

La consulta plantea la duda de “si se estaría incumpliendo con las premisas del RGPD por el hecho de comunicar la Oficina de Prevención y Lucha contra la Corrupción los datos personales de todos los ciudadanos vacunados sin que éstos estuvieran anonimizados o si bien, y atendiendo a la normativa anteriormente expuesta, sería coherente y suficiente proporcionar los datos anonimizados o limitarlos exclusivamente a los estrictamente necesarios para el objeto de la investigación iniciada por la citada Oficina los cuales en ningún caso se han detallado en la solicitud recibida”.

A estos efectos, se adjunta el requerimiento de información remitido por la Oficina de prevención y lucha contra la corrupción de las Illes Balears al Servicio de Salud de las Illes Balears, con el objeto de que se le facilite, en relación con los protocolos de vacunación de las Islas Baleares contra la COVID-19 y las actuaciones concretas de inoculación de las vacunas, y entre otra información solicitada, la siguiente:

2.1. Respecto de cada uno de los procesos y equipos de vacunación: establecimiento, oficina o local en el que se ha realizado la vacunación (residencias, PAC, hospitales, clínicas y otros), listados de personas inicialmente previstos para la vacunación, personas efectivamente vacunadas, viales suministrados y viales rechazados (en su caso).

2.2. Nombre, apellidos y DNI de la persona vacunada.

2.3. Identificación del grupo al que corresponde en el protocolo de vacunación.

2.4. Día y hora de la primera y la segunda dosis (en cuanto esta última, en el caso de que se haya inoculado).

2.5. Identificación del vial suministrado (código numérico).

I

Tal y como viene señalando esta Agencia de manera reiterada, en el momento de la formulación de la consulta debe partirse del nuevo régimen instaurado por 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, RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En efecto, como indica la Exposición de motivos de la Ley 3/2018 “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro

que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”.

Por consiguiente, es el responsable del tratamiento el que debe cumplir con los principios que se recogen en el artículo 5 del RGPD, entre los que se encuentra, según lo visto, el de responsabilidad proactiva, recogido en su apartado 2, “el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)”. Y entre los principios del apartado 1 se encuentra el de “licitud”, recogido en su letra a), de modo que los datos personales serán tratados de manera lícita, regulando el artículo 6 las bases jurídicas que determinan la licitud del tratamiento. Por lo tanto, es al responsable del tratamiento al que le corresponde determinar la base jurídica que puede amparar el tratamiento correspondiente.

Un papel fundamental, en fin, dentro de este nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeñará el delegado de protección de datos, que el Reglamento General regula en sus artículos 37 a 39. En particular, el artículo 37.1 a) impone obligatoriamente la designación de un delegado en los supuestos en que “el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial”.

A su vez, el artículo 38.1 establece claramente que “El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales” y el artículo 39.2 dispone que “El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento”.

Finalmente, el artículo 39.1 enumera las funciones del delegado de protección de datos, entre las que se encuentran “informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros” (apartado a), “supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes” (apartado b) y “ofrecer el asesoramiento que se le solicite

acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 (apartado c).

Asimismo le corresponde al delegado de protección de datos “actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto” (apartado e).

Por consiguiente, si el responsable del tratamiento tiene dudas sobre la base jurídica que pueda determinar la licitud de un determinado tratamiento deberá consultar a su delegado de protección de datos en los supuestos en que, como el presente, su designación es obligatoria, quien deberá prestarle el asesoramiento preciso.

Sólo en el caso de que el delegado de protección de datos tuviera dudas jurídicas sobre el asunto sometido a su consideración que no puedan resolverse con los criterios ya informados por la AEPD o por tratarse de cuestiones nuevas derivadas de la aplicación del nuevo régimen jurídico de protección de datos de carácter personal y que tengan un alcance general en el que resulte conveniente un informe que contribuya a la seguridad jurídica, podrá elevar dicho delegado consulta a este Gabinete Jurídico, acompañando a dicha consulta su propio informe en el que se analicen detallada y motivadamente las cuestiones objeto de consulta.

En el presente caso, la consulta se realice por el Delegado de Protección de Datos del Servicio de Salud de las Illes Balears mediante un documento breve en el que se limita a plantear la duda suscitada con una escueta fundamentación. Por ello, esta Agencia considera que, de acuerdo con los criterios señalados, hubiera sido necesario un análisis motivado y detallado de las cuestiones planteadas, atendiendo a la naturaleza de la entidad consultante y la entidad requirente de la información, así como a la normativa, jurisprudencia y doctrina aplicable. No obstante, dado el interés general apreciable en la consulta remitida y la urgencia de esta, se procede a la emisión del presente informe.

II

La Ley 16/2016, de 9 de diciembre, de creación de la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears crea, en su artículo 1, la citada Oficina, que depende orgánicamente del Parlamento de las Illes Balears y ejerce sus funciones con plena independencia, sometida únicamente al ordenamiento jurídico y se configura como una entidad de derecho público, con personalidad jurídica propia y plena capacidad de obrar para el cumplimiento de sus finalidades.

Entre sus funciones se encuentran, en relación con la prevención, la investigación y la lucha contra la corrupción, de acuerdo con el artículo 5.c).4º,

la de “Investigar o inspeccionar posibles casos de uso o destino irregulares de fondos públicos, así como las conductas opuestas a la integridad o contrarias a los principios de objetividad, eficacia y plena sumisión a la ley y al derecho”, delimitándose sus funciones en el artículo 6:

Artículo 6. Delimitación de las funciones.

1. La Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears actúa en cualquier caso en colaboración, y con el respecto a las funciones que les corresponden, con otros órganos y entidades públicas de las Illes Balears que ejercen competencias de control y supervisión de la actuación del Gobierno, de las administraciones públicas y del resto de entes del sector público. El reglamento de funcionamiento y de régimen interno de la Oficina regulará el procedimiento específico de actuación en los casos de ejercicio de funciones concurrentes con otros órganos.

2. La Oficina de Prevención y Lucha contra la Corrupción no tiene competencias en las funciones y materias que corresponden a la autoridad judicial, al ministerio fiscal y a la policía judicial, ni puede investigar los mismos hechos que sean objeto de sus investigaciones. En el supuesto de que la autoridad judicial o el ministerio fiscal inicien un procedimiento para determinar la relevancia penal de unos hechos que constituyan al mismo tiempo el objeto de actuaciones de investigación de la Oficina, esta deberá interrumpir acto seguido dichas actuaciones y aportar inmediatamente toda la información de que disponga a la autoridad competente, además de proporcionar, en lo que se refiere a las tareas de investigación, el apoyo necesario a la autoridad competente.

3. Cuando las investigaciones de la Oficina de Prevención y Lucha contra la Corrupción afecten al Parlamento de las Illes Balears, los entes estatutarios, las administraciones insulares y locales, la Universidad de las Illes Balears y, en general, los entes que gozan de autonomía reconocida constitucional o estatutariamente, se llevarán a cabo de modo que se garantice el debido respeto a su autonomía.

Por otro lado, el artículo 10 desarrolla las potestades de investigación e inspección:

Artículo 10. Potestades de investigación e inspección.

1. En el ejercicio de las funciones de investigación e inspección, la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears puede acceder a cualquier información que se encuentre en poder de los órganos, los organismos públicos o las personas físicas o jurídicas, públicas o privadas, incluidos en su ámbito de actuación. En el caso de los particulares, las potestades de inspección se limitarán a las actividades relacionadas con los contratos, las ayudas o las

subvenciones públicas otorgadas. En todo caso, el acceso a la información deberá estar justificado, se ha de motivar la relación con la actividad investigada y se debe dejar constancia de ello en el expediente.

2. El director o la directora de la Oficina de Prevención y Lucha contra la Corrupción o, por delegación expresa, el director adjunto o la directora adjunta o un funcionario o una funcionaria de la Oficina que tenga atribuidas funciones de investigación e inspección puede:

a) Personarse en cualquier oficina o dependencia de la Administración o centro afecto a un servicio público para solicitar información, realizar comprobaciones in situ y examinar los documentos, los expedientes, los libros, los registros, la contabilidad y las bases de datos, sea cual sea el soporte en el que estén registrados, así como los equipos físicos y logísticos utilizados, acreditando la condición de autoridad o agente de la Oficina.

b) Realizar las entrevistas personales que se estimen convenientes, tanto en la dependencia administrativa correspondiente como en la sede de la Oficina. Las personas entrevistadas que tengan o que se pueda deducir que tienen algún tipo de responsabilidad, pueden ir acompañadas y ser asistidas por la persona que designen. Asimismo, tienen los derechos y las garantías que establece la legislación vigente, incluidos los derechos a guardar silencio y a la asistencia letrada.

c) Acceder, si así lo permite la legislación vigente, a la información de cuentas bancarias en las que se hayan podido efectuar pagos o disposiciones de fondos relacionados con procedimientos de adjudicación de contratos públicos o de otorgamiento de ayudas o subvenciones públicas, por medio del requerimiento oportuno.

d) Determinar, a efectos de garantizar la indemnidad de los datos que se puedan recoger, que se hagan copias auténticas de los documentos obtenidos, sea cual sea el soporte en el que se encuentren almacenadas.

En cuanto a la conclusión de las actuaciones el artículo 16 prevé, fundamentalmente, la emisión de un informe razonado sobre las conclusiones de la investigación, que podrá incluir recomendaciones y recordatorios, que se remite al órgano que en cada caso corresponda:

Artículo 16. Conclusión de las actuaciones.

1. El director o la directora de la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears emitirá un informe razonado sobre las conclusiones de las investigaciones, que remitirá al órgano que en cada caso corresponda, el cual, posteriormente y en un plazo de tres meses, informará al director o a la directora de la Oficina de Prevención y Lucha contra la Corrupción sobre las medidas adoptadas o, en su caso, los

motivos que le impiden actuar de acuerdo con las recomendaciones y los recordatorios formulados.

2. Si en el curso de las actuaciones emprendidas por la Oficina de Prevención y Lucha contra la Corrupción se observan indicios de que se han cometido infracciones disciplinarias o han tenido lugar conductas o hechos presumiblemente delictivos, el director o la directora de la Oficina lo comunicará al órgano que en cada caso corresponda, así como, de forma inmediata, al ministerio fiscal o a la autoridad judicial en caso de indicio de delito. Se dará también traslado a la Sindicatura de Cuentas en caso de que de las investigaciones pueda derivarse una posible responsabilidad contable, directa o subsidiaria.

3. La Oficina de Prevención y Lucha contra la Corrupción puede dirigir recomendaciones razonadas a las administraciones y entidades públicas en las que inste la modificación, la anulación o la incorporación de criterios con la finalidad de evitar las disfunciones o las prácticas administrativas susceptibles de mejora, en los supuestos y las áreas de riesgo de conductas irregulares detectadas.

4. Si la relevancia social o la importancia de los hechos que han motivado la actuación de la Oficina de Prevención y Lucha contra la Corrupción lo requieren, el director o la directora de la Oficina puede presentar a la correspondiente comisión parlamentaria, a iniciativa propia o por acuerdo de la misma comisión, el informe o los informes extraordinarios que correspondan.

Asimismo, se prevé que las conclusiones derivadas de la actuación investigadora e inspectora se recogerán en la memoria anual que se remitirá a la Mesa del Parlamento, tal y como se regula en el artículo 13:

Artículo 13. Memoria anual.

1. En los tres primeros meses de cada anualidad, la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears elaborará una memoria anual descriptiva del conjunto de actuaciones desarrolladas durante el año anterior, en la que se recogerá un análisis global de las conclusiones derivadas de la actuación investigadora e inspectora, y la propuesta de medidas que se consideren apropiadas, así como la referencia a las medidas o actuaciones adoptadas por los órganos competentes.

No se incluirán los datos personales que permitan la identificación de las personas afectadas salvo que estos sean públicos como consecuencia de una sentencia firme o que hayan sido sancionadas en firme por contravenir el deber de colaboración establecido en el artículo 9 de esta ley. En todo caso, tienen que constar el número y el tipo de actuaciones emprendidas, con la indicación expresa de los expedientes iniciados, la dedicación, el tiempo y los recursos utilizados, los resultados de las investigaciones practicadas y la especificación de las recomendaciones

y los requerimientos cursados a las administraciones y los entes públicos, así como sus alegaciones.

La memoria contendrá, también, los expedientes tramitados que hayan sido enviados a la autoridad judicial o al ministerio fiscal, la estimación de las posibles cantidades económicas reclamadas en vía judicial o administrativa, las variaciones correspondientes a la gestión del personal propio y la liquidación del presupuesto de la Oficina de Prevención y Lucha contra la Corrupción del ejercicio anterior.

La liquidación del presupuesto de la Oficina de Prevención y Lucha contra la Corrupción en el ejercicio anterior y la situación de la plantilla, con la relación de puestos de trabajo, deben figurar también en la memoria anual.

2. La memoria anual se remitirá a la Mesa del Parlamento de las Illes Balears, a fin de que la traslade a la correspondiente comisión, la cual, en los términos previstos por el Reglamento del Parlamento y previa comparecencia del director o la directora de la Oficina de Prevención y Lucha contra la Corrupción, puede adoptar las resoluciones que considere oportunas

Por consiguiente, no se prevé la posibilidad de sancionar las posibles conductas ilícitas objeto de investigación, estableciéndose un régimen sancionador en la Ley 16/2016 referido, exclusivamente, a la infracción de las obligaciones de colaboración que impone la misma.

Por lo tanto, la Oficina de Prevención y Lucha contra la corrupción se configura como una Entidad de Derecho Público, adscrita al Parlamento, al que corresponde el control de la actuación de la Oficina y el nombramiento y el cese de su director o directora, así como la aprobación del reglamento de funcionamiento y régimen interno (artículo 7), estando prevista la iniciación de oficio de las actuaciones “Por iniciativa del Parlamento de las Illes Balears, mediante el acuerdo de la correspondiente comisión parlamentaria, tomado a instancia bien de dos grupos parlamentarios, bien de una quinta parte de los diputados y las diputadas de la cámara, bien a instancia de una comisión no permanente de investigación del propio Parlamento” (artículo 14.1.b).

Por consiguiente, su naturaleza jurídica se correspondería con la de un órgano auxiliar de los órganos parlamentarios, participando del control político que corresponde a los mismos.

Asimismo, queda excluida de su competencia las funciones que corresponden a la autoridad judicial y al ministerio fiscal, tal y como recuerda claramente su Exposición de Motivos (“ El cumplimiento de las funciones de la Oficina se entiende sin perjuicio de las encomendadas a otros órganos, a los que complementa actuando en diferentes estadios operativos, como la Intervención General e instituciones como el Síndic de Greuges o la Sindicatura de Cuentas y sus equivalentes insulares y municipales, y con exención de las que corresponden, de manera exclusiva, a la autoridad judicial y al ministerio

fiscal) y dispone su artículo 6.2: “La Oficina de Prevención y Lucha contra la Corrupción no tiene competencias en las funciones y materias que corresponden a la autoridad judicial, al ministerio fiscal y a la policía judicial, ni puede investigar los mismos hechos que sean objeto de sus investigaciones”.

Todo ello sin perjuicio de que se articule la debida colaboración de la Oficina con la autoridad judicial y el ministerio fiscal mediante la comunicación, cuando proceda, del resultado de las investigaciones (artículo 5.c) 2º y 16.2), la interrupción de las actuaciones, remisión de toda la información y prestación del apoyo que sea necesario cuando la autoridad judicial o el ministerio fiscal inicien un procedimiento para determinar la relevancia penal de unos hechos que constituyan al mismo tiempo el objeto de actuaciones de investigación de la Oficina (artículo 6.2), además de configurarse como una entidad de cooperación y relación permanente con la autoridad judicial y el ministerio fiscal (artículo 9.2.).

Por consiguiente, atendiendo a la naturaleza jurídica de la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears y a las funciones atribuidas a la misma, esta Agencia considera que los tratamientos de datos de carácter personal que se puedan realizar por la misma quedan sujetos al régimen general contenido en el RGPD y no al régimen especial de 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, y cuya norma de transposición se encuentra actualmente en tramitación en el Senado. A este respecto, se debe partir de lo señalado en el artículo 3.7 de la Directiva que define como autoridades competentes, a los efectos de la misma a “toda autoridad pública competente para la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública”, o “cualquier otro órgano o entidad a quien el Derecho del Estado miembro haya confiado el ejercicio de la autoridad pública y las competencias públicas a efectos de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluidas la protección y prevención frente a amenazas para la seguridad pública”.

En este sentido, el considerando 11 de la Directiva señala que

“Conviene por lo tanto que esos ámbitos estén regulados por una directiva que establezca las normas específicas relativas 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, incluidas la protección y la

prevención frente a las amenazas para la seguridad pública. 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. Cuando dicho organismo o entidad trate datos personales con fines distintos de los previstos en la presente Directiva, se aplica el Reglamento (UE) 2016/679. Así pues, el Reglamento (UE) 2016/679 se aplica en los casos en los que un organismo o entidad recopile datos personales con otros fines y proceda a su tratamiento para el cumplimiento de una obligación jurídica a la que esté sujeto. Por ejemplo, con fines de investigación, detección o enjuiciamiento de infracciones penales, las instituciones financieras conservan determinados datos personales que ellas mismas tratan y únicamente facilitan dichos datos personales a las autoridades nacionales competentes en casos concretos y de conformidad con el Derecho del Estado miembro. Todo organismo o entidad que trate datos personales en nombre de las citadas autoridades dentro del ámbito de aplicación de la presente Directiva debe quedar obligado por un contrato u otro acto jurídico y por las disposiciones aplicables a los encargados del tratamiento con arreglo a la presente Directiva, mientras que la aplicación del Reglamento (UE) 2016/679 permanece inalterada para el tratamiento de datos personales por encargados del tratamiento fuera del ámbito de aplicación de la presente Directiva”.

Y tal y como ya señaló esta Agencia al informar el anteproyecto de ley de transposición de la Directiva en su informe 122/2018, reiterado posteriormente en el informe 29/2002:

El ejemplo mencionado en el considerando 11 es expresivo al indicar claramente que el tratamiento llevado a cabo por el sujeto obligado a comunicar los datos a una autoridad competente está sometido a las disposiciones del Reglamento general de protección de datos y no a las de la Directiva, sin perjuicio de que una vez comunicados los datos a la autoridad competente sí será aplicable a ese tratamiento lo establecido en la Directiva, pero sin que esa aplicación implique que el sujeto obligado se encuentra sujeto a las previsiones de ésta última, toda vez que la comunicación se habrá llevado a cabo al amparo del artículo 6.1 c) del reglamento.

III

Una vez determinada la normativa aplicable a los tratamientos de datos personales que pueda realizar la Oficina de Prevención y Lucha contra la

Corrupción de las Illes Balears, procede atender al caso concreto, en el que se solicitan numerosos datos personales relacionados con las personas que han sido vacunadas contra la COVID19.

Para ello, debe partirse de la consideración de la información correspondiente al hecho de la vacunación como un dato relativo a la salud, dada la amplitud con la que se consideran dichos datos en el RGPD.

En este sentido, el artículo 4.15 del RGPD define como «*datos relativos a la salud*», aquellos *datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;*

Por su parte el Considerando (35) *Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. (...) todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.*

Y la jurisprudencia del Tribunal de Justicia de la Unión Europea viene abogando, igualmente, por una interpretación amplia del concepto, tal y como señalaba ya la Sentencia de 6 de noviembre de 2003 (asunto C-101/01, *Lindqvist*) interpretando la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en su apartado 50:

Teniendo en cuenta el objeto de esta Directiva, es preciso dar una interpretación amplia a la expresión «datos relativos a la salud», empleada en su artículo 8, apartado 1, de modo que comprenda la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona.

De lo expuesto debe concluirse que la información relativa a la condición de haberse recibido la vacuna, en cuanto revela información sobre el estado de salud de las personas que la han recibido, es un dato de salud, y por tanto debe incluirse dentro de las “*categorías especiales de datos*” de acuerdo con el artículo 9 del RGPD.

Respecto del tratamiento de datos personales correspondientes a las “categorías especiales de datos”, la regla general es su prohibición, tal y como se recoge en el artículo 9.1. del RGPD:

Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Por consiguiente, el tratamiento de las categorías especiales de datos personales debe encontrar cobertura en el artículo 9.2 RGPD y una vez excepcionada la prohibición general, hay que acudir a los supuestos del artículo 6 RGPD para dar licitud al tratamiento en cuestión. Así lo indicó ya el Grupo de Trabajo del Artículo 29 (cuyas funciones han sido asumidas por el Comité Europeo de Protección de Datos) en su dictamen “Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679” al indicar que (...) *Los responsables del tratamiento solo pueden tratar datos personales de categoría especial si se cumplen una de las condiciones previstas en el artículo 9, apartado 2, así como una condición del artículo 6.(...)*, y más recientemente, el Comité Europeo de Protección de Datos en sus “Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19, adoptadas el 21 de abril de 2020”:

Todo tratamiento de datos personales relativos a la salud debe cumplir los principios pertinentes establecidos en el artículo 5 del RGPD y ajustarse a una de las bases jurídicas y las excepciones específicas que se enumeran, respectivamente, en el artículo 6 y el artículo 9 del RGPD para la licitud del tratamiento de esta categoría especial de datos personales.

Por lo tanto, lo primero que procede analizar es si concurre alguno de las excepciones que *levantan la prohibición* del tratamiento de los datos relativos a la salud y que se recogen en el apartado 2 del artículo 9 del RGPD, al indicar que no será de aplicación en los siguientes supuestos:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la

seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de

datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. (...).

En relación con estas causas que levantan la prohibición del tratamiento de las categorías especiales de datos personales, la LOPDGDD contempla previsiones específicas en su artículo 9:

Artículo 9. Categorías especiales de datos.

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Asimismo, en relación con los tratamientos de datos de salud, la LOPDGDD contiene disposiciones específicas en su disposición adicional decimoséptima, señalando en su apartado 1 lo siguiente:

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

No obstante, como se señaló en el Informe de esta Agencia 101/2019,

[...] el contenido de la disposición adicional decimoséptima de la LOPDGDD ha de considerarse que si bien se establece una lista taxativa, dicha circunstancia no impide que el tratamiento de datos de salud pueda ampararse en otras normas que no se citen en la misma siempre y cuando que se de alguna de las circunstancias previstas en el artículo 9.2 del RGPD y la regulación establecida al efecto tenga rango de ley y cumpla las garantías que el Tribunal Constitucional considera esenciales cuando estamos ante el tratamiento de categorías especiales de datos.

Por su parte, el artículo 6 del RGPD establece los supuestos que permiten que el tratamiento de datos sea considerado lícito, a cuyo tenor se indica lo siguiente:

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

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.

Como se ha puesto de manifiesto, los artículos 6 y 9 del RGPD determinan los supuestos que permiten el tratamiento de datos personales, con carácter general, y con carácter específico respecto de las categorías especiales de datos, respectivamente.

Por su parte el artículo 8 de la LOPDGDD bajo la rúbrica “Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos” establece lo siguiente:

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.

Por último, una vez determinada la concurrencia de alguna de las excepciones del artículo 9.2. y una base jurídica del artículo 6.1., deberá darse cumplimiento al resto de principios contenidos en el artículo 5 del RGPD:

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

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»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

IV

Una vez expuesto, con carácter general, el marco jurídico aplicable a los tratamientos de salud procede analizar la posible concurrencia de alguno de los supuestos que permiten levantar la prohibición del tratamiento de datos de salud conforme al artículo 9.2. del RGPD y al artículo 9.2. de la LOPDGDD y, particularmente, dadas las competencias atribuidas a la Oficina requirente, la prevista en la letra g) del artículo 9.2. del RGPD:

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

En relación con la interpretación y el alcance de dicho precepto, se ha pronunciado recientemente esta Agencia en sus informes 31/2019 y 36/2020:

“Sin embargo, tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea “esencial”, adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados.

Dicho precepto encuentra su precedente en el artículo 8.4 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: “4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control”. No obstante, de su lectura resulta un mayor rigor en la nueva regulación por el RGPD, ya que se sustituye el adjetivo “importantes” por “esencial” y no se permite que la excepción pueda establecerse por las autoridades de control.

En relación con lo que debe entenderse por interés público esencial, debe tenerse igualmente en cuenta la Jurisprudencia del Tribunal Europeo de Derechos Humanos, que al amparo del artículo 8 del Convenio Europeo de Derechos Humanos, viene considerando que el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si se realiza de conformidad con la ley, sirve a un fin legítimo, respeta la esencia de los derechos y libertades fundamentales y es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo (D.L. contra Bulgaria, nº 7472/14, 19 de mayo de 2016, Dragojević contra Croacia, nº 68955/11, 15 de enero de 2015, Peck contra Reino Unido, nº 44647/98, 28 de enero de 2003, Leander contra Suecia, n.º 9248/81, 26 de marzo de 1987, entre otras). Como señala en la última sentencia citada, «el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue».

Asimismo, debe tenerse en cuenta la doctrina del Tribunal Constitucional respecto a las restricciones al derecho fundamental a la protección de datos, que sintetiza en su sentencia 292/2000, de 30 de noviembre, en la que después de configurar el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso, analiza los límites del mismo, señalando en lo siguiente:

Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no

le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2).

Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental

afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional [...]”. (Fundamento Jurídico 11)

“De un lado, porque si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril [RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley (STC 178/1985 [RTC 1985, 178]), éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación. Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [RTC 1993, 341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho

fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica [...]”. (FJ 15).

“Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [RTC 1989, 37], y 49/1999, de 5 de abril [RTC 1999, 49]).

De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. [...] (FJ 16)”.

Asimismo, nuestro Tribunal Constitucional ha tenido ya la ocasión de pronunciarse específicamente sobre el artículo 9.2.g) del RGPD, como consecuencia de la impugnación del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, introducido por la disposición final tercera de la Ley Orgánica 3/2018, de

5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, relativo a la legitimación de la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales, precepto que fue declarado inconstitucional por la Sentencia num. 76/2019 de 22 mayo.

Dicha sentencia analiza, en primer término, el régimen jurídico al que se encuentra sometido el tratamiento de las categorías especiales de datos en el RGPD:

De acuerdo con el apartado 1 del art. 9 RGPD, está prohibido el tratamiento de datos personales que revelen las opiniones políticas, del mismo modo que lo está el tratamiento de datos personales que revelen el origen étnico o racial, 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. No obstante, el apartado 2 del mismo precepto autoriza el tratamiento de todos esos datos cuando concorra alguna de las diez circunstancias allí previstas [letras a) a j)]. Algunas de esas circunstancias tienen un ámbito de aplicación acotado (laboral, social, asociativo, sanitario, judicial, etc.) o responden a una finalidad determinada, por lo que, en sí mismas, delimitan los tratamientos específicos que autorizan como excepción a la regla general. Además, la eficacia habilitante de varios de los supuestos allí previstos está condicionada a que el Derecho de la Unión o el de los Estados miembros los prevean y regulen expresamente en su ámbito de competencias: es el caso de las circunstancias recogidas en las letras a), b), g), h), i) y j).

El tratamiento de las categorías especiales de datos personales es uno de los ámbitos en los que de manera expresa el Reglamento General de Protección de Datos ha reconocido a los Estados miembros "margen de maniobra" a la hora de "especificar sus normas", tal como lo califica su considerando 10. **Este margen de configuración legislativa se extiende tanto a la determinación de las causas habilitantes para el tratamiento de datos personales especialmente protegidos -es decir, a la identificación de los fines de interés público esencial y la apreciación de la proporcionalidad del tratamiento al fin perseguido, respetando en lo esencial el derecho a la protección de datos- como al establecimiento de "medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2 g) RGPD]. El Reglamento contiene, por tanto, una obligación concreta de los Estados miembros de establecer tales garantías, en el**

caso de que habiliten para tratar los datos personales especialmente protegidos.

En relación con el primero de los requisitos exigidos por el artículo 9.2.g), la invocación de un interés público esencial y la necesaria especificación del mismo, el Alto Tribunal recuerda lo señalado en su sentencia 292/2000 en la que se rechazaba que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas, considerando que la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público" :

En la ya citada STC 292/2000 (RTC 2000, 292) , en la que también se enjuició una injerencia legislativa en el derecho a la protección de datos personales, rechazamos que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas:

"16. [...] De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concorra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.

17. En el caso presente, el empleo por la LOPD (RCL 2018, 1629) en su art. 24.1 de la expresión "funciones de control y verificación", abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la LOPD a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la

Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 LOPD, deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y suma en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.

Iguales reproches merece, asimismo, el empleo en el art. 24.2 LOPD de la expresión "interés público" como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE."

Esta argumentación es plenamente trasladable al presente enjuiciamiento. De igual modo, por tanto, debemos concluir que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público". Pues en otro caso el legislador habría trasladado a los partidos políticos -a quienes la disposición impugnada habilita para recopilar datos personales relativos a las opiniones políticas de las personas en el marco de sus actividades electorales- el desempeño de una función que solo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente sus límites y su regulación.

Tampoco puede aceptarse, por igualmente imprecisa, la finalidad aducida por el abogado del Estado, que se refiere al funcionamiento del sistema democrático, pues también encierra un grado elevado de incertidumbre y puede suponer un razonamiento circular. Por un lado, los partidos políticos son de por sí "cauces necesarios para el funcionamiento del sistema democrático" (por todas, STC 48/2003, de 12 de marzo (RTC 2003, 48) , FJ 5); y, por otro lado, todo el funcionamiento del sistema democrático persigue, en último término, la salvaguardia de los fines, valores y bienes constitucionales, pero ello no alcanza a identificar la razón por la cual haya de restringirse el derecho fundamental afectado.

Finalmente, debe precisarse que no es necesario que se pueda sospechar, con mayor o menor fundamento, que la restricción persiga una finalidad inconstitucional, o que los datos que se recopilen y procesen resultarán lesivos para la esfera privada y el ejercicio de los derechos de los particulares. Es suficiente con constatar que, al no poderse identificar con la suficiente precisión la finalidad del tratamiento de datos, tampoco puede enjuiciarse el carácter constitucionalmente legítimo de esa finalidad, ni, en su caso, la proporcionalidad de la medida prevista de acuerdo con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto.

Por otro lado, en cuanto a las garantías que debe adoptar el legislador, la citada sentencia núm. 76/2019 de 22 mayo, después de recordar que “A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”, analiza cuál es la norma que debe contener las citadas garantías:

“Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.

La cuestión solo puede tener una respuesta constitucional. La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.

Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de

derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares” (FJ 8).

Por consiguiente, el tratamiento de datos de salud al amparo del artículo 9.2.g) requiere que esté previsto en una norma de derecho europeo o nacional, debiendo tener en este último caso dicha norma, según la doctrina constitucional citada y lo previsto en el artículo 9.2 de la LOPDGDD, rango de ley. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en

conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6).”

Como ya se ha indicado, el TEDH considera que el derecho fundamental a la protección de datos de carácter personal forma parte del campo de aplicación del derecho al respeto de la vida privada y familiar, consagrado por el artículo 8 del CEDH. El apartado 2 de dicho precepto establece que *“no podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás”*.

En cuanto al tratamiento de los datos personales para una finalidad distinta, debe partirse del principio de limitación de la finalidad recogido en el artículo 5.1.b) del RGPD, según el cual los datos personales serán “recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales”.

En relación con el tratamiento para fines distintos, el artículo 6, en su apartado 4 señala que:

“Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

- a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;
- b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

- c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;
- d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;
- e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización”.

Atendiendo a dichos preceptos, la finalidad y la actividad legítima de quien trata los datos delimitarán la posibilidad de recogida y tratamiento de los mismos, debiendo además limitarse a los datos proporcionados o adecuados a tal finalidad. No es así lícito el tratamiento de datos que excedan de lo necesario para el cumplimiento del fin perseguido.

Al propio tiempo, los datos únicamente podrán emplearse para los fines que justifican esa recogida y, como veremos, de los que habrá debido ser informado el afectado, no siendo lícito el uso para otros fines.

Y el tratamiento para finalidades distintas sin el consentimiento del afectado es excepcional, hasta el punto de que el artículo 6.4 prevé que pueda establecerse por el Derecho de la Unión o de los Estados miembros siempre que “constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23.1”:

- 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”.

Por consiguiente, tanto por aplicación del artículo 9.2.g) como del artículo 6.4, el tratamiento de datos propuesto requiere una norma con rango de ley que lo habilite.

La STEDH de 4 de mayo de 2000 (Asunto Rotaru v. Rumanía), haciéndose eco de la citada sentencia de 16 de febrero de 2000, reiterada a su vez por muchas otras (dentro de las más recientes puede mencionarse la de 4 de diciembre de 2015 –asunto Zakharov v. Rusia–), recuerda que *“Tanto el almacenamiento de esos datos como su utilización, unida a la negativa de conceder al demandante la facultad de refutarlos, constituyen una injerencia en su derecho al respeto de su vida privada garantizado por el artículo 8.1”*. Dicha injerencia deberá resultar respetuosa con lo establecido en el mencionado artículo 8.1, recordando la STEDH de 16 de febrero de 2000 que “las palabras «previsto por la Ley» implican condiciones que van más allá de la existencia de una base legal en derecho interno y exigen que este sea «accesible» y «previsible»”, lo que exige analizar la “calidad” de la norma limitadora del derecho.

Esta doctrina, recogida por nuestro Tribunal Constitucional en los términos anteriormente señalados, implica que la Ley habilitante deberá encontrarse en vigor y cumplir el juicio de proporcionalidad, no bastando la mera adopción formal de la disposición para “validar” o “legitimar” sin más el tratamiento de datos de carácter personal.

V

Por otro lado, debe tenerse en cuenta, igualmente, la doctrina jurisprudencial contraria a las cesiones masivas de datos personales entre órganos administrativos.

En este sentido, es muy ilustrativa la interpretación que el Tribunal Constitucional hizo del artículo 16.3 de la Ley de Bases de Régimen en su sentencia 17/2013, de 31 de enero de 2013, en la que determinó la constitucionalidad del mismo.

Tal y como ha sido interpretado por el TC en dicha sentencia (FJ 8), este precepto se refiere a la cesión no consentida de los datos relativos a la residencia o el domicilio a otras Administraciones públicas que así lo soliciten solamente en aquellos casos en los que, para el ejercicio de sus competencias, sean aquellos datos relevantes. En suma, esta petición, que no se refiere específicamente a la cesión de datos del padrón en lo concerniente a los datos de los extranjeros, tiene por finalidad poder disponer de los datos relativos a la residencia o el domicilio que constan en el padrón municipal, (...). De esta forma, de acuerdo con la Ley Orgánica de protección de datos, la finalidad inicial que justificó la recogida de los datos por parte de una Administración pública no impide el destino posterior de los datos para su uso en finalidades diferentes de aquellas que motivaron su recogida respetando, en todo caso, el

principio de reserva de ley para establecer dicho cambio, (...) la Ley de bases de régimen local en su condición, además, de norma reguladora de un fichero como el padrón municipal puede prever cesiones de datos entre Administraciones públicas.

(...) los datos cedidos han de ser los estrictamente necesarios para el cumplimiento de las funciones asignadas a los órganos administrativos de forma que deberá motivarse la petición de aquellos datos que resulten relevantes, pues es necesario distinguir entre el análisis y seguimiento de una situación individualizada relativa a un caso concreto y el suministro generalizado e indiscriminado de toda la información contenida en un registro personal. El precepto ha contemplado ambos extremos de manera que cualquier cesión de los datos del padrón debe fundamentarse en la necesidad por parte de la Administración cesionaria actuando en el ejercicio de sus competencias, de conocer, en cada caso concreto, el dato relativo al domicilio de la persona afectada, extremos que han de ser adecuadamente valorados por la cedente a fin de apreciar si los datos que se solicita son realmente necesarios, pertinentes y proporcionados, atendiendo a la competencia que pretende ejercer la Administración cesionaria (art. 4 in fine de la Ley 30/1992). Se trata así de una regla de por sí restringida a los datos relativos a la residencia y al domicilio en cada caso concreto, y a la que le resultarán de aplicación, de más está decirlo, el resto de principios y previsiones que conforman el contenido del derecho reconocidos en la legislación sobre protección de datos.

Asimismo, la citada sentencia del Tribunal Constitucional 17/2013 analizaba, en su Fundamento Jurídico Noveno, un supuesto específico de acceso a los datos del padrón, por vía telemática, por la Dirección General de la Policía, para la exclusiva finalidad del ejercicio de las competencias establecidas en la Ley Orgánica de Derechos y Libertades de los Extranjeros en España y su Integración Social, sobre control y permanencia de extranjeros en España, y que se recoge en la disposición adicional séptima de la LBRL, introducida por el art. 3.5 de la Ley Orgánica 14/2003, de 20 de noviembre, en la que se señala lo siguiente:

“Ahora bien, dicha previsión legal ha de ser entendida de forma acorde con las exigencias de proporcionalidad que nuestra doctrina exige en la limitación de un derecho fundamental como es el aquí concernido, relativo la protección de datos de carácter personal. Eso significa que la cesión de datos que el acceso regulado por el precepto supone ha de venir rodeado de una serie de garantías específicas, garantías que, cumplimentadas por el órgano administrativo al que el precepto hace referencia, son, evidentemente, susceptibles de control. Entre ellas se encuentra la necesidad de motivar y justificar expresamente tanto la concreta atribución de la condición de usuario para el acceso telemático a los datos del padrón que el precepto prevé, como los concretos

accesos de que se trate, evitando –en cuanto que la exigible motivación de tales decisiones facilita su correspondiente control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional Contencioso-Administrativo– que se produzca tanto un uso torticero de dicha facultad como accesos indiscriminados o masivos. Límites al contenido del acceso que también resultan de determinadas previsiones de la legalidad ordinaria, las cuales han de ser aplicadas teniendo presente, en todo caso, la necesaria unidad del ordenamiento jurídico, tales como el art. 16.3 LBRL, que ya hemos examinado o, incluso, otras regulaciones específicas de la Ley Orgánica de protección de datos, en especial su art. 22.2. Resulta de ello que el acceso solamente será posible, en las condiciones antes dichas, cuando el concreto dato en cuestión resulte pertinente y necesario en relación con la finalidad que ha justificado el acceso, quedando garantizada la posibilidad de analizar si, en cada caso concreto, el acceso tenía amparo en lo establecido en la Ley pues, en caso contrario, no resultará posible su uso. Con tales garantías el acceso regulado en la disposición cuestionada resulta ser proporcionado en relación con la finalidad perseguida, ya que, en tanto que el dato resultante solo puede ser utilizado para la finalidad establecida en el precepto, ha de realizarse de forma puntual por quien se encuentre expresamente habilitado para ello y en relación a datos concretos cuya necesidad ha de ser también justificada de forma expresa y, por tanto, sometida a control, en los términos que acabamos de exponer.”

De lo anteriormente transcrito, y del resto de la fundamentación jurídica contenida en dicha sentencia resulta que el TC ha determinado que (i) habrá de evitarse el acceso indiscriminado y masivo a los datos personales (ii) el dato en cuestión solicitado habrá de ser pertinente y necesario (iii) para la finalidad establecida en el precepto (iv) la solicitud de acceso a los concretos datos personales habrá de motivarse y justificarse expresamente, (v) de manera que ello posibilite su control por el cedente (vi) y se evite un uso torticero de esa facultad con accesos masivos. Ello supone (vii) que ha de quedar garantizada la posibilidad de analizar si en cada caso concreto el acceso tenía amparo en lo establecido en la ley (art. 16.3 LBRL).

En idéntico sentido se ha pronunciado el Tribunal de Justicia de la Unión Europea, destacando los límites existentes a las comunicaciones masivas de datos personales incluso en los supuestos en que fueran solicitados por las autoridades competentes para la prevención, investigación, averiguamiento y enjuiciamiento de delitos.

En efecto, el Tribunal ha tenido la ocasión de pronunciarse acerca de la conformidad con el Derecho de la Unión, y particularmente con los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea de una norma de derecho derivado de la Unión, la Directiva 2006/24/CE, que permitía

la conservación por los operadores de los datos de tráfico generados por los abonados y usuarios de comunicaciones electrónicas para su comunicación a las autoridades competentes para la detección, prevención, investigación y enjuiciamiento de delitos graves, considerando que dicha medida vulnera dichos preceptos, por lo que la declara inválida (sentencia de 8 de abril de 2014, Asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland y otros).

Posteriormente, en su sentencia de 21 de diciembre de 2016 (Asuntos acumulados C-2013/15 y C-698/15, Tele2 Sverige AB y otros) el Tribunal analizó si las normas nacionales de trasposición de la mencionada Directiva 2006/24/CE podían considerarse conformes al Derecho de la Unión, apreciando que no existía dicha conformidad en una norma que previera la recogida generalizada e indiscriminada de los datos y no sometiera el acceso a los mismos al previo control administrativo y judicial.

En relación con la primera de las cuestiones mencionadas, el apartado 94 de la sentencia recordaba que “con arreglo al artículo 52, apartado 1, de la Carta, cualquier limitación del ejercicio de los derechos y libertades reconocidos por ésta deberá ser establecida por la ley y respetar su contenido esencial”, añadiendo el apartado 96 que “el respeto del principio de proporcionalidad se desprende igualmente de la reiterada jurisprudencia del Tribunal de Justicia según la cual la protección del derecho fundamental al respeto de la vida privada a nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (sentencias de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 56; de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 77; Digital Rights, apartado 52, y de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 92)”.

Dicho lo anterior, conforme al apartado 100, “la injerencia que supone una normativa de este tipo en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta tiene una gran magnitud y debe considerarse especialmente grave”. Y añade el apartado 103 que “si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 51)”.

Se concluye así que “una normativa nacional como la controvertida en el asunto principal excede, por tanto, de los límites de lo estrictamente necesario y no puede considerarse justificada en una sociedad democrática, como exige

el artículo 15, apartado 1, de la Directiva 2002/58, en relación con los artículos 7, 8, 11 y 52, apartado 1, de la Carta (apartado 107), siendo sin embargo conforme al Derecho de la Unión “una normativa que permita, con carácter preventivo, la conservación selectiva de datos de tráfico y de localización a efectos de la lucha contra la delincuencia grave, siempre que la conservación de los datos esté limitada a lo estrictamente necesario en relación con las categorías de datos que deban conservarse, los medios de comunicación a que se refieran, las personas afectadas y el período de conservación establecido” (apartado 108), para lo que la norma nacional “debe establecer, en primer lugar, normas claras y precisas que regulen el alcance y la aplicación de una medida de conservación de datos de este tipo y que establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos personales frente a los riesgos de abuso. Debe indicar, en particular, en qué circunstancias y con arreglo a qué requisitos puede adoptarse, con carácter preventivo, una medida de conservación de datos, garantizando que tal medida se limite a lo estrictamente necesario (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 54 y jurisprudencia citada)” (apartado 109). El apartado 11 señala que la delimitación del colectivo afectado “puede garantizarse mediante un criterio geográfico cuando las autoridades nacionales competentes consideren, sobre la base de elementos objetivos, que existe un riesgo elevado de preparación o de comisión de tales delitos en una o varias zonas geográficas”.

Por su parte, en cuanto a la segunda de las cuestiones señaladas; esto es, la relativa al control judicial o administrativo independiente y previo, el Tribunal señala en su apartado 116 que “en relación con el respeto del principio de proporcionalidad, una normativa nacional que regula los requisitos con arreglo a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder a las autoridades nacionales competentes acceso a los datos conservados debe garantizar, conforme a lo expresado en los apartados 95 y 96 de la presente sentencia, que tal acceso sólo se produzca dentro de los límites de lo estrictamente necesario”.

Será a juicio del Tribunal “el Derecho nacional en que debe determinar los requisitos conforme a los cuales los proveedores de servicios de comunicaciones electrónicas deben conceder dicho acceso. No obstante, la normativa nacional de que se trata no puede limitarse a exigir que el acceso responda a alguno de los objetivos contemplados en el artículo 15, apartado 1, de la Directiva 2002/58, ni siquiera el de la lucha contra la delincuencia grave. En efecto, tal normativa nacional debe establecer también los requisitos materiales y procedimentales que regulen el acceso de las autoridades nacionales competentes a los datos conservados (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 61)” (apartado 118).

El apartado 120 concluye que “Para garantizar en la práctica el pleno cumplimiento de estos requisitos, es esencial que el acceso de las autoridades nacionales competentes a los datos conservados esté sujeto, en principio, salvo en casos de urgencia debidamente justificados, a un control previo de un órgano jurisdiccional o de una entidad administrativa independiente, y que la decisión de este órgano jurisdiccional o de esta entidad se produzca a raíz de una solicitud motivada de esas autoridades, presentada, en particular, en el marco de procedimientos de prevención, descubrimiento o acciones penales (véase, por analogía, respecto a la Directiva 2006/24, la sentencia Digital Rights, apartado 62; véanse igualmente, por analogía, en relación con el artículo 8 del CEDH, TEDH, 12 de enero de 2016, Szabó y Vissy c. Hungría, CE:ECHR:2016:0112JUD003713814, §§ 77 y 80)”.

De este modo, tal y como viene señalando de manera reiterada esta Agencia, la doctrina que acaba de ponerse de manifiesto exige que el tratamiento masivo de datos para la persecución del delito se delimite claramente desde un triple punto de vista: por una parte se minimicen los datos objeto de tratamiento; por otra, se limiten los supuestos en que el acceso a los datos pueda llevarse, especificando por ejemplo la naturaleza de los delitos cuya gravedad justifica ese acceso; y por último, que exista un control, que en el caso de España debería ser judicial, previo al efectivo acceso a la información.

VI

Una vez expuesta la normativa y jurisprudencia aplicable para la resolución de la presente consulta, al objeto de valorar la adecuación a la normativa de protección de datos personales del requerimiento de información realizado por la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears debe destacarse lo siguiente:

En primer lugar, que la citada Oficina ha sido creada, tal y como señala en su Exposición de Motivos, como una medida de mejora de la calidad democrática y una herramienta de lucha contra el fraude y la corrupción, y “tiene como objetivo prevenir e investigar posibles casos de uso o de destino fraudulentos de fondos públicos o cualquier aprovechamiento ilícito, derivado de conductas que comporten conflicto de intereses o el uso particular de informaciones derivadas de las funciones propias del personal al servicio del sector público”. Asimismo, añade que “La creación de esta oficina cumple lo dispuesto en el artículo 6 de la Convención de las Naciones Unidas contra la corrupción, aprobada en Nueva York el 31 de octubre de 2003, por el hecho de que garantiza la existencia de un órgano especializado e independiente encargado de prevenir la corrupción”.

La citada Convención de las Naciones Unidas contra la corrupción, ratificada el 9 de junio de 2006 y en vigor para España desde el 19 de Julio de

2006, destaca en su Preámbulo la preocupación por “la gravedad de los problemas y las amenazas que plantea la corrupción para la estabilidad y seguridad de las sociedades al socavar las instituciones y los valores de la democracia, la ética y la justicia y al comprometer el desarrollo sostenible y el imperio de la ley”.

Asimismo, la lucha contra la corrupción se encuentra recogida en otras normas europeas, como el Convenio relativo a la lucha contra los actos de corrupción en los que estén implicados funcionarios de las Comunidades Europeas o de los Estados miembros de la Unión Europea, hecho en Bruselas el 26 de mayo de 1997, o en otras más recientes como las últimas Directivas sobre contratación pública, incorporadas a nuestro ordenamiento jurídico por la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Por consiguiente, la lucha contra la corrupción puede considerarse, a los efectos del artículo 9.2.g) del RGPD, como un interés público esencial.

Por otro lado, partiendo del deber de suministrar información que impone el artículo 10 de la Ley 16/2016, de 9 de diciembre, de creación de la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears, la misma prevé una serie de garantías, destacando el deber de secreto recogido en el artículo 7.3: “Las personas que ejerzan su actividad en la Oficina de Prevención y Lucha contra la Corrupción están obligadas a guardar secreto de todo cuanto conozcan por razón de su función en los términos legalmente establecidos, deber que perdura tras su cese en el ejercicio del cargo. El incumplimiento de este deber de secreto da lugar a la responsabilidad que, en cada caso, corresponda”. Asimismo, otra garantía serían las previstas en el propio artículo 10.1, cuando prevé que “el acceso a la información deberá estar justificado, se ha de motivar la relación con la actividad investigada y se debe dejar constancia de ello en el expediente”.

No obstante, si bien las circunstancias anteriores podrían llevar a considerar admisible, en un caso concreto y debidamente justificado, el acceso a determinados datos de salud, en el presente caso, dicha solicitud se considera excesiva y contraria a la normativa sobre protección de datos personales, por las siguientes razones:

En primer lugar, nada se indica en el requerimiento de información respecto de la finalidad concreta para la que se reclama la información, aunque atendiendo a la misma, parece que va referida a verificar el cumplimiento de los protocolos de vacunación respecto de las personas que han recibido la vacuna. Y el artículo 9.2.g) del RGPD requiere que el tratamiento sea necesario, y no se ha justificado en el requerimiento la necesidad de acceder a los datos personales de las personas vacunadas en relación con la investigación que se está realizando, lo que requeriría la realización del triple juicio de idoneidad,

necesidad y proporcionalidad, valorando si la comunicación de datos personales relativos a la salud de determinadas personas es necesaria para el cumplimiento de la finalidad de control de la acción administrativa perseguida, y si dicha finalidad no puede alcanzarse por otros medios que no requieran la comunicación de dichos datos, como podría ser, por ejemplo, la comunicación de la información agregada (es decir, anonimizada, de forma que no permita la identificación de personas físicas) referida a los distintos grupos de vacunación previstos en los protocolos de vacunación o la no pertenencia a alguno de ellos, indicando el número total de personas que se encontrarían en cada uno de esos supuestos.

Por otro lado, porque dicho requerimiento supone un tratamiento masivo de datos personales que, como se señala en la consulta, afectaría, al menos, a 108.500 personas, lo que es contrario al principio de minimización de datos y a la doctrina del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea anteriormente citada.

Madrid, a 04 de mayo de 2021