N/REF: 201876/2018

La Dirección General de Ordenación del Juego manifiesta en su consulta su voluntad de suscribir Memorandums de Entendimiento o Convenios de Colaboración con diversas entidades e instituciones (Fuerzas y Cuerpos de Seguridad del Estado, Consejo Superior de Deportes, Operadores con título habilitante para ofrecer actividades de juego en España y entidades deportivas) con la finalidad de desarrollar mecanismos de prevención de actividades relacionadas con el fraude en las apuestas deportivas y que se instrumentarán a través de una aplicación informática que denomina “Sistema de Alertas sobre apuestas deportivas”, gestionado por la citada Dirección General. Dicha aplicación tiene por finalidad prevenir el fraude y los amaños en el mercado de las apuestas deportivas, en beneficio no sólo de los apostantes y los participantes en el juego, sino también del propio mercado regulado de ámbito estatal.

En cuanto al suministro de información al sistema, cualquier miembro del mismo puede transmitir información sobre posibles fraudes o amaños relacionados con las apuestas deportivas que sean de su conocimiento, con la finalidad de que el resto de miembros del Sistema tenga constancia, mediante un acceso parcial a dicha información, de esta circunstancia, y pueda utilizarla con la finalidad de comprobar las implicaciones del posible fraude cometido en su específico ámbito de actuación.

En cuanto a las alertas sobre las que se remitiría información son de tres tipos:

- Por un lado, se remitirá información sobre apuestas deportivas irregulares, entendidas como aquellas apuestas deportivas que no se ajusten a las apuestas habituales o previsibles del mercado de que se trate o que guarden relación con una competición deportiva que se desarrolle conforme a pautas no habituales.
- Por otro, se remitirá información sobre apuestas deportivas sospechosas, entendidas como aquellas apuestas que, atendiendo a pruebas fiables y no contradictorias, parezcan estar vinculadas a una manipulación de la competición respecto de la cual se realiza dicha apuesta.

- Finalmente podría remitirse información que se considere relevante a efectos de prevenir posibles fraudes en el ámbito de las apuestas deportivas y que pudiera no quedar comprendida en alguna de las categorías anteriores.

Por lo que se refiere al acceso a la información del Sistema, el contenido completo de la información será accesible, sin restricciones, para la DGOJ y las FCSE. El resto de miembros tendrán un acceso limitado a la información, y en lo que se refiere a los datos de carácter personal, solo el emisor de la alerta tendrá acceso a los datos de carácter personal que hubiera introducido expresamente. Dichos datos no serán accesibles al resto de miembros, ni el emisor podrá acceder a aquéllos que no hubiera introducido expresamente.

I

En lo que a la materia de protección de datos personales respecta, la norma a la que debe ajustarse es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), plenamente aplicable desde el 25 de mayo de 2018.

El citado Reglamento extiende su protección, tal y como establece su artículo 1.2, a los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, definidos en su artículo 4.1 como “toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.”

Quedan, en consecuencia, excluidas de su protección las personas jurídicas, pero su ámbito protector se extiende a las personas físicas que las representan, cuyos datos personales deben ser tratados con sujeción a lo previsto en dicho Reglamento.

La protección conferida por el Reglamento (UE) 2016/679 comprende también a los empresarios individuales, a diferencia de la normativa anterior, en la que el artículo 2.3 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real decreto 1720/2017, de 21 de diciembre, excluía de su ámbito de aplicación los datos de los empresarios individuales, cuando el tratamiento de los datos a ellos referentes lo fuera en su calidad de comerciantes, industriales o navieros. El Reglamento (UE) 2016/679 no establece ninguna exclusión en este sentido, de modo que el tratamiento de los datos personales relativos a los empresarios individuales debe someterse a las previsiones contenidas en esta norma.

Por otro lado, tampoco quedarán protegidos por la normativas sobre protección de datos personales los correspondientes a las personas fallecidas. En este sentido, ya desde sus primeros informes, la AEPD ha venido defendiendo que el derecho a la protección de datos, en cuanto derecho de la personalidad, se extingue por la muerte de la persona conforme al artículo 32 del Código Civil. Así se recogía ya en un informe de 20 de mayo de 1999 (vigente la LORTAD) y ha sido doctrina reiterada desde entonces en numerosos informes, que fue recogida en el artículo 2.4 del Reglamento de desarrollo de la Ley Orgánica 15/1999 (Real Decreto 1720/2007, de 21 de diciembre):

"Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos".

Idéntico criterio es el que sigue el RGPD, cuyo Considerando 27 señala lo siguiente: *"El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas"*, criterio que se reitera en los Considerandos 158 y 160.

Partiendo de dicho precepto, la Ley Orgánica 3/2018, después de excluir de su ámbito de aplicación en su artículo 2.2.b a *"los tratamientos de datos de personas fallecidas"* regula los datos personales de las personas fallecidas en su artículo 3:

Artículo 3. Datos de las personas fallecidas.

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

Por consiguiente, en los supuestos en que sea necesario el tratamiento de datos personales correspondientes a personas fallecidas, los mismos no quedan sujetos a la normativa sobre protección de datos personales, lo que debe tenerse en cuenta por la DGOJ, especialmente en los casos en que sea necesario su tratamiento para la verificación de identidades.

En consecuencia, en los supuestos en que en el Sistema de Alertas sea necesario tratar datos personales de personas jurídicas o personas fallecidas, en los términos anteriormente expuestos, los mismos no quedarán sujetos a la normativa sobre protección de datos personales.

II

En lo que se refiere a la base jurídica del tratamiento determinante de su licitud, es preciso recordar, como ya se ha indicado en reiteradas ocasiones por esta Agencia, que la reforma operada por el Reglamento general de protección de datos respecto del régimen contenido en la Ley Orgánica 15/1999 exige un cambio de perspectiva en lo que respecta a los principios articuladores del derecho fundamental a la protección de datos de carácter personal y, en particular, a aquél que hacía del “principio de consentimiento” el eje central del derecho a la protección de datos.

En efecto, si bien la Ley Orgánica y el Reglamento no difieren excesivamente en lo que atañe a la enumeración de las causas legitimadoras del tratamiento, se produce una modificación sumamente relevante en el modo en que dichas causas aparecen recogidas por los textos aplicables: así, mientras del tenor de la Ley Orgánica 15/1999 parecía deducirse que la regla básica de legitimación era, con carácter general, el consentimiento, resultando las restantes causas legitimadoras excepcionales en relación con el consentimiento, que como regla general debía regir el tratamiento, en el texto del artículo 6.1 del Reglamento general de protección de datos el consentimiento se recoge como una de las seis causas de legitimación para el tratamiento sin ostentar mayor o menor importancia que las restantes que en a norma se enumeran.

A mayor abundamiento, el propio Reglamento general de protección de datos pone de manifiesto que el consentimiento del afectado no debe constituir la base legal del tratamiento en determinados supuestos. Así, el considerando 42 señala en su última frase que “El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno” y el considerando 43 añade que “Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular”.

De este modo, no procede recabar en ningún caso el consentimiento del afectado en los supuestos en los que el tratamiento se encuentre amparado por

cualquiera de las causas incluidas en las letras b) a f) del artículo 6.1 del reglamento general de protección de datos; es decir cuando:

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Asimismo, debe tenerse en cuenta lo establecido en el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

“Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley".

Partiendo de lo anterior, y tal y como se explica en la detallada y debidamente motivada consulta remitida, el Sistema de Alertas tiene por finalidad proteger a los participantes en el mercado de las apuestas de ciertas prácticas que, por alterar los resultados de un evento deportivo de manera fraudulenta, acaban por distorsionar gravemente su participación en el juego, las apuestas realizadas sobre un evento amañado lamentablemente ya no dependen del azar, como exige la Ley 13/2011, de 27 de mayo, de regulación del juego. Asimismo, el Sistema tiene por finalidad vigilar y controlar el segmento de las apuestas deportivas, con vistas a garantizar el orden público y proteger el mercado de juego regulado, por cuanto que el modelo de negocio de los operadores de juego de ámbito estatal con título habilitante queda alterado gravemente cuando se produce un amaño deportivo que violenta de manera incontestable el entorno predictivo diseñado por aquéllos.

Dicha finalidad encontraría su amparo en las competencias que la Ley 13/2011, de 27 de mayo, de regulación del juego atribuye a la Dirección General de Ordenación del Juego tras la asunción por ésta del objeto, funciones y competencias que la Ley 13/2011 atribuye a la extinta Comisión Nacional del Juego (disposición adicional décima de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia).

En este sentido, el artículo 21 de la Ley 13/2011 señala, entre las funciones de la DGOJ, las siguientes:

a) Vigilar, controlar, inspeccionar y, en su caso, sancionar las actividades relacionadas con los juegos (…). (apartado 7).

b) Asegurar que los intereses de los participantes y de los grupos vulnerables sean protegidos, así como el cumplimiento de las leyes, reglamentaciones y principios que los regulan, para defender el orden público y evitar el juego no autorizado" (apartado 9).

c) Colaborar en el cumplimiento de la legislación de prevención de blanqueo de capitales y de la financiación del terrorismo y vigilar el

cumplimiento de la misma, sin perjuicio de las competencias de otros órganos administrativos en relación con los operadores que realicen actividades de juego sujetas a reserva de actividad por la Ley" (apartado 14).

Junto a dichas funciones, el artículo 24.1 de la Ley 13/2011, de 27 de mayo, determina que a la Dirección General de Ordenación del Juego "Le corresponde la auditoría, vigilancia, inspección y control de todos los aspectos y estándares administrativos, económicos, procedimentales, técnicos, informáticos, telemáticos y de documentación, relativos al desarrollo de las actividades previstas en esta Ley."

Por otro lado, destaca la consulta cómo *"conectada directamente con la función del artículo 21.7 de la Ley 13/2011, de 27 de mayo, ("Vigilar, controlar, inspeccionar y, en su caso, sancionar las actividades relacionadas con los juegos…"), se encuentra todo el régimen sancionador del Título VI que atribuye competencias directas en este ámbito a la Dirección General de Ordenación del Juego. Interesa resaltar en este ámbito que en el elenco de conductas susceptibles de constituir infracción administrativa a los efectos de la Ley y, consecuentemente, poder dar lugar al inicio de un expediente sancionador, se encuentran las contenidas en los tipos infractores previstos en los artículos 41.a) y b), que pasan a relatarse a continuación:*

- *En primer lugar, la letra a) del artículo 41 establece que constituyen infracciones leves "a) La participación en actividades de juego, contraviniendo las prohibiciones establecidas en el artículo 6.2, letras c), d), e), f), g) y h), de esta Ley.): estas prohibiciones son las "prohibiciones subjetivas" asociadas a la práctica de juego, y las mismas tienen una conexión directa con el mundo del deporte. En este sentido, la ley prohíbe expresamente que formen parte de un entorno de juego los siguientes colectivos de personas:*

"d) Los deportistas, entrenadores u otros participantes directos en el acontecimiento o actividad deportiva sobre la que se realiza la apuesta.

e) Los directivos de las entidades deportivas participantes u organizadoras respecto del acontecimiento o actividad deportiva sobre la que se realiza la apuesta.

f) Los jueces o árbitros que ejerzan sus funciones en el acontecimiento o actividad deportiva sobre la que se realiza la apuesta, así como las personas que resuelvan los recursos contra las decisiones de aquellos."

La finalidad última de estas prohibiciones subjetivas es garantizar la limpieza de las apuestas, y la ratio que subyace es la de evitar la participación de quienes, debido a su actividad, se encuentran en una situación de privilegio respecto al resto de participantes en las apuestas, además de poder influir en el resultado.

Pues bien, desde esta perspectiva el Sistema de Alertas en materia de apuestas deportivas se constituye en un instrumento necesario para el ejercicio de esta potestad sancionadora legalmente atribuida y por ende a la misión atribuida a la Dirección General de Ordenación del Juego.

- *En segundo lugar, la letra b) del artículo 41 establece que constituyen infracciones leves "b) Los incumplimientos de las obligaciones contenidas en esta Ley, cuando no estuvieren expresamente tipificadas como infracciones graves o muy graves.".*

Entre estas obligaciones ex lege es sumamente importante la relativa al deber general de cualquier participante en el juego de "no alterar el normal desarrollo de los juegos", que queda expresamente recogido en el artículo 15.2.c) de la Ley 13/2011. No cabe duda que la posible práctica de un amaño deportivo, con vistas a obtener réditos a través de la formulación de apuestas viciadas desde su inicio, constituye un claro ejemplo de una alteración del normal desarrollo de los juegos, sobre la que la eficacia de la competencia sancionadora de la DGOJ debe quedar absolutamente garantizada.

Desde esta perspectiva, y al igual que en el epígrafe anterior, el Sistema de Alertas diseñadas se constituye en un instrumento esencial y necesario para el ejercicio de la señalada competencia y, por ende, contribuye al cumplimiento de la misión atribuida a la DGOJ".

Esta Agencia comparte la conclusión alcanzada y debidamente fundamentada por la DGOJ, en el sentido de que el Sistema de Alertas es un instrumento necesario para el ejercicio de las competencias que la Ley 13/2011 atribuye a la dicha Dirección General, especialmente las funciones de inspección y control que desarrolla el artículo 24 de la Ley 13/2011 anteriormente citado, y que entre otra cuestiones se refiere a la colaboración de las Fuerzas y Cuerpos de Seguridad del Estado, al seguimiento y control de los operadores y de las cuentas de usuario o al deber de colaboración de los operadores habilitados, sus representantes legales y su personal y que por su importancia se transcribe a continuación:

“Artículo 24. Inspección y Control.

1. Al objeto de garantizar lo dispuesto en esta Ley y en las disposiciones que la complementen, corresponderá a la Comisión Nacional del Juego la auditoría, vigilancia, inspección y control de todos los aspectos y estándares administrativos, económicos, procedimentales, técnicos, informáticos, telemáticos y de documentación, relativos al desarrollo de las actividades previstas en esta Ley.

Asimismo, corresponderá a la Comisión Nacional del Juego la investigación y persecución de los juegos ilegales, sin perjuicio de las facultades que correspondan a las Fuerzas y Cuerpos de Seguridad competentes y al Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias en los términos del artículo 45.4 f) de la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo. La Comisión Nacional del Juego establecerá los procedimientos necesarios en orden al cumplimiento de las funciones antes citadas.

Las Fuerzas y Cuerpos de Seguridad del Estado, de acuerdo con lo establecido en el artículo 12.1.A), letra d), de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, colaborarán con la Comisión Nacional del Juego en las funciones de vigilancia e inspección del cumplimiento de la normativa en materia de juego. Si como resultado de la actividad inspectora llevada a cabo por las Fuerzas y Cuerpos de Seguridad del Estado en el ejercicio de las funciones de colaboración con la Comisión Nacional del Juego se comprobara la existencia de indicios de la comisión de una infracción, se levantará la oportuna acta que será enviada a los órganos competentes para iniciar el procedimiento sancionador.

2. Por la Comisión Nacional del Juego se establecerán los procedimientos adicionales para el seguimiento y control de los operadores que realicen actividades de juego sujetas a reserva en virtud de una ley y del cumplimiento de las condiciones que se establezcan a los mismos, en especial, en relación con la protección del orden público y la prevención del blanqueo de capitales y financiación del terrorismo. En el supuesto de que, en el ejercicio de su labor inspectora, la Comisión Nacional del Juego apreciara posibles infracciones de las obligaciones establecidas en la Ley 10/2010, de 28 de abril, de prevención de blanqueo de capitales y de la financiación del terrorismo, informará a la Secretaría de la Comisión de Prevención del Blanqueo de

Capitales e Infracciones Monetarias en los términos del artículo 48.1 de la citada Ley.

3. La Comisión Nacional del Juego podrá efectuar un control sobre la cuenta de usuario del participante en las actividades de juego objeto de esta Ley, así como de los operadores o proveedores de servicios de juego. La Comisión Nacional del Juego tendrá acceso a los datos de carácter personal recogidos en la cuenta de usuario de los participantes, respetando en todo momento lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos y su normativa de desarrollo.

Las Administraciones Públicas darán acceso a la Comisión Nacional del Juego a sus bases de datos con la finalidad de comprobar la identidad del participante y, especialmente, su condición de mayor de edad.

4. Los operadores habilitados, sus representantes legales y el personal que en su caso se encuentre al frente de las actividades en el momento de la inspección, tendrán la obligación de facilitar a los inspectores y a su personal auxiliar el acceso a los locales y a sus diversas dependencias, así como el examen de los soportes técnicos e informáticos, libros, registros y documentos que solicite la inspección. El resultado de la inspección se hará constar en acta que tendrá la naturaleza de documento público y hará prueba, salvo que se acredite lo contrario, de los hechos y circunstancias que la motiven.

El acta deberá ser firmada por el funcionario que la extienda y por la persona o representante de la entidad fiscalizada, quien podrá hacer constar cuantas observaciones estime convenientes. Se entregará copia del acta a la persona o representante de la entidad fiscalizada, dejando constancia, en su caso, de su negativa a firmarla o a estar presente en el desarrollo de la inspección.

En el ejercicio de las funciones de inspección el personal de la Comisión Nacional del Juego tendrá la condición de autoridad. El ejercicio de las facultades de inspección y control podrá ser objeto de convenio con las Comunidades Autónomas respecto de las actividades y de los medios o instrumentos situados en su territorio, con excepción de las de carácter resolutorio.

La Comisión Nacional del Juego colaborará con otros organismos reguladores del Espacio Económico Europeo en la persecución del juego ilegal, mediante la adopción de medidas coordinadas para obtener la cesación en la prestación de servicios ilegales de juego y el intercambio de información.

> 5. La Comisión Nacional del Juego podrá firmar acuerdos de corregulación que coadyuven al cumplimiento de las obligaciones establecidas en esta Ley, en particular en lo referido a la publicidad, en los términos que se determinen reglamentariamente. En la medida en que dichos acuerdos afecten a la publicidad efectuada por los prestadores del servicio de comunicación audiovisual, deberá recabarse informe del Consejo Estatal de Medios Audiovisuales con carácter previo a la firma de los mismos. Los sistemas de autorregulación se dotarán de órganos independientes de control para asegurar el cumplimiento eficaz de los compromisos asumidos por las empresas adheridas. Sus códigos de conducta podrán incluir, entre otras, medidas individuales o colectivas de autocontrol previo de los contenidos publicitarios y deberán establecer sistemas eficaces de resolución extrajudicial de reclamaciones que cumplan los requisitos establecidos en la normativa comunitaria y, como tales, sean notificados a la Comisión Europea, de conformidad con lo previsto en la Resolución del Consejo de 25 de mayo de 2000 relativo a la red comunitaria de órganos nacionales de solución extrajudicial de litigios en materia de consumo o cualquier disposición equivalente".

Por todo ello debe concluirse que el Sistema de Alertas, en cuanto al tratamiento de datos personales que puedan realizarse, encuentra su fundamento en lo previsto en el artículo 6.1 letra e) del RGPD: el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Habiendo sido atribuida dicha competencia por una norma con rango de ley conforme a lo exigido por el artículo 8.2 de la LOPDPGDD.

III

Tal y como se señala en la Consulta, *"la gestión de la información transmitida por el Sistema de Alertas le corresponde exclusivamente a la DGOJ. La DGOJ se configura, por tanto, como el gestor del Sistema de Alertas y como el responsable del tratamiento de datos de carácter personal que pueden transmitirse a través de dicho Sistema. Por su parte, el resto de miembros del Sistema serán encargados del tratamiento de los datos de carácter personal que incorporen al Sistema"*.

Define el RGPD al "responsable del tratamiento", o "responsable", como "la persona física o jurídica, autoridad pública, servicio u otro organismo que,

solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros".

Como ya señaló en el Grupo del artículo 29 en su Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", "la distinción entre "responsable del tratamiento" y "encargado del tratamiento" sirve primordialmente para diferenciar entre quienes asumen la responsabilidad en tanto que responsables y quienes sólo actúan por cuenta de éstos. De acuerdo con el mismo, "el concepto de responsable del tratamiento es autónomo, en el sentido de que debe interpretarse fundamentalmente con arreglo a la legislación comunitaria de protección de datos, y funcional, en el sentido de que su objetivo es asignar responsabilidades en función de la capacidad de influencia de hecho, y, por consiguiente, se basa en un análisis de los hechos más que en un análisis formal". Asimismo, indica que "la determinación del «fin» del tratamiento es competencia del «responsable del tratamiento». Por consiguiente, quienquiera que tome esta decisión es (de facto) el responsable del tratamiento". Y en cuanto a los medios, señala que "no sólo se refieren a los medios técnicos de tratar los datos personales, sino también al «cómo» del tratamiento, que incluye preguntas como «¿qué datos deben tratarse?», «¿qué terceros deben tener acceso a estos datos?», «¿cuándo deben borrarse los datos?», etc". Y añade:

"Por lo tanto, la determinación de los «medios» abarca preguntas técnicas y organizativas cuando la decisión puede delegarse en los encargados del tratamiento (como, por ejemplo, «¿qué *harware* o *software* debe usarse?») y elementos esenciales que tradicionalmente y de forma inherente se reservaban para la determinación del responsable del tratamiento, como «¿qué datos deben tratarse?», «¿durante cuánto tiempo deben tratarse?», «¿quién debe tener acceso a ellos?», etc.

En estas circunstancias, mientras la determinación de los fines del tratamiento desembocaría en cualquier caso en la determinación del responsable del tratamiento, la determinación de los medios sólo implicaría un control si afectara a elementos esenciales de los medios.

Desde esta perspectiva, es perfectamente posible que los medios técnicos y organizativos los determine exclusivamente el encargado del tratamiento de los datos".

En el presente caso, atendiendo a los términos de la consulta plateada, el Sistema de Alertas será gestionado por la DGOJ y al mismo solo podrá tener acceso las entidades, organismos e instituciones que suscriban un Acuerdo con la DGOJ, que es quien define *"tanto el rol como las funciones y competencias de los miembros del Sistema de Alertas"*. Asimismo, es la DGOJ la que determina los datos personales que deben ser objeto de tratamiento y la forma y el alcance en el que se podrá tener acceso al mismo, por lo que la misma ostenta la condición de responsable del tratamiento según lo expuesto y, consecuentemente, a la misma le corresponderá cumplir con todas las obligaciones que la normativa sobre protección de datos personales impone a los responsables del tratamiento. Singularmente, al tratarse de uno de los sujetos del artículo 77.1 de la Ley Orgánica 3/2018 (Administración General del Estado) deberá incluir estos tratamientos en el inventario de actividades de tratamiento al que se refiere el artículo 31.2 de la misma.

En cuanto al «encargado del tratamiento» o «encargado», el RGPD lo define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento". Como señala el Dictamen 1/2010 del Grupo del 29 ya citado:

"La existencia de un encargado del tratamiento depende de una decisión adoptada por el responsable del tratamiento, que puede decidir que los datos se traten dentro de su organización, por ejemplo por personal autorizado para procesar datos bajo su autoridad directa, o delegar todas o una parte de las actividades de tratamiento en una organización externa, es decir -como se señala en la exposición de motivos de la propuesta modificada de la Comisión- en «una persona jurídicamente distinta que actúa por su cuenta».

Por lo tanto, para poder actuar como encargado del tratamiento tienen que darse dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste.

Esta actividad de tratamiento puede limitarse a una tarea o contexto muy específicos o ser más general y amplia.

Además, la función de encargado del tratamiento no se deriva de la naturaleza de un ente que trata datos, sino de sus actividades concretas en un contexto específico. En otras palabras, un mismo ente puede actuar a la vez como responsable del tratamiento para determinadas operaciones de

tratamiento y como encargado del tratamiento para otras, y la condición de responsable o encargado debe avaluarse respecto de unos conjuntos muy determinados de datos u operaciones".

En el presente caso, y respecto del tratamiento de los datos personales que se integran en el Sistema de Alertas, el resto de entidades que intervienen en él (Consejo Superior de Deportes, Operadores con título habilitante para ofrecer actividades de juego en España y entidades deportivas) actuarían como encargados del tratamiento por cuenta de la DGOJ, lo que requiere la existencia del contrato o acto jurídico al que se refiere el artículo 28.3 del RGPD: "El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable".

Por tanto, la primera observación que debe realizarse respecto a dicho contrato o acto es que el mismo tiene que ser jurídicamente vinculante, por lo que no sería admisible los Memorándums de Entendimiento a los que se refiere al apartado primero de la Consulta, al tratarse de meros acuerdos de intenciones que carecen de contenido obligatorio. En cuanto a la segunda observación que debe realizarse a estos efectos es que los Acuerdos o Convenios que se suscriban deberán ajustarse al contenido que señala el citado artículo 28.3:

"Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b)garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros".

No obstante, hay que reiterar que la consideración de encargados del tratamiento lo es a los exclusivos efectos de los datos personales y los tratamientos que se realizan en el Sistema de Alertas y de acuerdo con las instrucciones marcadas por la DGOJ, y no respecto de otros datos personales u otros tratamientos diferentes que realicen dichas entidades.

IV

En cuanto al acceso a los datos por las Fuerzas y Cuerpos de Seguridad del Estado, destaca la consulta que las Fuerzas y Cuerpos de Seguridad del Estado podrán tener acceso a toda la información obrante en el Sistema. En este punto hay que recordar que el artículo 24.1 de la Ley 3/2011 prevé expresamente la colaboración de las Fuerzas y Cuerpos de Seguridad del Estado en las funciones de vigilancia e inspección del cumplimiento de la normativa en materia de juego.

Por otro lado, 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 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece que dichos tratamientos continuarán rigiéndose por la Ley Orgánica 15/1999 (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.

Como señala el Informe de esta Agencia 97/2018, "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”.

Por otro lado, como añadía el Informe 94/2018, 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”.

Partiendo de lo anterior, el acceso por parte de la policía judicial al Sistema de Alertas se encontraría fundamentado en sus funciones de averiguación del delito y detención del responsable, para lo cual debería poder acceder tanto a las apuestas irregulares como a las sospechosas, con el fin de poder iniciar las investigaciones correspondientes, permitiendo de ese modo relacionar dicha información con aquélla otra de la que disponga (por ejemplo, en el caso de suplantación de identidades).

V

En cuanto a los datos de carácter personal que se pueden incluir de manera expresa en el Sistema de Alertas detalla la consulta los siguientes:

- *Identidad de los apostantes: información sobre aquellas personas que han realizado las apuestas y respecto a las que existen sospechas de que han incurrido en algún tipo de comportamiento o práctica fraudulenta.*
- *Identidad de los jugadores implicados en la alerta: información sobre aquellos deportistas o personas relacionadas con el mundo del deporte sobre los que existen sospecha de haber incurrido en algún tipo de práctica fraudulenta asociada a un evento deportivo determinado en el que participen de manera directa o indirecta.*
- *Identidad de otro tipo de personas: información sobre personas que, estando relacionadas de manera indirecta con un evento deportivo determinado, pueden haber incurrido en algún tipo de práctica fraudulenta para alterar su resultado.*
- *Otros datos relacionados con identidades de personas: datos de carácter personal que no remiten directamente a la identidad de una persona, pero que pueden servir para identificar la identidad de una persona, como puede ser la IP, su número de teléfono.*

A este respecto se hace preciso diferenciar entre las personas físicas cuyos datos personales pueden ser objeto de tratamiento y el tipo de datos que pueden ser objeto de tratamiento, atendiendo a los principios recogidos en el artículo 5 del RGPD, especialmente, una vez analizada la licitud del tratamiento en los apartados anteriores, a los principios de exactitud, minimización y limitación de la conservación que se recogen en el citado precepto, según el cual:

"1.Los datos personales serán:

[…]

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la

aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

La aplicación de los citados principios adquiere especial relevancia teniendo en cuenta que, dada la finalidad perseguida, se pueden introducir datos personales en el sistema que den lugar a una alerta que se demuestre que no está fundada, por lo que deberán adoptarse las cautelas necesarias para evitar que se introducen datos que carecen manifiestamente de fundamento, así como para proceder a la supresión inmediata de aquellos datos que se demuestren que no se corresponden con una actividad irregular (principio de exactitud de los datos), salvo que concurran otras circunstancias (por ejemplo, conductas que aisladamente no son irregulares pero que es su reiteración en un determinado espacio temporal las que ponen de manifiesto su irregularidad) en cuyo caso deberá establecerse un plazo para su conservación que no exceda de lo estrictamente necesario y que deberá fijarse por la DGOJ atendiendo a las circunstancias concurrentes y a su experiencia en relación con las actividades fraudulentas, estimándose adecuado, salvo concurrencia de otras circunstancias, el plazo de un año desde la última información añadida a la alerta (principio de limitación del plazo de conservación). Asimismo, en el caso de que como consecuencia de la alerta se incoara un procedimiento de investigación por la policía judicial o un procedimiento administrativo sancionador por la DGOJ, deberán incorporarse los datos al procedimiento correspondiente y suprimirse del Sistema de Alertas, teniendo en cuenta que para el tratamiento de datos de naturaleza penal y de datos relativos a infracciones y sanciones administrativas existen normas especiales en los artículos 10 y 27 de la Ley Orgánica 3/2018

Además, partiendo de los principios anteriormente citados de exactitud y minimización de datos, la posibilidad de que en el Sistema pueda tratarse “información que se considere relevante a efectos de prevenir posibles fraudes en el ámbito de las apuestas deportivas y que pudiera no quedar comprendida en alguna de las dos categorías anteriores” se considera demasiado genérica y ambigua, por lo que podría dar lugar a tratamientos de datos contrarios al RGPD, por lo que se considera necesario que la misma se suprima, debiendo reconducirse los supuestos a las categorías de “apuestas deportivas irregulares” y “apuestas deportivas sospechosas”.

Por otro lado, en cuanto a los concretos datos personales que sean objeto de tratamiento y de los que solo se identifican algunos en la consulta (IP,

nombre, teléfono, correo) deberán ser igualmente los mínimos imprescindibles para los fines perseguidos. En este punto, debe diferenciarse entre los datos personales de quienes participan en el sistema (como, por ejemplo, el usuario que creó la alerta, el contacto del origen de la alerta, el receptor de la alerta o el destinatario de la comunicación), en los que no existiendo dudas sobre la veracidad de la información, deberán ser los mínimos imprescindibles para su correcta identificación y en su caso, para poder contactar con el mismo, y los datos personales de quienes se incluyen en el sistema por su posible intervención en el fraude. En este caso, teniendo en cuenta, especialmente en el caso de los apostantes, que pueden utilizarse identidades falsas, incluso, como se apuntaba anteriormente, de personas fallecidas, los datos para su correcta identificación podrán ser mayores, pero en todo caso los mínimos imprescindibles para su correcta identificación. Por todo ello se considera necesario concretar en el Anexo III o, en su caso, en los Convenios que se suscriban, cuáles son los concretos datos de identificación que se pueden utilizar.

Asimismo, de los términos de la consulta se deriva que no serán objeto de tratamiento las categorías especiales de datos personales a las que se refiere el artículo 9 del RGPD (datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física). En efecto, de las categorías de datos personales señalados por la consultante, centrados en la correcta identificación de las personas y el contacto, en su caso, con las mismas, no resulta el tratamiento de dichos datos. Sin embargo, podría ocurrir que en alguno de los campos del Sistema, como pueda ser el de “descripción del hecho según el usuario de la alerta”, se introdujeran ese tipo de datos, como ocurriría, por ejemplo, si se hiciera referencia a un posible dopaje de un jugador, en cuyo caso nos encontraríamos ante una dato relativo a la salud. Por ello, partiendo de la genérica prohibición del tratamiento de dichos datos si no concurren algunas de las excepciones que se recogen en el artículo 9.2 del RGPD, se considera necesario que se adopten las cautelas necesarias para excluir su tratamiento, debiendo recogerse así en los Convenios que se suscriban.

Por otro lado, dentro de las medidas organizativas tendentes a garantizar el cumplimiento de la normativa sobre protección de datos, se prevé que la totalidad de los datos personales que figuren en el Sistema sólo serán

visibles por la DGOJ y por las FCSE, mientras que el resto de miembros del sistema solo tendrán acceso a aquellos datos personales que hayan introducido. No obstante, teniendo en cuenta que tendrán acceso a otro tipo de datos, y con el fin de minimizar la posibilidad de que de los mismos puedan inferirse datos personales ajenos a su actividad, se considera necesario que los restantes miembros solo tengan acceso a las alertas del Sistema que guarden relación con su actividad (así, por ejemplo, la Federación Española de Baloncesto solo debería tener acceso a las alertas que se produzcan en el ámbito del baloncesto y no de otros deportes).

VI

Por lo que se refiere a las personas físicas cuyos datos personales pueden ser objeto de tratamiento se hace preciso establecer una diferenciación a efectos de la aplicación del principio de transparencia y del deber de información regulado en los artículos 12 a 14 del RGPD.

En el caso de los apostantes, los datos se obtienen directamente del interesado, debiéndose cumplir con el deber de información conforme al artículo 13 por parte de los correspondientes operadores de juego en el momento de su obtención, como uno de los tratamientos de datos que pueden realizar en cumplimiento de una obligación legal, recogiéndose así en su política de privacidad.

En el caso de deportistas, personas relacionadas con el mundo del deporte u otras personas relacionadas con la alerta, nos encontramos en el supuesto contemplado en el artículo 14 del RGPD, relativo a la información que debe facilitarse cuando los datos personales no se hayan obtenido del interesado, debiendo facilitarse dicha información, con carácter general, “dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos” (artículo 14.3.a RGPD). No obstante, en este caso hay que tener en cuenta que dichos datos pueden ser utilizados con fines de investigación por la policía judicial, en cuyo caso, el artículo 13.3 de la Directiva (UE) 2016/680 establece que:

“3. Los Estados miembros podrán adoptar medidas legislativas por las que se retrase, limite u omita la puesta a disposición del interesado de la información en virtud del apartado 2 siempre y cuando dicha medida constituya una medida necesaria y proporcional en una sociedad democrática, teniendo

debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada, para:

a) evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;

b) evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) proteger la seguridad pública;

d) proteger la seguridad nacional;

e) proteger los derechos y libertades de otras personas."

En este sentido, el artículo 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, vigente en cuanto no se proceda a la transposición de la citada directiva conforme a la Disposición transitoria cuarta de la Ley Orgánica 3/2018, establece las correspondientes excepciones al deber de información cuando la información al afectado afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales.

Por otro lado, en cuanto a los tratamientos sometidos al RGPD, el artículo 23 del mismo establece lo siguiente:

"1.El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles."

En el presente caso, como hemos visto, la Ley 13/2011, de 27 de mayo, de regulación del juego atribuye a la DGOJ competencias de auditoría, vigilancia, inspección y control, incluyendo entre los posibles infractores a los deportistas, entrenadores, directivos de las entidades deportivas participantes u organizadoras, jueces o árbitros u otros participantes en el acontecimiento o actividad deportiva. Por tanto, la información gestionada en el Sistema de Alertas por la DGOJ debe ponerse directamente en relación con el ejercicio de la potestad sancionadora que a la misma le corresponde y que está sometida en nuestro ordenamiento jurídico a una normativa procedimental específica, contenida actualmente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Por consiguiente, es en dicha Ley en la que deben buscarse las excepciones a que se refiere el artículo 23 del RGPD.

En este sentido, en el artículo 53 de la propia Ley 39/2015, de 1 de octubre, bajo el epígrafe "Derechos del interesado en el procedimiento administrativo", se dispone que:

"1. Además del resto de derechos previstos en esta Ley, los interesados en un procedimiento administrativo tienen los siguientes derechos:

a) A conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados; el sentido del silencio administrativo que corresponda, en caso de que la Administración no dicte ni notifique resolución expresa en plazo; el órgano competente para su instrucción, en su caso, y resolución; y los actos de trámite dictados. Asimismo, también tendrán derecho a acceder y a obtener copia de los documentos contenidos en los citados procedimientos.

Quienes se relacionen con las Administraciones Públicas a través de medios electrónicos, tendrán derecho a consultar la información a la que se refiere el párrafo anterior, en el Punto de Acceso General electrónico de la Administración que funcionará como un portal de acceso. Se entenderá cumplida la obligación de la Administración de facilitar copias de los documentos contenidos en los procedimientos mediante la puesta a disposición de las mismas en el Punto de Acceso General electrónico de la Administración competente o en las sedes electrónicas que correspondan.

(…)

e) A formular alegaciones, utilizar los medios de defensa admitidos por el Ordenamiento Jurídico, y a aportar documentos en cualquier fase del procedimiento anterior al trámite de audiencia, que deberán ser tenidos en cuenta por el órgano competente al redactar la propuesta de resolución.

2. Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables tendrán los siguientes derechos:

a) A ser notificado de los hechos que se le imputen, de las infracciones que tales hechos puedan constituir y de las sanciones que, en su caso, se les pudieran imponer, así como de la identidad del instructor, de la autoridad competente para imponer la sanción y de la norma que atribuya tal competencia.

b) (…).”

Por otro lado, la regulación general de las actuaciones previas de investigación que, en su caso, preceden a la incoación de un expediente sancionador, se contiene en el artículo 55 de la Ley 39/2015, de 1 de octubre:

“Artículo 55. Información y actuaciones previas.

1. Con anterioridad al inicio del procedimiento, el órgano competente podrá abrir un período de información o actuaciones previas con el fin de conocer las circunstancias del caso concreto y la conveniencia o no de iniciar el procedimiento.

2. En el caso de procedimientos de naturaleza sancionadora las actuaciones previas se orientarán a determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la

identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros.

Las actuaciones previas serán realizadas por los órganos que tengan atribuidas funciones de investigación, averiguación e inspección en la materia y, en defecto de éstos, por la persona u órgano administrativo que se determine por el órgano competente para la iniciación o resolución del procedimiento."

Dichas actuaciones previas, que pueden realizarse con anterioridad a la iniciación del procedimiento con objeto de determinar con carácter preliminar si concurren circunstancias que justifiquen tal iniciación, poseen carácter reservado. Su práctica obedece a la necesidad de determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros. El carácter reservado de dichas actuaciones previas se ha puesto de manifiesto reiteradamente por la Jurisprudencia; por todas, la STS de 13 de septiembre de 2002 (Sala Militar).

Por consiguiente, el funcionamiento del Sistema de Alertas, en cuanto va a permitir "conocer las circunstancias del caso concreto y la conveniencia o no de iniciar el procedimiento" y está orientado a "determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros" participa de la naturaleza de las actuaciones previas y consecuentemente, de su carácter reservado. Todo ello sin perjuicio de que, como se ha indicado reiteradamente, el tiempo en el que los datos han de ser tratados en el Sistema ha de ser el mínimo imprescindible para la concreción de los hechos y las identidades correspondientes.

VII

Por último plantea la consulta la posibilidad del tratamiento en el sistema de los deportes de carácter individual, ya que en este caso los contrincantes que han de figurar en la Tabla 6 (datos relacionados con el evento deportivo sobre el que se produce la alerta) son personas físicas y, por ende, se trataría de un dato de carácter personal. De ahí que se limite el acceso en los mismos términos previstos para los datos de carácter personal a la DGOJ, FCSE y emisor de la alerta. No obstante, plantea la consulta que el resto de datos que

figuran en la Tabla 6 (nombre del evento, descripción del evento, deporte, clasificación del deporte dada por la DGOJ, descripción de la competición, partido, resultado del partido, fecha, país y género del evento) al ir referido a deportes individuales podrían permitir identificar a los contrincantes en cuyo caso se tratarían de datos de carácter personal al referirse a personas identificables. Por ello, se plantea limitar el acceso a dichos datos en el Sistema, además de a la DGOJ y las FCSE, a:

- Operadores de juego, al tener un interés legítimo.
- El Consejo Superior de Deportes, en virtud de las competencias en relación con las Federaciones Deportivas de acuerdo con la Ley 10/1990 de 15 de octubre, del Deporte).
- La Federación deportiva competente por razón del deporte, atendiendo a las competencias que, en materia disciplinaria, le atribuye la citada Ley 10/1990.

En este punto hay que destacar que el nombre de los contrincantes en un evento deportivo individual son datos personales relativos a personas físicas, si bien son datos públicos relativos a la actividad profesional de los deportistas. Como ya señaló la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 (asuntos acumulados C-468/10 y C-469/10) en sus Considerandos 44 y 45, cuando los datos figuran en fuentes accesibles al público, el responsable del tratamiento y, en su caso el tercero o tercero a quienes se comuniquen los datos no acceden a datos relativos a la vida privada del interesado, dado que la información ya es de público conocimiento. Como consecuencia hay un impacto menor en los derechos del interesado, lo que debe ser apreciado en su justo valor en la ponderación con el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos.

Y del mismo modo, dicho impacto menor derivaría también del hecho de tratarse de la actividad profesional de los afectados, tal y como ha declarado reiteradamente la Audiencia Nacional al analizar el ejercicio del “derecho al olvido”. En este sentido, señala en su sentencia de 26 de marzo de 2019 que *“como ha declarado esta Sala en la sentencia de 6 de junio de 2017 (R. 1797/2015) debe tenerse en cuenta, en primer lugar, que la información discutida se refiere a la vida profesional y no a la vida personal del reclamante, pues ello es muy relevante para modular la intensidad que ha de merecer la protección del derecho regulado en el artículo 18.4 de la Constitución, como ha*

señalado esta Sala y Sección en la sentencia de 11 de mayo de 2017 (Rec. 30/2016).

En este sentido, conviene hacer referencia a las directrices del Grupo de Trabajo del art. 29 en materia de derecho al olvido (Guidelines on the implementatión of the Courrt of Justice of the European Unión Judgmente on "Google Spain and inc v, AEPD and Mario Costeja C-131/12), a cuyo tenor:

"Hay una diferencia básica entre la vida privada de la persona y su vida pública o profesional. La disponibilidad de la información en los resultados de búsqueda deviene más aceptable cuanta menos información revele sobre la vida privada de una persona (…) es más probable que la información tenga relevancia si está relacionada con la vida profesional del interesado, pero dependerá de la naturaleza del trabajo del interesado y del interés legítimo del público en tener acceso a esa información a través de una búsqueda por su nombre".

Por tanto, podrá procederse al tratamiento de dichos datos, estimándose adecuadas las cautelas adoptadas en cuanto a la limitación de la visibilidad a aquellos que ostentan un interés legítimo (operadores del juego) o actúan en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos (Consejo Superior de Deportes y Federación deportiva competente en los términos que ya se indicaron en el informe de esta Agencia 16/2019). No obstante, en estos casos serán igualmente aplicables las consideraciones realizadas a lo largo del presente informe, especialmente las relativas a los principios de exactitud, minimización y limitación del plazo de conservación.