

0077/2023

La consulta plantea si es conforme al 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 (RGPD en lo sucesivo), a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo) y a la Ley 2/2023 de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, (Ley 2/2023 en lo sucesivo), la utilización por parte de la consultante de aquellas informaciones recibidas al amparo de dicha ley y que no entren dentro de su ámbito de aplicación para cumplir otras finalidades como la eficiencia, transparencia y buen gobierno.

En concreto, se plantea la viabilidad de llevar a cabo el tratamiento de aquella información (que contenga datos personales) que se comunique a través del Sistema Interno de Información y que no tenga relación con las conductas a que se refiere el artículo 2 de la Ley 2/2023 con el fin de atender eficientemente todas las comunicaciones recibidas a través de este Sistema.

I

La consulta planteada conlleva el tratamiento de datos de carácter personal por lo que será de aplicación el RGPD y la LOPDGDD.

Para que un tratamiento resulte conforme al marco jurídico actual en materia de protección de datos debe cumplir, entre otras cuestiones, los principios de protección de datos previstos en el artículo 5 del RGPD a cuyo tenor:

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»).

II

Teniendo en cuenta que la consultante propone un tratamiento consistente en que la información que se reciba en el Sistema de Información previsto en la citada Ley 2/2023 que contenga datos de carácter personal pueda utilizarse para otras finalidades, lo primero que hay que hacer es abordar la regulación de la citada ley 2/2023.

En efecto, conviene destacar lo dispuesto en el artículo 1 de esta, que dispone::

Artículo 1. Finalidad de la ley.

- 1. La presente ley tiene por finalidad otorgar una protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen sobre alguna de las acciones u omisiones a que se refiere el artículo 2, a través de los procedimientos previstos en la misma.*
- 2. También tiene como finalidad el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.*

Es decir, la finalidad a la que sirve la norma es clara y circunscrita a un propósito fundamental, que es el de otorgar la protección adecuada frente a las represalias que puedan sufrir las personas físicas que estén dentro del ámbito subjetivo de aplicación (artículo 3) y que informen de conductas a las que se refiere el ámbito objetivo de aplicación (artículo 2).

Respecto de la base jurídica que legitima el tratamiento en el Sistema Interno de información, la propia ley en su artículo 30 bajo la denominación “*licitud de los tratamientos de datos personales*” dispone en su apartado 2 lo siguiente:

2. El tratamiento de datos personales, en los supuestos de comunicación internos, se entenderá lícito en virtud de lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo, cuando, de acuerdo a lo establecido en los artículos 10 y 13 de la presente ley, sea obligatorio disponer de un sistema interno de información.

Si no fuese obligatorio, el tratamiento se presumirá amparado en el artículo 6.1.e) del citado reglamento.

Por lo tanto, la finalidad está descrita y la base jurídica para la consultante, al resultar afectada por la norma, será el cumplimiento de una obligación legal aplicable al responsable del tratamiento, de acuerdo con el artículo 6.1 c) RGPD y 8.1 de la LOPDGDD.

Teniendo en cuenta lo anterior, la consultante plantea en su consulta la posibilidad de que la información que se recabe por aplicación de la citada Ley 2/2023 y que tras su análisis se estime que dicha información no se refiere a las acciones u omisiones que se prevén en el artículo 2, pueda ser tratada (utilizada) para otras finalidades que interpreta que se extraen del artículo 112 de la Ley 40/2015 de 1 de octubre de Régimen Jurídico del Sector Público, justificando dicho tratamiento en la base jurídica del cumplimiento de una obligación legal y/o en la satisfacción de un eventual interés legítimo.

En concreto, el citado artículo 112 de la Ley 40/2015 indica lo siguiente:

La Administración General del Estado y las entidades integrantes del sector público institucional, en cuanto titulares del capital social de las sociedades mercantiles estatales, perseguirán la eficiencia, transparencia y buen gobierno en la gestión de dichas sociedades mercantiles, para lo cual promoverán las buenas prácticas y códigos de conducta adecuados a la naturaleza de cada entidad.

La consultante al amparo -alega- de la búsqueda de eficiencia, transparencia y buen gobierno propone trasladar aquellas informaciones que no entren dentro del ámbito de la Ley 2/2023 y que le hayan sido proporcionadas al área correspondiente de la entidad para su correcta gestión y resolución.

Así pues, por lo tanto, de un lado tenemos la base jurídica y la finalidad que prevé expresamente la Ley 2/2023, y por otro la base jurídica y las nuevas finalidades que propone la consultante para la información facilitada conforme a una finalidad diferente.

Planteados los términos de la consulta lo primero que conviene aclarar es que a aquellas informaciones que se reciban en el Sistema Interno de Información pero que en las cuales las personas informantes no están dentro de las categorías a las que se refiere el artículo 3, o los hechos denunciados no se refieren a conductas previstas en ámbito material de aplicación del artículo 2, se les sigue aplicando la citada Ley, pero en otra medida o con menor intensidad -por ejemplo, no se aplicarían las medidas de apoyo o la protección frente a represalias, pues puede no tener sentido.-

Sea como fuere, no desaparecen las garantías y salvaguardas para tratar la información y tampoco las obligaciones del responsable del tratamiento que se encuentran en el articulado de la norma.

En efecto, en la propia norma se encuentran preceptos de los que se deriva que la finalidad del tratamiento sigue vigente incluso respecto de aquellas informaciones que no pasen el “filtro” de los artículos 2 y 3 y, por tanto, dicha información será tramitada conforme a las previsiones que precisamente la norma haya establecido.

Así por ejemplo, respecto del Sistema interno de información, entre otras circunstancias, la ley 2/2023 desarrolla el Sistema interno de información de manera independiente de la información que se le proporcione. El artículo 5 de la ley indica en su apartado b) que dicho sistema estará *diseñado, establecido y gestionado de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación, y de las actuaciones que se desarrollen en la*

gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado. Quiere decir esto, que incluso aquellas informaciones que se inadmitan se sitúan bajo el abrigo de estas salvaguardas, pues como establece la Exposición de Motivos de la ley 2/2013: La configuración del Sistema interno de información debe reunir determinados requisitos, entre otros, su uso asequible, las garantías de confidencialidad, las prácticas correctas de seguimiento, investigación y protección del informante.

Asimismo en el apartado i) del art. 5 se establece la obligación de contar con un procedimiento de gestión de las informaciones recibidas, donde por ejemplo, resultará obligatoria una previsión sobre cómo actuar con las informaciones que se inadmitan, o en el propio apartado j), que indica que dicho sistema ha de establecer las garantías para la protección de los informantes en el ámbito de la propia entidad u organismo, *respetando, en todo caso, lo dispuesto en el artículo 9*, lo que nos lleva a considerar que incluso aquel informante que forme parte de la plantilla de empleados e informe sobre una conducta que, tras el análisis de admisibilidad se observe que la misma no está dentro del ámbito del artículo 3, seguirá gozando de la garantía de confidencialidad y en su caso anonimato.

Y no menos importante es la referencia que se hace a lo indicado en el artículo 9, que en su apartado h) hace a su vez una remisión al respeto a las disposiciones sobre protección de datos personales de acuerdo con el título VI.

Pues bien, del Título VI de la ley 2/2013, bajo la denominación “Protección de datos personales”, conviene citar los siguientes preceptos:

Artículo 29. Régimen jurídico del tratamiento de datos personales.

Los tratamientos de datos personales que deriven de la aplicación de esta ley se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (...)

No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una información específica o, si se recopilan por accidente, se eliminarán sin dilación indebida.

Por su parte, el artículo 32 de la misma norma, bajo la denominación “Tratamiento de datos personales en el Sistema interno de información” circunscribe en su apartado 1 el acceso a los datos personales obrantes en dicho sistema a aquellas personas incluidas en las letras a) a e).

Es decir, ese *numerus clausus* es otra manifestación del principio de limitación de finalidad traído a este ámbito, por cuanto los destinatarios que se incluyen

en el precepto ostentan unas competencias en el contexto de la propia ley, que coadyuvan a cumplir la finalidad prevista en el ya citado artículo 1 y que no desaparecen en aquellas informaciones que no pasen el filtro de los artículos 2 y 3, precisamente porque las mismas -aunque de modo temporal como a continuación se analiza- se encuentran incluidas en el Sistema Interno de información previsto en la ley.

Especial atención merece el inciso final del segundo párrafo del apartado 2 del citado artículo 32, cuando se refiere a que (...) *se suprimirán todos aquellos datos personales que se puedan haber comunicado y que se refieran a conductas que no estén incluidas en el ámbito de aplicación de la ley.* (...), por cuanto establece una previsión ad hoc sobre qué hacer con aquellas informaciones que no entran dentro del ámbito de aplicación de la norma, que a la sazón es lo que plantea la consultante. Esta indicación no hace otra cosa que recordarnos, sensu contrario, la vigencia del principio de limitación de la finalidad, por cuanto si respecto a determinados datos personales no es posible llevar a cabo los tratamientos de datos previstos en la ley 2/2023 (precisamente porque escapan del ámbito material o del ámbito subjetivo), habrá que proceder a su eliminación.

Pero es que, además, el apartado 4 del citado artículo 32 establece una cláusula de cierre que también se impregna del cumplimiento del principio de limitación de la finalidad, estableciendo una limitación temporal, al indicar lo siguiente:

4. En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

Es decir, si el tratamiento de los datos que se derive la presentación de informaciones no va a servir al propósito previsto en la norma, deberá, con carácter general procederse a su supresión.

Finalmente, otro precepto a tener en consideración pues también tiene incidencia sobre cómo obrar con las informaciones recibidas en el Sistema interno de información es el previsto en el artículo 26 bajo la rúbrica Registro de Informaciones y que en su apartado 2, nos indica que:

Los datos personales relativos a las informaciones recibidas y a las investigaciones internas a que se refiere el apartado anterior solo se

conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con esta ley. En particular, se tendrá en cuenta lo previsto en los apartados 3 y 4 del artículo 32. En ningún caso podrán conservarse los datos por un período superior a diez años.

Como puede observarse se incluyen todas las informaciones recibidas, hayan dado lugar a actuaciones o no. Es decir, también a las que hace referencia la consultante.

Sobre los deberes de conservación de la información que se reciba en los sistemas internos de información, a la luz de la interpretación de los artículos 32.3 y 4 de la citada ley, este Gabinete Jurídico se pronunció en el Informe 60/2023 estableciendo los siguientes criterios:

(...) tanto si no se han iniciado las actuaciones como si se han llevado a cabo, una vez transcurridos los plazos indicados, los datos personales deberán suprimirse del sistema, salvo que se conserven de manera anonimizada a los efectos de acreditar la existencia y funcionamiento del sistema, por ejemplo, ante la Autoridad Independiente de Protección del Informante.

Y, por otro lado, el libro-registro que contiene tanto las informaciones recibidas como las actuaciones realizadas, y cuyo acceso se encuentra más limitado, la propia norma indica que no es público, y únicamente se podrá acceder a petición razonada por la autoridad judicial competente, siendo los plazos de conservación los estrictamente necesarios para cumplir con la ley, y en todo caso de diez años como máximo.

Dicho lo anterior, respecto de las conclusiones de la consultante, cabe indicar que esta Agencia comparte la primera conclusión, la existencia de dos espacios (o repositorios en los términos utilizados por la consultante) perfectamente diferenciados para tratar la información.

(...)

Ahora bien, debe recordarse en este punto a la consultante, como responsable del tratamiento, las obligaciones que dimanen de tal condición, y en especial las medidas de responsabilidad proactiva que en este aspecto cobran especial relevancia por el modo de tratar y almacenar la información, de acuerdo con lo indicado en los artículos 24 y 32 del RGPD.

Respecto de la tercera cuestión, es en definitiva cómo actuar en el caso de que se haya llevado a cabo una investigación y ésta haya concluido. La consultante sostiene que, si el libro registro tuviera el

formato de gestor documental, se podrían eliminar del Sistema Interno de Información los datos personales quedando así la información anonimizada al igual que sucede cuando se recibe una información y no se inician actuaciones o no son admitidas a trámite.

Pues bien, como se ha indicado antes, si se han llevado a cabo actuaciones y han finalizado, se estaría a los plazos que la norma establece para llevar a cabo estas, 3 o 6 meses según los casos, y transcurridos los mismos, se suprimirían del sistema, salvo que quedaran de forma anonimizada a los únicos efectos antes indicados.

(...)

En mérito de lo que antecede, cabe considerar que las informaciones recibidas que no pasen el trámite de admisibilidad de acuerdo con los artículos 2 y 3 de la Ley no están excluidas de la finalidad del tratamiento previsto en el artículo 1, por lo que la base jurídica para tratar los datos personales que en ellas se encuentren siguen resultando de aplicación.

Por lo tanto, si la consultante pretende utilizar los datos a los que tiene acceso a raíz de ser sujeto obligado por la Ley 2/2023 y, por tanto, al amparo del artículo 6.1 c) RGPD y 8.1 LOPDGDD, debe acomodar este nuevo tratamiento al principio de finalidad y encontrar otra base jurídica de legitimación.

III

Llegados a este punto conviene traer a colación lo indicado en el Informe 89/2020 de esta AEPD, que aborda, entre otras cuestiones, el uso posterior de datos personales derivado de un tratamiento que se realiza en cumplimiento de una obligación legal (publicación en boletines oficiales), y recuerda los requisitos que han de darse para poder considerar lícito un tratamiento de datos que constituya una injerencia al derecho fundamental a la protección de datos personales:

(...)

Por ello, tal y como se ha ido adelantando, cuando se trata de la publicación de datos personales al amparo de las previsiones contenidas en las letras c) o e) del RGPD, debe tenerse en cuenta la jurisprudencia y la doctrina de esta Agencia respecto a los requisitos para legitimar la misma, al objeto de respetar el principio de proporcionalidad y establecer las garantías oportunas.

En este sentido, esta Agencia viene reiterando cómo, en los supuestos del artículo 6.1., letras c) y e), el RGPD contiene previsiones específicas al respecto, comenzando con las previstas en su propio artículo 6, apartados 2 y 3, cuya redacción es la siguiente:

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

Por otro lado, debe tenerse igualmente en cuenta que, en el caso de que la obligación venga impuesta por una norma de derecho interno, la misma deberá tener rango de ley, por exigirlo el artículo 53.1 de la Constitución, tal y como expresamente recoge el artículo 8.1 de la LOPDGDD, añadiendo 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” y deberá tenerse en cuenta la doctrina constitucional recogida, fundamentalmente, en las sentencias 292/2000 de 30 noviembre y 76/2019 de 22 de mayo, conforme a **la cual los límites al derecho fundamental a la protección de datos personales**

deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, siendo la propia ley la que habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El Tribunal Constitucional (TC) ha sido claro en cuanto a que 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 artículo 53.1 CE (...). Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...). Se trata, en definitiva, de “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”. Tampoco sirve por ello que para el establecimiento de dichas garantías adecuadas y específicas la ley se remita al propio RGPD o a la LOPDGDD.

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).”

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

*Pues bien, la **STJUE de 6 de octubre de 2020**, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, en su apartado 175, recuerda que:*

En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

*Igualmente, el apartado 65 de la **Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17)**, Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:*

Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice: Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos.

*Y en dicha **STJUE de 16 de julio de 2020**, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):*

176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado

La ya citada STJUE de 6 de octubre de 2020, en el caso C-623/17, añade la mención de las categorías especiales de datos:

68 (...) Estas consideraciones son aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles [véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].

En consecuencia, los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas.

(...)

En el presente caso, del análisis del precepto legal en que la consultante pretende basar el tratamiento de los datos que conozca a raíz de la Ley 2/2023, (es decir del artículo 112 de la Ley 40/2015), se ha de considerar que no se cumple los requisitos que se acaban de indicar para justificar la injerencia en el derecho a la protección de datos que se produciría.

Siendo la principal razón porque ni se prevé directa o indirectamente en dicho precepto la injerencia, y en consecuencia tampoco se justifica la obligación legal o el interés público que justificarían un tratamiento de datos personales diferente al previsto por la propia ley 2/2013, y obviamente tampoco se establecen garantías o límites de ninguna clase en la norma para el tratamiento concreto que se propone.

Por lo tanto, el cumplimiento una obligación legal ex artículo 6.1 c) RGPD, a la luz del artículo 112 de la Ley 40/2015 de 1 de octubre, tal y como propone la consultante, no serviría como base jurídica para poder considerar lícitos dichos tratamientos.

Asimismo, la consultante identifica como segunda opción para encontrar la legitimación en el nuevo tratamiento la prevista en el artículo 6.1 f) del RGPD, es decir, cuando el tratamiento es necesario para la satisfacción del interés legítimo del responsable o de un tercero.

Frente a ello que hay que indicar que, corresponde al responsable del tratamiento realizar el juicio de ponderación o prueba de sopesamiento teniendo en cuenta la injerencia en los derechos e intereses de los titulares de los datos. En el **Dictamen 6/2014 Sobre el concepto de interés legítimo** del Grupo de Trabajo del Artículo 29 – actualmente Comité Europeo de Protección de Datos- se muestran elementos o factores clave que el responsable ha de tener en cuenta a la hora de sopesar sus intereses y los derechos del interesado, concretándolos en los siguientes:

- a) evaluación del interés legítimo del responsable del tratamiento;
- b) impacto sobre los interesados;
- c) equilibrio provisional y
- d) garantías adicionales aplicadas por el responsable del tratamiento para impedir cualquier impacto indebido sobre los interesados

Pues bien, sin perjuicio de que corresponde al responsable del tratamiento su análisis y valoración al tratamiento concreto, conviene adelantar ya que en el siguiente apartado del presente informe se analiza la compatibilidad de la finalidad de un nuevo tratamiento como el que propone la consultante y cuyos elementos utilizados y resultado final resultarían determinantes y a tener en cuenta en un hipotético juicio de ponderación o prueba de sopesamiento.

Por su parte, el Considerando 47 RGPD dispone que:

(...) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable (...)

En efecto, procede destacar así la nota de previsibilidad en el tratamiento posterior, que resulta un elemento determinante tanto en la compatibilidad de finalidad como en la prueba de sopesamiento. En este sentido la reciente Sentencia del Tribunal de Justicia de la Unión Europea de fecha 7 de diciembre de 2023, Asuntos acumulados C-26/22 y C-64/22, SCHUFA Holding, indica en el apartado 80 que:

(...) como resulta del considerando 47 del RGPD, los intereses y los derechos fundamentales del interesado pueden, en particular, prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de datos personales en circunstancias en las que el interesado no espera razonablemente que se realice tal tratamiento [sentencia de 4 de julio de 2023, Meta Platforms y otros (Condiciones generales del servicio de una red social), C-252/21, EU:C:2023:537, apartado 112 y jurisprudencia citada].

Como más adelante se explica, difícilmente un hipotético informante que acude al Sistema interno de información, revestido por la ley de notas de confidencialidad y anonimato, puede esperar razonablemente que la información que aporta pueda usarse para otra finalidad como la que pretende la consultante.

IV

Respecto de la nueva finalidad que se pretende, hay que partir del respeto al principio de limitación de finalidad, según el cual (artículo 5.1 c) RGPD) *los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines*; y como se ha explicado antes la finalidad del tratamiento de datos personales que se derive la presentación de informaciones -hayan sido o no admitidas- está prevista en la propia ley, y en consecuencia, la aplicación de la misma, en cuanto al procedimiento a seguir, los deberes de confidencialidad y los plazos, modos y lugar de conservación, a cualquier información, tenga o no que ver con el objeto de la ley, está fuera de toda duda (así se desprende de los distintos preceptos que se han ido citando durante el presente informe).

Dicho lo anterior, el **Dictamen 3/2013** del Grupo de Trabajo del Artículo 29, actualmente Comité Europeo de Protección de Datos, sobre la “**Limitación de la Finalidad**” es perfectamente aplicable en la actualidad, y resulta especialmente clarificador dados los elementos afectados por la presente consulta.

Así como punto de partida, sobre el principio de limitación de finalidad, nos indica lo siguiente:

(...) el principio de limitación de la finalidad inhibe la «desviación de la misión», que de otro modo podría dar lugar a la utilización de los datos personales disponibles más allá de los fines para los que fueron inicialmente recogidos.

(...) La prohibición de la «incompatibilidad» que figura en el artículo 6, apartado 1, letra b), no excluye completamente nuevos usos de los datos, siempre que ello se lleve a cabo dentro de los parámetros de compatibilidad.

(...) El principio de limitación de la finalidad está concebido para ofrecer un enfoque equilibrado: un enfoque que tenga por objeto conciliar la necesidad de previsibilidad y seguridad jurídica en relación con los fines del tratamiento, por una parte, y la necesidad pragmática de una cierta flexibilidad por otra.

(...) La limitación debe, por ejemplo, impedir el uso de los datos personales de las personas de una manera (o para otros fines) que puedan encontrar inesperada, inadecuada o inaceptable por lo demás. Al mismo tiempo, el concepto de uso compatible también ofrece cierto grado de flexibilidad para los responsables del tratamiento de datos.

(...) El hecho de que el tratamiento ulterior tenga una finalidad distinta no significa necesariamente que sea automáticamente incompatible: esto debe evaluarse caso por caso, como se demostrará a continuación.

(...)

En el presente caso, al pretender la consultante una finalidad distinta a la establecida por la norma es preciso tener en cuenta aquellos parámetros que el propio Dictamen 3/2013 propone al responsable del tratamiento a la hora de evaluar la nueva finalidad.

(...) El tratamiento ulterior con un fin diferente no significa necesariamente que sea incompatible: la compatibilidad debe evaluarse caso por caso. Una evaluación de compatibilidad sustancial requiere una evaluación de todas las circunstancias pertinentes. Deben tenerse en cuenta, en particular, los siguientes factores clave:

- (i) la relación entre los fines para los que se recogieron los datos personales y los fines de su tratamiento ulterior;*
- (ii) el contexto en el que se recogieron los datos personales y las expectativas razonables de los interesados en cuanto a su uso ulterior;*
- (iii) la naturaleza de los datos personales y el impacto del tratamiento ulterior en los interesados;*
- (iv) las garantías adoptadas por el responsable del tratamiento para garantizar un tratamiento equitativo y prevenir cualquier repercusión indebida en los interesados.*

(...)

Teniendo en cuenta dichos parámetros procede abordarlos para proponer una respuesta en derecho.

En primer lugar, en cuanto a *la relación entre los fines para los que se recogieron los datos personales y los fines de su tratamiento ulterior*; podemos considerar que no hay relación de suficiente entidad para valorar positivamente dicha compatibilidad. Téngase en cuenta que la intención del hipotético informante sería poner de manifiesto conductas sobre corrupción y obtener la protección de la norma. Ahora, tras el análisis de admisibilidad y su desestimación se da traslado a otro departamento o área de la entidad para otras cuestiones, que si bien pueden ser indirectamente beneficiosas para la entidad, -como la eficiencia o el buen gobierno- están alejadas del fin último de la norma que es la lucha contra la corrupción. Como vemos son fines alejados, y para su cumplimiento se estaría produciendo una injerencia en el derecho a la protección de datos del interesado, que no cabe entender que puede ser positivo para el interesado. Bien al contrario, la mera posibilidad de que se conozca que una persona ha denunciado una actuación, aunque esta luego resulte no integrar los supuestos de aplicación de la ley 2/2023, resultaría -basta con que “pueda resultar”- en un desvalor o posibilidad de represión, en un sentido amplio, frente a dicha persona que haría incompatible la finalidad propuesta en la consulta.

En este orden de cosas, nos dice el citado Dictamen que:

(...) En cualquier caso, cuanto mayor sea la distancia entre los fines de la recogida y los fines de tratamiento ulterior, más problemática será la evaluación de la compatibilidad.

En segundo lugar, en cuanto al *contexto en el que se han recogido los datos y las expectativas razonables de los interesados en cuanto a su utilización ulterior*, aquí las notas de previsibilidad en el tratamiento cobran especial

importancia. Difícilmente puede representarse al hipotético informante un tratamiento posterior de ese tipo. Se ha de suponer que se acude al Canal del Informante con la confianza en las garantías y salvaguardas que la norma otorga, y para un propósito concreto, por lo que resulta coherente considerar que el tratamiento posterior que pretende la consultante no se espere y en consecuencia sea sorpresivo.

En este sentido nos indica el citado Dictamen lo siguiente:

En general, cuanto más inesperada o sorprendente que siga siendo de uso, más probable será que se considere incompatible.

Asimismo, también ofrece las siguientes consideraciones sobre esta previsibilidad atendiendo al contexto de la recogida de datos, téngase en cuenta que estaríamos en el contexto de un canal interno para denunciar casos de corrupción:

En todos estos casos, también es importante considerar si el estatuto del responsable del tratamiento, la naturaleza de la relación o el servicio prestado, o las obligaciones legales o contractuales aplicables (u otras promesas hechas en el momento de la recogida) podrían dar lugar a expectativas razonables de confidencialidad más estricta y a limitaciones más estrictas de utilización. En general, cuanto más específico y restrictivo sea el contexto en que se recogen los datos, mayor será las limitaciones que puedan existir para un tratamiento posterior. Una vez más, es necesario tener en cuenta el contexto fáctico en lugar de basarse simplemente en texto en letra pequeña.

En tercer lugar, en cuanto a la naturaleza de los datos y repercusión del tratamiento ulterior en los interesados; no podemos obviar que el hipotético informante podría aportar datos de muy diversa índole que, a su juicio, entrarían dentro del ámbito de aplicación de la ley, y que por tanto serían de posibles incumplimientos del ordenamiento jurídico. Podrían ofrecerse datos de los previstos en el artículo 10 del RGPD, o en los artículos 10 y 27 de la LOPDGDD; y también podrían darse categorías especiales de datos del artículo 9.1 del RGPD.

En el Dictamen se hace referencia a estas posibilidades:

La naturaleza de los datos tratados desempeña un papel fundamental en todas sus disposiciones. Por tanto, sería importante evaluar si el tratamiento posterior implica datos sensibles, ya sea porque pertenecen a las categorías especiales de datos contempladas en el artículo 8 de la Directiva, o por otras razones, como en el caso de los datos biométricos, la información genética, los datos de comunicación, los datos de

localización y otros tipos de información personal que requieren una protección especial. En general, cuanto más delicada sea la información, más restringido sería el ámbito de aplicación para un uso compatible.

Y finalmente, en cuanto a las salvaguardias aplicadas por el responsable del tratamiento para garantizar un tratamiento equitativo y prevenir cualquier repercusión indebida sobre los interesados, debemos tener en cuenta que la propia norma establece unas garantías muy estrictas de confidencialidad, anonimato, acceso no autorizado, supresión y en su caso conservación. Todas estas podrían verse afectadas según como se procediera con el nuevo tratamiento. De hecho, dado que se está presuponiendo que no entran dentro de los ámbitos de aplicación de la ley 2/2023 se estarían soslayando todas las garantías que esta establece.

En este sentido el Dictamen propone que:

En algunos casos, solicitar una autorización específica para el nuevo tratamiento puede, en particular, contribuir a compensar el cambio de fin. Es decir, un nuevo fundamento jurídico con arreglo al artículo 7, letra a), puede contribuir, en algunas situaciones, a compensar la incompatibilidad. No obstante, es importante reiterar que los requisitos de compatibilidad con arreglo al artículo 6, apartado 1, letra b), y la exigencia de una base jurídica adecuada con arreglo al artículo 7 son acumulativos. Es decir, un nuevo fundamento jurídico por sí solo no puede legitimar un nuevo uso incompatible.

Además, la aplicación de medidas técnicas y organizativas adicionales puede ser especialmente importante. La identificación de las medidas pertinentes se facilita si se tienen en cuenta determinados objetivos básicos de protección de datos y seguridad de los datos. Los objetivos clásicos de seguridad de los datos son la disponibilidad, la integridad y la confidencialidad. Para satisfacer efectivamente los requisitos de protección de datos, los objetivos de transparencia, aislamiento también debe tenerse en cuenta la posibilidad de intervención.

Cuando se trata de determinar medidas técnicas y organizativas que puedan considerarse garantías adecuadas para compensar el cambio de fin, la atención se centra a menudo en el concepto de aislamiento. Entre las medidas pertinentes cabe citar, entre otras, la anonimización total o parcial, la seudonimización o la agregación de los datos, las tecnologías de mejora de la privacidad, así como otras medidas para garantizar que los datos no puedan utilizarse para tomar decisiones u otras acciones con respecto a particulares («separación funcional»).

Teniendo en cuenta lo anterior, y sin perjuicio de que la determinación de la base jurídica para el tratamiento, así como el cumplimiento de los restantes principios *-incluido el de limitación de la finalidad-* corresponde en último término al responsable del tratamiento al amparo del principio de responsabilidad proactiva, del análisis que se ha realizado se concluye que **el nuevo tratamiento de datos propuesto no encontraría base jurídica suficiente y tendría una finalidad incompatible con la inicial.**