalización a los que se puede tener acceso", mediante la elevación a diferentes niveles de la información que en un primer nivel de contacto con la realidad social pudieran tener conocimiento quienes ocupen dicho primer nivel, que serían, de acuerdo con la memoria, "profesionales pertenecientes a distintas áreas administrativas, como puede ser asistencia social, nivel educativo, laboral, sanitario etc.". Se trataría, en definitiva, de personas integradas en una primera organización en un nivel de contacto primario, a los cuales podría llegar el conocimiento o determinados indicios, síntomas o información de una posible radicalización. Un segundo nivel o escalón estaría formado por los responsables de las áreas concretas de intervención en las que dicho profesional se encontraría integrado: así, asistencia social, sanidad, educación, a quienes las personas participantes como primer escalón transmitirían la información que pudiera ser susceptible de denotar la radicalización de un individuo. A continuación, un tercer escalón, que se denominaría "Grupo Local", estaría "formado por los responsables de gestionar las informaciones, conocimientos y acciones, en aras de la minimización de la conflictividad social en el ámbito de la radicalización violenta", y estaría "especializado por ámbito y tema concreto, *realizando su labor de coordinación entre distintas áreas con los responsables y coordinadores del Sistema en el CITCO*". Por último, y en el nivel superior se encontraría el CITCO, como "*encargado de dinamizar, coordinar e impulsar las acciones de lucha contra la radicalización violenta desde el ámbito nacional al local*".

Desde el punto de vista de la gestión técnica, este sistema comportaría la “creación de una plataforma con tecnología web donde plasmar los distintos escalones de la estructura funcional”. El portal web “sería la interfaz de gestión de una base de datos, accesible mediante internet. La citada base de datos sería *gestionada* técnicamente y administrativamente *por personal del CITCO*, Área de Estrategia y Prospectiva y Servicio de Informática”. La unidad básica de recogida de informaciones sería la “Ficha Básica” (información de un hecho concreto). Esta Ficha, en la inmensa mayoría de los casos, sería creada por aquellos *usuarios de primer nivel* que se encuentran en contacto directo con las primeras capas sociales susceptibles de radicalización. La identificación y autenticación de los distintos usuarios integrados en los diversos escalones de la estructura funcional se realizaría mediante su acceso al Portal Web utilizando, por un lado, la tecnología de firma electrónica de su DNI electrónico y, por otro, un nombre de usuario y una contraseña única. A dicha Ficha Básica podrían tener acceso, según se expone, los diferentes estratos implicados, pero corresponde a los distintos niveles determinar quién puede acceder a ellas. Desde el CITCO se impulsará la creación de Grupos Locales; sus miembros serán coordinados por un máximo responsable del área municipal donde se vaya a desplegar. Habrá un miembro del Grupo Local perteneciente a las Fuerzas y cuerpos de Seguridad del Estado (FCSE), que será designado por el responsable policial en cuya demarcación se encuentre el municipio o el grupo de municipios que se mancomune.

Un mayor desarrollo de esta política, y del sistema previsto, se contiene, fuera ya de la documentación aportada junto con la consulta, en la documentación oficial contenida en la página web del Ministerio del Interior. En ella se expone detenidamente el denominado “plan estratégico nacional de lucha contra la radicalización violenta” (PEN-LCRV). El objetivo de este plan se centra en “constituir un instrumento eficaz de detección temprana y neutralización de los brotes y focos de radicalismo violento, actuando sobre aquellas comunidades, colectivos o individuos en situación de riesgo o vulnerabilidad”. Dentro del apartado “Aplicación del plan” se dice que *[l]a Administración: Es el actor responsable que asume la implementación del Plan. El PEN-LCRV distingue los diferentes niveles en la Administración. Un órgano único centralizado e interministerial, máximo responsable nacional, y grupos multisectoriales a nivel local, provincial y/o autonómico. Siguiendo los criterios marcados, el Estado actuará a través de los diferentes departamentos de la Administración General del Estado (AGE), estableciéndose una obligada*

colaboración del resto de administraciones. Serán coordinados por el ámbito de la seguridad pública estatal.

Una presentación desarrolla las líneas generales citadas; en ella, en su página 4, se contiene el “ámbito interno” (nacional) de actuación, de la siguiente manera: *1. INTERNO: Afecta a todo el territorio nacional. El municipio (Nivel local) es el escenario principal de actuación de este fenómeno. Para ello, el Plan diseña **Grupos Locales de Lucha Contra la Radicalización Violenta** coordinados por las Fuerzas de Seguridad en el ámbito local y que, bajo la supervisión del Grupo Nacional, integrarán al resto de sectores sociales locales para conocer, prevenir y tratar los focos detectados.*

En la página 5 se dice al respecto: *El Grupo Local está formado por representantes de la Policía Local, Policía Autonómica en su caso, Ayuntamiento, Juzgados, Centros Escolares, Asuntos Sociales, Entidades Sociales y Colectivos de Riesgo. Se diseña un sistema específico de intercambio de información entre la Administración Local y Central. Además, está previsto una conexión específica del Grupo Nacional con Instituciones Penitenciarias sobre el tratamiento de la radicalización de los internos.*

Incluso, en la página 9 se pone un ejemplo: *“FOCO DE RADICALIZACIÓN: Detectado el foco de radicalización en una barriada de una localidad, un miembro del Grupo Local expone el caso ante dicho Grupo quien, a su vez, informa al Grupo Nacional para estudiar el caso. El Grupo Nacional dará respuesta inmediata al Grupo Local quien, a su vez, informará de las medidas a ejecutar”.*

Esta estrategia, tal y como se expone en las políticas citadas, y confirma la doctrina (véase Fernández De Mosteyrín, L.M. y P. Limón López (2017): “Paradigmas y prevención del terrorismo: una aproximación al Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV 2015)”, Política y Sociedad, 54(3), pp. 805-827) proviene, en sus líneas generales, de los países de nuestro entorno, de la UE:

Desde mediados de los años 2000 numerosos países han desarrollado políticas similares. En concreto, el Reino Unido es uno de los países pioneros. También Dinamarca, Australia, Alemania, Holanda y EEUU. En todos ellos las claves conceptuales son bastante similares. Sin duda, el más avanzado y complejo, pero también el que más rica investigación

está produciendo es el programa británico PREVENT para la prevención de la radicalización que se inserta en la estrategia antiterrorista CONTEST19. Si bien el modelo español ha incorporado mecanismos derivados de la experiencia británica, el PEN-LRV se ampara en las indicaciones establecidas por la UE en materia de terrorismo. Y, por ello, tanto la expansión del objeto susceptible de radicalizarse como la propia estructura de la respuesta provienen del diagnóstico europeo.

Dicho artículo, en suma, y al igual que hace el PEN-LCRV, se deriva de la estrategia de seguridad y lucha contra el terrorismo, entendido en un sentido amplio.

*El marco normativo en el que cobra sentido el Plan tiene un carácter regional que parte de la EES [Estrategia Europea de Seguridad] (2003-2015). En ella se prescribe un modelo común y pone el corazón de la prevención del terrorismo en el proceso de radicalización. La ESN2013 [Estrategia de Seguridad Nacional] comporta un diagnóstico en el que la seguridad debe ser entendida como “garantía de bienestar de los ciudadanos y de la estabilidad del propio Estado” y para la que es esencial “promover la participación del ciudadano y la colaboración público-privada, así como de toda la Administración en los ámbitos de su competencia”. Por esto la seguridad es “una tarea de todos” (ESN, 2013: 1). **La respuesta estratégica al terrorismo** ha de orientarse a “neutralizar la amenaza que representa el terrorismo y reducir la vulnerabilidad de la sociedad ante sus ataques, haciendo frente a los procesos de radicalización que lo puedan preceder o sustentar” (2013: 39)22.*

II

Tal y como esta AEPD ha expuesto en el Informe 0097/2018:

Los tratamientos de datos por las autoridades judiciales y las fuerzas y cuerpos de seguridad para la investigación y prevención de delitos se rigen por 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 (Directiva 2016/680). Dicha directiva aún no ha sido transpuesta al derecho español, por lo que la disposición transitoria cuarta del proyecto de ley orgánica de protección de datos actualmente en tramitación parlamentaria en las Cortes establece que dichos tratamientos continuarán rigiéndose por la LOPD, y en particular por su artículo 22, y por sus disposiciones de desarrollo, en tanto no entre en vigor la norma que transponga al derecho español lo dispuesto en la citada directiva.

Respecto de los tratamientos de datos realizados por las fuerzas y cuerpos de seguridad le sería aplicable el art. 22 LOPD, y por lo tanto también seguiría siendo aplicable la doctrina sentada por esta Agencia en los informes (entre otros) 0133/2008 y 0297/2005, que, en esencia, dicen así:

“[...] deberán distinguirse aquellas actuaciones de la Policía Judicial que son llevadas a cabo en cumplimiento de un mandato judicial o de un requerimiento efectuado por el Ministerio Fiscal de aquéllas otras que se llevan a cabo por propia iniciativa o a instancia de su superior jerárquico.

Respecto de las primeras resulta aplicable el artículo 11.2 d) de la Ley Orgánica 15/1999, no requiriéndose el consentimiento del interesado a la cesión, por cuanto los efectivos de la Policía Judicial solicitantes de los datos no son sino meros transmisores de la solicitud efectuada por el Ministerio Fiscal o el Órgano Jurisdiccional, actuando éste en el cumplimiento de las funciones que le han sido legalmente atribuidas y siendo el propio Juzgado o Tribunal o el Ministerio Fiscal el destinatario de los datos cedidos, como exige el artículo referido.

El problema se plantea, sin embargo, en relación con aquellos supuestos en los que la Policía Judicial requiere la cesión de los datos con el fin de ejercitar las funciones de averiguación del delito y detención del responsable, al no existir en ese caso mandamiento judicial o requerimiento del Ministerio Fiscal que dé cobertura a la cesión.

En este caso nos encontramos, a nuestro juicio, ante el ejercicio por los efectivos de la Policía Judicial de funciones que, siéndoles expresamente reconocidas por sus disposiciones reguladoras, se identifican con las atribuidas, con carácter general, a todos los miembros de las Fuerzas y Cuerpos de Seguridad del Estado.

Resultará, en consecuencia, aplicable a este segundo supuesto lo dispuesto en el artículo 22.2 de la Ley Orgánica 15/1999, según el cual “La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad”

*El citado artículo habilita, a nuestro juicio, a los miembros de la Policía Judicial para la obtención y tratamiento de los datos requeridos, **lo que llevará aparejada la procedencia de la cesión instada**, siempre y cuando, como se indica en el informe de la Comisaría General de la Policía Judicial adjunto a la consulta y esta Agencia Española de Protección de Datos ha venido indicando reiteradamente, se cumplan las siguientes **condiciones**:*

- a) Que quede debidamente acreditado que la obtención de los datos resulta necesaria para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales y que, tratándose de datos especialmente protegidos, sean absolutamente necesarios para los fines de una investigación concreta.*
- b) Que se trate de una petición concreta y específica, al no ser compatible con lo señalado anteriormente el ejercicio de solicitudes masivas de datos.*
- c) Que la petición se efectúe con la debida motivación, que acredite su relación con los supuestos que se han expuesto.*

d) Que, en cumplimiento del artículo 22.4 de la Ley Orgánica 15/1999, los datos sean cancelados “cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento”.

Sobre la base de la doctrina general contenida en dichos Informes cabe hacer las siguientes consideraciones:

Desde el momento en que la ley (por ejemplo, artículos 261, 262, 2634 etc. de la Ley de Enjuiciamiento Criminal) establece no sólo la posibilidad de denunciar los delitos, sino incluso, en algunos casos, la obligación de hacerlo, el tratamiento de datos personales para dichos fines ha de considerarse lícito desde la perspectiva de la normativa de protección de datos personales. Ello conlleva que la cesión de dichos datos personales a las autoridades públicas correspondientes haya de considerarse un tratamiento de datos personales igualmente lícito.

Del mismo modo, el tratamiento de datos personales con la finalidad de prevención de delitos por parte de las autoridades públicas ha de considerarse lícito no sólo como consecuencia de la necesidad de ser receptor de las denuncias de los particulares en la forma establecida en la ley de enjuiciamiento criminal, sino que la ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, en su artículo 11, establece que [l]as Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones: f) *Prevenir* la comisión de actos delictivos, o h) *Captar, recibir y analizar cuantos datos tengan interés para el orden y la seguridad pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia.*

Ciertamente, el tratamiento de datos personales relacionados con el objeto de la Directiva (UE) 2016/68 (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, que incluye expresamente, como explicita su Considerando (11), (i) la protección y la prevención frente a las amenazas para la seguridad pública, y que (ii) entre dichas autoridades competentes no solo se deben incluir autoridades públicas tales como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad, sino *también cualquier otro organismo o entidad en que el Derecho*



del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de la presente Directiva), habrá de llevarse a cabo de conformidad con las garantías que para la protección de las personas físicas se establecen en la tan reiterada directiva 2016/680, y que mientras se promulga la normativa de transposición de la misma en el ordenamiento español, dicho tratamiento o habrá de llevarse a cabo de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y sus disposiciones de desarrollo, tal y como establece, lo que también se ha mencionado ya, la disposición transitoria cuarta de la nueva Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, (LOPDGDD) aprobada definitivamente por las Cortes Generales el 21 de noviembre de 2018, pero que a la fecha de redacción de este informe aún no había sido publicada en el Boletín Oficial del Estado.

Dicha remisión a la LOPD 1999 incluye expresamente, como recuerda la disposición transitoria cuarta citada de la LOPDGDD, el artículo 22 LOPD de la misma y sus disposiciones de desarrollo, por lo que habrá de estarse a lo establecido en dicho precepto, y a los demás de la LOPD en relación con los derechos de las personas cuyos datos personales son tratados para las finalidades legítimas expuestas, de acuerdo con la legislación aplicable hasta el momento hasta la promulgación de la normativa de transposición de la reiterada Directiva (UE) 2016/680.

III

Desde la perspectiva de la normativa de protección de datos personales, si examinamos el *Plan estratégico nacional de lucha contra la radicalización violenta. (PEN-LCRV) “Un marco para el respeto y el entendimiento común”*, aprobado mediante Acuerdo del Consejo de Ministros de 30 de enero de 2015, (<http://www.interior.gob.es/documents/642012/5179146/PLAN+ESTRAT%C3%89GICO+NACIONAL.pdf/d250d90e-99b5-4ec9-99a8-8cf896cb8c2f>) podemos concluir que en los tratamientos de datos derivados de dicho marco estratégico corresponde la posición de *responsable del tratamiento* al CITCO, Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, dependiente de la Secretaría de Estado de Seguridad, del Ministerio del Interior, ya que a este órgano corresponde la determinación, por sí sola, de los fines y medios del tratamiento de los datos personales. En efecto, así resulta del PEN-LCRV, puesto que, si bien el plan busca establecer una colaboración

con el resto de las administraciones públicas, la Administración General del Estado, a través de este órgano, es considerada por el plan como el coordinador de las actividades que contempla. Así, el PEN-LCRV le reserva al CITCO las funciones de (entre otras, en otros ámbitos -internacional etc.-) de [...] *coordinar, con carácter general y a nivel nacional, toda actividad de la Administración pública central en las áreas funcionales establecidas y frentes de acción. Se exceptúa la labor específica contemplada en el tercer frente de acción para las FCS. Se configurará como el punto focal de la Administración central en la coordinación con la Administración local. Coordinará toda actividad de los grupos locales, provinciales y autonómicos, multisectoriales, de lucha contra la radicalización violenta que se creen para el desarrollo de este Plan. Dispondrá de una visión global e integral del fenómeno de la radicalización violenta en España e informará periódicamente a las Autoridades nacionales competentes de su situación y evolución, proponiendo aquellas políticas o medidas a escala nacional que se consideren necesarias para favorecer la convivencia e integración social y la confianza en las instituciones democráticas.* Por otro lado, y tal y como se ha recogido ya al inicio de este informe, de la consulta se desprende que el sistema informático creado para la gestión de este sistema de información corresponde técnica y administrativamente al CITCO, por lo que se entiende que este es el responsable único del tratamiento.

A través de la colaboración con la Administración Local mediante los denominados en el plan Grupos Locales de lucha contra la radicalización violenta (GL-LCRV) se pretende conseguir la coordinación necesaria para involucración de la sociedad civil las tareas previstas por el plan. La naturaleza jurídica de dichos grupos no está determinada en el PEN-LCRV puesto que, véase su página 17, *[l]a constitución, participantes, competencias y protocolo de actuación de estos grupos será objeto de regulación administrativa y normativa concreta*, y no parece que dicha regulación administrativa o normativa haya sido promulgada; pero el propio PEN-LCRV prevé que servirá como base de desarrollo para dicha regulación las “*comisiones específicas creadas en el seno de las Juntas Locales de Seguridad*” (...). Por dicha razón podemos acercarnos a su régimen jurídico mediante el análisis del Real Decreto 1087/2010, de 3 de septiembre, por el que se aprueba el Reglamento que regula las Juntas Locales de Seguridad, que desarrolla el artículo 54 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad.

El art. 2 de dicho Reglamento establece que *[l]as Juntas Locales de Seguridad son órganos colegiados para facilitar la cooperación y la coordinación, en el ámbito territorial del municipio, de las Administraciones Públicas en materia de seguridad, asegurando de forma específica la cooperación y la coordinación operativa de las Fuerzas y Cuerpos de Seguridad que intervienen en el término municipal*. El objetivo de dicho órgano es ser “un mecanismo capaz de fijar medios y sistemas de relación al objeto de lograr cierta homogeneidad y hacer factible actuaciones conjuntas, de colaboración mutua y de cooperación recíproca” y que cumple a la vez una labor no sólo [...] de coordinación operativa, sino también *informativa*, facilitando cauces de canalización que permitan la colaboración de los sectores sociales e institucionales afectados en la correcta planificación de la seguridad pública (Exposición de motivos del Reglamento). Dicho órgano puede considerarse como un órgano de cooperación de los previstos actualmente en la ley 40/2015, de 1 de octubre, y de acuerdo con el art. 141 y siguientes de la misma, puede considerarse que existiría un deber de cooperación entre Administraciones para alcanzar sus propios fines. Así, el art. 141 de la ley 40/2015 establece que 1. Las Administraciones Públicas deberán: c) Facilitar a las otras Administraciones la información que precisen sobre la actividad que desarrollen en el ejercicio de sus propias competencias (...). Y dicha colaboración puede articularse mediante diferentes técnicas de colaboración, y entre ellas (art. 142 ley 40/2015) a) *[e]l suministro de información, datos, documentos o medios probatorios que se hallen a disposición del organismo público o la entidad al que se dirige la solicitud y que la Administración solicitante precise disponer para el ejercicio de sus competencias*, o b) *La creación y mantenimiento de sistemas integrados de información administrativa con el fin de disponer de datos actualizados, completos y permanentes referentes a los diferentes ámbitos de actividad administrativa en todo el territorio nacional*. El art. 144 de la ley 40/2015 dice que 1. *Se podrá dar cumplimiento al principio de cooperación de acuerdo con las técnicas que las Administraciones interesadas estimen más adecuadas, como pueden ser: a) La participación en órganos de cooperación, con el fin de deliberar y, en su caso, acordar medidas en materias sobre las que tengan competencias diferentes Administraciones Públicas*. Y el art. 143 dice que 2. *La formalización de relaciones de cooperación requerirá la aceptación expresa de las partes, formulada en acuerdos de órganos de cooperación o en **convenios***.

De lo anterior resulta que, tal y como expone la consulta, se ha establecido un convenio tipo con la FEMP, Federación española de municipios



y provincias, que posteriormente se pretende firmar con los Ayuntamientos, de modo que dicho convenio tipo puede considerarse como el convenio o acuerdo en que se formalizará la cooperación, y de acuerdo con el artículo 144.2 de la ley 40/2015, el mismo deberá prever las condiciones y compromisos que asumen las partes que los suscriben. Pues bien, dado que el carácter de responsable recae sobre la Administración central, en concreto sobre el CITCO, y la Administración local presta la colaboración requerida por la norma para el ejercicio de funciones en materia de prevención de la lucha contra la radicalización violenta, cabe considerar que cada una de las Administraciones locales en que se constituye un GL-LCRV actúa como un **encargado del tratamiento**, siguiendo las instrucciones del CITCO en cuanto a fines y medios del tratamiento de los datos personales que se les comuniquen. El art. 3.9) de la Directiva 2016/680 define «**encargado del tratamiento**» o «**encargado**» como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales *por cuenta del* responsable del tratamiento. Por ello, si los Ayuntamientos son encargados del tratamiento, la relación con el responsable habrá de reflejarse necesariamente mediante un “contrato u otro acto jurídico” -por escrito, inclusive en formato electrónico- que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, su naturaleza y finalidad, el tipo de datos personales y categorías de interesados y las obligaciones y derechos del responsable. Dado que cada uno de los municipios que participen en la iniciativa, según el procedimiento descrito, habrán de firmar el convenio con el CITCO, deberían de recogerse en dicho convenio las circunstancias que establece el art. 22.3 de la Directiva 2016/680 (y mientras no se produce su transposición, las circunstancias recogidas en el art. 12 de la LOPD) de modo que quede plasmada la actuación que puede llevar a cabo el Ayuntamiento, a través de cada GL-LCRV, en relación con los tratamientos de datos personales. Dichas circunstancias que deberían de especificarse son la siguientes: que el encargado

- a) actúe únicamente siguiendo las instrucciones del responsable del tratamiento;
- b) garantice que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación profesional de confidencialidad;
- c) asista al responsable del tratamiento por cualquier medio adecuado para garantizar el cumplimiento de las disposiciones sobre los derechos del interesado;
- d) a elección del responsable del tratamiento, suprima o devuelva todos los datos personales al responsable del tratamiento una vez



finalice la prestación de los servicios de tratamiento, y suprima las copias existentes a menos que el Derecho de la Unión o del Estado miembro requieran la conservación de los datos personales;

- e ponga a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento del presente artículo;
- f respete las condiciones indicadas en los apartados 2 y 3 para contratar a otro encargado del tratamiento.

En cuanto a las personas que introducen los datos en el sistema informático (asistentes sociales, educadores etc.), de las que existen, de acuerdo con la consulta, dos escalones, uno primero más en contacto con la realidad social y otro superior formado por supervisores de los anteriores, cabe decir lo siguiente.

La consulta expone que estos primeros escalones sería los encargados de recabar la información primaria y de realizar un seguimiento singularizado de cada uno de los casos concretos. Ahora bien, y dado que no existe aún una normativa reguladora de este diseño funcional del módulo de información, no se desprende de la información proporcionada la manera de incardinarse exactamente estos profesionales en la estructura del GL-LCRV, dado que parecen, más que integrantes de dicho grupo local, ajenos al mismo, y son quienes únicamente proporcionan la información que el grupo local ha de asesorar y estudiar. Lo mismo resulta del segundo escalón, que serían los responsables de áreas concretas de intervención social, y cuya función parece ser la de supervisar las informaciones introducidas en el sistema por el primer escalón, pero aun así sin formar parte propiamente dicho del GL-LCRV.

Pues bien, la unidad básica de recogida de información de acuerdo con lo consulta sería la ficha básica, creada en la inmensa mayoría de los casos por los usuarios de primer nivel, que se encuentran en contacto directo con las capas sociales susceptibles de radicalización. Es decir, que si una persona cercana a la realidad social considera que existe un riesgo de radicalización, rellenaría la denominada ficha básica y la introduciría en el sistema gestionado por CITCO. Se repite que no aparece configurada normativamente la existencia o funciones de esta figura, y por lo tanto no se conoce su forma de incardinarse en el sistema, más allá de lo mencionado explícitamente en este párrafo. Ahora bien, como se ha dicho al inicio de este informe, existiría en un sentido amplio

un deber de denuncia establecido en las leyes para cumplimiento de las obligaciones de los fuerzas y cuerpos de seguridad del estado, entre ellas la de la prevención de la delincuencia. Si el usuario de primer nivel introduce la ficha básica, se considera que esta persona es precisamente eso, un usuario del sistema que cumple un deber, pero en modo alguno se convierte en responsable del tratamiento, característica está que le corresponde al CITCO, como se ha expuesto. Por esta razón, no se considera conveniente y acorde con la caracterización de la figura del usuario de primer nivel que a éste le corresponda decidir a qué personas o niveles se le ha de permitir el acceso a la ficha básica. Si el introductor de los datos es un usuario, la ficha básica introducida debería de seguir el protocolo establecido de control y supervisión de la radicalización violenta sin que tenga que decidir dicha persona que camino ha de seguir la información. Si al CITCO le corresponde la gestión técnica-administrativa y la responsabilidad del tratamiento, a éste le corresponde determinar los fines y los medios de tratamiento. El usuario no es responsable del tratamiento ni encargado del mismo. Como responsable del tratamiento, CITCO debería establecer unos parámetros que automáticamente determinen, según la información proporcionada por el usuario o de primera línea, cuál será el siguiente paso del tratamiento de datos necesario en la prevención de la radicalización.

Por lo demás cabe advertir que en el PEN-LCRV se contiene como estructura del mismo tanto un grupo nacional de lucha contra la radicalización violenta, GN-LCRV, como a nivel local los GL-LCRV (o a nivel provincial o autonómico), y en el plan se advierte que se trataría de “incorporar a la sociedad civil a dichos GL-LCRV”, pero no se contiene ninguna medida o prevención respecto de la existencia de una línea intermedia formada por los supervisores de las personas que en primera línea introducen los datos de personas susceptibles de radicalización violenta. Como se ha dicho anteriormente, el plan, en su página 17, establece que la constitución, participantes, competencias y protocolo de actuación de estos grupos sean objeto de una regulación administrativa, de la que aún se carece. Pero en cualquier caso, no se hace mención a los tratamientos de datos por personas intermedias, por lo que podría plantearse una cuestión acerca de la necesidad o conveniencia de esta segunda línea, ya que el Plan no las menciona, a menos que directamente se integrasen estas personas en los GL-LCRV. Si la base para el desarrollo de estos grupos locales es, como dice el Plan, la de las “comisiones específicas creados en el seno de las juntas locales de seguridad”, dichas comisiones se crean, de acuerdo con el art. 12 del Real Decreto

1087/2010, de 3 de septiembre, por el que se aprueba el Reglamento que regula las Juntas Locales de Seguridad, como *órganos de asesoramiento*, y su función es elevar para su valoración [a la Junta Local de Seguridad], los informes, propuestas y sugerencias que emitan. Como conclusión del anterior análisis entendemos que si se desea incorporar a profesionales que verifiquen o supervisen las informaciones contenidas en la ficha básica por las personas que están al nivel de la realidad social, dichos supervisores se integren en el grupo local directamente, de manera que toda la información que traten para los fines de la prevención de la radicalización violenta se realice en el seno del GL-LCRV.

No es aceptable decir que estas personas tratan información en un campo más amplio dentro de la estructura administrativa en la que se encuentran insertos (educativa, asistencial etc.) -como dice la consulta- porque el tratamiento de dichos datos personales se realizará siempre, dentro de dicha estructura administrativa, de conformidad con el Reglamento General de Protección de Datos (RGPD), y no de conformidad con la Directiva 2016/680, cuyo único objeto es la “prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos”, de modo que si el tratamiento de los datos personales se realiza para fines diferentes de los citados, su tratamiento deberá realizarse conforme al RGPD, que tiene requisitos más estrictos que la Directiva. Ello puede observarse en el artículo 9, apartados 1 y 2, de la Directiva 2016/680:

1. *Los datos personales recogidos por las autoridades competentes para los fines establecidos en el artículo 1, apartado 1, no serán tratados para otros fines distintos de los establecidos en el artículo 1, apartado 1 salvo que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro. **Cuando los datos personales sean tratados para otros fines, se aplicará el Reglamento (UE) 2016/679 a menos que el tratamiento se efectúe como parte de una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión.***
2. ***Cuando el Derecho del Estado miembro encomiende a las autoridades competentes el desempeño de funciones que no coincidan con los fines establecidos en el artículo 1, apartado 1, se aplicará el Reglamento (UE) 2016/679 al tratamiento con dichos fines**, incluidos fines de archivo en interés público, de investigación científica e histórica o estadísticos, salvo que el tratamiento se lleve a*

cabo en una actividad que quede fuera del ámbito de aplicación del Derecho de la Unión.

En definitiva, se recomienda separar las funciones de introducción de la información en la ficha básica por las personas más apegadas a la realidad social de cualquier otra función relativa al tratamiento de dichos datos, de manera que estas personas aparezcan únicamente como usuarios del sistema para poner de manifiesto posibles casos de radicalización violenta. El análisis posterior de dicha información debería de realizarse en un ámbito superior, ya dentro del GL-LCRV, y la normativa que regule estos grupos podría diferenciar entre comisiones o subcomisiones, pero todos ellos integrantes del GL-LCRV de manera que siempre pueda decirse que el tratamiento de dichos datos a los fines requeridos por la directiva, en general de prevención de infracciones/radicalización, se realiza dentro de dichos grupos locales, puesto que al ser, como ha quedado dicho, encargados del tratamiento, deberían de seguir las instrucciones que el responsable del tratamiento ha establecido en el convenio con la correspondiente administración local de la que depende dicho grupo local de lucha contra la radicalización violenta. Para evitar la posibilidad de que quien trate dichos datos fuera del GL-LCRV pudiera ser considerado responsable del tratamiento, es conveniente que el tratamiento de los datos personales lo realice siempre el encargado del tratamiento, esto es, el ayuntamiento a través del GL-LCRV correspondiente.

La regulación que se llevase a cabo de dichos grupos locales debería de contener deberes específicos de reserva y confidencialidad de la información tratada, tal y como para los miembros de las juntas locales de seguridad se establece en el artículo 11 del Reglamento de las Juntas locales de seguridad aprobado por Real Decreto 1087/2010.

Cabe por último reiterar lo mencionado al principio de este Informe, que siendo el CITCO responsable del tratamiento de datos, regulado este por la Directiva 2016/680 (y en tanto que ésta no sea transpuesta por lo establecido en la LOPD), le corresponde al CITCO la observancia y garantía de los derechos fundamentales a la protección de los datos personales de quienes son sometidos a dicho tratamiento de datos, de manera que habrá de regirse dicho tratamiento por lo establecido en dicha Directiva 2016/680 (y entre tanto por la LOPD), lo que incluye tanto los principios relativos a los tratamientos de datos personales contenidos en el artículo 4 de la Directiva, y los distintos derechos del interesado regulados en el capítulo III de esta, como el derecho

de información o el derecho de acceso; siempre teniendo en cuenta que el art. 13.2, 15 etc. de la Directiva establecen que los Estados miembros *podrán* adoptar **medidas legislativas** por las que se restrinjan total o parcialmente dichos derechos cuando dichas medidas constituyan una medida necesaria y proporcional en una sociedad democrática.

En definitiva, los tratamientos de datos llevados a cabo en el ejercicio de las funciones descritas habrán de cumplir con los requisitos establecidos en la normativa de protección de datos personales en su integridad, o en su caso estar excluidos, o limitados, dichos derechos en función de lo establecido en las medidas legislativas que, de conformidad con lo permitido por la Directiva 2016/638, pueda adoptar el Estado, según sea el caso.